universität wien

DISSERTATION | DOCTORAL THESIS

Titel | Title

Quantum cryptography with quantum dot single-photon sources

verfasst von | submitted by

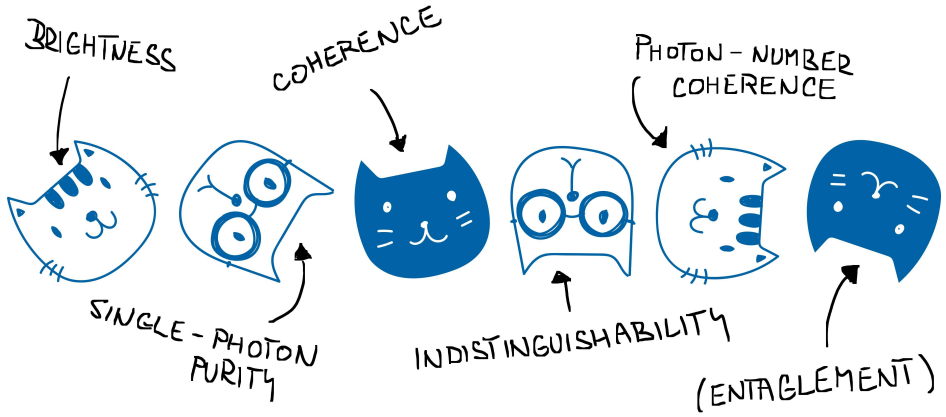
Mgr. Bc. Michal Vyvlečka

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Doktor der Naturwissenschaften (Dr.rer.nat.)

Wien | Vienna, 2024

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 796 605 411
Dissertationsgebiet lt. Studienblatt | Field of study as it appears on the student record sheet:	Physik
Betreut von | Supervisor:	Univ.-Prof. Dipl.-Ing. Dr. Philip Walther



"Creating an ideal single-photon source with all parameters set to unity is comparable to trying to align a group of kittens in a perfect line-an inherently impossible task." Chao-Yang Lu

To my grandfathers Jidřich and Milan, who have always been my inspiration and motivation and helped me discover my life values.

My grandfather Jidřich has a profound interest in everything around him-science, technology, history, politics-and he can discuss these topics for hours. Through his example, he taught me that I can achieve any dream with honesty, hard work, and respect. He always emphasizes that democracy isn't free and that we all need to contribute to its strength, such as by being active in our communities. My grandfather has served as president of the local gardening society for decades. He always dreamed of an academic degree and eventually completed his studies at the Technical University in Brno later in his life, despite our family's opposition to the communist regime. His perseverance taught me the importance of education, democracy, and family.

On the other hand, my grandfather Milan is a bit of a rebel. He showed me that even in 1997, shortly after the Yugoslavian war, when you're in the middle of the Balkans with a four-year-old nerdy kid (yes, that was me) and your car breaks down completely, it's still not a moment to panic. We travelled a lot together, always on a tight budget and always having adventures, mainly caused by the car he built from three non-working ones, which didn't survive crossing the Alps or the poor-quality roads in Bosnia in the 90s. He taught me that adventure is essential and that you must always try new things, overcome your fears, and embrace challenges. He also showed me that if there's a significant problem affecting those close to me, I must face it and fix it, no matter how painful it is. Thanks to him, I am creative, love to travel, enjoy pushing my limits, am less clumsy than I was as a kid, and have a keen sense of sarcasm.

Therefore, I dedicate this thesis primarily to my two grandfathers and the rest of my family.

Abstract

Quantum dot-based single-photon sources are highly appealing for various quantum information applications due to their ability to emit single photons on demand. This capability is especially valuable in quantum cryptography, where the security of each cryptographic primitive is directly related to the non-classical properties of photons. High source brightness is essential for achieving high-speed quantum communication, while a low multiphoton contribution is crucial for minimizing information leakage to potential eavesdroppers.

This work focuses on the investigation of quantum dots as single-photon sources for quantum cryptography and the future quantum internet. We simulate intracavity quantum dot dynamics under three main optical pumping schemes: resonant excitation, LA phonon-assisted excitation, and two-photon excitation. We identify the optimal optical pumping schemes for the main quantum cryptographic primitives and benchmark their performance against Poisson-distributed sources, such as attenuated lasers and down-conversion sources. Additionally, we demonstrate that quantum dots offer extra security benefits due to the tunability of coherence in the emitted photon-number states.

We also experimentally investigate the non-trivial dependence of brightness and purity of C-band single-photons with spectral detuning and pump pulse energy, for In(Ga)As quantum dots under LA phonon-assisted excitation. This scheme shows low sensitivity to environmental fluctuations, such as excitation power, polarization, and wavelength fluctuations, and allows for highly efficient spectral filtering of residual pump pulses from the emitted single photons. The emitted photons exhibit low multiphoton contribution, high brightness, and zero photon number coherence. Thus, LA phonon-assisted excitation is promising for implementing quantum dots in real-life quantum networks. We define the optimal pumping conditions for LA-pumped quantum dots to achieve the highest secure key rate in single-photon quantum key distribution and show how the optimal operation conditions depend on the total losses of the network.

This work also summarizes the results of implementing the BBM92 quantum key distribution protocol over a 350-meter-long deployed optical fiber, using entangled photon pairs emitted by GaAs quantum dots obtained by droplet epitaxy under two-photon excitation. Here, we demonstrate the feasibility of quantum dots for entanglement-based protocols and make an important first step in integrating quantum dots into future entanglement-sharing-based quantum repeater schemes.

We emphasize the importance of selecting an appropriate quantum dot excitation scheme based on its brightness, single-photon purity, and photon-number

coherence, recognizing that the optimal excitation scheme may vary between specific applications. We provide a crucial roadmap for optimizing quantum dots to maximize their potential as single-photon sources for quantum cryptography protocols.

Zusammenfassung

Quantenpunkt-basierte Einzelphotonenquellen sind von sehr hohem Interesse für Anwendungen im der Bereich Quanteninformation, da sie in der Lage sind einzelne Photonen auf Bedarf zu emittieren. Besonders in der Quantenkryoptographie ist diese Eigenschaft von großer Bedeutung, da dort die Sicherheit jedes einzelnen kryptographischen Primitivs direkt mit den nicht-klassischen Eigenschaften der Photonen verbunden ist. Eine hohe Helligkeit der Quellenist dabei eine wesentliche Voraussetzung für sehr schnelle Quantenkommunikation, während eine niedrige Wahrscheinlichkeit für Multiphotonen minimalen Informationsverlust an potentielle Abhörer sicherstellt.

Diese Arbeit fokussiert sich auf die Untersuchung von Quantenpunkten als Einzelphotonenquellen für Quantenkryptographie und das zukünftige Quanteninternet. Wir simulieren die Dynamik eines Quantenpunkts innerhalb eines optischen Resonators unter drei grundlegenden optischen Pumpmechanismen: resonante Anregung, LA Phononen-assistierte Anregung und Zwei-Photonen Anregung. Wir bestimmen den optimalen optischen Pumpprozess für die wichtigsten quantenkryptographischen Primitive und prüfen ihre Leistungsfähigkeit im Vergleich zu Poissonverteilten Quellen, wie etwa abgeschwächte Laser oder Systeme basierend auf parametrischer Fluoreszenz. Des Weiteren demonstrieren wir, dass Quantenpunkte durch die Einstellbarkeit der Kohärenz in den emittierten Fockzuständen zusätzliche zusätzliche Sicherheitsvorteile bieten.

Wir führen eine experimentelle Untersuchung der nicht-trivialen Abhängigkeit von Helligkeit und Reinheit vom spektralen Abstand sowie der Energie des Pumppulses durch. Die hier untersuchten C-Band Einzelphotonen wurden durch LA-Phononenassistierter Anregung von In(Ga)As Quantenpunkten erzeugt. Dieses Schema zeigt eine niedrige Sensitivität gegenüber umfeldbedingten Fluktuationen, wie Leistung, Polarisation und Wellenlänge der Anregung, und ermöglicht eine hocheffiziente spektrale Filterung des restlichen Pumppulses von den emittierten Einzelphotonen. Die emittierten Photonen zeigen eine niedrige Wahrscheinlichkeit für Multiphotonenevents, hohe Helligkeit und keine Kohärenz in den Fockzuständen. Deshalb ist LA Phononen-assistierte Anregung vielversprechend für Implementierungen von Quantenpunkten in Quantennetzwerken unter Praxisbedingungen. Wir definieren die optimalen optischen Anregungsbedingungen für Quantenpunkte unter LA-Anregung, um die maximale sichere Schlüsselübertragungsrate für Quantenschlüsselaustausch mit Einzelphotonen zu erreichen, und zeigen, wie die optimalen Arbeitsbedingungen von den resultierenden Verlusten im Netzwerk abhängen.

Diese Arbeit fasst ebenso die Ergebnisse einer Implementierung des BBM92 Protokolls für Quantenschlüsselaustausch über eine 350m lange, unterirdisch verlegte Glasfaser zusammen, wobei verschränkte Photonenpaare verwendet werden, welche von GaAs Quantenpunkten, hergestellt durch Tröpfchenepitaxie, unter Zwei-Photonen Anregung emittiert werden. Dabei demonstrieren wir die Möglichkeit, Quantenpunkte für verschränkungsbasierte Protokolle zu verwenden, und machen einen wichtigen, ersten Schritt für die Integration von Quantenpunkten in zukünftige Quantenrepeaterschemata basierend auf Verschränkungsaustausch.

Wir unterstreichen die Notwendigkeit an die Anwendung angepasster Anregungsschemata bei der Verwendung von Halbleiterquantenpunkten. Diese richten sich vornehmlich nach deren Helligkeit, Einzelphotonenreinheit und Kohärenz in der Fockbasis. Wir stellen einen wichtigen Leitfaden für die Optimierung von Quantenpunkten bereit, um deren Potential als Einzelphotonenquellen für Quantenkryptographieprotokolle zu maximieren.

Publications

Papers

Quantum cryptography with highly entangled photons from semiconductor quantum dots
C. Schimpf, M. Reindl, D. Huber, B. Lehner, S. F. C. D. Silva, S. Manna, M. Vyvlecka, P. Walther, and A. Rastelli, Sci. Adv., vol. 7, p. 16, 2021.
Chapter 4

Enhancing quantum cryptography with quantum dot single-photon sources
M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler, and P. Walther, npj Quantum Inf., vol. 8, p. 104, 2022. **Chapter** 5 and **Chapter** 6

Robust excitation of C-band quantum dots for quantum communication
M. Vyvlecka, L. Jehle, C. Nawrath, F. Giorgino, M. Bozzio, R. Sittig, M. Jetter, S. L. Portalupi, P. Michler, and P. Walther, Applied Physics Letters, vol. 123, 2023. **Chapter** 7 and **Chapter** 8

Papers not directly related to this dissertation

Single-active-element demultiplexed multi-photon source
M. Hansen, L. Carosini, L. Jehle, F. Giorgino, R. Houvenaghel, M. Vyvlecka, J. C. Loredo, and P. Walther, Optica Quantum 1, 1-5, 2023.

Patents

Optical apparatus for quantum computing, system, method and storage medium
M. Vyvlecka, P. Walther, E. Lerchbaumer, US Patent App. 18/144,508.

Acknowledgements

First and foremost, I would like to thank my supervisor, Philip, for providing me with an incredible opportunity many years ago, an opportunity that I embraced fully. Starting quantum dots research in the quantum information group from scratch, and with little experience, was a significant challenge for me. However, it was also the experience that had the most profound impact on me, serving as the foundation for all the work presented in this thesis and the ongoing research in various teams across Europe.

Philip, I am deeply grateful for all our discussions, your supervision, the moments we shared over shots and beers, and the countless support calls throughout my PhD studies. You often recounted the story of my transformation from a disciplined professional, always in a shirt and responding with "Yes, Sir!" to a relaxed hiker in a t-shirt with mountains, casually replying, "I don't think so!" Despite my hiking t-shirts and a kickbike parking in an office, I am now more determined than ever to pursue my academic career and contribute to systemic change. Thank you for giving me that push!

My deepest thanks go to my closest colleague and friend, Mathieu. Without your presence in our group, this thesis would have turned out very differently. Our discussions over hikes in the Wiener Wald during the COVID lockdowns laid the foundation for this work. The initial equations we scribbled on paper napkins over Saturdays in Vienna cafes are now crucial parts of the following pages. We spent an incredible amount of time together, both at work and outside of it, and those moments were truly special and will always bring me happiness. Thank you for all the trips, cheeky evenings, teaching me to appreciate red wine, leisurely hikes, and countless adventures.

A lot of this work would not have been possible without the great master students who worked with me: Marco, Francesco, and Sophie. My respect for enduring my supervision style. A special thanks to Sophie for all the great times, funny memories, spontaneous trips, and your friendship. Especially for being an essential part of the team during the setup of the new quantum dot laboratory, your organization skills were the part of our collective mind that I often lacked. Our symbiosis will benefit the quantum dot team for years to come. Thank you for everything!

The Telecom quantum dot team was my work universe over the last few years, and it's hard to imagine it without Lennart. He was always there, standing beside me in the laboratory, sitting behind me in the office, or even cleaning the dishwasher with me. Always a bit annoying with his German perfectionism, but a great colleague and an even better friend. Together, we pushed the experimental

part of the work forward and spent many evenings at Clash or later at Cafe Benno, drinking beer, discussing work, hiking, climbing, and playing board games. I can't dream about anyone better to take over these projects. So, vielen Dank, Lennart, and I can't wait for the next peaks we'll climb together.

Speaking of the quantum dot team, I also want to thank Lena, who has made a significant impact on the Sensengasse office since she joined us. Thank you for all the support and motivation you've provided over the past few years.

The first half of my PhD is closely tied to our Essen group, including Valerie, Marie-Christine, Giulia, Teo, and Peter. It was a great pleasure to be a part of your work family. You inspired me immensely in the early years and continued to motivate me as time went on. It's hard to express my gratitude for all the discussions about academia, science, and life, the great times in the office, and the guidance during the challenging moments of the PhD. A special thanks to Peter, who was with me from the first day to the last, enduring the entire PhD journey together. Thank you for all your support, for listening to my problems and helping solve them, and for the countless adventures, from hiking across continents to enjoying pudding in the Swedish wilderness and enduring long swims across lakes. I can't wait for our next travel expeditions!

I would also like to thank the rest of the Walther group for making my time at the University of Vienna enjoyable. A special thanks go to Lee, Philipp, Alessandro, Christofer, Michael, Josip, Daniel, Raffaele, Beate, Daniel, Michele, Jonas, and Celine for all the support, beers, and help.

I've always been somewhat phlegmatic when it comes to administrative tasks, which a few times led to extreme situations, like being kicked out of the PhD program. Therefore, I wouldn't have reached this point without the tremendous work and support from the people in the quantum office, including Petra, Miriam, Susi, Elisabeth, Verena, Milena, Agnezka, Bianca and Soli. Thanks to all of you, I managed to get here, you were always a reliable backup, resolving my issues before I even noticed them. A special thanks to Petra, who over the years became like an "adoptive mom" to me. I'm grateful for all the dinners, the unwavering support, and the hidden whiskey in the quantum office, which was always there just like you, whenever I needed it.

I also want to acknowledge the VDS Physics and COQUS programs, which felt like an extended PhD family to me. I will always cherish the fond memories of retreats and outreach events with fellow students. A heartfelt thank you to Christiane for taking care of us, providing strong support over the years, introducing me to faculty politics, and organizing amazing outreach events.

I must also mention Charlie and his wife, whose ever-present smiles and technical expertise could resolve even the most challenging problems in the lab or office. They made the impossible possible in a single day. It was a pleasure working with you or simply encountering you in the corridor. Thanks to you, our laboratory was always running smoothly.

This thesis is built upon a strong collaboration with the Rastelli group from Jo-

hannes Kepler University Linz, the Michler group from the University of Stuttgart, and the Axt group from the University of Bayreuth. Thank you all for joining us on this challenging but exciting project and for the hard work you and your teams put into it. Without your contributions, this thesis wouldn't have been possible. Special thanks to Armando, Peter, and Simone, who, over the years, were like second supervisors to me, guiding me through the fascinating field of quantum dots.

When discussing collaborations, I must highlight the University of Stuttgart a bit more. I still recall bringing back the first quantum dot sample to Vienna, our first quantum dots ever, in my backpack on a low-cost flight. Our collaboration was always close, largely thanks to the friendship between two sarcastic PhD students who loved to insult everything, especially each other: myself and Cornelius. So, Cornelius, thank you for the great friendship, all the bottles, "research" visits, and the extremely dangerous hikes. It was a fantastic time.

As I write this acknowledgement, I've already spent half a year working in Stuttgart in Professor Michler's group as a "PostDoc without the Doc." I'd like to thank my new colleagues - Raphael, Tim, Uli, Simone, Lukas, Ilenia, and Ponraj - for their support during the final stages of my thesis.

My free time in Vienna was spent mostly at my home with our amazing community at FBW20. There are no words to express my gratitude for all the love and support you've given me. My time at FBW has been some of the happiest of my life, especially during the first COVID lockdown when we all spent time together. You will always be like family to me, and coming back to FBW will always feel like coming home. So, thank you, Paul, for everything - for the cozy evenings, Tesla trips, winter holidays, and hikes. Thanks, Jason, for your unwavering support, whiskey, long discussions, and sharp knives. Thanks, Jessi, for being like a sister to me, always there when I need you and for all the cocktail evenings. Thanks, Mathieu, for all the hugs, happiness, and questions that always make me shy. Thanks, Sophie, for the crazy and spontaneous moments. And thanks to Evi, Johana, Sarah, and Ellie for your warmth, laughter, and the countless memories we've shared.

Our small Czech-speaking group - Richard, Valerie, Martin, Petr, Radim, Honza, and Klára - was bonded not only by language but also by a shared love of hiking and beer. We shared wonderful moments in the mountains and in Vienna pubs. Special thanks to Richard for all the spontaneous "Beer?" messages that always led to a meeting at Clash within an hour, for your incredible friendship, for all the hikes with Tatratea, and for your unwavering support throughout my entire PhD studies.

SCI Austria has been my welcome escape from physics over the last few years, offering a space to discuss politics, gender, history, and nature protection. It was a place where I felt my work truly made a difference and contributed to meaningful change. So, thank you to everyone at the SCI office for the wonderful moments and all the work we accomplished together. Thanks also to the people from National

Park Gesäuse for the thousands of invasive plants we removed together. Among all the amazing people at SCI, I want to give a special thanks to Mirna. It was a great pleasure working with you, having our office days while listening to Azra, organizing workcamps, and enjoying friendly evenings over beer or spontaneous parties at your flat.

I think I was 16 when I first met Ondra and Michaela during the "Expedition Mars" project. It's amazing to reflect on how, 15 years ago, we all dreamed of earning PhDs in Physics, and now we're achieving that goal in the same year. It's been a long journey, and I couldn't have asked for better companions to share it with. Over the years, we've supported each other through countless moments, from wild mountain adventures to wine Skype calls in recent years. Thank you for being such incredible support over the past 15 years. I look forward to the many years ahead!

The biggest thanks go to Soňa, my soulmate and closest person. It's impossible to fully express my gratitude for all the countless moments we've shared, from holidays and near-death experiences to festivals, and, most importantly, the times when I was completely down, and you were always there to lift me up. The experiences we've had together could fill several books, each one a bestseller filled with exciting life memories. Thank you for making my life truly great.

Soňa and I are part of a wonderful group of best friends: Panda, Bea, Sam, Eliška, Katka, Klaudie, Martin and Píp. They are part of my daily life as same as big dreams for the future. Thank you, guys, for all the wonderful traditions, like Christmas in May, cocktails in pots, micro holidays, extreme hikes, and New Year trips. Without your constant support over the years, I wouldn't have reached the point of submitting my thesis. You are my chosen family, the best I could ever ask for! Thanks for literally everything!

Together with my best friends, we run the NGO "Education42morrow" and the project "Expedition Mars," which has been a part of my life for over 17 years. These projects played a crucial role in my decision to become a physicist and pursue an academic career, providing me with immense support along the way. Together, we have done incredible work in scientific education and inspiring young people to join us on the exciting adventure of becoming scientists. For me, science outreach is an important part of my work, so thank you to everyone involved for helping us make this breathtaking impact on the Czech and Slovak students.

Speaking of outreach, I must also mention the "Talent Academy" project, which I started together with my colleagues Radka and Hanka six years ago. They work in the PR department at the laser centres in Dolní Břežany, part of the Czech Academy of Sciences, where I was a master's student. Over the years, we've encouraged many high school students to pursue careers in science. A big thank you to everyone involved in this incredible work. Special thanks to Radka, who has been an amazing friend, for all the support, drinks, and for pushing me to write press releases late into the night. I also want to thank another Talent Academy friend, Yoann, for being a great support and commiserating with me over the

challenges of academic writing during the final months of this thesis. I'm also grateful for the 4-day hike we took in the week before the thesis submission. It reminded me of the truly important things in life, like whether we'd make it to the next hut before a storm, whether I'd survive the Via Ferrata trail, and whether I wanted one more radler.

Among the many others, I want to thank, though I can't spend another page doing so, I want to name the Expedition Club members, especially Standa, and old family friends, the Řezníčkovi, Skopalovi, and Jehlářovi families. You've always been a great support.

Finally, I want to thank my family, especially my parents, sister, grandparents, and aunt. Your support from my first moments in this world to the completion of this thesis has been invaluable. It has been such a long journey, and I truly wouldn't have made it without your love, support, and motivation. The journey was full of both hard failures and great successes, and you were always there to share them with me. Thank you for always supporting my countless crazy dreams, with being a scientist being one of them!

I also want to extend my thanks to those who helped with proofreading this thesis: Mathieu, Lennart, Peter, Raphael, Simone, Yoann, Lukas, Tim and Philip. Your feedback and comments were greatly appreciated!

Contents

List of Figures

List of Tables

List of Acronym

1 Introduction **1**

2 Quantum Information **5**
2.1 Building blocks of the quantum information 5
2.1.1 The qubit 5
2.1.2 Density operator 7
2.1.3 Quantum gates 10
2.1.4 Measurement 12
2.1.5 Quantum information with photons 14
2.2 Quantum cryptography with single photons 18
2.2.1 The no-cloning theorem 19
2.2.2 Quantum-cryptographic primitives 20
2.2.3 Security of quantum cryptography 29
2.2.4 Practical attacks at a quantum cryptographic protocol . . . 37

3 Quantum-light sources **41**
3.0.1 Quantum light 41
3.0.2 Properties of quantum-light sources 45
3.1 Poisson-distributed sources 54
3.1.1 Weak coherent state sources 55
3.1.2 Spontaneous parametric down-conversion sources 56
3.2 Quantum dots single-photon sources 57
3.2.1 Energy levels 58
3.2.2 Excitation schemes 60
3.3 Emission in the optical communication band 75

4 Summary of "Quantum cryptography with highly entangled photons from semiconductor quantum dots" **77**
4.1 Experimental setup 78
4.1.1 Quantum dot characterization 79
4.2 QKD with entangled photon pairs 80

5 Methods for "Enhancing quantum cryptography with quantum dot single-photon sources" 83
5.1 Quantum dots dynamics and simulations 84
5.1.1 Model of two-level system 84
5.1.2 Model of three-level system 86
5.1.3 Methods and parameters 87
5.1.4 Pumping schemes results 89
5.1.5 Collection efficiency and state encoding 93
5.2 Quantum cryptography primitives with quantum dots 97
5.2.1 BB84 quantum key distribution 98
5.2.2 Twin-field quantum key distribution 103
5.2.3 Unforgeable quantum tokens 105
5.2.4 Quantum strong coin flipping 107
5.2.5 Quantum bit commitment 109

6 Reprint of "Enhancing quantum cryptography with quantum dot single-photon sources" 113
6.1 Introduction 113
6.2 Results 115
6.2.1 Comparison of pumping schemes 115
6.2.2 Photon-number coherence 116
6.2.3 Practical sources and security 117
6.2.4 Quantum key distribution 118
6.2.5 Quantum primitives beyond QKD 120
6.3 Discussion 124
6.4 Methods 124

7 Methods for "Robust excitation of C-band quantum dots for quantum communication" 125
7.1 Experimental Setup 126
7.1.1 Evaluation of measured time tags 128
7.2 Parameter Estimation for Quantum Key Distribution with Quantum Dots 129
7.2.1 Maximum QKD-distance approximation from experimental measures 129

8 Reprint of "Robust excitation of C-band quantum dots for quantum communication" 131
8.1 Introduction 131
8.2 Results 133
8.2.1 Excitation parameter investigation 133
8.2.2 Quantum key distribution 135

9 Conclusion and future challenges **139**
9.1 The advantages of quantum dots in quantum cryptography 139
9.2 Practical challenges in utilizing quantum dots as usable sources . . 141
9.3 Vision for quantum dots in future quantum networks 142

A APPENDIX: Mathematical tools for quantum cryptography **143**
A.1 Semidefinite programming 143
A.2 Security of quantum cryptography primitives 144
A.2.1 Security of BB84 quantum key distribution 144
A.2.2 Security of twin-field quantum key distribution 145
A.2.3 Security of unforgeable quantum tokens 146
A.2.4 Security of quantum strong coin flipping 148
A.2.5 Security of quantum bit commitment 152

B APPENDIX: Photon-number optimization via variable attenuation **155**

Bibliography **159**

List of Figures

2.1 Polarization single-qubit measurement 17
2.2 BB84 Quantum key distribution protocol scheme 22
2.3 Wiesner's quantum money protocol scheme 25
2.4 Quantum strong coin-flipping protocol scheme 27
2.5 Quantum bit commitment protocol scheme 28
2.6 Comparison of secure key rate of BB84 QKD and Decoy state QKD protocols 36

3.1 Properties of quantum light source 46
3.2 Schemes for brightness measurement 47
3.3 Schemes for $g^{(2)}(\tau)$ measurement 48
3.4 Schemes for photons' indistinguishability measurement. 51
3.5 Scheme for photon coherence measurement. 52
3.6 Scheme for photon number coherence measurement. 53
3.7 Schematic depiction of QD's energy levels. 59
3.8 QD's excitation schemes. 60
3.9 Photon-number probabilities and second-order correlation functions for state generated by a two-level system resonantly pumped by square pulsed of $T = 0.3/\gamma_x$ 65
3.10 Scheme of longitudinal acoustic phonon-assisted pumping 67
3.11 Comparison of simulated values of $g^{(2)}(0)$ for RE and TPE as a function of the pump pulse length 70
3.12 Single-photon purity and indistinguishability for sTPE in dependence on the delay between excitation and stimulation pulse. . . . 73

4.1 Experimental setup for QKD with entangled photon pairs 78
4.2 Key generation and post-processing for QKD with entangled photon pairs 80

5.1 Scheme of the quantum-dot–cavity system 84
5.2 Simulation of photon-number probabilities under different excitation schemes 90
5.3 Simulation of single-photon purity and brightness under different excitation schemes 90
5.4 Simulation of $g^{(2)}(0)$ under different excitation schemes 91
5.5 Simulation of coherence between vacuum and single-photon component under different excitation schemes 92

5.6 Collection efficiency modelling and state encoding 95
5.7 Source comparison for BB84 QKD without decoy states 99
5.8 Collection efficiency comparison for BB84 QKD without decoy states 100
5.9 Collection efficiency comparison for BB84 QKD without decoy states for low sources efficiencies $\eta \leq 1\,\%$ 100
5.10 Source comparison for BB84 QKD with decoy states 101
5.11 Collection efficiency comparison for BB84 QKD with decoy states . 102
5.12 Source comparison for twin-field QKD 104
5.13 Collection efficiency comparison for twin-field QKD 105
5.14 Source comparison for unforgeable quantum tokens 106
5.15 Collection efficiency comparison for unforgeable quantum tokens . 107
5.16 Source comparison for quantum strong coin flipping 108
5.17 Collection efficiency comparison for quantum strong coin flipping . 109
5.18 Source comparison for quantum bit commitment under the bounded storage assumption 110
5.19 Collection efficiency comparison for quantum bit commitment under the bounded storage assumption 111

6.1 Simulation of emission properties under different pumping schemes 116
6.2 Source comparison for three main QKD schemes 119
6.3 QDs performance for the main quantum primitives 122
6.4 Source comparison for unforgeable quantum tokens 123

7.1 Scheme of the experimental setup 126
7.2 Time-resolved fluorescence measurement 127

8.1 Characterisation of the positively-charged exciton transition under pulsed LA excitation 134
8.2 Measured photon-number statistics and extrapolated QKD secure key bits per pulse for LA excitation 135
8.3 Secure key rates of BB84 QKD for varying communication distances 136

B.1 Secure key bits per pulse over distance for variable signal attenuation. 156

List of Tables

2.1 Frequently used photonic qubit physical implementation 15
2.2 Overview of model parties used for the description of quantum cryptographic protocols 19
2.3 Main quantum primitives 21
2.4 Probability that Bob will get an error in the result during the intercept-resend attack with fix Eve's measurement bases for Alice's state $|0\rangle$ 30

3.1 Summuary of QD's excitation schemes properties. 61

5.1 Phyiscal parameters used in the simulations 87
5.2 Optimal photon number populations for resonant excitation (RE), longitudinal acoustic phonon-assisted excitation (LA) and resonant two-photon excitation (TPE) 92

List of Acronyms

APD	avalanche photodiode	39
ARP	adiabatic rapid passage	61
BS	beam splitter	48
cps	counts per second	79
CPTP	completely positive trace-preserving	143
DBA	detector blinding attack	39
DBA	detector blinding attack	39
DBR	distributed Bragg reflector	76
EOM	electro-optic modulator	15
EQKD	quantum key distribution with entangled photon pairs	3
FP PDS	fixed-phase Poisson distributed source	97
FSS	fine structure splitting	61
FWHM	full width at half maximum	85
G	ground state	62
HBT	Hanbury Brown and Twiss experiment	48
HBT	Hanbury-Brown and Twiss experiment	48
HOM	Hong–Ou–Mandel	49
HWP	half-wave plate	16
LA	longitudinal acoustic phonon-assisted excitation	4
LA-TPE	phonon-assisted two-photon excitation	62
MBE	molecular-beam epitaxy	58
MOVPE	metalorganic vapour-phase epitaxy	58
MP-QKD	mode-pairing quantum key distribution	24
NIR	near-infrared	3
PBS	polarizing beam-splitter	18
PDS	Poisson distributed source	2
Ph	longitudinal acoustic phonons	84
PNC	photon-number coherence	3
PNS	photon-number splitting	35

POVM positive operator-valued measuremet 14
QBC quantum bit commitment 20
QBER quantum bit error rate 23
QCF quantum coin flipping 2
QD quantum dot 2
QDC quantum-dot–cavity system 4
QKD quantum key distribution 1
QT quantum tokens 2
QWP quarter-wave plate 16
RE resonant excitation 3
RP PDS randomized-phase Poisson distributed source 98
SK secure key bits per pulse 18
SK secure key 18
SKG Stranski–Krastanov growth 57
SKR secure key rate 24
SNSPD superconducting nanowire single-photon detector 40
SPDC spontaneous parametric down-conversion 2
sTPE stimulated two-photon excitation 62
TF-QKD twin-field quantum key distribution 24
THA Trojan horse attack 39
THA Trojan horse attack 39
3LS three-level system 61
2LS two-level system 61
TPE resonant two-photon excitation 61
USD unambiguous state discrimination 38
USD unambiguous state discrimination 38
VBG volume Bragg grating 127
WCS weak coherent state 2
WSEE weak string erasure sub-routine with errors 152
X exciton state 59
XX biexciton state 59

1 Introduction

In recent years, significant efforts from major international companies, startups, and researchers have been directed towards the construction of a universal quantum computer. The number of qubits available on superconducting chips [1–4] or optical platforms [5–7] is steadily increasing, and these devices may employ Shor's algorithm to factor large integers in the foreseeable future [8–10]. This development poses a potential threat to the security of the RSA protocol, protocols based on a discrete logarithm and other public key cryptosystems [11]. Classical cryptography is not challenged only by the rise of quantum technologies but also by progress in number theory, which may yield an algorithm capable of polynomial-time factorization of large integers.

It is crucial to emphasize that this advancement currently does not pose an immediate threat to existing cryptograms but primarily represents a potential risk of breaking current cryptographic systems in the future. As of today, eavesdroppers can archive encrypted messages beyond their current decryption capabilities. However, as technology advances, there may come a time when these encrypted communications can be read, placing a finite lifespan on the confidentiality of messages. This motivates researchers to develop cryptographic protocols that are information-theoretic secure, meaning their security doesn't rely on assumptions of computational complexity.

Laws of quantum theory, such as the no-cloning theorem and the uncertainty principle, have been successfully employed to design cryptographic protocols that provide security against adversaries with unlimited computational power [12, 13]. Over the last decades many quantum cryptographic primitives, fundamental building blocks which can be combined to build various applications, have been theoretically described and demonstrated by proof-of-principle experiments [14–19]. The most technologically mature quantum cryptographic protocol, quantum key distribution (QKD), is nowadays implemented in many real-life applications, where a high level of provided security is required [20–25]. These advancements motivate researchers to develop a universal quantum network, known as the quantum internet, which will enable the connection of quantum computers secured by quantum cryptography [26, 27].

The development of a functional quantum internet is one of the greatest challenges in quantum information for the coming decades. Its success will largely depend on efficient and reliable quantum hardware, such as single-photon sources,

single-photon detectors, and quantum repeaters, ideally operating at telecommunication wavelengths [27]. An ideal single-photon source for quantum cryptography applications must have several optimized parameters. Source brightness and low dead time are crucial for high-speed quantum communication [28, 29]. A low multiphoton component is essential to minimize the risk of information leakage to malicious eavesdroppers [30]. Additionally, zero photon-number coherence significantly enhances the security of various quantum cryptographic protocols, providing robust protection against potential threats [14, 16, 31–34].

Furthermore, assuming compatibility of the source with various quantum repeater schemes, quantum memories or multiple-photon quantum cryptographic protocols, additional parameters such as single-photon indistinguishability, spectral coherence, and the ability to emit high-fidelity entangled photon pairs must also be considered [27]. Optimizing all these parameters simultaneously is the current goal of researchers working on different single-photon source platforms.

The leading single-photon sources in quantum technology today are Poisson distributed sources (PDSs), such as spontaneous parametric down-conversions (SPDCs) and weak coherent states (WCSs), which emit photon statistics following a Poisson distribution [14,35]. This means there is a trade-off between their brightness and single-photon purity. Despite these limitations, PDSs are routinely used in quantum information applications due to their experimental feasibility, robustness, tunability, good interference properties, and ability to generate high-fidelity entangled states [36–47].

Moreover, several ingenious techniques have been proposed to address the main limitations of PDSs in photon-number statistics. Methods such as multiplexing and heralding have been demonstrated to achieve high source brightness without significantly affecting single-photon purity [48, 49]. The decoy states protocol has enhanced the achievable communication distance of QKD by mitigating the impact of the multiphoton component [15, 50]. Additionally, various active phase scrambling methods have been developed to break the photon-number coherence in the emitted state [29, 51]. Thanks to these methods, PDSs have played a crucial role in advancing quantum information research. However, they still fall short of being ideal single-photon sources [14].

The main limitation of PDSs becomes increasingly critical as we consider the development of a universal quantum internet. For cryptographic protocols involving untrusted parties, such as quantum coin flipping (QCF) or quantum tokens (QT), the decoy-state method can't always be implemented [14, 52]. The presence of multiphoton components reduces the efficiency of quantum repeaters [53, 54], while the requirement for active phase scrambling imposes technological constraints on the maximum communication rate [29, 51]. Therefore, there is an urgent demand for a more ideal single-photon source to address these challenges effectively.

Single-photon sources based on semiconductor quantum dots (QDs) are remarkable candidates for quantum cryptography as they can, in principle, emit

photons on demand, with high brightness and low multiphoton contribution [55]. Recently, a QD under resonant excitation (RE) reached a remarkable end-to-end efficiency of 71.2 % while maintaining a high single-photon purity of 98 % and a high photon indistinguishability of 98.6 %. [56]. However, the most advanced QDs currently emit in the near-infrared (NIR) spectral range around 900 nm [55]. Recent developments in QDs emitting at telecommunication wavelengths, specifically in the optical O-band and C-band, promise to achieve similar performance to their NIR counterparts in the coming years [57–61].

This progress has motivated numerous implementations of QDs in quantum information experiments, such as boson sampling [62] and QKD [63–71]. Moreover, many fundamental building blocks of a future quantum internet, including emission of high-fidelity entangled photon pairs [72], quantum teleportation [73, 74], entanglement swapping [75,76] and compatibility with quantum memories [77] have been demonstrated with QD based single-photon sources. Recent advancements in the deterministic growth of QDs, their integration into photonic structures such as microcavities [55, 56, 78–80] and photonic crystals [81, 82], and the direct coupling of emitted single photons to single-mode fibers [83, 84] push QDs toward routine implementation in quantum information applications.

Compared to PDS, QDs allow for various excitation schemes due to their energy levels [85, 86]. Many excitation schemes, including resonant [56, 87–89], off-resonant phonon-assisted [90, 91], and stimulated [92–94], have been proposed and demonstrated. These schemes differ in several parameters, including reachable source brightness, single-photon purity, photon indistinguishability, the possibility of generating entangled photon pairs, and sensitivity to environmental fluctuations [85, 86, 95, 96]. Moreover, it has been shown that resonant schemes can emit photon states with a photon-number coherence (PNC) [94, 97, 98]. Therefore, a suitable excitation scheme must be chosen to optimize the performance of a QD in a given quantum information application.

The primary focus of this work is the synergy between quantum hardware and quantum software to achieve the highest performance of quantum cryptographic protocols using QD-generated single photons. The main motivation for our further investigation of QDs as single-photon sources for quantum cryptography was an experiment led by Prof. Armando Rastelli's group (Johannes Kepler University Linz), in which we collaborated [68]. In this experiment, we used entangled photon pairs generated from a QD to implement a quantum key distribution with entangled photon pairs (EQKD) protocol between two buildings connected by a 350 m-long deployed single-mode fiber. This experiment demonstrates the feasibility of QDs for entanglement-based protocols and marks an important first step in integrating QDs into future entanglement-sharing-based quantum repeater schemes [68]. The results of this experiment are summarized in chapter 4.

Despite the high brightness and single-photon purity of QD, their performance in quantum cryptographic protocols did not surpass that of protocols using PDS. To address this, together with Prof. Peter Michler (University of Stuttgart) and

Prof. Vollrath Martin Axt (University of Bayreuth), we theoretically analyzed the performance of a QD single-photon source in key quantum cryptographic primitives and we compared its performance to the theoretical maximum achievable with PDSs [52].

Our theoretical model of quantum-dot–cavity system (QDC) and security proofs helped us to identify the optimal optical pumping scheme for these quantum cryptographic primitives. Specifically, we elaborated on the advantages of using phonon-assisted and two-photon excitation over resonant excitation for QKD and other primitives. Additionally, we demonstrated that QDs offer extra security benefits due to the tunability of coherence in emitted photon-number states. This work outlines a crucial roadmap for further optimizing QD-based single-photon sources to achieve high performance in quantum cryptographic applications [52]. The results are discussed in chapter 5 and chapter 6.

Furthermore, we explored the advantages of longitudinal acoustic phonon-assisted excitation (LA) pumped QDs with emission in the telecom C-band as a core hardware component of the quantum internet. In collaboration with Prof. Peter Michler (University of Stuttgart), we conducted an experiment demonstrating how varying the pump power and spectral detuning relative to the excitonic transition can enhance quantum-secured communication rates and provide stable emission statistics regardless of network-environment fluctuations [99]. These findings have significant implications for the general implementation of QD single-photon sources in practical quantum communication networks. The overview of the results can be found in chapter 7 and chapter 8.

Although QDs are close to becoming ideal single-photon sources, significant research is still needed before they reach the same level of technological readiness as PDS and this work is just one piece of the puzzle on the path toward a QD-based quantum internet.

2
Quantum Information

Quantum information theory explores how the principles of quantum mechanics enable the encoding, manipulation, and distribution of information. The connection between the frameworks of physics and information is well-known from information entropy theory, which allows us to use methods of statistical physics to describe information protocols [100]. As a consequence of this equivalence principle, all information must be fundamentally encoded in a degree of freedom of a physical system. Just as classical information theory examines scenarios where information is encoded onto macroscopic systems, using classical physics methods like transistor voltage or electromagnetic wave modulation, quantum information theory focuses on cases where the information carriers are so small that they adhere to the principles of quantum mechanics.

The quantum nature introduces new principles to information theory, such as quantum superposition and interference, as well as the no-cloning theorem. These phenomena, unique to the quantum world, have been effectively used to build quantum computing algorithms and quantum cryptographic protocols, which by their performance surpass their classical counterparts [101–104]. As this work primarily centres on quantum cryptography, this chapter provides a concise overview of the framework for quantum cryptography, with a brief exploration of the principles of quantum computing.

2.1 Building blocks of the quantum information

Every quantum information protocol is built from the same fundamental building blocks. Starting with the unit of quantum information, qubit, followed by manipulation of the information by quantum logic gates and finishing with information measurement. This chapter defines these foundational components and describes their implementation on a single-photon platform, so we can use them to build actual quantum cryptography protocols later on.

2.1.1 The qubit

A qubit, short for a quantum bit, is the basic unit of information used in quantum computing. Unlike classical bits, whose logical value can be either 0 or 1, a qubit can be in an infinite number of states, thanks to principles of superposition. A qubit, as any other quantum pure state, can be represented as a complex vector

in a Hilbert space. In this mathematical representation, we can see superposition as a direct consequence of the vector space condition of completeness, where every vector in a vector space can be expressed as a linear combination of the vector space basis. In the quantum information theory the standard basis vectors of the qubit two-dimensional Hilbert space $\mathbb{C}^2$, so-called computational basis, correspond to logical 0 and logical 1. In Dirac representation we can write the basis vectors as $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. A qubit can then be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \ , \tag{2.1-1}$$

where α and β are complex probability amplitudes. Their modulus squared corresponds to the probability of a projection onto $|0\rangle$ or $|1\rangle$, therefore they have to satisfy the following normalization condition

$$|\alpha|^2 + |\beta|^2 = 1 \ . \tag{2.1-2}$$

From Eq. 2.1-1 and Eq. 2.1-2 we can get a more intuitive geometric representation of the qubit

$$|\Psi\rangle = \mathrm{e}^{i\gamma}\left[\cos\left(\frac{\theta}{2}\right)|0\rangle + \mathrm{e}^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right] \ , \tag{2.1-3}$$

where θ, Φ and γ are real numbers. The angles θ and Φ can be identified as a polar angle and an azimuth respectively and we usually use them to represent qubit as a complex vector in spherical coordinates. The factor $\mathrm{e}^{i\gamma}$ is a global phase and mostly it doesn't have any observable effect and can be neglected.

2.1.1.1 Multi-qubit states and quantum entanglement

Many applications are based on multi-qubit states, which can be composed as tensor products of single-qubit states, which we defined as elements of two-dimensional Hilbert space $\mathbb{C}^2$ in the previous chapter. A straightforward example of a two-qubit state is

$$|0\rangle \otimes |1\rangle = |01\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \ . \tag{2.1-4}$$

However, not all multi-qubit states can be factorized into single-qubit spaces. An example of such a state is illustrated as follows

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle \ . \tag{2.1-5}$$

We called these states entangled. From a mathematical perspective, an entangled state cannot be expressed as a tensor product of single-qubit states $|\psi_A\rangle \otimes |\psi_B\rangle$. The two-qubit entangled states most commonly used, due to their maximal entanglement, are the Bell states

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \ , \tag{2.1-6}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \ . \tag{2.1-7}$$

2.1.2 Density operator

In the previous chapter, we defined a qubit using a state vector $|\psi\rangle$ within a Hilbert space. These quantum states, represented by state vectors, are known as pure states and serve as idealized representations based on our complete knowledge of the quantum system. In practice, uncertainty or incomplete knowledge about the exact state of the quantum system often arises due to interactions with the environment, such as macroscopic experimental setups or other sources of noise. In such cases, the quantum system is described by a statistical mixture of pure states, known as a mixed state. To mathematically describe these general quantum states, we now introduce the density operator. For a pure state, the density operator is defined as

$$\hat{\rho} = |\psi\rangle \, |\psi\rangle^{\dagger} = |\psi\rangle\langle\psi| \ . \tag{2.1-8}$$

The general density operator we can construct as a sum of all pure states $|\psi_i\rangle$, in which the quantum system can be observed with given probabilities p_i

$$\hat{\rho} = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \ . \tag{2.1-9}$$

Now we can use probabilities requirements to define the properties of a density operator which describes a physical quantum system

- The probabilities p_i are normalized $\sum_i p_i = 1 \implies \mathrm{Tr}[\hat{\rho}] = 1$.
- The probabilities p_i are real $\implies \hat{\rho}$ is Hermitian $\hat{\rho}^{\dagger} = \hat{\rho}$.
- The probabilities p_i are not negative $\implies \hat{\rho}$ is semidefinite positive $\hat{\rho} \geq 0$.

Unlike pure states, mixed states lack well-defined probabilities for all potential projection outcomes. Instead, they are described by the probabilities p_i associated with different pure states that the system could be in, as described by Eq. 2.1-9. Let's define the purity of a quantum state as

$$\mathrm{P} = \mathrm{Tr}[\hat{\rho}^2] \ , \tag{2.1-10}$$

intuitively if the $\mathrm{P} = 1$ the $\hat{\rho}$ will describe pure state and if $\mathrm{P} < 1$ the state described by $\hat{\rho}$ will be mixed. Now we can list a few simple examples to get some intuition about pure and mixed states. The density operator of pure state $|1\rangle$ can be written by using Eq. 2.1-8 as

$$\hat{\rho}_{|1\rangle} = |1\rangle\langle 1| = \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} . \tag{2.1-11}$$

We know that by a linear combination of computational basis, we can construct a vector, which is part of Hilbert space, so in other words it is a pure state. As an example, take an equal superposition of $|0\rangle$ and $|1\rangle$, which can be described by state vector $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and for next we will refer it as a diagonal state. Then the density operator of the diagonal state is

$$\hat{\rho}_{|+\rangle} = |+\rangle\langle +| = \frac{1}{2} \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} . \tag{2.1-12}$$

It's evident that the purity of $\hat{\rho}_{|+\rangle}$ equals one. While we have focused so far on density operators for pure states, let's now consider a simple example of a mixed state. Assume an incoherent equal mixture of $|0\rangle$ and $|1\rangle$ pure states. To calculate the given density operator we will use Eq. 2.1-9

$$\hat{\rho}_{|mix\rangle} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} . \tag{2.1-13}$$

The purity of $\hat{\rho}_{mix}$ is equal to $\frac{1}{2}$. By comparing Eq. 2.1-12 and Eq. 2.1-17 we can describe the physical meaning of diagonal and off-diagonal elements of a density operator. The diagonal elements represent probabilities to observe the different pure states and they are always real-positive values. In both of our examples, we used the same probability amplitudes of the given pure states $|0\rangle$ and $|1\rangle$, so the diagonal elements of both density operators are the same. The difference is coming in the off-diagonal elements, which describe coherent superposition between different pure states and in general, they are complex numbers. A completely mixed state is represented by a diagonal matrix as there is no coherence between the bases' pure states.

The purity can be a useful parameter for some applications, such as security analysis of quantum cryptography protocols, see Ch. 2.2.3.4. However, in most of the applications, we will be more interested in how far is our experimentally prepared state from its theoretical image. For that, we have to define the fidelity of a quantum state

$$\mathrm{F}(\hat{\rho}, \hat{\sigma}) = \mathrm{Tr}\left[\sqrt{\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}}\right]^2 . \tag{2.1-14}$$

Fidelity measures the closeness between two states represented by density operators $\hat{\rho}$ and $\hat{\sigma}$, where one denotes the experimental state and the other represents its theoretical counterpart. In terms of measurement, fidelity can be viewed as the probability that state $\hat{\sigma}$ will collapse to state $\hat{\rho}$. The fidelity of experimentally prepared quantum states is a critical parameter for the effective implementation of quantum cryptographic and computing protocols.

2.1.2.1 Partial trace of a density operator

Often, we want to describe only a specific subsystem of a larger system using a density operator, without needing to account for the entire system. This larger system may include elements such as an environment, field, cavity, or entangled states that we do not have access to. To address this, we define the partial trace of the density operator, which effectively discards the information about the parts of the system that are irrelevant or inaccessible to us. However, this process may result in a mixed-state density operator, reflecting the incomplete knowledge about the system as a whole.

To define a partial trace we will assume a bipartite system described by a density operator $\hat{\rho}_{AB}$ defined on a Hilbert space $\mathcal{H}_{AB}$, which is given as a tensor product of two Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$. Then we can see a partial trace as linear map $\mathrm{Tr}_B[.]$ from $\mathcal{H}_{AB} \to \mathcal{H}_A$ (or $\mathcal{H}_B$ respectively) defined as

$$\mathrm{Tr}_B[\hat{\rho}_A \otimes \hat{\rho}_B] = \hat{\rho}_A \mathrm{Tr}[\hat{\rho}_B] \ , \tag{2.1-15}$$

where $\hat{\rho}_A$ and $\hat{\rho}_B$ are density operators describing systems on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. This definition describes a situation when we are tracing out the system $\hat{\rho}_B$ from a bipartite system, the generalisation to more-dimensional systems is quite straightforward.

The partial trace is commonly used in many security analyses of quantum cryptographic protocols. Therefore, a more intuitive understanding of Eq. 2.1-15 and its implementation will help for further reading. Let's assume a Bell state Ψ^+ as an example of a simple bipartite pure state. By applying Eq. 2.1-8 we can write its density operator

$$\hat{\rho}_{\Psi^+} = |\Psi^+\rangle\langle\Psi^+| = \frac{1}{2}\left[(|00\rangle + |11\rangle) \otimes (\langle 00| + \langle 11|)\right] = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \ . \tag{2.1-16}$$

As a Bell state describes two entangled qubits we can easily imagine a situation when one of the qubits is lost or we simply do not have access to it (it is held by another party for example). Then the density operator of the remaining qubit $\hat{\rho}_A$ can be reached as a partial trace of the Bell state density operator $\hat{\rho}_{\Psi^+}$ over the inaccessible one

$$\hat{\rho}_A = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \ . \tag{2.1-17}$$

We already know this density operator represents an incoherent equal mixture of $|0\rangle$ and $|1\rangle$ pure states. In this case, similar to many cases in general, the result of partial trace over a pure state is a mixed state, due to losing information about part of the large system. In this example, we can also see an interesting feature of maximally entangled states' partial trace

$$\mathrm{Tr}(\hat{\rho}_{AB}) = \frac{1}{2}\mathbb{I}\,, \text{where}\,\mathbb{I}\,\text{is identity matrix}\,. \tag{2.1-18}$$

2.1.3 Quantum gates

Quantum gates, also known as quantum logic gates, are fundamental building blocks in the quantum information theory that enable the manipulation of quantum states. Similar to classical logic gates in traditional computing, quantum gates are used to perform specific operations on qubits.

Quantum gates are represented by unitary matrices that describe the transformation they induce on the quantum state. These matrices ensure that the gate operation is reversible and preserves the normalization of the quantum state. Unitary matrices are $n \times n$ complex matrices which satisfy the following property

$$\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{I}\,, \tag{2.1-19}$$

where $\hat{U}^\dagger$ denotes the Hermitian conjugate of $\hat{U}$. An effect of a unitary operation on a quantum state vector can be seen as a transformation in the vector space

$$\hat{U}\,|\psi\rangle = |\psi'\rangle\ . \tag{2.1-20}$$

The simplest example of quantum gates is a set of single-qubit gates. In principle, any unitary 2×2 matrix is a valid single-qubit gate however the commonly used ones are the following

- **Pauli gates:** These gates are represented by Pauli matrices and perform specific rotations or flips on the single-qubit state. The set of these gates includes the X gate (bit flip gate), Y gate (bit and phase flip gate), and Z gate (phase flip gate). They are represented by the corresponding Pauli matrices

$$\hat{X} = \hat{\sigma}_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \hat{Y} = \hat{\sigma}_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ \hat{Z} = \hat{\sigma}_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\ . \tag{2.1-21}$$

- **Hadamard gate:** This gate puts the qubit $|0\rangle$ or $|1\rangle$ into a superposition state, equally likely to be measured as 0 or 1. It is often used for creating superposition states and performing basis transformations

$$\hat{H} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\ . \tag{2.1-22}$$

- **Phase gates:** These gates introduce a phase shift ϕ to the qubit state without changing the probability amplitudes. The general phase gate is then represented by the matrix

$$\hat{P} = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\phi} \end{bmatrix} . \tag{2.1-23}$$

The most common phase gates are the $\hat{S}$ gate and $\hat{T}$ gate

$$\hat{S} = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\frac{\pi}{2}} \end{bmatrix} , \tag{2.1-24}$$

$$\hat{T} = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\frac{\pi}{4}} \end{bmatrix} . \tag{2.1-25}$$

The $\hat{T}$ gate is often used in more advanced quantum algorithms, such as Shor's algorithm [10] and the quantum phase estimation algorithm.

In order to not produce only trivial results we have to define two-qubit gates, which will allow us to advance operations such as entanglement generation or quantum teleportation. Here the three most common two-qubit gates are listed

- **Controlled-NOT (CNOT) gate:** It is a widely used two-qubit gate which applies a NOT gate (bit flip) operation to the target qubit if and only if the control qubit is in the state 1

$$\hat{U}_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} . \tag{2.1-26}$$

- **Controlled-Z gate:** It is also known as the controlled-phase gate or fusion gate, and applies a phase flip to the target qubit if and only if the control qubit is in state 1. It is the fundamental gate for cluster state generation

$$\hat{U}_{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} . \tag{2.1-27}$$

- **Swap gate:** This gate exchanges the states of two qubits. It seems to be trivial but it is crucial for the generation of complex cluster states

$$\hat{U}_{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} . \tag{2.1-28}$$

All general qubits' transformations can be decomposed into a set of two-qubit and one-qubit quantum gates [105]. We then can identify the smallest set of universal quantum gates to perform any operation on an arbitrary number of qubits. It has been demonstrated that any two-qubit quantum gate can be constructed using the CNOT gate combined with one-qubit gates. Additionally, for one-qubit gates, a sufficiently long sequence of H and T gates can substitute for any general one-qubit gate. Consequently, the set $\{\hat{U}_{CNOT}, \hat{H}, \hat{T}\}$ forms a universal set of quantum gates, enabling the construction of a universal quantum computer capable of implementing all types of quantum algorithms [105].

2.1.4 Measurement

In the previous chapters, we defined qubit and qubit processing. To have available all the tools, which we need to build up quantum information theory we now need to define the measurement operation, which refers to a physical quantity that can be measured or observed in an experiment. The measurement is defined by a postulate of quantum mechanics as a set of measurement operators $\{\hat{M}_m\}_{m=1}^{n}$, where the index m refers to a possible measurement outcome. Let's assume the measurement of a general pure state $|\Psi\rangle$ then the probability of observing measurement outcome m is given as

$$p_m = \langle\Psi| \hat{M}_m^\dagger \hat{M}_m |\Psi\rangle \ . \tag{2.1-29}$$

Since the sum of probabilities for all possible measurement outcomes must equal 1, the measurement operators must satisfy the completeness relation given by

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = 1 \ . \tag{2.1-30}$$

In quantum mechanics, it is well understood that the act of measurement changes the measured quantum system, a phenomenon known as the wave function collapse. If a quantum system $|\Psi\rangle$ is measured and yields an outcome m, the state immediately after the measurement is described as follows

$$|\Psi'\rangle = \frac{\hat{M}_m |\Psi\rangle}{\sqrt{\langle\Psi| \hat{M}_m^\dagger \hat{M}_m |\Psi\rangle}} \ . \tag{2.1-31}$$

2.1.4.1 Projective measurement

The most straightforward example of measurement is called projective measurement and it is defined as

$$\hat{M} = \sum_i \lambda_i \hat{P}_i = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| \ , \tag{2.1-32}$$

where λ_i are eigenvalues with corresponding eigenvectors $|\psi_i\rangle$ of the measurement operator $\hat{M}$ and $\hat{P}_i$ are orthogonal projectors which obey the standard projector

definitions: $\hat{P}_i^2 = \hat{P}_i$ and $\hat{P}_i\hat{P}_j = \delta_{ij}$. The probability that a measurement $\hat{M}$ on a quantum state $|\Psi\rangle$ will give a result λ_i is than given by

$$p(\lambda_i) = \langle\Psi|\,\hat{P}_i\,|\Psi\rangle = |\,\langle\Psi|\psi_i\rangle\,|^2 \ . \tag{2.1-33}$$

Apart from probabilities of individual measurement outcomes, we are often interested in an averaged value of measurement results with respect to a quantum state. This averaged value we usually call the expected value and define as

$$\langle\hat{M}\rangle_\Psi = \langle\Psi|\,\hat{M}\,|\Psi\rangle = \sum_i \lambda_i p(\lambda_i) \ . \tag{2.1-34}$$

If the state $|\Psi\rangle$ is described by its density operator $\hat{\rho}$ the expectation value can be defined as the following

$$\langle\hat{M}\rangle_{\hat{\rho}} = \mathrm{Tr}[\hat{M}\hat{\rho}] \ . \tag{2.1-35}$$

A simple practical example of the projective measurement is a measurement of a qubit, defined by Eq. 2.1-1 in the $|0\rangle$, $|1\rangle$ basis, where the corresponding measurement operators can be written as

$$\hat{M}_0 = |0\rangle\langle 0| \quad \hat{M}_1 = |1\rangle\langle 1| \ . \tag{2.1-36}$$

At the moment of the measurement the quantum state $|\Psi\rangle$ immediately collapses to state $|\psi_i\rangle$ which corresponds to the result of the measurement λ_i. The measurement itself then changes the quantum system. Therefore if we want to measure two properties of one quantum system, which are described by measurement operators $\hat{M}$ and $\hat{N}$, the measurement results are in general dependent on the order of our measurement. And only if the related observables commute ($[\hat{M}, \hat{N}] = \hat{M}\hat{N} - \hat{N}\hat{M} = 0$) we can measure the two properties of the system together since the commutation equation implies an existence of a simultaneous eigenbasis for the operators $\hat{M}$ and $\hat{N}$. For this reason, it is impossible to get all the information about a quantum system itself.

2.1.4.2 Quantum state tomography

Characterizing a real quantum state is a fundamental experimental task in quantum information theory. This typically involves estimating the density operator of an unknown state by performing a series of measurements whose outcomes fully describe the state. This process is known as quantum state tomography. Due to the destructive nature of measurements and the no-cloning theorem, reconstructing an unknown quantum state from a single copy is strictly impossible. Therefore, tomography must always be performed on a set of independently and identically prepared states.

The simplest example is reconstructing the unknown density operator $\hat{\rho}$ of a single qubit state. In this case, quantum state tomography aims to estimate the following expectation values

$$\mathrm{Tr}[\hat{X}\hat{\rho}],\ \mathrm{Tr}[\hat{Y}\hat{\rho}],\ \mathrm{Tr}[\hat{Z}\hat{\rho}]\ , \tag{2.1-37}$$

where $\hat{X}$, $\hat{Y}$, $\hat{Z}$ are Pauli gates, which were defined in Ch. 2.1.3. To fully characterize a single qubit state, only three measurements are necessary. However, for multi-qubit states, the number of required measurement settings increases exponentially with the number of qubits. As a result, more efficient methods, such as quantum witnesses, are employed for large-scale systems. While these methods do not reconstruct the state's density operator, they provide valuable information in the form of purity or fidelity of the quantum states, see Ch. 2.1.2.

2.1.4.3 General concept of measurement

Projective measurements, as defined by Eq. 2.1-32, are the most commonly used in quantum information. However, they are not the most general type of measurement allowed by quantum theory. For certain applications, such as the security analysis of quantum cryptographic communication protocols, we need to define a more general measurement concept known as a positive operator-valued measuremet (POVM). A POVM is represented by a set of Hermitian positive semidefinite operators $\hat{E}_i$ (POVM elements) that sum to the identity operator

$$\sum_i \hat{E}_i = \mathbb{I}\ , \tag{2.1-38}$$

where the number of POVM elements can be arbitrarily high. In analogy to quantum pure state and mixed state, we can see POVM as a statistical mixture of projection measurement elements $\hat{E}_i = |\psi_i\rangle\langle\psi_i|$.

2.1.5 Quantum information with photons

The previous sections established a theoretical framework for the three key components of quantum information: the qubit, quantum gates, and the measurement. Before delving into the integration of these foundational building blocks into quantum protocols, we will provide a condensed overview of the experimental implementation of these blocks for a qubit encoded in the polarization state of a single photon.

2.1.5.1 Photonic qubit

A qubit can be realized using any quantum-mechanical system with two orthogonal levels. However, using quantum states of light as qubits offers several practical advantages. Photons, as decoherence-free quantum systems, enable high-fidelity qubit implementation and operation even at room temperature [106]. Additionally, they can be transmitted over long distances through optical fibers, making photonic qubits ideal for long-distance quantum communication. Various physical encodings of such qubits have been implemented, an overview of the most commonly used ones is provided in Tab. 2.1.

Encoding	**Quantum state of light**	**Commonly used computational basis**
Polarization	Single photon	Horizontal and vertical linear polarization
Time-bin	Single photon	Early and late time of arrival
Photon number	Fock states	Vacuum and single-photon state
Quadrature	Squeezed state	Amplitude-squeezed state Phase-squeezed state

Table 2.1: **Frequently used photonic qubit physical implementation.**

The polarization of photons is a frequently used option for implementing photonic qubits, primarily because manipulating polarization in an experimental setup is relatively straightforward using polarizers, half- and quarter-wave plates or electro-optical modulators. In addition, the polarization state of a single photon can be transferred to long distances, by fiber or free-space propagation, with a minimal decrease in its fidelity. The common choice of computational basis ($|0\rangle, |1\rangle$) is vertical and horizontal linear polarization ($|V\rangle, |H\rangle$), but without any loss of generality, a qubit can be represented by any two orthonormal polarization state, such as diagonal and anti-diagonal linear polarization ($|+\rangle, |-\rangle$) or left and right circular polarization ($|L\rangle, |R\rangle$). The other polarization states are used mainly in quantum cryptography applications, where encoding to multiple bases is needed, see Ch. 2.2.2.

In this work, we mostly assume single-photon-based qubits encoded in a polarization state in the Z computational basis, where $|0\rangle = |V\rangle$ and $|1\rangle = |H\rangle$. The generation of single photons is in detail described in Ch. 3.

2.1.5.2 Manipulation of single polarization photonic qubit

Any general single-qubit unitary operation, including single-qubit quantum gates, can be decomposed into three rotations about some Bloch sphere's axis. In the context of polarization-encoded photonic qubits, this rotation is achieved through propagation within birefringent material. Here, the rotation axis on the Bloch sphere is determined by the orientation of the optical axis of the nonlinear crystal, and the rotation angle is set by the total phase shift acquired during the propagation. In practice, two types of devices are used to implement single-qubit unitaries:

- **Variable retarders:** The optical axis is fixed and the birefringence is tunable. Usually electro-optic modulator (EOM) or liquid crystals, where the final phase shift is linearly dependent on the controlled voltage, are used. This

approach is chosen if fast changes of implemented phase shifts are needed (information encoding in quantum cryptography, feed-forward operation in quantum computing,...).

- **Waveplates:** The birefringence is fixed and the optical axis can be rotated. This cost-efficient approach is widely used in applications where rapid phase shift changes are not required.

The unitary operation corresponding to a phase shift $\Delta\phi$ acquired from propagation through birefringent material is described by a matrix from Jones calculus

$$\hat{U}_{\Delta\phi} = \begin{bmatrix} \mathrm{e}^{i\phi_x} & 0 \\ 0 & \mathrm{e}^{i\phi_y} \end{bmatrix} = \mathrm{e}^{i\phi_x} \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{-i\Delta\phi} \end{bmatrix} \ , \tag{2.1-39}$$

were ϕ_x and ϕ_y are the phase shifts acquired from propagation along the crystallographic axes x and y, respectively. We used $\phi_y = \phi_x - \Delta\phi$, assuming that $\phi_x < \phi_y$, the x-axis is denoted as the fast axis. Then the matrix $\hat{U}_{\Delta\phi}$ illustrates the situation where the fast axis is aligned with H polarization. In the case of EOM and liquid crystals the $\Delta\phi$ is given as

$$\Delta\phi = \frac{\pi n^3 r V}{\lambda} \frac{l}{d} \ , \tag{2.1-40}$$

where parameters (n, r) characterize the birefringent material, the first is the refractive index and the second one is the given element of the electro-optic tensor. On the other hand, (l, d) characterize the crystal's geometry, where l corresponds to the interaction length, and d denotes the electrode separation. It is evident that the phase shift exhibits a linear dependence on the applied voltage V.

The general situation, where the fast axis of the crystal is rotated from the H polarization plane by angle θ is described by the following matrix

$$\hat{U}_{\Delta\phi}(\theta) = \hat{R}(-\theta)\hat{U}_{\Delta\phi}\hat{R}(\theta) \ , \tag{2.1-41}$$

where the rotation transformation matrix $\hat{R}(\theta)$ is defined as

$$\hat{R}(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \ . \tag{2.1-42}$$

However, utilizing waveplates, elements with constant birefringence, is often the most practical and cost-effective approach. Commonly accessible materials like quartz exhibit linear birefringence and can be manufactured with precise thickness to achieve the desired phase shift. In practice, two types of waveplates are used: half-wave plate (HWP) with a total phase shift of π and quarter-wave plate (QWP) implementing a phase shift of $\frac{\pi}{2}$. Waveplates with their fast axis rotated by an angle θ from the H polarization plane are described by the following matrices

$$\hat{U}_{HWP}(\theta) = \hat{R}(-\theta)\mathrm{e}^{-i\frac{\pi}{2}}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\hat{R}(\theta)$$
$$= \mathrm{e}^{-i\frac{\pi}{2}}\begin{bmatrix}\cos^2\theta - sin^2\theta & 2\sin\theta\cos\theta\\ 2\sin\theta\cos\theta & \sin^2\theta - \cos^2\theta\end{bmatrix}, \quad (2.1\text{-}43)$$

$$\hat{U}_{QWP}(\theta) = \hat{R}(-\theta)\mathrm{e}^{-i\frac{\pi}{4}}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\hat{R}(\theta)$$
$$= \mathrm{e}^{-i\frac{\pi}{4}}\begin{bmatrix}\cos^2\theta + i\sin^2\theta & (1-i)\sin\theta\cos\theta\\ (1-i)\sin\theta\cos\theta & i\cos^2\theta + \sin^2\theta\end{bmatrix}. \quad (2.1\text{-}44)$$

In this convention, HWP and QWP correspond to rotations around an axis situated in the X-Y-plane of the Bloch sphere. The rotation angles are 180° and 90°, respectively. The rotation axis's orientation is given by the physical alignment of the optical axis. It was mathematically proven that arbitrary single-qubit unitary, so arbitrary rotation at the Bloch sphere, can be implemented by a set of three waveplates (QWP-HWP-QWP) [107, 108]. In other words, every unitary can be decomposed into three waveplates' matrices

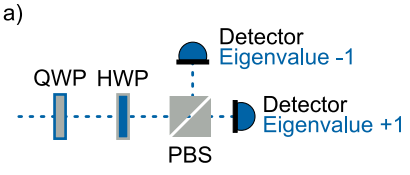
$$\hat{U} = \hat{U}_{QWP}(\theta_1)\hat{U}_{HWP}(\theta_2)\hat{U}_{QWP}(\theta_3)\ . \quad (2.1\text{-}45)$$

This is a strong universal framework for the general manipulation of a single photonic qubit.

2.1.5.3 Projective measurement of polarization photonic qubits

The last building block of quantum information protocol is a single-qubit projective measurement. The straightforward way is employing the Von Neumann approach, where the polarization basis states are coupled into two different spatial modes. The polarization state of the photon could be then determined by state tomography, where spatial mode occupations are measured [109].

a)



b)

Computational bases	QWP angle	HWP angle
X	45°	22.5°
Y	0°	67.5°
Z	0°	0°

Figure 2.1: **Polarization single-qubit measurement. a)** Setup for projective measurement of single-qubit polarization state. **b)** Angles θ of a quarter-wave plate (QWP) and a half-wave plate (HWP) to implement measurement in the free conjugate computational bases (X, Y, Z).

In polarisation degree of freedom, the projective measurement is implemented by using polarizing beam-splitter (PBS), which typically transmits H polarization and reflects V polarization. PBS is therefore equivalent to a measurement in Z computational basis, where detection of a single photon in transmitted port reveals eigenvalue $+1$ and in the reflected one reveals -1. A measurement in different computational bases can be implemented by performing single-qubit rotation $\hat{U}$ before the PBS. Assume that $|e_+\rangle$ and $|e_-\rangle$ are eigenvectors of the given computational basis with corresponding eigenvalues ± 1. Then we search a rotation $\hat{U}$, which maps the eigenvector with positive eigenvalue to $|H\rangle$ port and the negative eigenvector to the $|V\rangle$ port

$$\hat{U}\,|e_+\rangle = |H\rangle\,, \quad \hat{U}\,|e_-\rangle = |V\rangle \ . \tag{2.1-46}$$

From the previous chapter, we know that every single-qubit unitary can be implemented by a set of three waveplates. Nevertheless, the present scenario is more straightforward since our goal isn't to find a unitary mapping from any arbitrary state to another arbitrary state. Instead, we aim to map an arbitrary state to $|H\rangle$ and $|V\rangle$. Consequently, employing just one QWP and one HWP together with the PBS proves sufficient to implement Von Neumann measurement in any computational basis, see Fig. 2.1. The first QWP maps the general positive eigenstate to the linear plane of the Bloch sphere

$$\hat{U}_{QWP}(\theta_{QWP})\,|e_+\rangle = \alpha_R\,|0\rangle + \beta_R\,|1\rangle\,, \quad |\alpha_R|^2 + |\beta_R|^2 = 1\ , \tag{2.1-47}$$

where α_R and β_R are real probability amplitudes. The following HWP transform the general state in the linear plane to $|H\rangle$

$$\hat{U}_{HWP}(\theta_{HWP})\hat{U}_{QWP}(\theta_{QWP})\,|e_+\rangle = |H\rangle \ . \tag{2.1-48}$$

As was defined in Ch. 2.1.4.2 a measurement in three measurement bases (X,Y and Z) is needed to reconstruct the single-qubit state by quantum tomography approach. The corresponding angles θ_{QWP} and θ_{HWP} can be found based on the result of Ch. 2.1.5.2 and they are listed for the three computational bases in Fig. 2.1.

2.2 Quantum cryptography with single photons

Quantum cryptographic protocols are based on quantum-mechanical laws and can inherently resist eavesdropping attempts even from adversaries with unlimited power [12, 14]. Quantum cryptography is more than just secure key (SK) sharing represented by well-known QKD [14], it enables applications such as remote coin flipping [110] or bit commitment [16]. To describe quantum cryptographic protocols we will use three model parties, as illustrated in Tab. 2.2. The first two,

Alice and Bob, are the communication parties who execute the protocol [11]. Alice generates quantum states and encodes information onto them. She transmits these states through a quantum communication link to Bob, who performs measurements. In a general scenario, a third party known as Eve, the eavesdropper, enters the scene intending to compromise the protocol. Eve aims to read the shared information or manipulate the protocol to her advantage. This chapter provides a summary of fundamental quantum cryptographic protocols, offering insights into security proofs and Eve's potential hacking strategies.

Name of the party	**Icon used in this work**	**Available resources**
Alice		Single-photon source, Single-qubit gates (state encoding)
Bob		Single-photon detectors Single-qubit gates (measurement bases)
Eve		All resources allowed by laws of the nature

Table 2.2: **Overview of model parties used for the description of quantum cryptographic protocols.**

2.2.1 The no-cloning theorem

Classical information can be copied arbitrarily many times which allows us to easily work with our data, amplify information transmitted through communication networks, and operate the global classical internet effectively. But this property also opens security loopholes, which can be exploited for data interceptions. On the other hand, quantum information has a completely different nature and already in 1982, the impossibility of creating an independent and identical copy of an unknown quantum state was proven [111, 112]. This statement is known as the no-cloning. Undoubtedly, the theorem sparked the rapid advancement of quantum cryptography. It took only one year until no-cloning was used to construct the first cryptographic protocol, quantum money [113], followed soon by the most famous BB84 QKD protocol [12]. Even the foundation of the most advanced modern protocols remains rooted in the straightforward concept that quantum information cannot be copied. It is important to note here, that the no-cloning theorem is true

only for unknown quantum states. If we know the density operator of the state, by knowing the state preparation procedure, for example, we can prepare as many copies of it as we want. This principle is used in quantum state tomography, as described in Ch. 2.1.4.2.

This crucial property of quantum information can be easily seen from the linearity of quantum mechanics. Let's assume we have a quantum copy machine, which can copy quantum information from state S to state C. The copy machine is fed by blank states $|b\rangle_C$, we can imagine it as blank paper sheets which we put into a regular copy machine. For simplicity, we will use a general one-qubit state $|\psi\rangle_S = \alpha\,|0\rangle_S + \beta\,|1\rangle_S$ as the state S. The ideal quantum copy machine should then work as follows

$$(\alpha\,|0\rangle_S + \beta\,|1\rangle_S)\,|b\rangle_C = \alpha\,|0\rangle_S\,|b\rangle_C + \beta\,|1\rangle_S\,|b\rangle_C \longrightarrow \alpha\,|0\rangle_S\,|0\rangle_C + \beta\,|1\rangle_S\,|1\rangle_C \ , \quad (2.2\text{-}1)$$

where the arrow represents the ideal quantum copying process. If our quantum copy machine works properly it has to be able to copy arbitrary quantum states without knowing the probability amplitudes α and β.

$$|\psi\rangle_S\,|b\rangle_C \longrightarrow |\psi\rangle_S\,|\psi\rangle_C = \alpha^2\,|0\rangle_S\,|0\rangle_C + \alpha\beta\,|0\rangle_S\,|1\rangle_C + \alpha\beta\,|1\rangle_S\,|0\rangle_C + \beta^2\,|1\rangle_S\,|1\rangle_C \ . \quad (2.2\text{-}2)$$

As we see these two equations are in direct contradiction and therefore the ideal quantum copy machine cannot exist.

2.2.2 Quantum-cryptographic primitives

Quantum-cryptographic primitives are fundamental building blocks, which can be combined with one another to provide various security guarantees in applications such as online banking, anonymous messaging, software licensing and digital signatures [13]. In this work four main quantum cryptography primitives are investigated, QKD [14, 15, 114, 115], quantum bit commitment (QBC) [16, 17, 36], QT [18, 31, 116], QCF [19, 110, 117]. For their overview see Tab. 2.3.

2.2.2.1 Quantum key distribution

QKD is one of the most mature quantum-cryptographic primitives developed so far. It has successfully transitioned from proof-of-principle laboratory experiments to practical implementation in real-life scenarios, such as metropolitan networks [20–22], fiber links connecting cities [23, 24], and even intercontinental land-space-land connections [25].

In general, QKD protocols allow two parties, Alice and Bob, to establish a uniformly distributed SK over a public quantum channel. The parties could use this

Protocol	Description	Application
Quantum key distribution (QKD)	Alice and Bob wish to establish a secret key over an eavesdropped channel	message encryption, digital signatures, authentication
Quantum bit commitment (QBC)	Alice sends a bit to Bob, such that: • Alice cannot change the bit after committing to its value. • Bob cannot discover the value until she reveals it.	multiparty computing, verifiable secret sharing, zero-knowledge proofs
Quantum tokens (QT)	Alice issues a token or program to Bob, such that he may use it once and only once.	unforgeable money and credit cards, license protection, one-time programs, unique voting tokens
Quantum coin flipping (QCF)	Alice and Bob wish to remotely toss a fair coin, such that none of the two parties can bias the outcome towards: • any value (generates randomness): Strong QCF • their preferred, opposite value (there is a winner and a loser): Weak QCF	multiparty computing, unbiased e-voting, secure online gaming

Table 2.3: **Main quantum primitives.** A description of each primitive and its variants is provided, along with example applications to illustrate the role of each primitive within quantum networks.

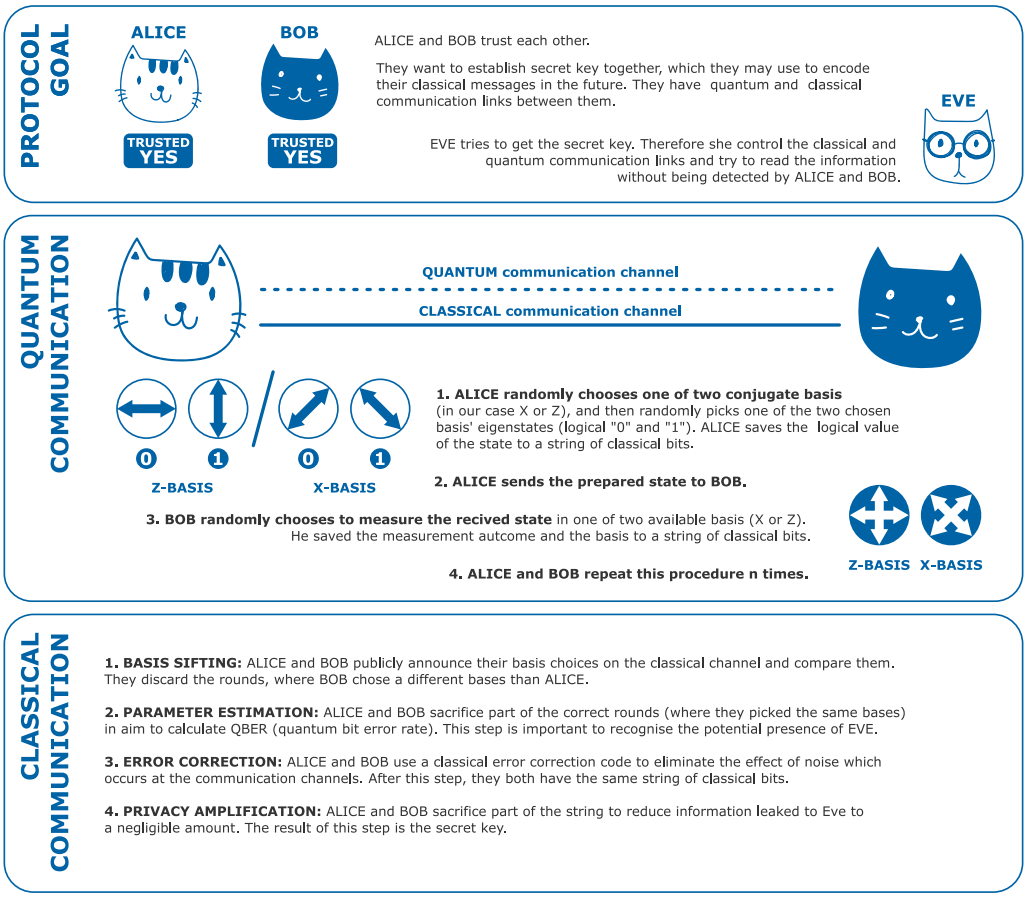


Figure 2.2: **BB84 Quantum key distribution protocol scheme.**

SK to encrypt their classical messages in the future. The quantum link between Alice and Bob is controlled by an eavesdropper, Eve, who tries to obtain some information about the shared key. Due to the no-cloning theorem, Eve cannot perfectly retrieve the sent information while her measurements introduce additional disturbance at the communication channel. Therefore Alice and Bob can reveal the presence of unwanted eavesdroppers with arbitrarily high probability by detecting a level of an error introduced on the sent information during propagation through the quantum link.

Let's describe the QKD protocol in its most standard BB84 form [12]. We will assume that Alice and Bob are connected by a public quantum channel and a public authenticated classical channel. The protocol can be divided into two main phases, quantum communication and classical communication, see Fig. 2.2. During the quantum phase, Alice prepares a sequence of four random quantum states, which are eigenstates of two conjugate bases, which are usually chosen as Z basis (eigenstates $|0\rangle$ and $|1\rangle$) and X basis (eigenstates $|+\rangle$ and $|-\rangle$). Alice

correlates the logical "0" with the nonorthogonal states $|0\rangle$ and $|+\rangle$, while the logical "1" is associated with states $|1\rangle$ and $|-\rangle$, respectively. The set of such four states is generally called BB84 states [12].

Alice sends the prepared states to Bob by the quantum communication link. He measures the received states in randomly chosen bases (X or Z basis). It becomes evident that if Bob measures the state using the same basis as Alice did, he will obtain the logical information that Alice encoded. On the other hand, if the preparation and measurement bases are not aligned the output of the measurement is random. Therefore after the quantum communication phase, Bob informs Alice about his measurement basis via the authenticated classical communication channel and Alice in the same fashion informs Bob about her preparation bases. After that, they both discard events when the measurement and preparation bases aren't aligned. Because Alice and Bob chose the bases randomly and independently they discard statistically 50 % of the events. At the end of that procedure, the so-called sifting phase, which is the start of the classical communication phase, both should have the same string of logical "0" and "1", which we call the sifted key.

In real-life protocols, the strings of Alice and Bob aren't the same after the sifting phase due to the present noise. This can have several sources, such as channel-environment noise, quantum state preparation error, quantum state measurement error or in the worst-case scenario the noise can be fully associated with Eve's presence. The level of noise is investigated in the parameter estimation phase. Let's define here the quantum bit error rate (QBER), which is the key parameter to judge the security of realistic QKD protocols. The QBER represents the probability that a generic bit of Bob's sifted string is different from the corresponding bit of Alice's sifted string. To estimate QBER value, Alice and Bob disclose a random subset of their strings and compare them. If the estimated QBER is higher than the theoretical security threshold of the given protocol, the presence of Eve can be detected and the sifted strings can't be used to establish a SK. If the QBER is lower Alice and Bob have more shared information than Eve has access to and the protocol is secure. For detailed theoretical calculation of secure QBER threshold see Ch. 2.2.3. The subset of sifted strings used for parameter estimation is discarded.

Alice's and Bob's strings aren't still the same due to the effect of noise, which occurred during the quantum communication phase. Therefore they implement classical error correction codes, which, in the ideal scenario, leads to the same classical strings on both sides. In the first step, Alice and Bob collaborate to generate a syndrome, a set of classical information derived from the observed errors in the parameter estimation phase. The syndrome serves as a fingerprint of the error pattern and helps identify which qubits are affected and how they are changed by the error. Using the syndrome information, Alice and Bob apply an error correction code to correct the errors in their respective received data. This process ensures that both parties obtain an identical, error-free version of the

shared SK. However the error correction codes leak a finite amount of information to Eve, therefore a privacy amplification procedure has to be implemented. Here Alice and Bob sacrifice a fraction of their error-corrected key as an input to serve as a key for 2-universal hashing. By this process, the probability of Eve gaining any information about the SK is reduced to a negligible amount. The final sifted strings constitute the SK.

In the real-life point-to-point implementation of the QKD protocol, the final secure key rate (SKR) is affected by losses of the communication channel, such as losses of used optical fiber or propagating losses in free space. The maximum SKR which parties can share over a lossy link is upper-bounded by the SK capacity of the channel, which can be defined by Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [118]

$$SKR_{PLOB} = -log_2(1-\eta) \approx 1.44\eta \ , \tag{2.2-3}$$

where η is the transmission of the lossy communication link. This theoretical limit for SKR can be overcome by implementing quantum repeaters in the communication channel. Recently a few protocols overcoming the repeater-less rate-distance limit of standard QKD were proposed. The first one was twin-field quantum key distribution (TF-QKD) [115], where the measurement setup is delegated to a third untrusted party, called Charlie, situated halfway between Alice and Bob. The quantum states sent by Alice and Bob travel only half the communication distance of standard QKD. The secure key is extracted from the resulting single-photon interference at Charlie's station, therefore the secure key rate scales with the square root of the channel transmittance instead of scaling linearly as was described in Eq. 2.2-3.

Since the TF-QKD protocol relies on first-order single-photon interference, Alice and Bob must share a global phase reference, making experimental implementation technically challenging [37, 119]. The more recent mode-pairing quantum key distribution (MP-QKD) protocol overcomes the need for global phase locking [120]. It is based on second-order single-photon interference, with the encoded key bits and bases determined during data post-processing. This advantage makes the implementation of MP-QKD more accessible compared to the twin-field protocol, while still maintaining the square root dependence of the SKR on channel transmission [121].

2.2.2.2 Quantum tokens

This primitive allows a central authority to issue quantum state-based tokens. Thanks to the no-cloning theorem there is no method to produce identical copies of such tokens by anyone but the authority. Such a property is called unforgeability [113]. The famous application of this primitive is quantum money, which can prevent credit card double spending [31, 122] or guarantee user privacy [123].

Various QT protocols are available, ranging from private-key to public-key systems, offering either quantum verification [113] or classical verification [122]. Certain schemes necessitate quantum memory [18, 31], while others eliminate this strong requirement by implementing no-signalling constraints [123]. In this section, we present the original Wiesner's quantum money [113] as a straightforward example of a private-key quantum token scheme with quantum verification that assumes quantum storage and can provide information-theoretic security for unforgeability. The protocol is illustrated in Fig. 2.3.

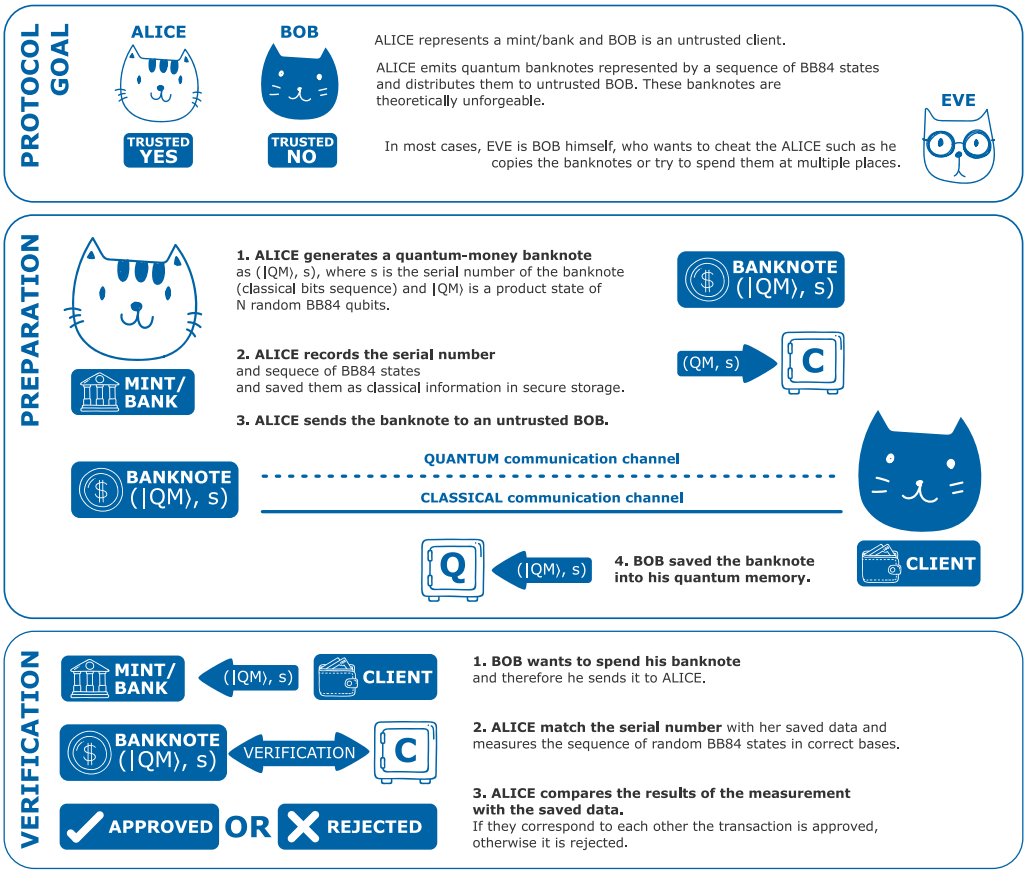


Figure 2.3: **Wiesner's quantum money protocol scheme.**

In Wiesner's scheme, the BB84 quantum states of each quantum banknote are encoded according to a random secret classical key, which is known by the central authority (Alice), and a bank or a mint usually represents it. In addition to the quantum state, Alice assigns a unique serial number to each banknote and sends it to a client (Bob). The fundamental properties of BB84 state ensure that a dishonest Bob willing to duplicate the money state will introduce errors in at least one of two states, due to no-cloning. These errors will be detected during verification by Alice when Bob decides to spend the given banknote. During the verification process, Alice connects the banknote serial number with her saved SK, measures the quantum state in the correct basis and compares the measurement outcomes with the saved information. If they correspond with each other Alice will approve Bob's transaction otherwise she will reject it.

2.2.2.3 Quantum strong coin-flipping

A strong QCF protocol allows Alice and Bob to generate and agree on a random bit. Regardless of the lack of trust between them, they wish to ensure that the bit is truly random. Therefore the QCF is called fair if a given bit is chosen with probability $\frac{1}{2}$. This probability represents the probability that two honest parties will agree on bit 0. When it equals $\frac{1}{2}$, then the probability of obtaining bit 1 is also $\frac{1}{2}$. In a dishonest protocol, each of the two parties can force a preferred outcome $i \in \{0,1\}$ with probability $P_i = \frac{1}{2} + \epsilon^{(i)}$ where $\epsilon^{(i)}$ is the protocol bias. The protocol is balanced of Alice's and Bob's cheating probability are equal, however, this is not a general case.

Achieving information-theoretically secure strong QCF with an arbitrarily small bias is beyond the reach of quantum mechanics alone [124, 125] and requires employing additional space-time constraints [126], which increase the experimental complexity of protocol implementations. Nevertheless, it has been demonstrated that even in the absence of such constraints, quantum mechanics can yield strong QCF protocols that outperform classical counterparts in terms of information-theoretic security and bias [127].

To achieve a fair and balanced strong QCF Alice usually doesn't generate states encoded in standard BB84 bases. Instead, the four coin-flipping states must allow for an extra free parameter $y \in (\frac{1}{2}, 1)$, which will be varied to guarantee the security of the protocol. The states generated by Alice are defined as

$$\begin{aligned} |\Psi_{\alpha,0}\rangle &= \sqrt{y}\,|0\rangle - (-1)^{\alpha}\sqrt{1-y}\,|1\rangle\,, \\ |\Psi_{\alpha,1}\rangle &= \sqrt{1-y}\,|0\rangle - (-1)^{\alpha}\sqrt{y}\,|1\rangle\,, \end{aligned} \tag{2.2-4}$$

where $\alpha \in \{0,1\}$ denotes the encoding basis. The four states used in the protocol are then $\{\Psi_{0,0}, \Psi_{0,1}, \Psi_{1,0}, \Psi_{1,1}\}$.

In the strong QCF protocol Alice generates N random states in randomly picked bases α and sends them to Bob. He measures all the received states in random bases α and informs Alice about the position of the first measured state

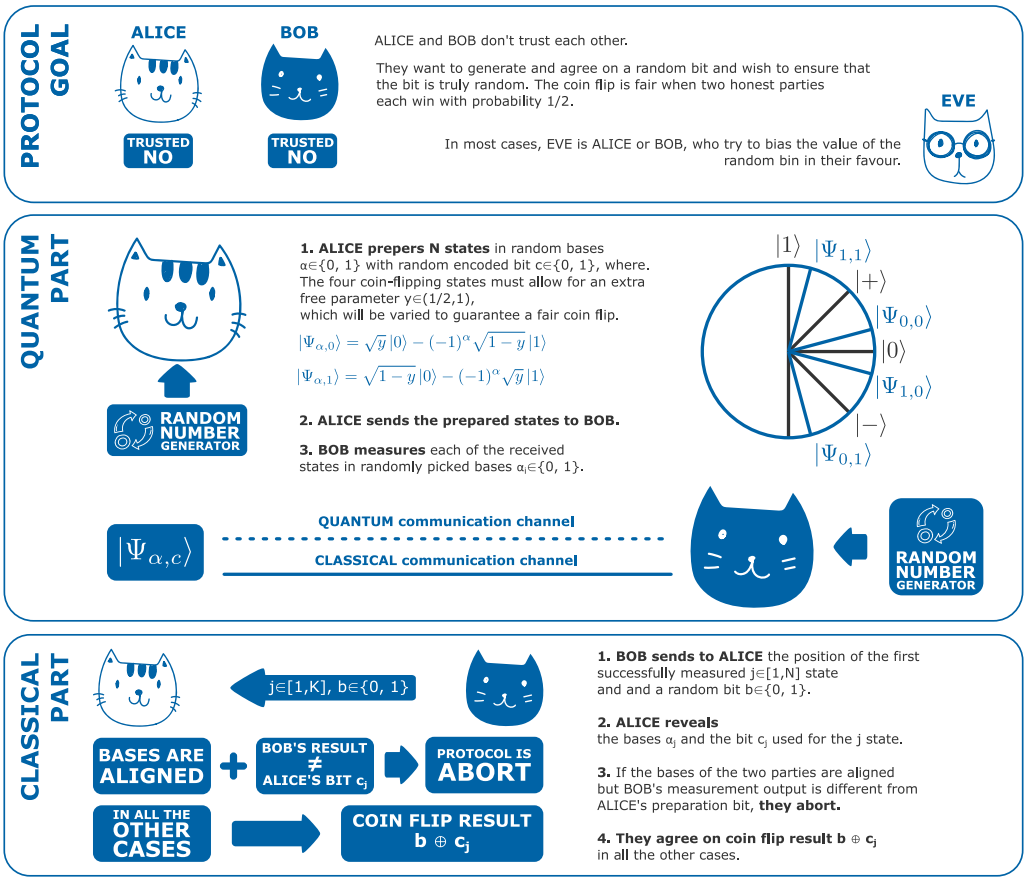


Figure 2.4: **Quantum strong coin-flipping protocol scheme.**

and the value of his randomly generated classical bit b. Alice then reveals the encoding bases and the bit value encoded in that state. If their bases are aligned and Bob's result of the measurement doesn't agree with Alice's encoded bit they abort the protocol. In all the other cases they agree on the result of the coin flip as $[(c_j + b) \mod 2]$, here c_j is the value of the measurement outcome of the state, which Bob labelled as the first detected one [110]. The strong QCF protocol is described in Fig. 2.4.

2.2.2.4 Quantum bit commitment

QBC protocol can be described by its two phases: the commit phase and the open phase. In the commit phase, honest Alice chooses a bit $b \in \{0,1\}$ and provides honest Bob with some form of evidence that she committed to one of the bit values without revealing her choice. The involved parties wait for some agreed time and then continue with the open phase, where honest Alice reveals b to honest Bob. In the ideal protocol, Bob doesn't know anything about the committed bit value

until Alice reveals her choice (hiding property) and at the same time, Alice cannot change the committed bit value (binding property).

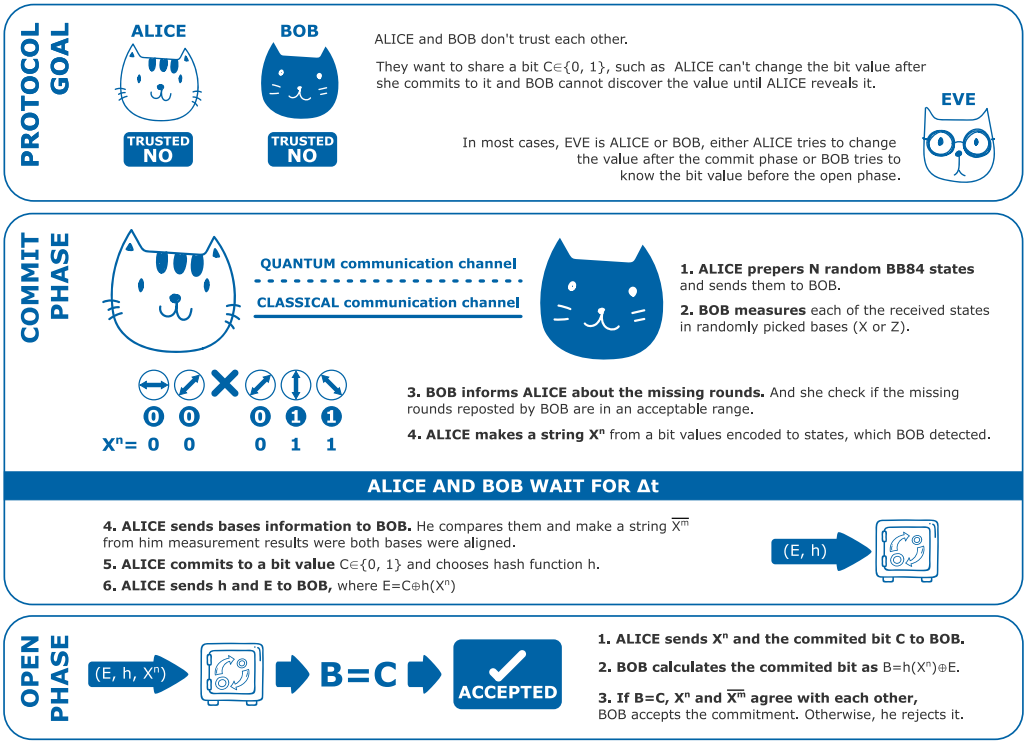


Figure 2.5: **Quantum bit commitment protocol scheme.**

Similar to strong QCF, the quantum version of bit commitment cannot provide perfect information-theoretic security for both parties without additional space-time constraints [128, 129]. However, this strong restriction can be circumvented by placing restrictions on dishonest Bob's storage capabilities [128, 129].

Here we focus on the quantum protocol from [16], secure under noisy storage assumption. The protocol is illustrated in Fig. 2.5. In this protocol, we assume that Alice and Bob agreed to wait in the middle of the commit phase for time Δt, which is significantly longer than the storage time of all existing quantum memories. During the commit phase, honest Alice generates N BB84 states and sends them to Bob. He performs random X or Z measurements at each of the states and reports to Alice about states, which were lost. Alice makes a string X^n from bits, which she encodes in the states detected by Bob and waits for the given time Δt. Then Alice sends all the preparation bases to Bob, he makes a string $\overline{X^m}$ from his measurement results where their bases were aligned. Alice commits to a bit value $C \in \{0, 1\}$, choses a hash function h and calculate $E = C \oplus h(X^n)$. She sends $\{C, E\}$ and closes the commit phase.

At the beginning of the open phase, Alice sends the string X^n and the commit-

ted bit C to Bob. He calculates a value of control committed bit as $B = h(X^n) \oplus E$. If $B = C$ and X^n agree with $\overline{X^m}$ Bob accepts the bit commitment. In all the other cases he rejects it.

2.2.3 Security of quantum cryptography

In this chapter, we will examine the security of a quantum cryptographic protocol using a QKD protocol as an example. We will first describe the simplest eavesdropping strategy, the intercept-resend attack, and then outline the optimal attack on an ideal QKD system. Following this, we will address the practical security of QKD protocols, which are no longer ideal and involve various types of errors. We will specify security proofs for QKD protocols where PDSs are employed.

2.2.3.1 Intercept-resend attack on ideal QKD

The intercept-resent attack is the basic eavesdropper strategy against many quantum cryptographic primitives. Eve interrupts the quantum communication channel and measures all the states, which Alice sent to Bob. She either randomly chooses measurement bases from Bob's set or measures all the quantum states in one base, which is optimized to maximise the success of her strategy. Later we will see, which one of these two approaches is more efficient. In general, the basic intercept-resent attack is not an efficient eavesdropping strategy and can be easily spotted by Alice and Bob due to the high level of produced noise. We will study the success of this attacking technique on BB84 QKD protocol as described in Ch. 2.2.2.1.

Consider a scenario where Eve breaks the protocol and performs measurements on every state sent by Alice using a random basis (either X or Z). Subsequently, she prepares a new quantum state based on the measurement results and chosen basis and sends it to Bob. Because Alice and Eve chose their bases randomly the probability that they will be aligned, which is also Eve's success probability, is 50 %. In all the other states Eve will just introduce noise. Bob chose his measurement bases also randomly and therefore he will spot the error introduced by Eve in half of the cases. We can then easily see that QBER introduced by this simple intercept-resend attack is 25 %. Eve after this attack has at least the same amount of information as Bob and the SK cannot be established.

In the second scenario, Eve will measure all the states in general bases $\{|\theta\rangle, |\theta_\perp\rangle\}$ defined by two orthonormal vectors in two-dimensional Hilbert space

$$|\theta\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \ , \tag{2.2-5}$$

$$|\theta_\perp\rangle = \sin\frac{\theta}{2}|0\rangle - e^{-i\phi}\cos\frac{\theta}{2}|1\rangle \ . \tag{2.2-6}$$

Eve will then assign a logical bit "1" (corresponding to Alice's states $|1\rangle$, $|-\rangle$) to outcome $|\theta\rangle$ and logical bit "0" (corresponding to Alice's states $|0\rangle$, $|+\rangle$) is signed to Eve's outcome $|\theta_\perp\rangle$. We can now calculate conditional probabilities

Alice's state	**Eve's measurement outcome**	**Eve's measurement probability**	**Bob's error probability**
$\|0\rangle$	$\|\theta\rangle$	$P(\theta \mid 0) = \cos^2 \frac{\theta}{2}$	$P(1 \mid \theta) = \sin^2 \frac{\theta}{2}$
	$\|\theta_\perp\rangle$	$P(\theta_\perp \mid 0) = \sin^2 \frac{\theta}{2}$	$P(1 \mid \theta_\perp) = \cos^2 \frac{\theta}{2}$

Table 2.4: **Probability that Bob will get an error in the result during the intercept-resend attack with fix Eve's measurement bases for Alice's state** $|0\rangle$.

$$P(\theta \mid 0) = P(\theta_\perp \mid 1) = \cos^2 \frac{\theta}{2} \ , \tag{2.2-7}$$

$$P(\theta \mid +) = P(\theta_\perp \mid -) = \frac{1 + \sin\theta \cos\phi}{2} \ . \tag{2.2-8}$$

By considering a sifting scenario, we can use Bayes's theorem to demonstrate that Eve's probability of guessing Alice's state, based on her measurement outcomes in the general basis $|\theta\rangle, |\theta_\perp\rangle$, is given by the following equations [102]

$$P(0 \mid \theta) = P(1 \mid \theta_\perp) = P(\theta \mid 0) = P(\theta_\perp \mid 1) = \cos^2 \frac{\theta}{2} := P_E^Z \ , \tag{2.2-9}$$

$$P(+ \mid \theta) = P(- \mid \theta_\perp) = P(\theta \mid +) = P(\theta_\perp \mid -) = \frac{1 + \sin\theta \cos\phi}{2} := P_E^X \ , \tag{2.2-10}$$

where P_E^Z and P_E^X are probabilities that Eve will decode a state, which Alice sent in Z or X bases. For bases defined by angles $\theta = \frac{\pi}{4}$ and $\phi = 0$ these two probabilities will equal

$$P_E^Z = P_E^X := P_E \approx 0.85 \ . \tag{2.2-11}$$

We see that Eve's success probability, P_E, is now higher compared to the scenario where Eve measures randomly in the Z or X bases. Now, we will estimate QBER associated with this attack. The intuition behind the calculation is shown in the example for Alice's state $|0\rangle$, see Tab. 2.4. Then for the probability that Bob will get an error in the measurement result if Alice prepared the state in Z-bases, we can write

$$P(1 \mid 0) = P(1 \mid \theta)P(\theta \mid 0) + P(1 \mid \theta_\perp)P(\theta_\perp \mid 0) = \frac{\sin^2\theta}{2} \ , \tag{2.2-12}$$

$$P_{error}^Z = P(0 \mid 1) = P(1 \mid 0) \ . \tag{2.2-13}$$

The same calculation can be done also for Alice's state in X-bases, where we get

$$P^X_{error} = P(- \mid +) = P(+ \mid -) = \frac{1 - \sin^2\theta\cos^2\phi}{2} \ . \tag{2.2-14}$$

Because Alice changes Z and X bases randomly the final QBER can be calculated as an arithmetic average of these two probabilities

$$QBER = \frac{(P^Z_{error} + P^X_{error})}{2} = \frac{1 + (1 - \cos^2\phi)\sin^2\theta}{4} \ . \tag{2.2-15}$$

If we calculate it for the bases defined by angles $\theta = \frac{\pi}{4}$ and $\phi = 0$ we get 25 % as in the previous case. The intercept-resend attack always introduces high noise to the protocol. Therefore, it is not an ideal hacking strategy for BB84 QKD protocol.

2.2.3.2 Optimal attack on ideal QKD

To determine the minimum QBER that Eve can introduce during a successful attack on the ideal BB84 QKD protocol, we will assume that Eve has access to an ancilla system of arbitrary dimension, which she can entangle with Alice's states. Throughout the protocol, all of Alice's states interact with Eve's ancillae, which she can store in a lossless quantum memory. Eve will then use an optimal coherent measurement based on the information obtained during the sifting phase.

The security proof for this type of abstract attack is based on the concept that QKD aims to share maximally entangled states between Alice and Bob. We can map the QKD protocol to an entanglement distillation protocol [130], which starts with a set of non-maximally entangled states and, through local operations and classical communication, produces a smaller number of states with a higher degree of entanglement. This approach closely parallels the general framework of the BB84 QKD protocol discussed in Ch. 2.2.2.1.

By optimization over the set of all possible POVMs, it was shown that BB84 QKD can be secure with a data rate of at least

$$SKR_{min} = 1 - 2H_2(\epsilon) \ , \tag{2.2-16}$$

where ϵ is QBER of the protocol and $H_2(\epsilon)$ is Shannon binar entropy defined as

$$H_2(x) = -xlog_2x - (1 - x)log_2(1 - x) \ . \tag{2.2-17}$$

The SKR defined by Eq. 2.2-16, reaches 0 for QBER around 11 % [130], which is regarded as the minimum acceptable level of the error caused by Eve's successful attack on the protocol. In simpler terms, the QBER arising from technical imperfections in the QKD implementation must always be below 11 % for the ability to detect Eve's presence, otherwise the QKD implementation is not secured.

2.2.3.3 Practical security of QKD

Up to this point, we have not considered any practical imperfections in QKD implementation, such as finite key effects, errors in state preparation and measurement, or multi-photon contributions in the states generated by Alice. These imperfections introduce errors into the final protocol and open the door to various new strategies for successfully attacking the protocol. In practical security, we account for a defined small error, denoted by ϵ, which arises from all these protocol imperfections., and then we will say about such QKD protocol, that it is ϵ secure.

Before we delve into the details of practical security, let's first summarize the general security criteria that will serve as the foundation for the subsequent security proofs. We will start by defining an ideal SK based on the following three requirements:

- *Requirement of correctness:* Alice's and Bob's key bit strings are identical.
- *Requirement of secretness:* The key bit string is known only by Alice and Bob.
- *Requirement of uniformity:* The final shared key has to be uniformly random.

We can decompose the error ϵ into two components, $\epsilon = \epsilon_{cor} + \epsilon_{sec}$, which quantify how the practical SK deviates from its ideal correct and secret image. Let K_A and K_B represent the classical registers of Alice and Bob, respectively, and assume they have the same length m. The state shared among Alice, Bob, and Eve in a general QKD protocol can then be described by the following joint state

$$\hat{\rho}_{ABE} = \sum_{k_A,k_B} Pr(k_A,k_B)\,|k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \hat{\rho}_E^{(k_A,k_B)} \ , \tag{2.2-18}$$

where $k_A, k_B \in \{0,1\}^m$ are the key logical bits of Alice and Bob, $Pr(k_A,k_B)$ is a probability of getting given logical bits values of k_A, k_B and $\hat{\rho}_E$ is Eve's quantum state, which is correlated with the key strings. In the ideal scenario, Alice and Bob possess identical key strings, $k_A = k_B = k$, and the shared key is uniformly random, so we can write $\sum_{k_A,k_B} P_r(k_A,k_B) = 2^{-m}$. Additionally, Eve has no information about the key, her state $\hat{\rho}_E$ is independent of k. This we can describe by an ideal joint state

$$\hat{\rho}_{ABE}^{ideal} = 2^{-m} \sum_k |k\rangle_A \langle k| \otimes |k\rangle_B \langle k| \otimes \hat{\rho}_E \ . \tag{2.2-19}$$

We will say about real QKD protocol that it is ϵ-correct if the following inequality holds

$$Pr(k_A \neq k_B) \leq \epsilon_{cor} \ . \tag{2.2-20}$$

In the same fashion, we will call a real QKD protocol ϵ-secure if the joint state share between Alice and Eve $\hat{\rho}_{AE}$ is close to its ideal image $\hat{\rho}_{AE}^{ideal}$.

$$\min_{\hat{\rho}_E} \frac{1}{2}(1 - p_{abort})\|\hat{\rho}_{AE} - \hat{\rho}_{AE}^{ideal}\|_1 \leq \epsilon_{sec} \ , \tag{2.2-21}$$

where $\|\hat{A}\|_1$ is trace norm, p_{abort} is probability that the protocol will aboard and $\hat{\rho}_{AE}^{ideal}$ can be define directly from $\hat{\rho}_{ABE}^{ideal}$ as

$$\hat{\rho}_{AE}^{ideal} = 2^{-m} \sum_k |k\rangle_A \langle k| \otimes \hat{\rho}_E \ . \tag{2.2-22}$$

Now we can put all the requirements together and say that QKD protocol is ϵ secure and correct if the following holds

$$\min_{\hat{\rho}_E} \frac{1}{2}(1 - p_{abort})\|\hat{\rho}_{ABE} - \hat{\rho}_{ABE}^{ideal}\|_1 \leq \epsilon \ . \tag{2.2-23}$$

2.2.3.4 Practical security of quantum cryptography with Poisson distributed sources

To estimate the expected SKR of a practical QKD protocol, we need to define Alice's source of quantum states. In the following analysis, we will assume that Alice holds a PDSs, such as a WCSs source or a source based on SPDC. PDSs represent easy-to-use and robust technologies, making them widely used in quantum cryptography applications [14]. As we will discuss in the Ch. 3.1, PDSs generate quantum coherent states, which can be mathematically described as a coherent superposition on photon-number states

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \ , \tag{2.2-24}$$

where α is a coherent state amplitude and it is in general complex number and $|n\rangle$ in a photon-number state. From here we can define the average photon number as

$$\mu = \mid \alpha \mid^2 \ . \tag{2.2-25}$$

To see how information, in our case BB84 states, is encoded into the coherent state we may express the coherent state in two modes [14]

$$|\alpha_{\beta k}\rangle = \left| e^{i\theta} \frac{\alpha}{\sqrt{2}} \right\rangle \otimes \left| e^{i(\theta+\phi_k)} \frac{\alpha}{\sqrt{2}} \right\rangle \ , \tag{2.2-26}$$

where the index $\beta \in X, Z$ indicates Alice's preparation basis, the index $k \in \{0, 1\}$ gives the encoded logical bit, θ is a global phase and $\phi_k \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ is a relative phase between the modes and it is given by $\{\beta, k\}$. In the context of an attack on a quantum cryptography protocol, Eve must gain access to the relative phase ϕ_k to reveal the information encoded in the quantum state.

The most common security analyses for QKD protocols using PDSs or coherent states assume that the global phase θ is continuously randomized through a

phase-scrambling process [14, 131]. If the global phase is not randomized, the security of the protocol implementation is significantly compromised [132], as also demonstrated by experimental quantum attacks showing that a QKD protocol can be vulnerable when the phase is not randomized [33, 133]. When we randomize the global phase of the coherent state we get a new state in the form of a number-state mixture

$$\hat{\rho}_\mu = \frac{1}{2\pi}\int_0^{2\pi} d\theta \, |\alpha e^{i\theta}\rangle\langle\alpha e^{i\theta}| = \sum_{n=0}^{\infty} P_\mu(n) \, |n\rangle\langle n| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\,|n\rangle\langle n| \ , \quad (2.2\text{-}27)$$

where $P_\mu(n)$ is the probability distribution for the photon-number states in the given coherent state characterised by the average photon number μ, which is described by Poisson distribution as $P_\mu(n) = e^{-\mu}\frac{\mu^n}{n!}$.

From this point onward, we will assume that Alice has PDSs with an actively scrambled global phase, and her state before encoding information is represented as a mixture of number states, as shown in Eq. 2.2-27. We can now calculate the expected SKR for a practical QKD protocol. Let Y_k denote the yield of a k-photon state, which is the probability of a click on Bob's detector resulting from Alice's k-photon state.

$$Y_k = Y_0 + (1 - Y_0)\left[1 - (1 - \eta_d\eta_t)^k\right] \ , \quad (2.2\text{-}28)$$

where η_d represents Bob's detection efficiency, η_t denotes the channel transmission, and Y_0 is the probability of a dark count, which is the likelihood of the detector clicking in the absence of a signal. We define the gain Q_k as the combined probability that Alice generates a k-photon state and Bob successfully detects it

$$Q_k = P_\mu(k)Y_k \ . \quad (2.2\text{-}29)$$

Then we can lower-bound the SKR after privacy amplification and error correction as following [134]

$$SKR \geq \frac{1}{2}\left[Q_1(1 - H_2(\epsilon_1)) - fQ_\mu H_2(E_\mu)\right] \ , \quad (2.2\text{-}30)$$

where Q_μ is a gain of the signal state and E_μ is its QBER. Additionally, ϵ_1 stands for the QBER generated by single-photons only, f represents the error-correction efficiency based on a one-way classical code assumption, and $H_2(x)$ is Shannon binary entropy as it was defined by Eq. 2.2-17.

In practical sources, such as PDSs, multi-photon contributions are unavoidable and introduce additional security loopholes. Specifically, Eve can split a multi-photon pulse, where each photon carries the same encoded information, and store one of these photons in a lossless memory for a delayed-choice attack. Meanwhile, Alice and Bob cannot distinguish whether a detection click results from a single-photon or multi-photon component. In other words, they cannot directly

determine Q_1 and ϵ_1 in Eq. 2.2-30. As a result, Eve can alter the photon statistics of the state without being detected by Alice and Bob. To account for this, we assume the most conservative scenario where all losses and errors are attributed to the single-photon contribution, implying $Y_k = 1$ and $\epsilon_k = 0$ for $k \geq 2$. This scenario can seen as separating multi-photon states, which may leak information to Eve, from single-photon states, which do not. We can then proceed to estimate the parameters related to the single-photon contribution as

$$Q_1 \geq \sum_{k=0}^{\infty} Q_k \sum_{k=2}^{\infty} P_\mu(k) \ , \tag{2.2-31}$$

$$\epsilon_1 \leq \frac{E_\mu Q_\mu}{Q_1} \ , \tag{2.2-32}$$

$$E_\mu = \frac{1}{Q_\mu} \sum_{k=0}^{\infty} \epsilon_k Q_k \ , \tag{2.2-33}$$

$$\epsilon_k = \frac{\epsilon_0 Y_0 + \epsilon_d \left[1 - (1 - \eta_d \eta_t)^k\right]}{Y_k} \ , \tag{2.2-34}$$

where ϵ_d is detection error probability, which comes from setup imperfections.

This conservative assumption, that SKR derives solely from single-photon states, imposes strong limits on the mean photon number μ and the secure communication distance between Alice and Bob. To ensure the protocol remains secure, Alice must minimize the multi-photon contribution by keeping the mean photon number low. Additionally, she can further optimize the mean photon number based on the setup efficiency η to achieve the highest possible SKR at given setup losses. For a rough estimate, the optimal mean photon number can be approximated by the formula $\mu_{opt} \approx \eta = \eta_d \eta_t$ [135].

2.2.3.5 Decoy state method

The decoy-state method is the most widely used practical countermeasure against the security loopholes associated with multi-photon components in QKD protocols, such as the photon-number splitting (PNS) attack discussed in Ch. 2.2.4.1. In the previous security analysis, we assumed that Eve could fully exploit the multi-photon components, and since she controls the communication channel, Alice and Bob cannot differentiate whether detection is coming from a single-photon or a multi-photon component. Consequently, they pessimistically assume that all the losses and errors come only from single photons, which, as we saw, significantly restrict the value of the final SKR. Quantitatively, this assumption typically limits the secure communication distance of practical QKD protocol to below 30 km [134], assuming a loss of 0.21 dB/km for single-mode telecommunication optical fiber at 1550 nm.

This significant limitation was effectively mitigated by employing the decoy-state method [136]. Instead of sending WCS at a single optimal mean photon

number, Alice varies the intensities of the coherent states across different pulses. After Bob detects the signals, Alice reveals the mean photon number μ for each pulse. This allows Alice and Bob to separately assess the transmittance of each photon-number component and tightly bound the single-photon detections. Since Eve lacks information about Alice's decoy-state preparation, she cannot adapt her attack strategy to the different photon-number statistics and therefore she will always change the statistics of signal and decoy-state differently. In general, the decoy-state method significantly enhanced the performance of QKD with practical sources, demonstrating that the SKR is linearly dependent on the setup efficiency η, compared to the quadratic dependence observed in standard QKD systems, see Fig. 2.6

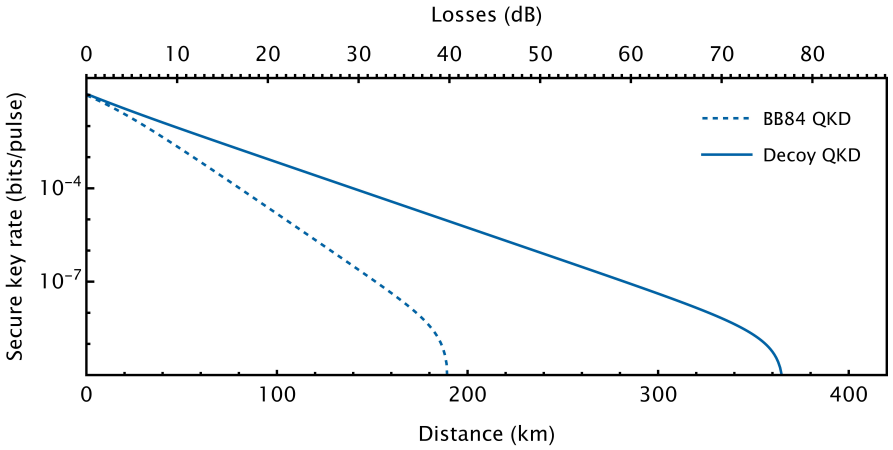


Figure 2.6: **Comparison of secure key rate of BB84 QKD and Decoy state QKD protocols.** The parameters of acqkd protocol were fixed as: alignment error rate $e_d = 2\,\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\,\%$, and error-correcting code inefficiency $f = 1.2$. The curves were calculated as the best performance of randomized-phase PDS.

The conventional source for the decoy method is a phase-randomized WCS source, where Alice has the capability to randomly modulate the mean-photon number for each pulse. This is typically achieved by using an actuated laser with a fast variable attenuator. The main assumption for the decoy-stated QKD security analysis is that the signal state and decoy state are identical apart of their mean-photon number. Consequently, Eve is not able to differentiate between signal pulses and decoy pulses based on her photon-number measurements. Alice and Bob can estimate the protocol parameters, such as a gain Q_μ and QBER E_μ, for each mean-photon number based on the following equations

$$Q_\mu = \sum_{n=0}^{\infty} P_\mu(n) Y_n \ , \tag{2.2-35}$$

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} P_\mu(n)\epsilon_n Y_n \ , \tag{2.2-36}$$

where Y_n and ϵ_n are the yield and error of the n-photon number component, respectively. And P_n is Poisson distribution of coherent state with mean-photon number μ given as $P_\mu(n) = e^{-\mu}\frac{\mu^n}{n!}$. Following the security analysis given by Eq. 2.2 -30 we estimate the SKR as the following

$$SKR \geq -Q_\mu H_2(E_\mu) + Q_1\left[1 - H_2(\epsilon_1)\right] \ , \tag{2.2-37}$$

where the Q_μ and E_μ can be obtain from experimental data and Q_1 can be calculated as $Q_1 = Y_1\mu e^{-\mu}$.

To achieve the security benefits of the decoy-state method, it is not necessary to use an infinite number of different WCS intensities. In practice, a limited number of intensities suffices for accurate parameter estimation. The most commonly used decoy-state method involves coherent states with three distinct intensities: $0, \nu, \mu$. Here, states with a mean photon number of μ are used as signal states, while states with intensity $\nu < \mu$ and vacuum states with intensity 0 are utilized for parameter estimation [134].

2.2.4 Practical attacks at a quantum cryptographic protocol

Up until now, we have primarily focused on the theoretical aspects of attacks on the QKD protocol. We described the intercept-resend attack, which has proven to be suboptimal, see Ch. 2.2.3.1. Moreover, in the previous chapter, we also defined the most common countermeasure to attacks using multi-photon contributions in a real photonic state, used in QKD implementations.

Here, we will move beyond theoretical approaches and describe several practical attack implementations. These have proven to be quite powerful and significantly limit the security of practical quantum cryptography protocols [14, 137].

2.2.4.1 Multi-photons attacks

The first group of attack strategies lies on a multi-photon component of the quantum state generated by Alice's imperfect single-photon source. Currently, the most common sources in quantum cryptography are WCSs [14] whose photon number distribution follows Poisson's statistics and therefore there is a non-zero probability of multi-photon generation, see Eq. 2.2-24.

The PNS attack is a well-known strategy that leverages pulses containing two or more photons with the same encoded information to gain partial knowledge of the SK in QKD protocols [135]. In the first phase, Eve uses a quantum non-demolishing measurement to detect multi-photon pulses. Based on the measurement outcome, she either blocks the pulse if it contains only a single photon or splits a multi-photon pulse into two. In the latter case, she stores one of the photons and

sends the other to Bob. During the reconciliation phase, she can potentially gain significant information about the SK.

To understand the effectiveness of the PNS attack, consider a BB84 protocol with a fiber link that has losses of $(1 - \eta_t)$. The probability that a single-photon pulse generated by Alice's PDS will be transmitted to Bob is given by $(1-e^{-(1-\eta_t)})$. Conversely, the probability that at least one photon from a two-photon pulse sent by Alice will reach Bob is $(1 - e^{-2(1-\eta_t)})$. As the communication channel experiences losses, Bob's detection events will increasingly be based on Alice's multi-photon pulses.

In general, we assume Eve can replace the lossy link with a lossless one. In this scenario, she can simulate channel losses by blocking single-photon pulses and fully exploit multi-photon pulses to obtain substantial information about the SK without being detected by Alice and Bob. The simplest countermeasure to the PNS attack is the decoy-state method, as described in Ch. 2.2.3.5.

2.2.4.2 Phase-discrimination attacks

As we discussed in Ch. 2.2.3.3 the global phase randomization of the used WCS stands as one of the most fundamental assumptions in QKD security proofs. Only if the overall phase is equally spanned over the interval $[0, 2\pi]$ the original WCS pure state is reduced into a mixture of photon-number states, see Eq. 2.2-27. Let's discuss Eve's strategies if this fundamental assumption doesn't hold and the phase is not perfectly scrambled.

The security of the decoy-state method relies on the assumption that signal and decoy states share identical characteristics, making them indistinguishable. This assumption holds only when the phase of the utilized WCS is entirely random. In contrast, if the phase is not scrambled, Eve can employ an unambiguous state discrimination (USD) type attack, enabling her to differentiate between signal and decoy states without perturbing the state sent by Alice. Subsequently, she can implement the PNS attack on the signal states and transmit the decoy ones to Bob without any action [33].

An effective countermeasure against phase discrimination attacks is the implementation of a robust phase-randomization technique for WCS. Phase scrambling is commonly achieved using an active phase modulator. However, this method limits communication rates to just a few MHz [138]. To achieve higher rates, up to several GHz, phase randomization based on laser gain switching is often employed [51].

An attenuated semiconductor laser diode is a commonly used source of WCS in quantum cryptography. In general, the lasing process begins with the spontaneous emission of a photon, which is then amplified within the laser gain medium. In the case of a laser diode, this amplification is driven by an electric field. The initial photon sets the global phase of the generated laser beam. To actively randomize the phase from pulse to pulse, the laser can be switched on and off between each pulse generation. Each pulse originates from its own spontaneously

emitted photon, which is independent of the previous one and therefore each pulse has an independent global phase reference. For semiconductor laser diodes, this operation can be easily achieved using a current pulse drive [51].

2.2.4.3 Side-channels attacks

In reality, Eve's capabilities extend beyond relying solely on imperfections in Alice's phase-scrambling technique. She can actively manipulate the phase-randomization process. Let's suppose Alice employs laser gain switching for phase randomization, where every WCS pulse starts from an independent spontaneously emitted photon. However, the same process can be triggered by a seed photon with a given characteristic, which comes to the laser gain media from the outside environment. This is the basic motivation for the laser seed-control attack [139], where Eve holds her own semiconductor laser diode with the same characteristics as Alice's one and uses it to back-propagate WCS pulses to Alice. If some of Eve's photons reach the gain media of Alice's laser diode, they can serve there as seed photons to start the next lasering process and Eve can fully determine the phase of all Alice's WCS pulses.

The laser seed-control attack is the first example of so-called side-channels attacks, which exploit a physical implementation of quantum cryptography protocols. These attack strategies are performed via channels or mediums that are created as a side effect of the main practical hardware implementation. A famous example is the Trojan horse attack (THA) [140], where Eve sends a back propagated light to Alice or Bob as a probe of their physical setups. From the back reflection, she can get all the information about the encoded state or measurement bases.

Detectors are significantly more vulnerable to side-channel attacks than the source. Since Eve controls the communication channel, she can send various types of radiation to Bob. Because he is unable to adequately isolate his laboratory and close off all potential side channels, he is likely to receive Eve's signals in most scenarios.

An example of such hacking strategies is the detector blinding attack (DBA) [141,142]. Let's consider a scenario in which Bob uses common avalanche photodiodes (APDs) as his single-photon detectors. When these detectors are exposed to a high-energy optical pulse, known as a blinding pulse, they switch from their single-photon operation mode to a linear mode. In this linear mode, only optical pulses with energy above a certain threshold trigger a click response. Consequently, Bob records these clicks but cannot distinguish between those resulting from single-photon detection under normal conditions and those caused by the blinding pulses in linear mode.

In a typical DBA protocol, Eve initiates the attack by blinding Bob's detectors with a high-energy optical pulse. She then performs an intercept-resend attack, where she measures the quantum states sent by Alice using randomly chosen bases. Based on the outcomes of these measurements, Eve sends coherent pulses with

energy just above the detection threshold of the blinded detectors to Bob. If Bob uses the same measurement bases as Eve, he will obtain the same measurement outcome. If their measurement bases are not aligned, the optical pulse splits into two, with each pulse having energy below the detection threshold, resulting in no click recorded by Bob. This typically introduces an additional 50 % loss, though Eve can compensate for these losses using her lossless communication channel. This strategy allows Eve to recover the entire SK without increasing the QBER. The DBA attack is not limited to APDs, it has also been demonstrated against other single-photon detector platforms, such as superconducting nanowire single-photon detectors (SNSPDs) [143].

The other possible side-channel attacks on detectors investigate double-clicks [135], time dependence of detector efficiency [144] or issues with time synchronization [145]. In theory, Eve can use any possible side channel, including gravitation waves or X-ray beams to name the most outstanding ones, to make Alice's and Bob's devices work to her advantage. To make a practical implementation of a quantum cryptography protocol secure against these attacks is therefore a real challenge mainly due to their huge variety. Although several practical countermeasures have been implemented [146], they often come at the cost of reduced setup efficiency.

3
Quantum-light sources

The intensive development of quantum-light sources in recent decades has been strongly motivated by the increasing demand for emerging quantum technologies, such as quantum computing, cryptography, quantum metrology, and sensing [147]. The diverse applications harness specific quantum states [5, 14, 148–152], and the ideal quantum light source for each application should generate the required state with near-perfect fidelity on demand. In this context, the focus of this thesis is on applications in single-photon quantum cryptography, where the fundamental state is a qubit encoded in a general degree of freedom of a single photon, as previously described in Chapter 2.1.5.1. Various platforms for single-photon generation have been explored, including spontaneous parametric down-conversion [48, 153], nitrogen-vacancy centres [154], trapped atoms [155], biomolecules [156], and semiconductor quantum dots [55].

3.0.1 Quantum light

Before we start describing quantum light sources more in detail, let's look at the theory of quantum light itself. The electromagnetic field in free space can be described by vector potential $\vec{A}$, which satisfies the wave equation given as

$$-\Delta\vec{A} + \frac{1}{c^2}\frac{\partial^2\vec{A}}{\partial t^2} = 0 \ , \tag{3.0-1}$$

where c is the speed of light in vacuum. We assumed the Coulomb gauge $\nabla \cdot \vec{A} = 0$. In this specific condition, the longitudinal part of the vector potential is transformed away and $\vec{A}$ is fully defined by its transverse part. The transverse part of electric intensity can be then defined as a negative time derivative of the vector potential $\vec{E}_T = -\partial_t\vec{A}$.

For a quantum description of the electromagnetic field, we have to replace $\vec{A}$ with its quantum mechanical operator $\hat{A}$. To do so we will use an analogy between the electromagnetic field and harmonic oscillator. Let's assume a cubic region of a space with volume V. We can imagine it as a cubic cavity, which just doesn't have any real boundaries, we call such an object quantization cavity. The vector potential of running wave under quantization cavity boundaries can be written as

$$\vec{A}(\vec{r},t) = \sum_{\vec{k}}\sum_{\lambda\in\{1,2\}} \vec{e}_{\vec{k},\lambda}(A_{\vec{k},\lambda}\mathrm{e}^{i(-\omega_k t+\vec{k}\vec{r})} + A^*_{\vec{k},\lambda}\mathrm{e}^{i(\omega_k t-\vec{k}\vec{r})}) \ , \tag{3.0-2}$$

where the oscillation mode k is described by its wave vector $\vec{k}$ and polarization state λ. Then ω_k is the frequency of the mode k and $\vec{e}_{\vec{k},\lambda}$ is the unit vector describing its propagation direction. The total radiative energy of the field is given as a sum of all time-independent contributions from all the modes

$$E_R = \varepsilon_0 V \sum_{\vec{k},\lambda} \omega_k (A_{\vec{k},\lambda} A^*_{\vec{k},\lambda} + A^*_{\vec{k},\lambda} A_{\vec{k},\lambda}) \ . \tag{3.0-3}$$

The Hamiltonian of the radiative field can be written as a sum of harmonic oscillators describing the individual modes $\vec{k}\lambda$ [157]

$$\hat{H}_{\vec{k}\lambda} = \frac{\hbar\omega_k}{2}(\hat{a}_{\vec{k}\lambda}\hat{a}^\dagger_{\vec{k}\lambda} + \hat{a}^\dagger_{\vec{k}\lambda}\hat{a}_{\vec{k}\lambda}) = \hbar\omega_k(\hat{n}_{\vec{k}\lambda} + \frac{1}{2}) \ , \tag{3.0-4}$$

where $\hat{a}^\dagger_{\vec{k}\lambda}$ and $\hat{a}_{\vec{k}\lambda}$ stands for creation and annihilation operator of mode $\vec{k}\lambda$. We defined photon number operator as $\hat{n}_{\vec{k}\lambda} = \hat{a}^\dagger_{\vec{k}\lambda}\hat{a}_{\vec{k}\lambda}$.The operator $\hat{n}_{\vec{k}\lambda}$ states how many photons are in the mode $\vec{e}_{\vec{k},\lambda}$. The mean photon number of a mode denoted as $\langle\hat{n}_{\vec{k}\lambda}\rangle = \overline{n_{\vec{k}\lambda}}$, serves as a crucial metric for assessing the properties of light states. Together with the photon number variance, $(\Delta\hat{n}_{\vec{k}\lambda})^2 = \langle\hat{n}^2_{\vec{k}\lambda}\rangle - \langle\hat{n}_{\vec{k}\lambda}\rangle^2$, we will employ these parameters to distinguish between various light states and classify light sources. We can define amplitude operators of vector potential as

$$\begin{aligned} \hat{A}_{\vec{k},\lambda} &= \sqrt{\frac{\hbar}{2\varepsilon V\omega_k}}\hat{a}_{\vec{k}\lambda} \ , \\ \hat{A}^*_{\vec{k},\lambda} &= \sqrt{\frac{\hbar}{2\varepsilon V\omega_k}}\hat{a}^\dagger_{\vec{k}\lambda} \ . \end{aligned} \tag{3.0-5}$$

Now we have all the building blocks to set up the operator of the electric field as

$$\hat{E} = -\partial_t\hat{A}(\vec{r},t) = \sum_{\vec{k},\lambda}\vec{e}_{\vec{k},\lambda}\sqrt{\frac{\omega_k\hbar}{2\varepsilon V}}(\hat{a}_{\vec{k}\lambda}\mathrm{e}^{-i(\omega_k t-\vec{k}\vec{r})} - \hat{a}^\dagger_{\vec{k}\lambda}\mathrm{e}^{i(\omega_k t-\vec{k}\vec{r})}) \ . \tag{3.0-6}$$

From here on we will assume only one mode field, so just one combination of $\vec{k}$ and λ.

3.0.1.1 Coherent states

Coherent state $|\alpha\rangle$ describes a quantum light emitted by a single-mode laser well above its threshold [158]. It is defined as the eigenstate of the annihilation operator $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$ with eigenvalue α representing a complex amplitude of the coherent state. Therefore the coherent state remains unchanged after a one-photon absorption. It can be expressed in the basis of the photon number operator [157]

$$|\alpha\rangle = \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \ . \tag{3.0-7}$$

Then the probability distribution P for the number of photons in the given coherent state $|\alpha\rangle$ is described by Poisson distribution

$$P(n) = \mid \langle n|\alpha\rangle \mid^2 = \mathrm{e}^{-|\alpha|^2} \frac{\mid \alpha \mid^{2n}}{n!} \ . \tag{3.0-8}$$

Because of the specific distribution, the coherent states are often called Poisson distributed states. The mean photon number of a coherent state is given as

$$\overline{n} = \langle\alpha| \hat{n} |\alpha\rangle = \mid \alpha \mid^2 \ . \tag{3.0-9}$$

The variance of a coherent state is then given as

$$(\Delta n)^2 = \mid \alpha \mid^2 = \overline{n} \ . \tag{3.0-10}$$

Any light state with larger (smaller) variance is called super (sub)- Poissonian light.

3.0.1.2 Fock states

The Fock state or photon number state $|n\rangle$ is defined as the eigenstate of the number operator $\hat{n}|n\rangle = n|n\rangle$ and it is a direct result of electromagnetic field quantization. The eigenvalue n is the number of photons in the given Fock state. The photon number is fully determined and the probability distribution of the photon number is then described by the Kronecker δ-function. Therefore the mean photon number in a Fock state is equal to the number of photons in the state with a variance equal to zero

$$\overline{n} = \langle n| \hat{n} |n\rangle = n \ , \tag{3.0-11}$$

$$(\Delta n)^2 = 0 \ . \tag{3.0-12}$$

The classical electromagnetic theory is unable to describe this sub-Poisson statistic, therefore we call such a state of light non-classical.

3.0.1.3 Thermal state

The thermal state describes black-body radiation and it is defined as an incoherent mixture of different Fock states. To describe this mixed state, we employ the density matrix operator, defined as follows [157]

$$\hat{\rho} = \sum_{n=0}^{\infty} P(n) |n\rangle\langle n| \ , \tag{3.0-13}$$

where $P(n)$ stands for the probability of a certain number state and it follows the Bose-Einstein distribution

$$P(n,\overline{n}) = \frac{\overline{n}^n}{(1+\overline{n})^{(n+1)}} \ . \tag{3.0-14}$$

The variance is given as

$$(\Delta n)^2 = \overline{n}^2 + \overline{n} \ . \tag{3.0-15}$$

The fluctuation in photon number is larger than the mean photon number, therefore we call this state chaotic light. The thermal state is a typical example of light with the super-Poissonian statistics.

3.0.1.4 Correlation functions

To characterize these quantum light states, we need to analyze the correlation properties of photons. This will involve establishing first- and second-order correlation functions using creation and annihilation operators. The first-order correlation function describing light field correlations is defined as

$$g^{(1)}(t,\tau) = \frac{\langle \hat{a}^\dagger(t)\, \hat{a}(t+\tau)\rangle}{\langle \hat{a}^\dagger(t)\, \hat{a}(t)\rangle} \ . \tag{3.0-16}$$

It characterizes the coherence properties of light. If $g^{(1)}$ is not time-dependent it can be used directly to calculate the coherence time of the light

$$\tau_c = \int_{-\infty}^{\infty} d\tau \mid g^{(1)}(\tau) \mid^2 \ . \tag{3.0-17}$$

The spectral distribution will be then given by a Fourier transformation of the time-independent first-order correlation function

$$s(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} d\tau \, \mathrm{e}^{-i\omega\tau} g^{(1)}(\tau) \ . \tag{3.0-18}$$

The second-order correlation function relates to the intensity auto-correlation, allowing us to differentiate between various light states by examining its value at zero time delay, $\tau = 0$. It is defined as follows

$$g^{(2)}(t,\tau) = \frac{\langle \hat{a}^\dagger(t)\, \hat{a}^\dagger(t+\tau)\, \hat{a}(t+\tau)\, \hat{a}(t)\rangle}{\langle \hat{a}^\dagger(t)\, \hat{a}(t)\rangle \langle \hat{a}^\dagger(t+\tau)\, \hat{a}(t+\tau)\rangle} \ . \tag{3.0-19}$$

For a light that follows Poisson statistics, such as the coherent state, the value of $g^{(2)}(0) = g^{(2)}(\tau = 0)$ equals 1. In the case of nonclassical light, as Fock states, photon antibunching is a common feature, leading to $g^{(2)}(0) < 1$. It's also possible for the second-order correlation function to exceed 1 at zero delay. This phenomenon, known as photon bunching, is characteristic of thermal states, where $g^{(2)}(0) = 2$, indicating a higher probability of detecting two or more photons simultaneously.

3.0.2 Properties of quantum-light sources

When characterizing a quantum light source, two key parameters are typically considered. The first is the fidelity of the generated quantum state, and the second is the source's determinism, which reflects the probability that a trigger, such as a laser or electric pulse, will successfully generate the desired state.

Our primary focus here will be on single-photon sources and therefore the properties of generated single photons will be crucial parameters to describe the source itself, see Fig. 3.1. The ideal single-photon source generates identical single-photons on demand, so the emission efficiency is equal to unity. In the case of quantum light sources, this property is often called brightness [86]. Real sources' brightness is always $< 100\,\%$, which means that some photons are missing in the ideal continuous stream. As we will see later small brightness reduces the source performance in its application, such as limiting the complexity of quantum computing algorithms or communication speed of quantum cryptographic protocols.

The ideal single-photon source generates the number state $|1\rangle$. Instead of measuring the fidelity of the generated state referring to its theoretical picture we usually characterize the real source by a set of parameters, which are easy to measure and give a straightforward intuition, of how to given source will perform in various applications. The first of these parameters is single-photon purity, which describes the probability that the generated wave packet includes only one photon. This is measured by the static second-order correlation function on zero delays $g^{(2)}(0)$, which is for the ideal case of the one-photon number state equal to zero.

Another fundamental characterization parameter is coherence, which, similar to classical light, can be described as the phase stability of the generated wave packet over time. This is measured by the first-order correlation function and directly influences the spectral linewidth of the generated photons. Beyond spectral linewidth, photons can also be differentiated based on various other parameters, including the temporal width of the wave packet, polarization, carrier frequency, time jitter, or spatial mode profile. Photons that are identical in all of these parameters are considered indistinguishable. Since various mechanisms can reduce the indistinguishability of photons from quantum light sources, measuring the mutual two-photon interference visibility provides insight into the actual degree of indistinguishability.

When the brightness and single-photon purity are below 1, another critical parameter becomes important for characterizing the source. The relative phase between different photon number components in the generated state, known as PNC, plays a significant role in the practical applications of single-photon sources. This can be evaluated through number state purity, which determines whether the generated state is pure or mixed in photon number bases.

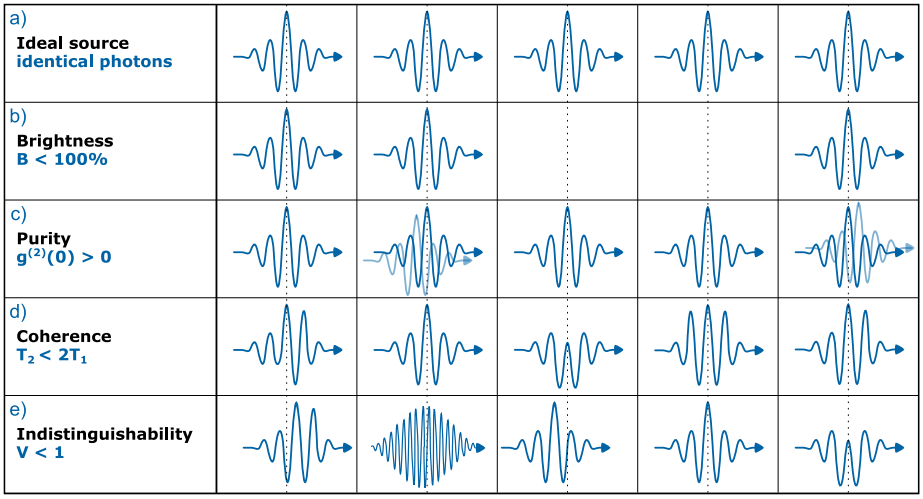


Figure 3.1: **Properties of quantum light source. a)** The ideal single-photon source generates a stream of identical single photons, where a photon is generated for every single excitation (laser pulse, electrical pulse. etc.). **b)** For sources with brightness lower than 100 % not every excitation trigger leads to single-photon emission and some photons are missing in the continuous stream. **c)** If there are multi-photons present in some cases we say that the single-photon purity is lower than 1, which is usually described by a non-zero second-order correlation function for zero delay $g^{(2)}(0) > 0$. **d)** The loss of single-photon coherence is usually schematized as a broken line in the single-photon wave packet. **e)** The generated single photons can still differ in some of their properties, rendering them partially distinguishable, so their mutual two-photon interference visibility is lower than 1. The indistinguishability can be reduced by many factors, such as different wavelength/frequency, phase variations or time jitter. This figure is a variation of the figure published in [86].

3.0.2.1 Brightness

The brightness, a fundamental parameter of single-photon sources, has led to some confusion within the scientific community. Currently, there is no widely accepted method for measuring brightness or a clear consensus on its precise definition. Typically, brightness is characterized as the sum of all photon-number probabilities, excluding the vacuum state, expressed as follows

$$B = \sum_{k=1}^{\infty} p_k \ . \tag{3.0-20}$$

This definition can be viewed from an experimental perspective as the probability that a single-photon detector with unit efficiency, connected to the source, will register a detection event when the source is excited. Due to the normalization of probabilities this definition restricts brightness values to be less than

or equal to one. However, this definition does not convey information about the single-photon emission probability. Mostly in theoretical works, we can also see brightness defined as an integration of all photon contributions in a given time interval normalized by the number of excitation events in that interval [91]. Based on this definition brightness is not normalized to 1. This definition doesn't include the probability that the excitation event will turn into an emission and therefore is not really useful for general source characterization. From now going we will stick to the definition given by Eq. 3.0-20.

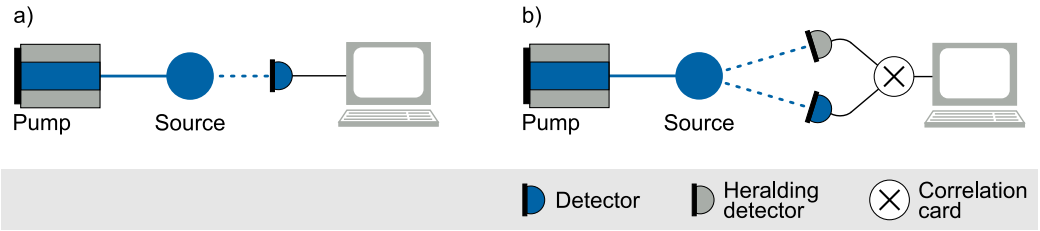


Figure 3.2: **Schemes for brightness measurement.** Brightness is experimentally defined as the probability that a single-photon detector with unit efficiency, connected to the source, will register a detection event when the source is excited. **a)** The direct brightness measurement. The number of detected clicks is normalized to the number of excitation events. **b)** The heralded brightness measurement scheme is typical for single-photon sources emitting two correlated photons, such as down-conversion sources or three-level solid-state sources. Here we count only the events, where both the detectors click and normalize it by clicks of the heralding detector.

We also distinguish between direct brightness and heralded brightness, see Fig. 3.2. In the case of the first one, we have a threshold detector with unit efficiency directly connected to the source and count all the emitted events. The heralded scenario is then typical for single-photon sources emitting two correlated photons, such as down-conversion sources or three-level solid-state sources. Here we count only the events, where both the detectors click and normalize it by clicks of the heralding detector. The heralded brightness then tells us the probability, that there is a photon in the main channel if a heralding photon is emitted.

The last thing that brings an ambiguity to brightness definitions is where the brightness is measured. The first idea is to count all the emission events without looking at their spatial mode and polarization. This brightness we usually call the quantum efficiency of the source, counts all wave packets emitted to a space without any information if we can collect them. The more realistic is the first lens brightness, which counts all the emission events at the first lens of the setup, usually the collection lens. It includes only the events emitted in the spatial modes, which a lens of a given numerical aperture can collect. The most realistic one is then the fiber brightness. It includes all the losses during filtering out residual pump beam and collecting the emission events to a single-mode fiber. Therefore the fiber brightness gives us direct information about counts which we can use for our

experiment or application. The last brightness specification can done by assuming only one polarization of the emitted photons, then we speak about polarized fiber brightness.

3.0.2.2 Single-photon purity

Single-photon purity refers to the probability that a generated wave packet will exclusively contain a single photon. In a general context, purity can be defined as the probability of a single photon normalized to the brightness of the source

$$P = \frac{p_1}{B} \ . \tag{3.0-21}$$

Single-photon purity is commonly determined through the second-order correlation function, as defined by Eq. 3.0-19. The function value in zero delay $g^{(2)}(0)$ describes multi-photon contribution in generated wave packets. This can be measured using the standard Hanbury-Brown and Twiss experiment (HBT) [159], as illustrated in Fig. 3.3. The measurement can be performed directly or in its heralded version. In the case of down-conversion sources the heralded measurement of $g^{(2)}(0)$ becomes crucial. Direct measurements in such cases reveal the thermal nature of the source, originating from a spontaneous process following a Bose-Einstein distribution. On the other hand, the heralded photons follow the Poisson distribution, where the multiphoton component scales with the pump power.

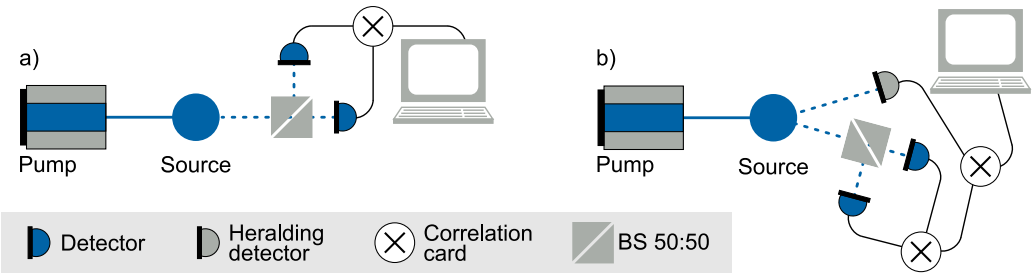


Figure 3.3: **Schemes for $g^{(2)}(\tau)$ measurement.** Experimentally the single-photon purity is determined from the value of the second-order correlation function in zero delay $g^{(2)}(0)$, which is measured by Hanbury-Brown and Twiss (HBT) experiment. **a)** The direct HBT measurement. **b)** The heralded HBT measurement scheme is typical for single-photon sources emitting two correlated photons.

Let's describe the direct HBT experiment more in detail. The wave packets generated by a source under pulsed excitation are directed to a 50 : 50 beam splitter (BS), followed by two single-photon threshold detectors with unit efficiency. The outputs of these detectors are then sent to correlation electronics, which assess the time delay between coincident detection events, where both detectors register a click. Correlations are analyzed across multiples of the source repetition periods, reflecting coincidences for photons emitted in different pulses. The magnitude of the peak at zero delay, where coincidences occur only if more than one photon is

present in the given wave packet, provides valuable insight into the single-photon purity. However, the second-order correlation function doesn't include all the information to derive single-photon purity as was defined by Eq. 3.0-21.

Usually, the source is characterized just by the $g^{(2)}(0)$ value. But in some cases, such as security analyses of a quantum cryptographic protocol, we need an estimation of the multi-photon contribution based on experimental characterisation of the given source. Here we will describe one of the possible bounds for multi-photon contribution, which was published in our work [99]. We bound $p_{k\geqslant 2}$ starting from the second-order auto-correlation function, along with the reasonable assumptions for single-photon sources that $p_{k\geqslant 4} = 0$ and $p_1 > p_{k\geqslant 2}$,

$$g^{(2)}(0) = \frac{2p_2 + 6p_3}{(p_1 + 2p_2 + 3p_3)^2} = \frac{2p_{k\geqslant 2} + 4p_3}{(p_1 + 2p_{k\geqslant 2})^2} \times \left[1 + \frac{p_3}{p_1 + 2p_{k\geqslant 2}}\right]^{-2} \simeq \frac{2p_{k\geqslant 2}}{(p_1 + 2p_{k\geqslant 2})^2} \ , \tag{3.0-22}$$

and then truncate it at the zeroth order in Taylor expansion in p_3. Computing the error $F(p_1, p_2, p_3)$ introduced by our approximations on the $g^{(2)}(0)$, we note that $F(p_1, p_2, p_3) > 0$ for all $p_k \in (0, 1)$ with $k = 1, 2, 3$ proving that the right-hand side of Eq. 3.0-22 provides an actual lower bound and $F(p_1, p_2, 0) = 0$ showing that it holds tight in the limit of vanishing p_3. After rewriting 3.0-22 as a lower bound and expressing it in terms of brightness B,

$$g^{(2)}(0) \geq \frac{2p_{\mathrm{m}}}{(B + p_{\mathrm{m}})^2} \ , \tag{3.0-23}$$

we expand the Taylor expansion to 2nd order in p_m and rearrange again

$$p_{\mathrm{m}}^2 + \left(2B - \frac{2}{g^{(2)}(0)}\right) p_{\mathrm{m}} + B^2 \geq 0. \tag{3.0-24}$$

Since $p_{\mathrm{m}} \geq 0$ and $1 \geq B \geq 0$, the inequality has only one solution for a single-photon source (i.e. $\frac{1}{2} \geq g^{(2)}(0) \geq 0$ [160])

$$p_{\mathrm{m}} \leq \frac{1 - Bg^{(2)}(0) - \sqrt{1 - 2Bg^{(2)}(0)}}{g^{(2)}(0)} \ . \tag{3.0-25}$$

This holds for any source with sub-Poissonian emission and provides an explicit bound which only depends on experimentally accessible parameters [99].

3.0.2.3 Photon indistinguishability

The photon indistinguishability describing the mean overlap of two light wave packets can be measured by Hong–Ou–Mandel (HOM) experiment [161], see Fig. 3.5. In the ideal case, two indistinguishable single-photon wave packets are sent to the

two inputs of a 50 : 50 BS with perfect spatial and temporal overlap and we observe quantum interference. The probability amplitudes *"both photons reflected"* and *"both photons transmitted"* vanished due to destructive interference given by the relationships between the reflection and transmission coefficients of the BS. So in the ideal case, both photons can be found in the same BS output and we observe only events *"the first photon reflected/the second photon transmitted"* and *"the first photon transmitted/the second photon reflected"*, where each of them has a probability equal to $\frac{1}{2}$. This bunching can be characterized by the visibility of the quantum interference V_{HOM} and corresponds to photon indistinguishably M.

To calculate the interference visibility we first measure the second-order coincidence count $C_{\parallel}$ by two threshold single-photon detectors with unit efficiency placed in two BS outputs. For normalization, the input wave packets can be made maximally distinguishable by varying an accessible degree of freedom, commonly the arriving time at the BS or polarization of the photons. This cancels the quantum interference effect and we will observe also the events, where each photon is stated into a different BS output. This yields a coincidence count $C_{\perp}$ and then we can calculate

$$V_{HOM} = M = \frac{C_{\perp} - C_{\parallel}}{C_{\perp}} \ , \tag{3.0-26}$$

where the coincidence counts are integrated over the entire wave packet temporal duration, as any temporal post-selection artificially increases photon indistinguishably M. The indistinguishability of real single-photon sources is reduced by its imperfect single-photon purity ($g^{(2)}(0) > 0$), where the additional multi-photon terms give additional coincidences in both $C_{\parallel}$ and $C_{\perp}$. For real sources with high single-photon purity, where we can use an assumption $g^{(2)}(0) \ll 1$, it is common to define the corrected indistinguishability $M^* = M + g^{(2)}(0)$, which describes the wave packet overlap for all degrees of freedom other than photon number.

The indistinguishability of a pulsed pumped single-photon source is typically measured through HOM interference between two consecutively emitted photons. This measurement uses an unbalanced Mach-Zehnder interferometer, where one of the arms introduces a delay equivalent to the time separation of two consecutively emitted photons, denoted as $\Delta\tau$. Subsequently, we observe HOM interference between these two photons on the interferometer's second BS. However for some sources, typical for solid-state single-photon sources, the degree of indistinguishability generally depends on the chosen time delay between the interfering photons [87]. In this case, a measurement of indistinguishability between photons emitted further apart can be crucial.

In cases where sources emit two correlated photons, their mutual indistinguishability is often assessed. In such instances, we allow the two photons emitted by the same pump pulse to interfere on one BS and measure the interference visibility. The spatial overlap of the two wave packets on the BS limits the final V_{HOM}, and for precise characterization, a fiber BS is often employed to erase limitations

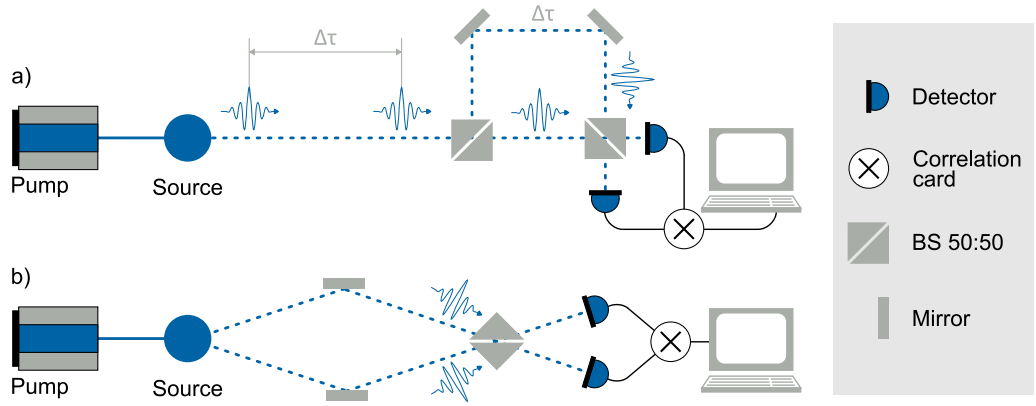


Figure 3.4: **Schemes for photons' indistinguishability measurement.** Photons' indistinguishability is experimentally measured as visibility of Hong–Ou–Mandel (HOM) 2-photon interference. **a)** The interference between two consecutively emitted photons is measured with an unbalanced Mach-Zehnder interferometer, which delays one of the photons by time separation between the excitation pulses. The two photons then temporarily and spatially overlap at the second beam splitter (BS) and we observe HOM interference. **b)** The measurement of HOM interference visibility between two photons emitted by one excitation event, typical for sources of correlated photons' pairs.

associated with alignment precision.

3.0.2.4 Coherence

Like classical light, the coherence of single photons can be described as a measure of the temporal phase stability of the light. The coherence is described by the first-order correlation function $g^{(1)}(\tau)$, defined by Eq. 3.0-16, which can be measured directly by the Fourier-transform spectroscopy. The measurement scheme is based on an unbalanced interferometer, we chose the Mach-Zehnder system, one of the interferometer arms is fixed and the length of the second one can be carried by a tunable delay line, see Fig. 3.5. The length of the implemented delay is dependent on the temporal profile of characterized wave packets. But for common single-photon sources delay lines with a range up to several nanoseconds with a resolution of sub-femtosecond are used. The delay is varied and the signal in one of the outputs is detected. Due to the delay variation the relative phase between the interferometer arms is changing and oscillating between constructive and destructive interference conditions. This we can observe by oscillations of the signal intensity with visibility

$$V = \frac{I_{MAX} - I_{MIN}}{I_{MAX} + I_{MIN}} , \tag{3.0-27}$$

where I_{MAX} and I_{MIN} stands for maximal and minimal detected intensity, respectively. The function of V over the relative time delays τ between the interferometer arms is equal to the real part of the first-order correlation function $g^{(1)}(\tau)$.

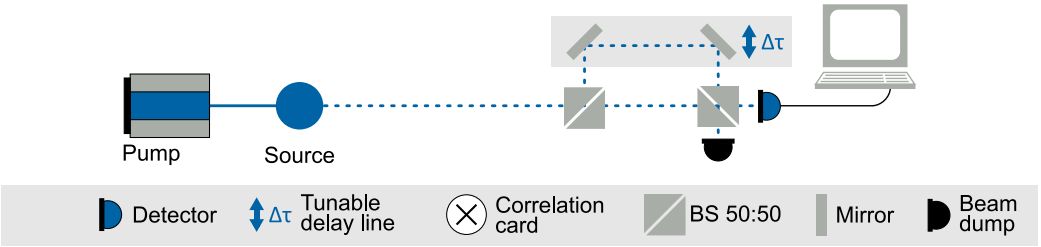


Figure 3.5: **Scheme for photon coherence measurement.** The photon coherence characterized by the first-order correlation function $g^{(1)}(\tau)$ is directly measured by the method of the Fourier-transform spectroscopy. The measurement scheme is based on an unbalanced Mach-Zehnder interferometer, where one of the interferometer arms is fixed and the length of the second one includes a tunable delay line. The signal in one of the outputs is measured during the delay is varied. The function of interference visibility over the relative time delays τ between the interferometer arms is equal to the real part of the first-order correlation function.

Alternatively, the coherence property can be computed through measurements in the spectral domain. The $g^{(1)}(\tau)$, as a consequence of the Wiener-Khintchine theorem, is expressed as the inverse Fourier transformation of the spectral linewidth of the given wave packets, see Chapter 3.0.1.4.

3.0.2.5 Photon-number coherence

A PNC is a consequence of photonic state purity in the Fock basis. As discussed in Chapter 2.2.3.3, the significance of this parameter in the realm of quantum technologies is widely recognized. However, it is not typically encompassed in "*the ideal single-photon source definition*" [86]. Our paper, in particular, introduced PNC primarily to the solid-state single-photon sources community as a fundamental parameter essential for validating the potential applications of a source [52].

To characterize a state in photon-number bases, a state tomography can be used to reconstruct the complete density matrix. This measurement relies on homodyne or heterodyne detection techniques, which makes it experimentally challenging [162–164]. Therefore, for simplicity, we will assume that the state consists only of a vacuum and a one-photon contribution. In such a scenario, the 2×2 density matrix in the Fock bases can be reconstructed only from probability amplitudes and the coherence of the relative phase between the one-photon and vacuum components. The measurement of PNC between only the two lowest number states is commonly employed for characterizing phase-scrambled coherent states in quantum cryptography [51]. Therefore, for intuition purposes, we will assume that this measurement serves as a sufficient witness for the overall state purity.

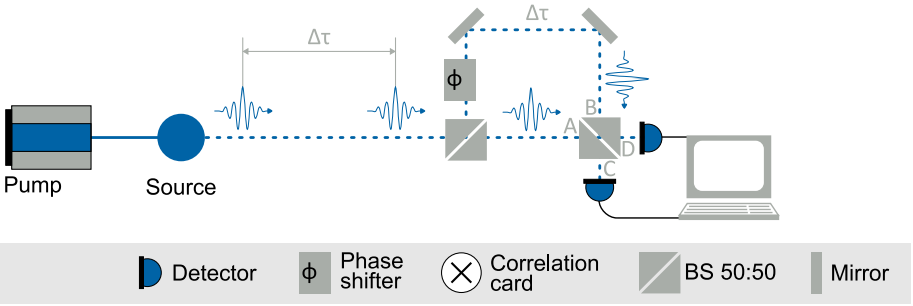


Figure 3.6: **Scheme for photon number coherence measurement.** The photon number coherence (PNC) is characterised by interference between two consecutively emitted wave packets. In comparison with the HOM effect, we are not focused on the two-photon interference but on interference between one photon and vacuum. The measurement setup is based on an unbalanced Mach-Zehnder interferometer, which delays one of the photons by time separation between the excitation pulses. By a phase shifter, we can tune the relative phase between the arms from 0π to 2π. The scouts at the second BS output are measured individuals in dependence on relative phase, the PNC can be calculated from the interference visibility.

Here we will describe an interference technique for PNC estimation [51,97]. In the same fashion, as in the case of the indistinguishability measurement, the core of the setup is an unbalanced Mach-Zehnder interferometer, where the longer arm adds a delay $\Delta\tau$ equal to the temporal separation of two consecutively generated wave packets, see Fig. 3.6. For PNC measurement, we add a phase shifter, which can scan the relative phase from 0π to 2π between the interferometer arms and we will not look at correlations between the second BS outputs, but we will measure the counts independently. For the following description name the second BS inputs A, B and the outputs C, D.

Let's assume that wave packets at the BS input are indistinguishable and we can describe them as pure states in the photon-number basis

$$\begin{aligned} |\psi_A\rangle &= \sqrt{p_0}\,|0_A\rangle + \sqrt{p_1}\mathrm{e}^{i\theta}\,|1_A\rangle \\ |\psi_B\rangle &= \sqrt{p_0}\,|0_B\rangle + \sqrt{p_1}\mathrm{e}^{i(\theta+\phi)}\,|1_B\rangle \end{aligned} \tag{3.0-28}$$

where ϕ is the relative phase implemented by the phase modulator and $p_0+p_1 = 1$. In an extreme case, where $p_1 = 1$ the interference of these states turns into the already discussed HOM effect and we will observe a bunching of photons on the BS outputs $\frac{1}{2}(|2_C 0_D\rangle - |0_C 2_D\rangle)$. If $p_1 < 1$ the mean photon number at the BS outputs will oscillate with amplitude equal to p_0 [97]

$$N_{C,D} = p_1(1 \pm p_0 \cos\phi)\ . \tag{3.0-29}$$

This outcome shouldn't be surprising, considering that the state tomography in Fock bases can be achieved through homodyne detection. The setup outlined here

simply substitutes the local oscillator with the previous emission from the same source. While this modification enhances experimental feasibility, it does come with a limitation, we are restricted to sensitivity to the relative phase between only the two lowest number states. Let's consider a more general case, where a state at the BS input is described as a combination of pure and mixed state, we can write its density matrix as follows [97]

$$\begin{aligned} \hat{\rho} &= \lambda\hat{\rho}_{pure} + (\lambda - 1)\hat{\rho}_{mixed} \ , \\ \hat{\rho}_{pure} &= |\psi_i\rangle\langle\psi_i| \ , \text{where}\, i = A, B \ , \\ \hat{\rho}_{mixed} &= diag\{p_0, p_1\} \ . \end{aligned} \tag{3.0-30}$$

The parameter λ is equal to state purity in the photon-number basis and it is normalized to 1. It can be shown that normalized counts at the BS outputs will oscillate as

$$n_{C,D} = \frac{N_{C,D}}{N_C + N_D} = \frac{1}{2}(1 \pm \lambda^2 p_0\sqrt{M}\cos\phi) \ , \tag{3.0-31}$$

where M is the mean wave packets overlap, which includes photon indistinguishability and other spatial overlap at the BS and can be measured as V_{HOM} at the same setup. Therefore if we know the vacuum probability amplitude and V_{HOM} we can measure PNC between the two lowest number states by simply varying the relative phase between the interferometer arms and fitting the interference visibility from the measured data.

As was already mentioned, this technique is really strong in terms of its experimental simplicity and the fact that it is based on the standard HOM setup. However, it gives a state purity in terms of the one photon Fock state, as was described by Eq. 3.0-28. The states generated by real sources are in general more complex and include multi-photon contributions. In such cases, this technique just gives an intuition about the full density matrix under strong assumption [52]. On the other hand, if we need to characterize higher Fock states generated from our source we have to always employ the full number-state tomography routine [162–164].

3.1 Poisson-distributed sources

All the sources that generate states following a Poisson distribution in their photon-number probabilities will henceforth be referred to as PDS. In general, this broad definition encompasses two main technologies: weak coherent state sources and spontaneous parametric down-conversion sources. While PDSs, in an approximation of low probabilities, can be utilized as single-photon sources, they do not theoretically fulfil the ideal single-photon source definition. Due to the Poisson distribution, their brightness and single-photon purity are not independent parameters, and we always need to seek a sufficient trade-off for the given application.

Despite their limitations in photon-number statistics, primarily owing to their experimental feasibility, robustness, tuneability, good interference properties, and the ability to generate high-fidelity entangled states, PDSs are the leading sources in quantum technology. Key experiments in quantum cryptography [36–39], quantum computing [40–43], and quantum sensing [44–47] have been implemented using PDS sources. This has been made possible mainly through clever techniques such as multiplexing, heralding, or decoy states, which overcome their statistical limitations. Therefore, when evaluating a single-photon source based on its potential for application in quantum technology, we must not only compare it with the general definition of the ideal single-photon source [86] but also compare it with the performance of a PDS source in the given application. This chapter describes PDSs, even though they are not the focus of this work. We will need to compare the performance of QD single-photon sources in quantum cryptographic protocols with them.

3.1.1 Weak coherent state sources

WCS sources rely on strongly attenuated coherent states produced by a laser source. As a result, these sources offer a practical and accessible method for generating probabilistic single-photon pulses. Due to their evident experimental simplicity, they find widespread use in quantum cryptographic applications, particularly in implementations of the QKD protocols [14].

The probabilities of multi-photon contributions in the WCS follow a Poisson distribution and can be computed using Eq.3.0-8. Because all the photon-number probabilities are strongly correlated, it is impossible to generate only a single-photon pulse in a given time interval with certainty. Primarily, the multi-photon probabilities need to be carefully adjusted by varying the level of attenuation for a given source application. However, we are consistently constrained by the trade-off between source brightness and single-photon purity. Let's leverage the findings from our earlier QKD practical security analyses, as detailed in Chapter 2.2.3.3, to illustrate the application of WCS sources.

In the context of the QKD BB84 protocol, the presence of multi-photon contributions introduces security loopholes, such as the PNS attack, significantly compromising protocol security. Consequently, strong attenuation is necessary to minimize multi-photon components. Therefore WCSs with a mean photon number per pulse μ, as defined in Eq. 2.2-25, lower than one are typically employed to ensure acceptable QKD protocol security [14]. This weak regime constrains the ratio between multi-photon and single-photon probabilities to $\frac{\mu}{2}$ with a cost of a high vacuum component $1 - \mu$, limiting the maximum communication rate of cryptographic protocols. Moreover, given its coherent state nature, the generated state is pure in a photon number basis. For the majority of applications in quantum cryptography, its phase has to be actively scrambled, as discussed in Chapter 2.2.3.3.

However for some applications, particularly for QKD, we can use clever counter-

measures against multi-photon-based security loopholes. One of the most widely recognized techniques is decoy states, which allow us to use higher μ, reaching higher communication rates without making compromises on the protocol security, see Ch. 2.2.3.5.

The big limitation of WCS sources apart from the trade-off between brightness and single-photon purity is also limited HOM interference visibility to 50 % because of multiphoton emission [165, 166]. This makes WCS sources unfeasible for two-photon interference-based applications.

3.1.2 Spontaneous parametric down-conversion sources

These sources are based on the optical 2^{nd} order nonlinear process of SPDC, where a single pump photon spontaneously decays into photon pair, signal and idler, with lower frequency

$$|1\rangle_{\omega_p} \rightarrow |1\rangle_{\omega_s} + |1\rangle_{\omega_i} \ . \tag{3.1-1}$$

The process must follow the laws of energy and momentum conservation and therefore the following constraints, known as phase-matching conditions, must be satisfied

$$\begin{aligned} \omega_p &= \omega_s + \omega_i \\ \vec{k_p} &= \vec{k_s} + \vec{k_i} \ . \end{aligned} \tag{3.1-2}$$

The spontaneous decay of the pump photon via a virtual energy level into two photons satisfying the phase-matching conditions is classically forbidden. In classical description, two fields, pump and signal, are needed at the input, and then phase-matching conditions fully define the generated idler. Therefore the classical approach can't be used for SPDC description and we usually define the process as an amplification of quantum vacuum energy fluctuations by a strong pump field, where only the vacuum modes fulfilling phase-matching conditions are amplified [167]. In the second quantization, we can write interaction Hamiltonian describing the SPDC as

$$\hat{H}_{int} = \hbar g(\hat{a}_p \hat{a}_s^\dagger \hat{a}_i^\dagger + h.c.) \ . \tag{3.1-3}$$

where g is the coupling constant, which is dependent on used nonlinear media. From the Hamiltonian, we can easily see that it describes the annihilation of one pump photon and the creation of two photons, signal and idler. In a parametric approximation, we can replace the general pump field with a coherent state $|\alpha\rangle$. And because the coherent state is an eigenstate of the annihilation operator with eigenvalue α we can simplify the interaction Hamiltonian

$$\hat{H}_{par} = \hbar g(\alpha \hat{a}_s^\dagger \hat{a}_i^\dagger + h.c.) \ . \tag{3.1-4}$$

For fixed interaction time we can now write a general solution of the Schrodinger equation in the following form

$$|\psi_{SPDC}\rangle = \mathrm{e}^{-it\hat{H}_{par}} |\alpha\rangle |0\rangle_s |0\rangle_i = \\ = |\alpha\rangle |0\rangle_s |0\rangle_i - it\hbar g\alpha |\alpha\rangle |1\rangle_s |1\rangle_i - it\hbar^2 g^2 \alpha^2 |\alpha\rangle |2\rangle_s |2\rangle_i + ... \quad (3.1\text{-}5)$$

From the solution, it is evident that SPDC sources generate a superposition of photon pairs. The two-photon term is linearly dependent on the pump power α, while other photon-number probabilities adhere to a Poisson distribution. In reality, the creation and annihilation operators are dependent on frequency, wave vector and polarization and therefore the full quantum description of the SPDC process is not trivial.

SPDC sources find widespread use in quantum technology, and as a result, various implementations exist, categorized by the phase-matching condition (*type-I, type-II, type-0*), the spectral properties of the signal and idler (*degenerated, non-degenerated*), the source geometry (*colinear, non-colinear*), or whether the generated photon pair is entangled in some degree of freedom.

Given the significance of these sources in the development of quantum technology, let's describe one of the commonly used SPDC sources based on $\beta-$Barium Borate (BBO) birefringent crystal in detail [168]. The II-order phase-matching conditions result in the emission of single photons along two cones—one containing V-polarized photons and the other containing H-polarized ones. By adjusting the tilt of the optical axis of the crystal, these cones can overlap. In these overlapping regions, Bell states $|\Phi^{\pm}\rangle$ can be directly generated from the crystal by carefully balancing the coupling efficiencies and compensating for the walk-off between the two polarizations. Similar to WCS sources, SPDC sources produce states with photon number probabilities that follow the Poisson distribution and are pure in photon number bases. However, the strength of SPDC sources lies in the generation of correlated photons, allowing for the use of heralding techniques and even the generation of entangled photon pairs.

3.2 Quantum dots single-photon sources

Another method of single-photon state generation relies on the excitation of discrete energetic levels. In contrast to WCS or SPDC sources, the brightness of these sources can inherently be independent of single-photon purity. Various solid-state single-photon sources, including nitrogen-vacancy centers [154], trapped atoms [155], biomolecules [156], and semiconductor quantum dots [55], are being explored. Nonetheless, our attention will be specifically directed towards QD, which are nano-sized inclusions of one semiconductor type within a second one with a larger bandgap energy.

One common fabrication process for QDs is based on Stranski–Krastanov growth (SKG), where one semiconductor material is deposited onto another (ma-

trix) with a different lattice constant [86, 169, 170]. Induced mechanical stress between the two materials, which is relaxed by the formation of a 2D strained layer (wetting layer) and 3D islands, representing QDs. The structure is covered by a capping layer usually made of the same material as the matrix. The shape of QDs produced by SKG is similar to a plano-convex lens, with a large radius and small thickness [86]. To obtain higher symmetry, which is crucial for entanglement generation [171, 172], other QD growth techniques, such as droplet epitaxy can be used [173–175]. The QDs fabrication is usually made by methods of molecular-beam epitaxy (MBE) or metalorganic vapour-phase epitaxy (MOVPE).

QDs made by SKG or droplet epitaxy are self-formed and therefore they exhibit random spatial positions and spectral distribution. The light emission from an ensemble of many QDs fabricated within one grow is characterized by inhomogeneous broadening due to variations in their size and the local environment. However, these QDs, which are situated away from processed interfaces, so they are well isolated from the local environment defects, demonstrate close to unity quantum efficiency and low dephasing [55].

QDs hold great promise for quantum technologies, primarily due to their theoretically achievable high brightness, approaching unity, and ultra-low multiphoton contribution in the emitted photonic state. However, their main limitations stem from the requirement for operation at low temperatures, typically around 4 K, and the random distribution due to the probabilistic growth method, leads to variations in spectral and temporal characteristics of emitted photons. This variability poses challenges in scaling QDs for applications relying on interference among multiple sources. The emitted quantum state from a QD is given also by the excitation scheme employed to achieve population inversion on the QD's energy levels. The next chapter will focus on the details of the main QD's excitation schemes.

3.2.1 Energy levels

The energy potential of a QD can be expressed as a product of the component along the growth direction, denoted as the z-direction, and the in-plane component. Given the small extension in z-direction, this can be described as a quantum well where only one bound state can be considered due to the large energy splitting. The in-plane component (x, y) can be represented using the model of a quantum harmonic oscillator with energy given as

$$E_{n_x,n_y} = \hbar\omega_x \left(n_x + \frac{1}{2}\right) + \hbar\omega_y \left(n_y + \frac{1}{2}\right) \ , \tag{3.2-1}$$

where n_x and n_y are quantum numbers in x and y direction. Assuming a QD potential symmetrical in x and y the in-energy levels can be described as

$$E_s = \hbar\omega \left(s + 1\right) \ , \tag{3.2-2}$$

where $\omega = \omega_x = \omega_y$ and we introduced a new quantum number $s = n_x + n_y$ numbering the QD's shells, which are in the analogy to atom physics named in the

order s, p, d, ... The degeneracy of each shell is expressed as $2(s+1)$, accounting for possible spin orientations. The projection of angular momentum is further characterized by an additional quantum number, denoted as $l = n_x - n_y$, which has values between $-s$ and $+s$. The matrix material is characterized by the band gap and band structure of the bulk semiconductor. The wetting layer is modelled as a quantum well, forming a step-like offset from the band gap of the matrix material, see Fig. 3.7.

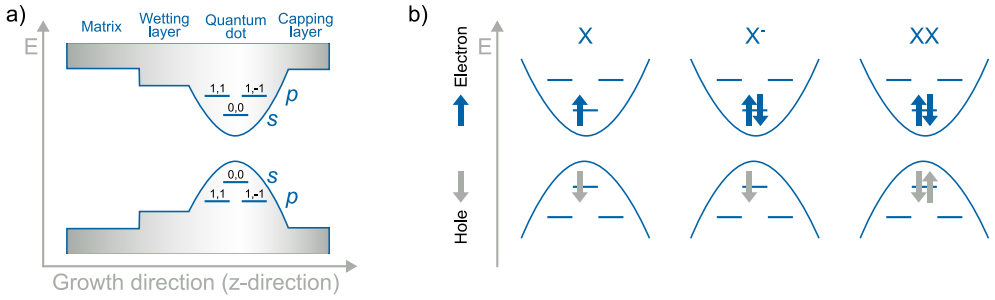


Figure 3.7: **Schematic depiction of QD's energy levels. a)** Schematic depiction of the QD's confinement potential as a function of the energy E surrounded with matrix and wetting layer with conduction band (upper part) and valence band (lower part). QD is represented in the harmonic potential approximation which discrete energy into levels for a single charge carrier indicated by the quantum numbers s and l. **b)** Schemes of the charge carrier configuration of different multi-particle states (exciton X, negatively charged exciton X^- and biexciton XX).

For the following, we will assume only three multiparticle states, which all are located at s-shell, as illustrated schematically in Fig. 3.7. It is exciton state (X) consisting of one electron and one hole, charged exciton state, also called trion, which can be positively charged X^+ (one electron, two holes) or negatively charged X^- (two electrons, one hole). And finally biexciton state (XX) where s-shell is fully occupied by two electrons and two holes. All of these states, apart from X, exhibit no dark state, therefore radiative recombination of an electron-hole pair in the s-shell with opposite spins is always possible. It is important to note, that states occupying higher shells, such as a double-charged exciton, also exist, however, they are out of the scope of this work.

3.2.2 Excitation schemes

QDs can be excited under different optical pumping schemes, resulting in distinct outcomes such as brightness, single-photon purity, indistinguishability, or purity of the generated photonic state in Fock bases [85, 86]. The different schemes also have different experimental complexity and robustness against environmental fluctuations [86]. Therefore a detailed understanding of QD's excitation scheme is crucial for the effective utilization of QDs in quantum technology applications [52]. This work provides a detailed description of six primary excitation schemes, as illustrated in Fig. 3.8.

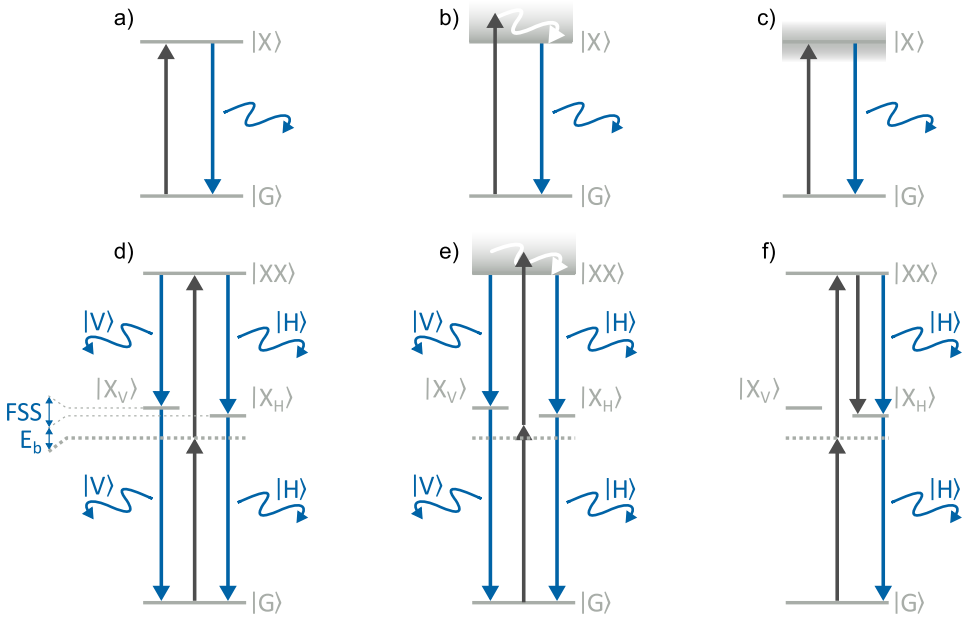


Figure 3.8: **QD's excitation schemes. a)** Resonant excitation (RE), **b)** Longitudinal acoustic phonon-assisted excitation (LA), **c)** Adiabatic rapid passage (ARP), **d)** Resonant two-photon excitation (TPE), **e)** Phonon-assisted two-photon excitation (LA-TPE) and **f)** Stimulated two-photon excitation (sTPE).

The commonly used excitation scheme for QDs is RE, where the excitation laser is in resonance with the X energy level [55]. This primarily results in decoupling from all dephasing processes and the generation of highly indistinguishable single photons [88]. However, single-photon purity is still limited by re-excitation probability and, in general, due to state dynamics following Rabi oscillation, RE is sensitive to excitation power fluctuations [95]. Moreover, the requirement to suppress the excitation field commonly done based on cross-polarization extinction limits the brightness, which can otherwise theoretically reach unity, typically to 50 % in the absence of specially tailored QD-microcavity systems [86].

The RE sensitivity to excitation field fluctuations was overcome by pumping the

Excitation scheme	B	P	I	PNC	Advantages	Technological challenges
RE	~ 1 (~ 0.5) (limited by pol. supp.)	$\sim \gamma T$	~ 1 transform limited linewidth	Yes $(\|0\rangle+\|1\rangle+\ldots)$	no coupling to dephasing channels	polarization suppression (50% loses), sensitive to excitation field fluctuations
LA	$< 90\%$ given by $J(\omega)$	$< \gamma T$	~ 0.9 limited by phonon dephasing	No	robust against environmental fluctuations, simple spectral suppression of excitation field	
ARP	~ 1 (~ 0.5) (limited by pol. supp.)	$\sim \gamma T$	< 1 limited by dephasing	N/A	robust against environmental fluctuations	need of spectrally broad polarization suppression, chirp pulsed preparation
TPE	~ 1	$\sim (\gamma T)^2$	$< 66\%$ $V_{HOM} = 1/(1+\tau_{xx}/\tau_x)$	Yes $(\|0\rangle+\|2\rangle+\ldots)$	entanglement generation, high single-photon purity, simple spectral suppression of excitation field	sensitive to excitation field fluctuations
LA-TPE	$< 90\%$ given by $J(\omega)$	$< (\gamma T)^2$	$< 66\%$ $V_{HOM} = 1/(1+\tau_{xx}/\tau_x)$	No	entanglement generation, robust against environmental fluctuations, spectral suppression of excitation field	high excitation power, excitation field spectral close to XX
sTPE	~ 1 polarized brightness	$< (\gamma T)^2$	~ 1 transform limited linewidth	Yes $(\|0\rangle+\|1\rangle+\ldots)$	polarized emission, high single-photon purity, high indistinguishability	two synchronized lasers are needed (excitation and stimulation pulse)

Table 3.1: **Summary of QD's excitation schemes properties.** The table was made from the following references: Resonant excitation (RE) [88,95,97,98,176,177], Longitudinal acoustic phonon-assisted excitation (LA) [52,90,91,98,178], Adiabatic rapid passage (ARP) [179], Resonant two-photon excitation (TPE) [98,164,172,180–183], Phonon-assisted two-photon excitation (LA-TPE) [91,184,185] and Stimulated two-photon excitation (sTPE) [93]. The duration of the excitation pulse is denoted as T, and γ represents the decay rate of the X state.

two-level system (2LS) with a spectral chirped pulse, a scheme known as adiabatic rapid passage (ARP), which achieves similar performance to RE. While the system dynamics do not follow Rabi oscillation, the brightness and purity remain almost constant within a broad interval of excitation powers [179]. The experimental complexity of ARP is demanding, and this scheme is hardly used in reality.

A promising scheme for real-world applications is LA, which relies on off-resonant pumping and uses phonon decay to achieve population inversion [186]. The excitation is robust against environmental fluctuations, and the excitation laser can be easily spectrally suppressed due to different wavelengths [90, 178]. It has been demonstrated that LA can theoretically reach higher single-photon purity than RE [91]. However, quantum efficiency and photon indistinguishability are limited by phonon interaction [90].

More complex excitation schemes involve the pumping of a three-level system (3LS) (in practical QDs, the system is a four-level one due to the energy split of the X state by the fine structure splitting (FSS) [86]). This system can be resonantly pumped by resonant two-photon excitation (TPE). The population inversion decays with equal probability through one of the two cascades, result-

ing in the emission of two photons in either H or V polarization. Consequently, the two generated photons are entangled [85]. Moreover, TPE achieves ultra-high single-photon purity and enables easy spectral separation of the pump and the two emitted photons [180]. While TPE follows Rabi oscillation, making it sensitive to excitation field fluctuations, the time entanglement of the two generated photons significantly restricts their indistinguishability to $\sim 66\,\%$ [181]. Off-resonant pumping of the 3LS with additional phonon decay known as phonon-assisted two-photon excitation (LA-TPE) improves the excitation scheme robustness while the other specification remains very similar to resonant TPE [184, 185].

The main limitation for single-photon generation of TPE and LA-TPE can be improved by stimulating one of the two cascades with an additional laser pulse with fixed polarization, this scheme is called stimulated two-photon excitation (sTPE). Apart from reaching theoretically perfect indistinguishability it also provides polarized brightness, which makes the scheme highly appealing for future applications [93].

All the excitation schemes are described more in detail in the following chapters and their performances, advantages and technological challenges are summarized in Tab. 3.1

3.2.2.1 Resonant excitation

QDs under RE are commonly used triggered sources of high-quality single photons [55, 87, 88, 177]. The RE can greatly suppress decoherence processes, leading to the generation of highly indistinguishable single photons [88, 177] with nearly transform-limited linewidth [176]. On the other hand, the single-photon purity of emitted photons is constrained by the non-zero probability of spontaneous emission followed by a system re-excitation during a single pump pulse which leads to multi-photon emission [95].

The spectral degeneracy between the excitation laser and emitted photons requires separation, typically achieved through polarization filtering, incurring significant collection losses, which can be as high as $50\,\%$ [86]. Nevertheless, this limitation can be overcome by exploiting dichromatic pumping [187], charge exciton recombination in asymmetric cavities [188] or spatial separation of pumping field and emitted single photon with the use of photonic structures [189]. To date, the highest fiber brightness of QDs, reaching $71\,\%$, has been achieved with a cavity-enhanced system under RE [56]. Recently, it was shown that the photonic state emitted from RE is pure in the photon-number bases, making this scheme suitable for on-demand Fock states generation [97]. The decoupling from dephasing mechanisms and the potential for significant enhancement through a photonic structure make resonant excitation a fitting pumping scheme for high-performanceQD single-photon sources [87, 88].

RE of QDs can be simply modelled by an ideal 2LS, with ground state (G) and X which are energy separated by $\hbar\omega_0$, where the frequency of pumping field is $\omega_L = \omega_0$. In the following, we will apply the quantum trajectory model to derive

the photon number probabilities of the state produced by this pumping scheme, as outlined in [95].

Assume that the 2LS is resonantly driven by an optical pulse in time $t = 0$ in the rotating wave approximation. Then the system will coherently oscillate between G and X in dependence on the pump pulse area $A(t)$, which is defined as

$$A(t) = \frac{1}{\hbar} \int_0^t dt' \mu E(t') \ , \tag{3.2-3}$$

where μ is system's dipole moment and $E(t)$ is amplitude of pulse electric field. If the system is initially prepared in the state G, it can be represented as a coherent superposition after interacting with the pump pulse

$$|\psi_s(A)\rangle = \sqrt{1 - P_e(A(t))}\,|G\rangle + \mathrm{e}^{-i\phi}\sqrt{P_e(A(t))}\,|X\rangle \ . \tag{3.2-4}$$

Here, ϕ is a phase given by the pumping field and $P_e(A(t))$ is a possibility that the system will be excited by a pulse of area $A(t)$. This probability can be written as

$$P_e(A(t)) = \sin^2\left(\frac{A(t)}{2}\right) \ , \tag{3.2-5}$$

which shows that the oscillations are perfectly sinusoidal. Assuming an initial state of G, $A = \frac{\pi}{2}$ corresponds to a superposition state of G and X, $A = \pi$ leads to a full inversion and $A = 2\pi$ puts the 2LS back to G. Such oscillations of 2LS populations with pump pulse area are called Rabi oscillations and they are specific for resonant pumping schemes.

The pump pulse of length T can run an arbitrary number of rotations between G and X. The next calculations will be made in area theorem approximation, which assumes that Rabi oscillations are a function of the total interaction area of the pulse. So the probability of finding 2LS in X after the interaction is $P_e(A(t = \infty))$. In reality, the pulse power is distributed only over the pulse length T, so we can assume $A(\infty) \approx A(T)$.

Let's now investigate photon-number probabilities of the state generated by resonantly pumped 2LS. At any time when the state is excited, spontaneous emission can happen and restart the state to grand state and, in some sense, also restart the area theorem [95]. We can define the spontaneous decay rate of the excited level as

$$\gamma_x = \frac{1}{\tau_x} \ , \tag{3.2-6}$$

where τ_x is life time of X. Now we can easily calculate the spontaneous emission rate as $\gamma_x P_e(A(t))$. Then, the system is again excited within the same pump pulse and follows the deterministic evolution given by the area theorem until the next spontaneous emission or until the pump pulse is still present. This process will repeat until the pulse fully interacts. After the pulse, the system can decay only spontaneously. Based on the described system dynamic we can construct inclusive

probabilities F_n, which describe the probability that n and more photons will be emitted

$$F_n = \int_0^\infty dt_1 \int_{t_1}^\infty dt_2 \ldots \int_{t_{n-1}}^\infty dt_n f_n(t_1, \ldots, t_n) \ , \tag{3.2-7}$$

where t_n are photons' emission times and $f_n(t_1, \ldots, t_n)$ is associated probability density. We will assume short-pulse approximation $T \ll \tau_x$, where the average excited state has a dominant probability that it will not spontaneously decay within the pump pulse interaction window. We will now show how $f_n(t_1, \ldots, t_n)$ are constructed on the easy example of $f_1(t_1)$ in assumption of a square pulse pulse.

First, we will define $f_1(t_1)$ for times within pump pulse duration $0 \leq t_1 \leq T$. The probability of zero emission before t_1 is given as $\mathrm{e}^{\frac{1}{2}\gamma_x t_1}$, which multiplied by the true instantaneous emission rate $\gamma_x P_e(A(t_1))$ gives us the first inclusive probability density

$$f_1(t_1) \approx \gamma_x \sin^2\left(\frac{A(t)}{2}\right) \mathrm{e}^{\frac{\gamma_x t_1}{2}} \text{ if } 0 < t_1 < T \ . \tag{3.2-8}$$

Now we will look at system evaluation after the interaction with the pump pulse, times $t_1 > T$. In such case, the excited level can emit only spontaneously with characteristic exponential decay and the first inclusive probability density for times after the pulse interaction is given as

$$f_1(t_1) \approx \gamma_x \sin^2\left(\frac{A(\infty)}{2}\right) \mathrm{e}^{\frac{\gamma_x T}{2}} \mathrm{e}^{-\gamma_x (t_1 - T)} \text{ if } T < t_1 \ . \tag{3.2-9}$$

From the probability densities, we can calculate the first inclusive probability as defined by Eq. 3.2-7

$$F_1 = \gamma_x \int_0^T dt_1 \sin^2\left(\frac{A(t)}{2}\right) \mathrm{e}^{\frac{\gamma_x t_1}{2}} + \gamma_x \sin^2\left(\frac{A(\infty)}{2}\right) \mathrm{e}^{\frac{\gamma_x T}{2}} \int_T^\infty dt_1 \mathrm{e}^{-\gamma_x (t_1 - T)} \tag{3.2-10}$$

Analogically we can construct all the higher inclusive probability densities and by related integration derive the inclusive probabilities. The full derivation can be found in the paper by Fisher, where this RE description based on quantum trajectories was introduced [95]. Here we just write down the final equations for the first three inclusive probabilities for square pump pulse in approximation of short pulses

$$F_1 \approx \mathrm{e}^{-\frac{\gamma_x T}{2}} \left(\sin^2\left(\frac{A(\infty)}{2}\right) + \frac{\gamma_x T}{2}\left(1 - \frac{\sin(A(\infty))}{A(\infty)}\right)\right)$$
$$F_2 \approx \mathrm{e}^{-\frac{\gamma_x T}{2}} \frac{\gamma_x T}{8}\left(2 + \cos(A(\infty)) - 3\frac{\sin(A(\infty))}{A(\infty)}\right)$$
$$F_3 \approx \mathrm{e}^{-\frac{\gamma_x T}{2}} \frac{(\gamma_x T)^2}{64 A(\infty)^2}\left(4(A(\infty)^2 - 6) - (A(\infty)^2 - 24)\cos(A(\infty)) + 9A(\infty)\sin(A(\infty))\right) \tag{3.2-11}$$

These results we can directly use to construct parameters, which we already know. The brightness of resonantly pumped QD is equal to F_1, the photon-number probabilities are defined as $P_1 = F_1 - F_2$ and $P_2 = F_2 - F_3$, and then we can define second-order correlation function as $g^{(2)}(0) \approx \frac{2P_2}{(P_1+2P_2)^2}$. Now we can estimate the brightness and purity of the source just from the exciton lifetime τ_x and pump pulse length T.

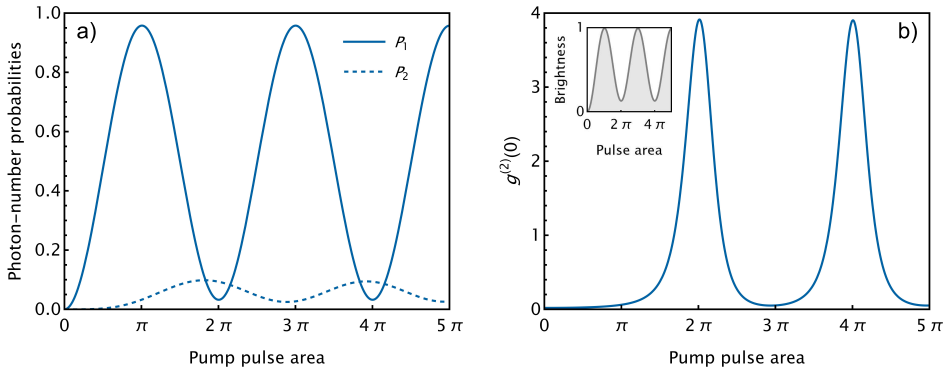


Figure 3.9: **Photon-number probabilities for state generated by a two-level system resonantly pumped by square pulsed of** $T = 0.3/\gamma_x$**.** Photon statistics calculated for an ideal two-level system in an approximation of short pulses and assuming area theorem. **a)** Probabilities of generating single photon (P_1) and two photons (P_2) in dependence on pump pulse area. **b)** The second-order correlation function $g^{(2)}(0)$ calculated from derived probabilities P_1 and P_2. The insert shows the total source brightness following the Rabi oscillations.

Here we characterize a system defined by $\gamma_x T = 0.3$, see Fig. 3.9. We see that the QD's brightness follows the Rabi oscillations, however, it doesn't reach zero for the even-π pulses due to the non-zero probability that a photon will be emitted spontaneously within the pulse duration. The interesting consequence of the area theorem and spontaneous decay during the pulse interaction is the high probability of two photons emission for even-π pulses, which is even higher than the probability of emitting just a single photon. Therefore at the minima of Rabi oscillations, we can observe bunching of the second-order correlation function $g^{(2)}(0)$.

To evaluate the source performance in the optimum (π-pulse) we can, in the short pulse approximation, use the following estimations of two-photon probability and purity

$$P_2 \approx \frac{\gamma_x T}{8}$$
$$g^{(2)}(0) \approx \frac{\gamma_x T}{4} \ . \tag{3.2-12}$$

It's evident that the single-photon purity gets worse with longer pulses. However, in reality, employing extremely short pulses does not further enhance $g^{(2)}(0)$. This limitation arises from the simplifications made in the model of the 2LS. The use of short pulses introduces spectral broadening due to Fourier transformation properties. Consequently, these short pulses not only resonantly pump the 2LS but also exhibit spectral overlap with higher-lying states [190]. As a result, the pumping mechanisms other than RE contribute to the degradation of single-photon purity for short pulses. Therefore, an optimal pumping pulse is short enough while being narrow in spectra to pump only the RE process selectively. Typically, pulses of around 10 ps are employed [55].

For the sake of completeness, it is worth noting here that in the case of long pulses where $\gamma_x T \gg 1$, the photon-number probabilities will follow the Poisson distribution [95].

3.2.2.2 Longitudinal acoustic phonon-assisted pumping

In general, RE suffers from its sensitivity to pump fluctuations. The brightness and purity of the resonant scheme are significantly influenced by pump pulse power due to Rabi oscillations, as illustrated in Fig. 3.9. Additionally, for RE, the pump must be in resonance with the 2LS, making any wavelength fluctuations a limiting factor for excitation probability. These obvious limitations of RE can be overcome by LA, where the pump is positively detuned from X within the longitudinal acoustic phonon sideband, with its peak typically positioned around 1 meV above the excitonic level.

Efficient light-phonon coupling is defined by the spectral phonon density, denoted as $J(\omega)$, which exhibits a broad maximum [186,191]. In the phonon-assisted process, the dephasing time is shorter than the pump pulse length. As a result, LA does not exhibit Rabi oscillations [91,186]. Instead, a typical brightness saturation is observed with varying pump power. Consequently, LA provides stable emission unaffected by small pump power and spectral fluctuation [90, 91]. This stability allows for pumping many slightly different QDs with a single excitation laser, representing a significant advancement toward the scalability of these sources [185].

Due to the spectral detuning of the pump laser from the X level, the single-photon spectral emission line in LA is laser-free, so there is no necessity for polarization filtering as required in RE. This allows the single photons generated

by LA to be separated through lossless spectral filtering. Additionally, the high population of the X state is achieved through adiabatic undressing, resulting in a delay from the pump pulse and a reduction in the re-excitation probability. As a result, LA can provide higher overall brightness and greater single-photon purity compared to RE [90, 91]. The HOM visibility is constrained by emission time uncertainty (jitter) coming from phonon decay, limiting the visibility values to $< 90\,\%$ [90, 178]. Because of the fast decoherence mechanisms and suppressed Rabi oscillations we assume that the PNC is close to zero and the generated photonic state is mixed in the Fock bases [52], which was recently confirmed by an experimental investigation [98].

Let's look briefly at the physical description of LA. We will assume that the pump laser detuned above the X level is still far from XX and we can treat QD as 2LS [186]. Then the phonon-assisted pumping can be described as a three-step process consisting of optical dressing, phonon relaxation and adiabatic undressing illustrated by Fig. 3.10.

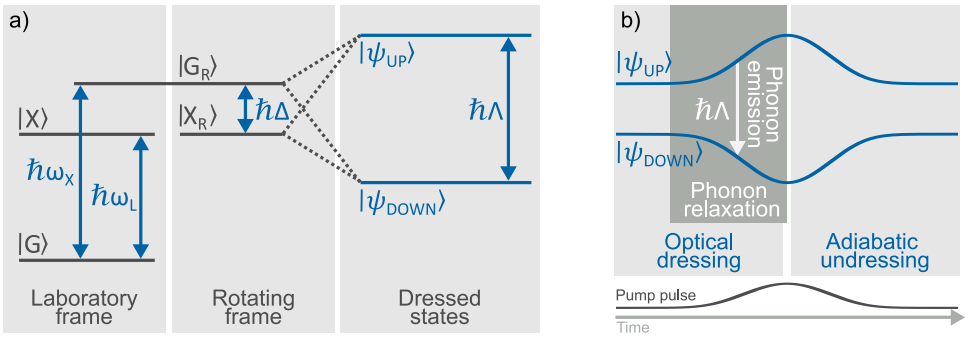


Figure 3.10: **Scheme of longitudinal acoustic phonon-assisted pumping. a)** Scheme of QD's states in laboratory frame ($|G\rangle$, $|X\rangle$), rotated frame ($|G_R\rangle$, $|X_R\rangle$) and optically dressed states ($|\psi_{up}\rangle$, $|\psi_{down}\rangle$), which are driven by a pump laser detuned by Δ from the X. **b)** Time evolution of the optically dressed states within the Gaussion pump pulse duration.

Switching on the pump laser will transfer the QD energy states to new bases commonly known as laser-dressed states defined as

$$\begin{aligned} |\psi_{up}\rangle &= \cos\Theta\,|G_R\rangle + \sin\Theta\,|X_R\rangle \\ |\psi_{down}\rangle &= -\sin\Theta\,|G_R\rangle + \cos\Theta\,|X_R\rangle \end{aligned} \quad , \tag{3.2-13}$$

where $|G_R\rangle$ and $|X_R\rangle$ are ground and excited state in rotating frame and Θ is mixing angle given by

$$\tan\Theta = \frac{\hbar f}{\Delta + \hbar\Omega} \quad , \tag{3.2-14}$$

where f represents the pumping field strength, the detuning from X in the laboratory frame is denoted as Δ, and Ω represents the Rabi frequency, which can be calculated as $\hbar\Omega = \sqrt{(\hbar f)^2 + \Delta^2}$. The two dressed state are split by effective Rabi splitting

$$\hbar\Lambda(t) = \hbar\sqrt{\Delta^2 + \Omega(t)^2} \ . \tag{3.2-15}$$

The assumed time dependence of Rabi frequency arises from the time-dependent pump field. Assuming that the system is excited by Gaussian pulses, the effective Rabi splitting between the dressed states will follow the Gaussian envelope of the pulse.

Both of the dressed states have an excitonic component allowing for relaxation between them through the emission of a phonon with energy equal to the effective Rabi splitting. The states' energy separation is typically on the order of a few meV therefore it can be easily overcome by a longitudinal acoustic phonon [191].

As the laser intensity drops out the admixing of the dressed states is reduced and the relaxation is stopped. With decreasing the pump intensity the states are undressed, ideally in an adiabatic manner. The lower dressed state $|\psi_{down}\rangle$ is then transformed into the X state in the laboratory bases, boosting the X population, but only after the pump pulse [91]. This population inversion boost is observable in the case of Gaussian pump pulses, where undressing is a continuous process following the decay of the pump intensity. on the other hand, for rectangular pulses with an instant intensity drop, the X boost will not occur [191]. The maximal population inversion of 2LS reachable by LA can be in the assumption of Gaussian pump pulse of a high pulse area estimated as [186]

$$C_X - C_G = \tanh\left(\frac{\hbar\Delta}{2k_BT}\right) \ , \tag{3.2-16}$$

where C_X and C_G are population of X and G in laboratory bases. Therefore at lower temperatures $\sim 4\,\mathrm{K}$ the inversion of LA pumped process can be $> 90\%$, which allows to reach high brightness of this pumping scheme [91,186]. The photon emission probability is low during the phonon relaxation process, primarily because of the diminished population of X. Only after the inversion is boosted up by adiabatic undressing the photon emission grows. Since this occurs just after the pump pulse, the re-excitation is minimized and photons with high single photon purity are emitted [91].

3.2.2.3 Resonant two-photon excitation

The non-zero probability of photon emission during the presence of the excitation pulse, resulting in re-excitation and multi-photon emission, stands as a fundamental limit to the single-photon purity achievable through RE of a 2LS. However, this strong constraint can be overcome by TPE of the exciton-biexciton cascade [180].

In addition to achieving significantly higher single-photon purity, TPE is an appealing pumping scheme due to its capability to generate high-fidelity entangled photon pairs on demand [172, 182, 192].

The XX energy is shifted from 2X by a binding energy E_b which is a consequence of the Coulomb interaction of the electron-hole pairs. Therefore the XX level can be pumped by a two-photon absorption process, where the energy of the pump laser is detuned by $\frac{E_b}{2}$ from the X energy. A typical spectrum for TPE is presented by the insert of Fig. 3.11.The spectral separation between the pump and the photons emitted from the X and XX decays allows for effective filtering of the strong pump field. This approach, in principle, leads to higher single-photon counts compared to the typical outcomes of RE, where more complex pump field suppression methods are necessary.

TPE is a resonant process and therefore it follows Rabi oscillations which scale linearly with the pulse area defined as

$$A_{TPE}(t) = \frac{1}{\hbar E_b} \int_0^t dt' (\mu E(t'))^2 \ . \tag{3.2-17}$$

In contrast to the pulse area defined for RE by Eq. 3.2-3, here, the intensity of the pulse electric field is squared. This is a consequence of the nonlinear nature of the two-photon absorption process. Therefore more pump power will be needed to reach the first inversion of the system by TPE (π-pulse).

Let's compare RE and TPE based on the single-photon purity of the emitted state. In the short pulse approximation, we demonstrated that the two-photon generation probability for RE is linearly dependent on the pump pulse length, given by $P_2 \approx \frac{\gamma T}{8}$. This re-excitation process can be schematically written as $|G\rangle \rightarrow |X\rangle \rightarrow |G\rangle \rightarrow |X\rangle$. In contrast, two-photon emission in the TPE process occurs only through the following sequence: $|G\rangle \rightarrow |XX\rangle \rightarrow |X\rangle \rightarrow |G\rangle \rightarrow |XX\rangle$. This sequence we can use to derive the emission probability density for TPE. We again assume short-pulse approximation, area theorem and square pump pulses. The first emission $|XX\rangle \rightarrow |X\rangle$ can be described by the Rabi oscillation factor, well known already from RE description, $\gamma_{xx} \sin^2\left(\frac{A(t)}{2}\right)$, where γ_{xx} is the decay rate of biexciton level. After the first emission, the system is exclusively in $|X\rangle$, which is not driven by the pumping field, therefore the emission $|X\rangle \rightarrow |G\rangle$ contributes by spontaneous emission factor $\gamma_x e^{-\gamma_x t}$. Finally, the re-excitation of XX level contributes again by the Rabi factor $\gamma_{xx} \sin^2\left(\frac{A(t)}{2}\right)$. The inclusive emission probabilities can be derived using a similar approach to what we did for RE in Chapter 3.2.2.1, with the addition of the spontaneous emission factor arising from the X decay. The complete result can be found in Hanschke's paper [180]. Here, we simply present the final estimations of the two-photon probability and single-photon of the state purity generated by TPE driven by a π-pulse

$$P_2 \approx \gamma_{xx}\gamma_x T^2 \frac{\pi^2 - 8}{8\pi^2}$$
$$g^{(2)}(0) \approx \gamma_{xx}\gamma_x T^2 \frac{\pi^2 - 8}{4\pi^2} \ . \tag{3.2-18}$$

Compared with RE the two-photon emission probability is quadratic dependent on pulse length T and therefore for short pulses TPE generate single-photon state with significantly higher purity, see Fig. 3.11.

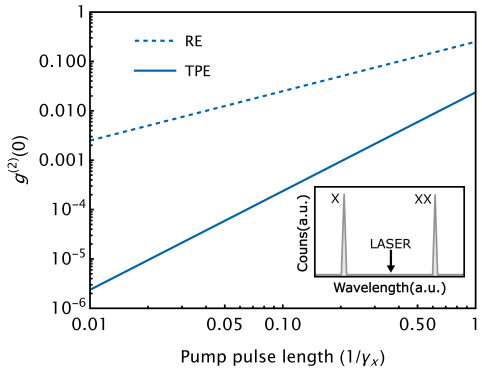


Figure 3.11: **Comparison of simulated values of $g^{(2)}(0)$ for RE and TPE as a function of the pump pulse length.** The calculation was made in short pulse approximation assuming square pump pulse and area theorem. The XX lifetime was set as $\tau_{xx} = \frac{1}{2}\tau_x$. The insert shows a scheme of modelled TPE spectrum.

On the other hand, the indistinguishability of single photons generated by TPE is strictly limited compared to RE, where it can theoretically be equal to unity [88, 177]. In TPE processes, the decays of the XX and X states are causally connected, resulting in emitted photons that are partially entangled in the time domain [181,183]. Consequently, this entanglement influences the temporal profiles of single photons, leading to linewidths that are not transform-limited. The degree of this entanglement depends on the lifetimes of the XX and X states, defining the upper bound of the HOM visibility for photons generated by TPE

$$V_{\mathrm{HOM}}^{TPE} = \frac{1}{1 + \tau_{xx}/\tau_x} \ . \tag{3.2-19}$$

The XX can be for a general QD approximated as $\tau_{xx} \approx \frac{1}{2}\tau_x$ [193]. Therefore, the HOM visibility of TPE process can be bounded by $\sim 66\,\%$. This limitation can be overcome by designing photonic cavities in a manner that only the transition $|XX\rangle \rightarrow |X\rangle$ will be enhanced by the Purcell effect. This selective shortening of the XX lifetime can improve the upper limit for the V_{HOM}. However, it is crucial to note that TPE will never achieve ideal photon indistinguishability.

TPE, similar to RE, is a coherent process, where the system and pumping are described by a pure state outlined in Eq.3.2-4. Consequently, one would anticipate that the resulting photonic state is also pure. The PNC of photons generated through the transition $|X\rangle \rightarrow |G\rangle$ in the context of TPE was recently studied using the approach delineated in Ch. 3.0.2.5 [94]. Notably, the active control of relative phase in the interferometer wasn't used in this work, and based solely on random phase evolution, it was concluded that there is no PNC observed. Although photon number state tomography has not yet been done with QD. However, from detailed studies of exciton-biexciton cascades on different systems, such as microwave photon generators, we know that the state generated from TPE process is pure and has a form of [164]

$$|\psi_{TPE}\rangle = \sqrt{p_0}\,|0_x 0_{xx}\rangle + \sqrt{p_1}\,|1_x 1_{xx}\rangle + \ \dots\ . \tag{3.2-20}$$

We are already aware that the method detailed in Chapter 3.0.2.5 is capable of measuring the purity of a state only in reference to the pure state $|0\rangle+|1\rangle$. Selective measurement of PNC on the X photon is equivalent to tracing out XX photon from the pure state defined by Eq. 3.2-20 and assessing the coherence of the resultant state. Tracing out a part of the pure state always results in a mixed state, therefore such a measurement fails to provide any insights into the original state's purity.

The intriguing feature of TPE is its ability to generate entangled photon pairs on demand. Assuming perfect in-plane symmetry of QD's confinement potential, then the intermediate X states in the H and V exciton-biexciton cascade are degenerate in energy. The combined two-photon state of the emitted X and XX photons are in the polarization space represented by the maximally entangled Bell state

$$|\phi^{\dagger}\rangle = \frac{1}{\sqrt{2}}(|H_x H_{xx}\rangle + |V_x V_{xx}\rangle)\ . \tag{3.2-21}$$

In the general case, however, the symmetry is imperfect and the energy levels are split by a finite FSS. The generated state can be described as

$$|\psi_{TPE}(t)\rangle = \frac{1}{\sqrt{2}}(|H_x H_{xx}\rangle + \mathrm{e}^{-\frac{i}{\hbar}St}\,|V_x V_{xx}\rangle)\ , \tag{3.2-22}$$

where S is the magnitude of FSS splitting and t is the time difference between the XX and X photons. The state describes a maximally entangled state, where the phase oscillates with an angular frequency $\frac{S}{\hbar}$, which leads to $|\psi_{TPE}(t)\rangle$ oscillations between $|\phi^{\dagger}\rangle$ and $|\phi^{-}\rangle$ Bell states. However, the state is maximally entangled at each single time difference, the real measurements are based on time averaging and the measured state can be described by a density matrix representing a statistical mixture

$$\hat{\rho}_{TPE} = \frac{1}{\tau_x}\int_0^T dt\,\mathrm{e}^{-\frac{t}{\tau_x}}\,|\psi_{TPE}(t)\rangle\langle\psi_{TPE}(t)|\ , \tag{3.2-23}$$

where we integrate over the measurement time window T. This density matrix can be then used to calculate the estimated state fidelity.

To reach higher fidelities of the generated entangled state we can either apply time filtering, so decrease our measurement window and reduce brightness, or use QD with symmetrical confinement potential. The droplet etching method can be used to grow highly symmetrical QDs reaching entanglement fidelity of generated state up to 94 % [172]. The fidelity can be further improved by mechanical stretching of QD by piezo actuators, which leads to complete suppressing of FSS and fidelities up to 98 % [72]. The reason, why even for zero FSS the fidelity of entangled state does not reach unity was explained only recently by breaking the confinement potential symmetry by pump pulse generated Stark shift. This effect is persistent throughout the TPE process, thus imposing a fundamental constraint on the maximum achievable fidelity [194, 195]. Nevertheless, the phase evolution within the state defined by Eq. 3.2-23 is deterministic, allowing for its complete compensation to reach the perfect fidelity. With this motivation, various approaches, such as utilizing electro-optical modulators [196] or rotating waveplates with the given angular frequency [197], have been suggested to counteract the phase evolution in the generated state.

3.2.2.4 Stimulated two-photon excitation

The primary constraint associated with TPE is the restricted HOM visibility. This limitation can be addressed by stimulating $|XX\rangle \rightarrow |X\rangle$ transition with an additional laser pulse, this pumping scheme is referred to as sTPE. Same as in the standard resonant version the sTPE leads to single-photon generation with ultralow multi-photon component. The precisely timed stimulation pulse prepares X in a predetermined time, which reduces the timing jitter given by XX lifetime and consequently enhances photon indistinguishability [93]. Furthermore, the polarization of the stimulation pulse selectively determines one of the decay cascades, $|XX\rangle \rightarrow |X\rangle \rightarrow |G\rangle$. Consequently, the emitted single photons are exclusively in either the H or V polarization state [92]. Therefore sTPE can reach the highest polarized brightness from all of the assumed pumping schemes.

Let's assume the exciton-biexciton cascade, where we will now distinguish between the two X states as X_H and X_V. The system dynamic is given by Rabi oscillations dependent on the pump pulse area defined by Eq. 3.2-17, same as TPE. A short excitation π-pulse, with time width $T_{pulse} \ll \tau_x$ inverses the system and XX population reach almost unity. After the excitation, the system follows free evolution and it starts decay to X_H and X_V with equal probabilities. A stimulation π-pulse with a fixed polarization, just assuming H polarized pulse, is implemented with a delay Δt. Such pulse inverters population between XX and X_H. H polarized single-photon is then emitted from transition $|X_H\rangle \rightarrow |G\rangle$.

Independently on the delay between excitation and stimulation Δt the second-order correlation function $g^{(2)}(0)$ of the emitted single-photons is two magnitudes lower than for RE, see Fig. 3.12 However, for short delays, where the two pulses

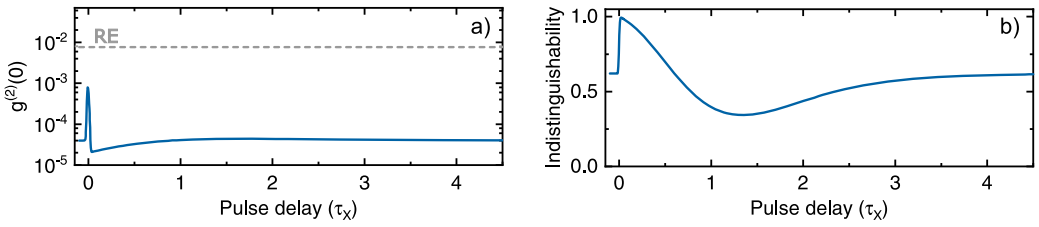


Figure 3.12: **Single-photon purity and indistinguishability for sTPE in dependence on the delay between excitation and stimulation pulse. a)** Calculated second-order coherence of the $|X_H\rangle \rightarrow |G\rangle$ transition compared with the value for RE of X (dashed line). **b)** Calculated photon indistinguishability. *Figure taken with small changes from [93].*

temporally overlap, we see a sharp peak of $g^{(2)}(0)$ as a consequence of τ_{xx} reduction which increases the re-excitation probability. The peak is directly followed by a steep dip, where for delays $\sim 0.02\tau_x$ second-order correlation function reaches its minima even lower than for TPE, which comes from strong suppression of probability that the system will freely decay via the V cascade. Then the $g^{(2)}(0)$ value is practically constant for longer Δt and it is approximately equal to single-photon purity reachable by TPE [93].

The maximum indistinguishability is reached when both of the pulses still have a small temporal overlap and then it decreases to its local minimum ($\Delta t \sim 1.4\tau_x$. At this delay, the stimulation pulse effectively increases the time jitter by re-exciting the XX by the transition $|X_H\rangle \rightarrow |XX\rangle$. For longer delays, most of the population already decays by $|X_H\rangle \rightarrow |G\rangle$ before the stimulation pulse and therefore the indistinguishability reaches the standard TPE limit given by Eg. 3.2 -19 [93].

The recent measurement of the PNC between the $|0\rangle$ and $|1\rangle$ photon number states of single photons emitted by sTPE has demonstrated that the generated state is pure in Fock bases [94]. This sets apart this excitation scheme from TPE, where the PNC is limited to even photon states, as detailed in Eq. 3.2-20.

Generally, the use of sTPE appears well-suited for various applications, thanks to its high polarized brightness with ultra-low multi-photon emission, potential spectral suppression of excitation and stimulation pulses, and high indistinguishability $\sim 99\,\%$ [93, 94]. However, it is important to note that the general improvement of polarized brightness and HOM visibility over TPE was possible only by sacrificing entangled photon pairs generation.

3.2.2.5 Phonon-assisted two-photon excitation

Similar to the case of a 2LS, a longitudinal-acoustic phonon can be employed to initiate an exciton-biexciton cascade. This off-resonant approach is called LA-TPE. It combines the benefits of TPE, such as achieving high single-photon purity and

generating entanglement, with the resilience of LA phonon against fluctuations in the excitation field [184].

It was demonstrated that LA-TPE achieves comparable brightness and single-photon purity to TPE [184, 185]. Additionally, it appears that even the fidelity of entanglement remains unaffected by phonon decay [185]. Although the PNC has not been explored to date, it is reasonable to assume that, similar to 2LS, incoherent phonon interactions will result in mixed-state emission.

The primary constraint of LA-TPE is the relatively high excitation power needed to reach the maximal population inversion, which is the highest of all the presented schemes here. The positively off-resonant detuning of the excitation laser causes its spectral line to shift toward the X. The sift is usually $\sim 1\,\mathrm{meV}$, coming from the spectral phonon density $J(\omega)$. The combination of a small spectral line separation and high excitation power makes the spectral suppression of the pumping field challenging [184]. Consequently, LA-TPE is suitable for QDs with larger binding energy E_b.

3.2.2.6 Adiabatic rapid passage

Resonant schemes, represented by RE and TPE, face a significant challenge due to the strong dependence of photon-number probabilities on factors such as excitation power, dipole momentum, or interaction time. One approach to overcome this limitation is the utilization of off-resonant schemes, where phonon interactions are used to reach population inversion, resulting in the suppression of Rabi oscillations. Another option, in contrast to these off-resonant methods, involves employing an ARP, wherein a QD is resonantly pumped using a spectrally chirped pulse [179].

During the interaction of 2LS with a chirped pulse, the energy eigenstates are switched from $|G_R\rangle$ and $|X_R\rangle$ in rotated bases representation to dressed states $|\psi_{up}\rangle$ and $|\psi_{down}\rangle$, which are expressed as coherent superpositions of the original states, as shown in Eq. 3.2.2.2. The 2LS initiates in $|G_R\rangle$ and during the interaction with the pulse it adiabatically evolves along the dressed state to $|X_R\rangle$ [179], when the excitation laser frequency due to the chirp sweeps around the resonant frequency slower than Rabi oscillations.

Using a positively chirped pulse (red detuned) will make the system follow the dressed state $|\psi_{down}\rangle$ and the negatively chirped pulse will lead to evolution along the $|\psi_{up}\rangle$. In the case of negative chirp, the source will reach maximal brightness for power $\sim 1.5\pi$, where π-pulse is given as a pulse area for which the same 2LS will reach maximal inversion under RE with a Furrier limited pump pulse. After the maximum, the decrease in brightness for higher powers can be observed. This can be explained by system relaxation from $|\psi_{up}\rangle$ to $|\psi_{down}\rangle$ by phonon emission, which breaks the ARP process and reduces the source brightness. On the other hand, the positively chirped pulse doesn't have this issue as long as a relaxation from $|\psi_{down}\rangle$ to $|\psi_{up}\rangle$ is based on a phonon absorption, which is hardly probable on low temperatures, where QDs are usually operated. Therefore the ARP excited by the positively chirped pulse is robust against pump field fluctuations and after

the maximum of its brightness $\sim 1.5\pi$ the emitted photons counts are saturated for the higher excitation powers [179].

In general ARP is a robust version of RE, which reaches comparable single-photon purity and indistinguishability in the generated photon states. However, the investigation of PNC for this excitation scheme remains unexplored. The principal drawback of the ARP lies in its experimental complexity, primarily coming from the requirement for chirped pulse preparation and spectral broad polarization suppression of the excitation pulse. Consequently, the ARP is not frequently employed, and in scenarios demanding a robust excitation, the LA is usually preferred.

3.3 Emission in the optical communication band

Until now we have been comparing quantum-light sources based on parameters such as brightness, single-photon purity, or PNC. However, the central wavelength of the emitted wave packet is also crucial, especially when aiming to optimize the performance of associated hardware components such as communication links, single-photon detectors, optical modulators, or quantum memories and repeaters [198]. Photons emitted within the telecom original band (O-band) spanning wavelengths from 1260 nm to 1360 nm or the telecom central band (C-band) defined between 1530 nm and 1565 nm, are appealing for applications in quantum communication. This is primarily attributed to the exceptionally low transmission loss ($0.35\,\mathrm{dBkm}^{-1}$ at 1310 nm and $0.2\,\mathrm{dBkm}^{-1}$ at 1550 nm) in common silica optical fibre links [199], as well as the comparatively low background solar irradiance and Rayleigh scattering in free space in satellite-based quantum communication [39]. Moreover, these wavelength intervals are compatible with mature silicon platforms, which allows further information processing within complex and highly integrated photonic chips [200, 201].

Furthermore, quantum applications relying on photons within the communication band derive advantages from well-established technologies originally developed for classical optical communications. Beyond the existing global fiber communication network operating in the optical O-band and C-band, mature telecommunications technology provides many advanced, off-the-shelf components such as high-performance laser sources, fast optical modulators, and highly efficient photon detectors [198]. These components are easily accessible due to their mass production. The prospect of using components and infrastructures from real-world classical communication encourages quantum researchers to align their hardware with the same communication wavelength, which holds the potential for widespread implementation of quantum communication protocols soon.

The wavelength of emitted photons by WCS and SPDC sources can be precisely adjusted by selecting the suitable pump laser and nonlinear crystal, enabling coverage of telecommunication bands [202, 203]. Therefore, these sources are currently the most widely employed for communication protocols [204]. Various material

platforms can host solid-state single-photon emitters within the desired wavelength range. These include silicon carbide [205,206], carbon nanotubes [207], gallium nitride [208], yttrium orthosilicate [209,210] or atomic vapours [211]. However, all of these have not outperformed PDSs in key parameters such as brightness and single-photon purity [204].

During the SKG process, the strain resulting from the mismatch of lattice constants between InAs and GaAs leads to the formation of small QDs emitting in the near-infrared range [86]. Therefore, in the case of QDs, the leading emission wavelength is $\sim 900\,\text{nm}$ [55]. To shift the emission wavelength into the telecom interval methods of spectral conversion can be employed [212,213]. It has already been demonstrated that the frequency conversion process preserves the single-photon purity [213,214], indistinguishability [215] and even entanglement fidelity [216,217]. However, the limiting factor is the conversion efficiency reducing QD brightness and the technological overhead [217,218]. This process also suffers from spontaneously emitted photons, which are not correlated to the input signal and limit the signal-noise ratio of the converted states [218]. This constraint impacts the security parameters of quantum cryptography protocols employing such sources.

InAs QDs emitting single photons directly in telecommunication C-band can be grown on the InP platform, where the lattice constants mismatch is reduced and the formed QDs are larger compared to InAs/GaAs ones [219]. However, using InP material is technologically challenging due to its poor heat conductivity and fragility [220]. Also, there is no compatible binary material combination with a large refractive index difference, which complicates the implementation of efficient distributed Bragg reflector (DBR) structures. The significant difference between InP and Si lattice constants limits further integration [204]. Moreover, when QDs are fabricated by SKG method on the InP platform with a focus on C-band emission, it often leads to a high QDs density [221] and the formation of highly asymmetric complexes known as quantum dashes or quantum wires [222–224]. The first makes it challenging to address individual emitters, while the second contributes to a large FSS, thereby limiting the application range of these complexes. This can be overcome by precise optimization of the growing process [225,226] or using droplet epitaxy [227–229].

The technological limitation of the InP platform can be overcome by employing GaAs material, which is a well-established platform for the fabrication of photonic structures, which allows to implementation of efficient binary AlAs/GaAs DBRs. To reach the emission in telecommunication bands the strain between InAs and GaAs has to be reduced. This is usually done via a strain-reducing layer [57, 58, 230–232] or an InGaAs metamorphic buffer with graded In content [59–61,233–240]. The QDs based on GaAs emitting in telecom C-band recently reached high brightness and single-photon purity by a circular Bragg grating enhancement [61]. The study of the potential of telecom C-band QDs based on GaAs for implementation in quantum communication is the focus of this work.

4

Summary of "Quantum cryptography with highly entangled photons from semiconductor quantum dots"

This chapter summarises the paper titled "Quantum cryptography with highly entangled photons from semiconductor quantum dots" [68]. The experiment was performed by the group of Professor Armando Rastelli at Johannes Kepler University Linz with our support. Motivated by this project we started investigating QDs' performance in various quantum cryptographic protocols. Therefore, it is accurate to say that this collaboration played a crucial role in shaping the theme of this thesis.

My contribution: *I collaborated with Christian Schimpf on the optical part of the experimental setup, mainly on the design and realization of Alice's and Bob's stations. I supported the measurement and collaborated on data processing, mainly the quantum cryptography part. I investigated the performance comparison of the used QD with PDSs in the BBM92 QKD protocol.*

Emission from GaAs QDs obtained by droplet epitaxy under TPE shows a multiphoton probability as low as $8(2) \times 10^{-5}$ [175, 241]. Additionally, the weak confinement of the multiparticle wave functions in these QDs [242], along with their high in-plane symmetry [171], enables the generation of entangled photon pairs with high fidelity of 0.987(8), without the need for time filtering or post-growth tuning [72]. The high single-photon purity and entanglement fidelity contribute to a low QBER and are therefore vital for the effective SKR of EQKD implementations [101, 243–245]. Successful demonstrations of quantum teleportation [74] and entanglement swapping with droplet-etched QD [76, 246] further promote the development of QD-based quantum networks for long-distance communication [75].

In this work, entangled photon pairs generated by GaAs QDs at 780 nm are employed to implement the EQKD protocol between two buildings connected by a 350 m single-mode fiber. Using the BBM92 protocol, the key generation yields an average raw key rate of 135 bits/s, which is reduced to 86 bits/s for the SKR, with the QD being driven at a pumping rate of 80 MHz. A QBER as low as 1.9 % is demonstrated over a continuous 13-hour period.

4.1 Experimental setup

The experimental setup for EQKD implementation is illustrated in Fig. 4.1. The parties, Alice and Bob, are located in separate buildings. Alice and the GaAs QD-based source of entangled photons are housed in a laboratory, while Bob, as a mobile unit, is positioned at an office desk connected to the laboratory via a 350 m deployed single-mode fiber. The entangled photon pairs are transmitted through the fiber, and polarization controllers correct any polarization state rotation caused by random birefringence in the fibers.

In the BBM92 QKD protocol, Alice randomly measures one photon from the pair in one of two conjugate bases, projecting the other photon into the BB84 state, which is sent to Bob. A 50 : 50 BS splits the incoming photons for measuring the incoming photons in either of the two conjugate bases (Z or X), and they are subsequently detected by APDs. The key sifting and other classical communication parts of the protocol are carried out over a standard LAN network. Synchronization between Alice and Bob is maintained using external 10 MHz Rb frequency standards.

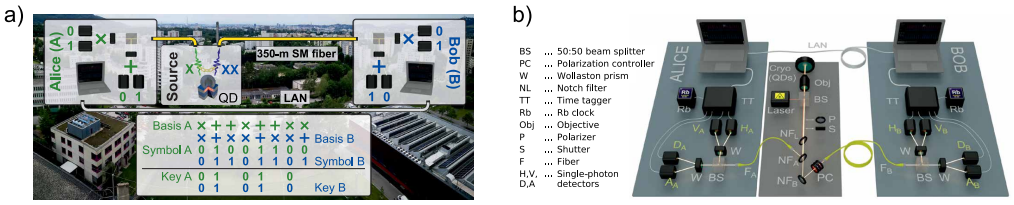


Figure 4.1: **Experimental setup for QKD with entangled photon pairs. a)** Configuration of the fiber-based EQKD system using highly entangled photons from a GaAs QD photon source. Alice and the QD are situated in the laboratory. Bob is assembled in a transportable box placed in a separate building and connected to the photon source via a 350 m-long single-mode fiber. The photons are analyzed in the X and Z basis, and each outcome is assigned to a "0" or a "1" symbol. The key sifting, as sketched in the table, is performed over a 100-Mbits/s LAN connection. **b)** Illustration of the optical and electronic components of the setup.

We utilize the maximally entangled polarization state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$, ensuring that when Alice's and Bob's measurement bases are aligned, they obtain identical outcomes, thus generating a matching key string of 0s and 1s. The entangled photon pairs are produced using a QD excited via TPE, driven by a pulsed laser with a repetition rate of 80 MHz.

4.1.1 Quantum dot characterization

The single-photon purity was determined as described in Ch. 3.0.2.2. We used Bob's detectors to measure the second-order correlation function, as his setup, located in a box exposed to daylight, represents a worst-case scenario for the impact of ambient light on the measurement. This scenario aligns with the parameter estimation phase of the QKD protocol, which is always conducted on Bob's side after the communication channel. The measured values at zero time delay were $g_X^{(2)}(0) = 0.017(2)$ and $g_{XX}^{(2)}(0) = 0.025(2)$. These values are primarily influenced by ambient light ($\sim$ 1000 counts per second (cps)) and dark counts from the APDs ($\sim$ 200 cps). The contribution of the QD single-photon emission is highly negligible [241].

The maximum excitation pump rate for a QD sources is only limited by the XX and X radiative lifetime τ_{XX} and τ_X, as no following excitation can occur before the QD decayed to its ground state. For the used quantum dot the radiative decay times were measured as $\tau_{XX} \approx 120\,\mathrm{ps}$ and $\tau_X \approx 230\,\mathrm{ps}$. Therefore a pump rate $\sim 1\,\mathrm{GHz}$ is accessible.

The time-averaged fidelity of the generated entangled state is limited by the FSS as the real state generated by a QD has a relative phase oscillating with the period given by FSS magnitude as described by Eq. 3.2-22. As no time filtering is used, the two-qubit density matrix is composed of all possible time-dependent states weighted by their emission probability

$$\hat{\rho}_S = \int_0^\infty dt\, \frac{1}{\tau_X}\, \mathrm{e}^{-\frac{1}{\tau_X}}\ |\psi(t)\rangle\langle\psi(t)| \ . \tag{4.1-1}$$

The nonzero $g_X^{(2)}(0)$ and $g_{XX}^{(2)}(0)$ approximately leads to a mixing the pure state $\hat{\rho}_S$ to the Wigner state

$$\hat{\rho} = (1-g)\hat{\rho}_S + g\frac{\mathbb{I}^{(4)}}{4} \ , \tag{4.1-2}$$

where $g := \frac{1}{2}\left(g_X^{(2)}(0) + g_{XX}^{(2)}(0)\right)$ and $\mathbb{I}^{(4)}$ is 4×4 identity matrix. Now we can finally calculate the fidelity of the state $\hat{\rho}$ by using the definition from Eq. 2.1-14 as

$$F(\phi^+\hat{\rho}) = \mathrm{Tr}\left[\sqrt{\sqrt{\hat{\rho}}\,|\phi^+\rangle\langle\phi^+|\,\sqrt{\hat{\rho}}}\right]^2 \ . \tag{4.1-3}$$

Because of the high symmetry, GaAs QDs grown by the droplet epitaxy typically experience a FSS magnitude on the order of $S \sim 5\,\mu\mathrm{eV}$ and it is straightforward to find a QD with $S < 1\,\mu\mathrm{eV}$. The QD used here exhibits $S = 0.39\,\mu\mathrm{eV}$ and $g = 0.021$ yielding a fidelity of $F(\phi^+\hat{\rho}) = 0.985$. This aligns closely with the experimentally measured state fidelity obtained through the tomography method, measured as 0.987(8).

4.2 QKD with entangled photon pairs

Before implementing the EQKD, it is essential to assess the probability of detecting false correlations clicks due to experimental imperfections in the BBM92 measurement configuration with actual state $\hat{\rho}$ given by Eq. 4.1-2. This probability, referred to as QBER in Ch. 2.2.2.1, can be theoretically estimated as follows

$$QBER = \frac{1}{2}\sum_{j=1}^{4} \langle O_j | \hat{\rho} | O_j \rangle \ , \tag{4.2-1}$$

where $|O_j\rangle \in \{|H\rangle_A |V\rangle_B, |V\rangle_A |H\rangle_B, |+\rangle_A |-\rangle_B, |-\rangle_A |+\rangle_B\}$ corresponds to cross-correlation measurements between Alice's and Bob's photons in the conjugate basis. The QBER for the used state $\hat{\rho}$ is 1.5 %.

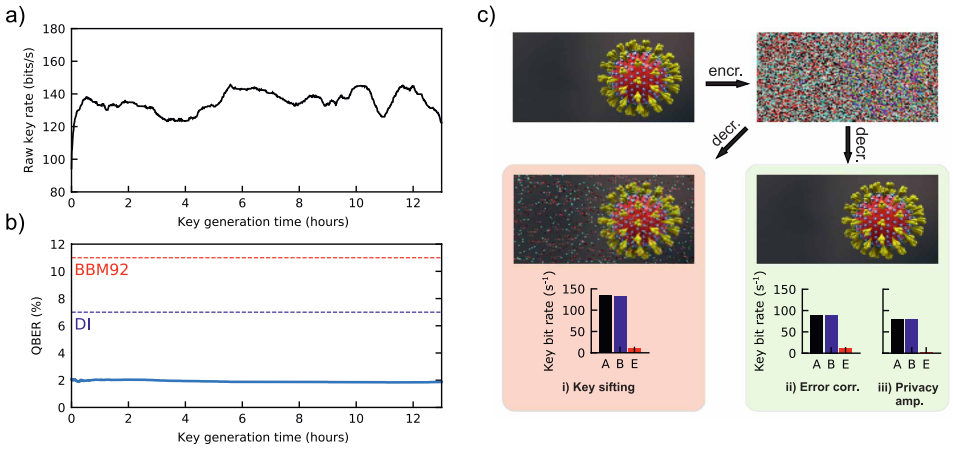


Figure 4.2: **Key generation and post-processing for QKD with entangled photon pairs.** **a)** Raw key rate and **b)** QBER over a time of 13 hours. The dashed lines indicate the upper limits of 11 % for the BBM92 and 7 % for the device-independent protocols. **c)** Exemplary encryption (encr.) of a 29.2-kilobyte large bitmap with Alice's key using the one-time pad method, with subsequent decryption (decr.) with Bob's key. The decrypted bitmaps are shown for cases ***i)*** directly after key sifting and (***ii)*** and ***iii)***) after error correction and privacy amplification. The bar charts indicate the distribution of information over Alice (A), Bob (B), and the eavesdropper (E) after each step.

During SK generation, Alice and Bob permanently monitor the QBER by comparing random subsets of the generated key, which they then discard. The random choice prevents a potential eavesdropper from finding predictable time windows, where he can attack the protocol without being detected. During the standard run of the EQKD protocol, only a negligible part of the SK has to be discarded for QBER monitoring. However, here we aim to record QBER with high frequency and accuracy and therefore we sacrifice 10 % of the transmitted key for its estimation.

The APDs were operated in gated mode with time bin 1 ns, which is approximately four times longer than the X decay time τ_X. This detection window allows us to include $\sim 97\,\%$ of the photons generated by the QD and suppress the number of background photons from the ambient light.

The average raw key is 135 bits/s calculated over a time span of 13 hours as shown by Fig. 4.2. The bit rate of the experiment is mainly limited by the extraction and collection efficiency of the photons emitted by the QD. Additionally, blinking [247, 248] decreases the fraction of the time where the QD is optically active. The QD used here is active only for 30 % of the time. However, blinking is not a fundamental limitation and can be overcome by improving the QD growing technique. The average QBER was 1.91 %, which is close to the theoretically calculated value given by Eq. 4.2-1. The dashed lines in Fig. 4.2 show the maximal acceptable QBER of 11 % for EQKD [101, 244] protocol and 7 % for the device-independent QKD protocol [245], below which it is still possible to distil a SK. We observed a variation of QBER between 1.84 % and 2.06 % over the measurement, which probably stems from slight changes in the fiber environment.

The finite QBER can be reduced by an error correction routine [243, 246, 249], which, however, leaks a negligible part of the SK to the public channel. The number of leaked bits can be estimated by $l = 4Nq + 5\sqrt{12Nq}$ [243], where N is the length of the key and q is the QBER. To erase this leaked information the privacy amplification method is used [249]. It is based on a universal hash function, which Alice and Bob agree on over the public channel. The privacy amplification compresses the SK to a length of $N - l$.

We encrypted a bitmap using 29.2 kB of Alice's key, see Fig. 4.2. The key string was acquired in about 46 min. The bitmap was encrypted by applying the bit-wise XOR operation of the original bitmap and Alice's key. The decryption is done by performing the same operation with the encrypted message and Bob's key. The bar charts in (i) to (iii) depict the distribution of information about the key among Alice (A), Bob (B), and a potential eavesdropper (E) after key sifting, error correction, and privacy amplification, respectively. The resulting SKR here is 86 bits/s with zero QBER.

We demonstrated that QDs under TPE are remarkable candidates for EQKD protocols implementations mainly because of the high fidelity of generated entangled pair and high single-photon purity resulting in low QBER. Exploiting a substantially higher extraction efficiency, increasing the pump rate to 1 GHz, and eliminating blinking [250], raw key rates of hundreds of megabits per second are realistic while leaving the QBER unaltered. By reducing the radiative lifetimes via Purcell enhancement and by using timing hardware and detectors with higher time resolution (like SNSPDs), the pump rate could even be further increased and bring raw key rates of gigabits per second in reach.

5

Methods for "Enhancing quantum cryptography with quantum dot single-photon sources"

The following two chapters introduce the paper titled "Enhancing Quantum Cryptography with Quantum Dot Single-Photon Sources" [52] and provide a more detailed context for it. The research project began as a general interest of two scientists, Mathieu Bozzio and myself, to explore the potential of quantum dots for applications in quantum cryptography. What initially seemed like a straightforward task evolved into a complex problem, leading to the involvement of Prof. Peter Michler's group from the University of Stuttgart and Prof. Vollrath Martin Axt's group from the University of Bayreuth. Thanks to these collaborations, we were able to deliver this comprehensive study.

My contribution: *Together with Mathieu Bozzio, I defined and led the project from its beginning. Initially, I focused on our simulations of QD emission based on 2LS and 3LS using an area theorem approximation, which provided crucial insights for QDC simulations via Lindblad equations. I supported Michael Cosacchi on the QDC model, particularly its implementation under TPE. Alongside Cornelius Nawrath and Simone Luca Portalupi, I interpreted our results from the perspective of quantum dot physics. I also worked with Mathieu Bozzio on part of the security proofs. Finally, I was responsible for the entire data analysis.*

In the paper titled *"Enhancing quantum cryptography with quantum dot single-photon sources,"* we explore how QDs can surpass currently employed sources in quantum cryptography, such as attenuated lasers and SPDC sources [52]. So far, QDs have been valued for their bright emission of high-quality single-photon states, especially beneficial for quantum cryptography applications [55, 68]. However, our publication reveals that QD single-photon sources offer an additional significant advantage through the tuning of PNC via control of the pump laser [52]. This remarkable capability enhances security levels in various quantum cryptography protocols, including QKD, as well as protocols extending beyond QKD, such as QCF [110], QT [31], and QBC [16, 36].

We investigate the performance of the primary QD excitation schemes (RE, LA, and TPE) for quantum cryptography primitives. This chapter provides a summary of the theoretical models employed and delves into a detailed discussion of all results. For a comprehensive understanding of the mathematical tools used in the security analyses of quantum cryptography, refer to Appendix A.

5.1 Quantum dots dynamics and simulations

To describe the maximal performance of realistic QDs in different quantum cryptographic primitives without the influence of experimental imperfections, such as inefficient single-photon coupling or limited filtering of the excitation laser, we decided to simulate QDC by the Jaynes-Cummings model, the system is illustrated by Fig. 5.1. We were studying the QD's emission under three main pumping schemes: RE, LA and TPE.

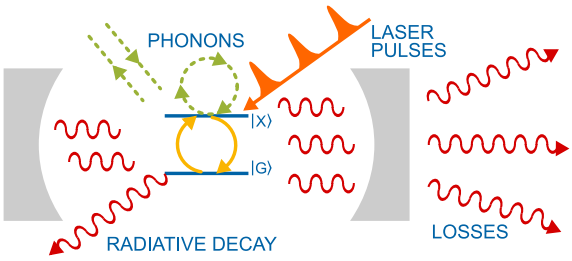


Figure 5.1: **Scheme of the quantum-dot–cavity system.** A QD is represented as a two-level system with a ground state $|G\rangle$ and an exciton state $|X\rangle$ coupled to a lossy single-mode microcavity. The transition $|G\rangle \rightarrow |X\rangle$ is driven by external laser pulses and the $|X\rangle$ is coupled to LA phonons in a pure-dephasing manner. The QD can decay radiatively by photon emission.

The investigated QDC consisting of a laser-driven strongly-confined self-assembled semiconductor QD coupled to a single-mode microcavity influenced by an environment of longitudinal acoustic phonons (Ph) was modelled by the following Hamiltonian

$$\hat{H} = \hat{H}_{\mathrm{QDC}} + \hat{H}_{\mathrm{Ph}} \ . \tag{5.1-1}$$

In this chapter, we will deliver the form of $\hat{H}_{\mathrm{QDC}}$ and $\hat{H}_{\mathrm{Ph}}$ for 2LS and 3LS.

5.1.1 Model of two-level system

QDs are frequently described using the 2LS model. This simplification is applicable when the exciton level energy splitting is not observed. For instance, we assume just a charged exciton, where no splitting is observed, or the FSS vanishes by pumping degenerate neutral exciton by circularly polarized light [251]. In our model, we employ circular light excitation for the neutral exciton.

The considered 2LS consisted of an excited state $|X\rangle$ at energy $\hbar\omega_{\mathrm{X}}$ and a ground state $|G\rangle$ with energy set to zero. Assuming that the cavity supports only a single mode with nearly resonant coupling to the 2LS, the Jaynes-Cummings Hamiltonian can be used. Denoting the frequency of the microcavity mode by ω_{C} and the coupling strength by $\hbar g$, the QDC Hamiltonian in a frame co-rotating with the laser frequency ω_{L} is given as

$$\hat{H}_{\mathrm{QDC}} = \hbar\Delta\omega_{\mathrm{XL}}\,|X\rangle\langle X| + \hbar\Delta\omega_{\mathrm{CL}}\hat{a}^{\dagger}\hat{a} + \hbar g\left(\hat{a}\hat{\sigma}^{\dagger} + \hat{a}^{\dagger}\hat{\sigma}\right) - \hbar\frac{f(t)}{2}\left(\hat{\sigma}^{\dagger} + \hat{\sigma}\right)\ , \quad (5.1\text{-}2)$$

where $\Delta\omega_{\mathrm{XL}} = \omega_{\mathrm{X}} - \omega_{\mathrm{L}}$ is the exciton-laser detuning, $\Delta\omega_{\mathrm{CL}} = \omega_{\mathrm{C}} - \omega_{\mathrm{L}}$ is the cavity-laser detuning, $\hat{a}\,(\hat{a}^{\dagger})$ is the annihilation (creation) operator for a cavity photon, $\hat{\sigma} = |G\rangle\langle X|$ is the QD transition operator. The cavity mode is assumed to be in resonance with the $|X\rangle \rightarrow |G\rangle$ transition, in other words, the cavity-exciton detuning $\Delta\omega_{\mathrm{CX}} = \omega_{\mathrm{C}} - \omega_{\mathrm{X}}$ is equal to zero. The $f(t)$ is the real envelope of the driving laser, which is in our model considered to be Gaussian

$$f(t) = \frac{A}{\sqrt{2\pi}\tau_{\mathrm{G}}}\mathrm{e}^{-\frac{t^2}{2\tau_{\mathrm{G}}{}^2}}\ , \quad (5.1\text{-}3)$$

where A is the pulse area and τ_{G} is the pulse width, which can be used to calculate full width at half maximum (FWHM) as $\tau_{\mathrm{FWHM}} = 2\sqrt{2\ln 2}\,\tau_{\mathrm{G}}$.

The interaction between QD and the phonon environment is modeled by the following Hamiltonian [251–255]

$$\hat{H}_{\mathrm{Ph}} = \hbar\sum_{\mathbf{q}}\omega_{\mathbf{q}}\hat{b}^{\dagger}_{\mathbf{q}}\hat{b}_{\mathbf{q}} + \hbar\sum_{\mathbf{q}}\left(\gamma^{\mathrm{X}}_{\mathbf{q}}\hat{b}^{\dagger}_{\mathbf{q}} + \gamma^{\mathrm{X}*}_{\mathbf{q}}\hat{b}_{\mathbf{q}}\right)|X\rangle\langle X|\ , \quad (5.1\text{-}4)$$

where $\hat{b}_{\mathbf{q}}\,(\hat{b}^{\dagger}_{\mathbf{q}})$ is an annihilation (creation) operator for a phonon with energy $\hbar\omega_{\mathbf{q}}$ in the mode $\mathbf{q}$. The coupling between QD and Ph environment is described by the constant $\omega_{\mathbf{q}}$, which is fully determined by the phonon spectral density $J(\omega) = \mid\ \omega_{\mathbf{q}}\mid^2 \delta(\omega - \omega_{\mathbf{q}})$. In the assumption of harmonic confinement and linear dispersion of mode frequencies $\omega_{\mathbf{q}} = c_s \mid \mathbf{q} \mid$, where c_s is sound velocity, the phonon spectral density can be written as [254]

$$J(\omega) = \frac{\omega\hat{a}^3}{4\pi^2\rho_D\hbar c_s^5}\left(D_e\mathrm{e}^{-\frac{\omega\hat{a}^2 a_e^2}{4c_s^2}} - D_h\mathrm{e}^{-\frac{\omega\hat{a}^2 a_h^2}{4c_s^2}}\right)^2\ , \quad (5.1\text{-}5)$$

where the deformation potential coupling is assumed, as it is the dominant compiling mechanism between electrons-phonons in semiconductor QDs [254]. $D_e\,(D_h)$ is the electron (hole) deformation potential, $a_e\,(a_h)$ is the electron (hole) confinement length and ρ_D is the density of the material. Note that the electronic density matrix is influenced by phonons only via the phonon spectral density $J(\omega)$. For QDs of any shape, it is always possible to obtain a spherical dot model, which generates the identical $J(\omega)$ [256]. Therefore, the smallest dimension of the nonspherical QD has the largest influence on the phonon coupling.

To derive the time evolution of the QDC we have to account for the radiative decay of the QD exciton to the free field outside the cavity with rate γ and cavity losses with rate κ. Both processes are well approximated by a phenomenological Markovian description using Lindblad superoperators acting on a density matrix $\hat{\rho}$, which can be written for general cases as

$$\mathcal{L}_{\hat{O},\Gamma}\,\hat{\rho} = \Gamma\left(\hat{O}\hat{\rho}\hat{O}^{\dagger} - \frac{1}{2}\left\{\hat{\rho}, \hat{O}^{\dagger}\hat{O}\right\}\right) , \tag{5.1-6}$$

where Γ is the decay rate associated with a process described by the operator $\hat{O}$ and $\left\{\hat{A}, \hat{B}\right\}$ denotes the anti-commutator of operators $\hat{A}$ and $\hat{B}$. Now the system dynamics can be finally described by the Liouville-von Neumann equation for the density matrix

$$\frac{\partial}{\partial t}\hat{\rho} = -\frac{i}{\hbar}\left[\hat{H}, \hat{\rho}\right] + \mathcal{L}_{\hat{\sigma},\gamma}\,\hat{\rho} + \mathcal{L}_{\hat{a},\kappa}\,\hat{\rho} , \tag{5.1-7}$$

where $\left[\hat{A}, \hat{B}\right]$ denotes the commutator of operators $\hat{A}$ and $\hat{B}$.

5.1.2 Model of three-level system

As was discussed in the Ch. 3.2.2.3 the XX can decay via two polarization-distinguished cascades. Here, we will assume that these two oppositely polarized modes in the microcavity have a large energetic mismatch and the external driving has a defined linear polarization. Hence, one of the two oppositely polarized exciton states is decoupled from the dynamics. This assumption can be made as long as we are not interested in the entanglement generation by a 3LS. Therefore, including the biexciton state $|XX\rangle$ in this situation amounts to the addition of only one further electronic level and the QDC Hamiltonian can be written as

$$\begin{aligned}\hat{H}_{\mathrm{QDC}} =& \hbar\Delta\omega_{\mathrm{XL}}\,|X\rangle\langle X| + (2\hbar\Delta\omega_{\mathrm{XL}} - E_B)\,|XX\rangle\langle XX| \\ &+ \hbar\Delta\omega_{\mathrm{CL}}\hat{a}^{\dagger}\hat{a} + \hbar g\left(\hat{a}\hat{\sigma}^{\dagger} + \hat{a}^{\dagger}\hat{\sigma}\right) - \hbar\frac{f(t)}{2}\left(\hat{\sigma}^{\dagger} + \hat{\sigma}\right) .\end{aligned} \tag{5.1-8}$$

The QD transition operator now contains both transitions which are optically excited in the QD and can be written as $\hat{\sigma} := |G\rangle\langle X| + |X\rangle\langle XX|$. The phonon coupling strength of the biexciton state is assumed to be twice the one of the single exciton and the interaction Hamiltonian can be straightforwardly written as

$$\hat{H}_{\mathrm{Ph}} = \hbar\sum_{\mathbf{q}}\omega_{\mathbf{q}}\hat{b}^{\dagger}_{\mathbf{q}}\hat{b}_{\mathbf{q}} + \hbar\sum_{\mathbf{q}}\left(\gamma^{\mathrm{X}}_{\mathbf{q}}\hat{b}^{\dagger}_{\mathbf{q}} + \gamma^{\mathrm{X}*}_{\mathbf{q}}\hat{b}_{\mathbf{q}}\right)\left(|X\rangle\langle X| + 2\,|XX\rangle\langle XX|\right) . \tag{5.1-9}$$

Finally, the biexciton is assumed to radiatively decay with twice the exciton decay rate γ. Therefore, the dynamical equation becomes

$$\frac{\partial}{\partial t}\hat{\rho} = -\frac{i}{\hbar}\left[\hat{H}, \hat{\rho}\right] + \mathcal{L}_{|G\rangle\langle X|,\gamma}\,\hat{\rho} + \mathcal{L}_{|X\rangle\langle XX|,2\gamma}\,\hat{\rho} + \mathcal{L}_{\hat{a},\kappa}\,\hat{\rho} . \tag{5.1-10}$$

5.1.3 Methods and parameters

We employ a numerically exact iterative real-time path integral method to solve the Liouville-von Neumann equation for the QDC reduced density matrix $\widetilde{\rho} := \mathrm{Tr}_{\mathrm{Ph}}[\hat{\rho}]$, where the phonon subspace is traced out. Details of the method are explained in [257–259]. We assume a GaAs QD with standard material properties and identical confinement potentials for electrons and holes. The confinement ratio is for GaAs fixed by the effective masses as $a_h = a_e/1.15$. The electron confinement length a_e is then the only free parameter, which scales with the size of the QD. Here, we choose $a_e = 3\,\mathrm{nm}$ which has already produced results in good agreement with the experiment [184, 186, 260].

The biexciton binding energy is set at $E_B = 4\,\mathrm{meV}$, a notably high value for typical QDs. Although it may be hard to find a natural QD with such rather large E_B it always can be achieved by applying biaxial stress [261]. This assumption implies that all photons coupled to the cavity mode originate from the $|X\rangle \rightarrow |G\rangle$ transition. The cavity loss rate is defined as $\kappa = 0.577\,\mathrm{ps}^{-1}$ which implies Purcell enhancement of factor 10 to $|X\rangle \rightarrow |G\rangle$ transition. All relevant QDC parameters used for the calculations are listed in Tab. 5.1.

Quantum dot-cavity coupling	$\hbar g$	$0.05\,\mathrm{meV}$
Biexciton binding energy	E_B	$4\,\mathrm{meV}$
Radiative decay rate	γ	$1\,\mathrm{ns}^{-1}$
Cavity loss rate	κ	$0.577\,\mathrm{ps}^{-1}$
Temperature	T	$4.2\,\mathrm{K}$
Cavity-exciton detuning	$\hbar\Delta\omega_{CX}$	$0\,\mathrm{meV}$

Table 5.1: **Phyiscal parameters used in the simulations.**

For the 2LS, we consider two different excitation conditions (RE, LA). In the RE, the laser is in resonance with the exciton energy, i.e. $\Delta\omega_{\mathrm{XL}} = 0$ and the excitation pulse has the area $A = \pi$. In the LA, the laser is detuned above the exciton energy by $\Delta\omega_{\mathrm{XL}} = -0.9\,\mathrm{meV}$ and the pulse has an area of $A = 10\pi$. In the case of the 3LS, we only consider the TPE of the XX, i.e. $2\hbar\Delta\omega_{\mathrm{XL}} - E_B = 0$.

For every T_{FWHM} chosen for the simulation, first, the pulse area A that achieves unity occupation of the excited state (X/XX) after the excitation is identified. This calibration is done for a standalone QD ($g = 0$), and without any losses ($\gamma = \kappa = 0$).

5.1.3.1 Derivation of photon number populations

To obtain the multiphoton population of the cavity state we calculated the second-order correlation function defined as

$$G^{(2)}(t,\tau) = \langle \hat{a}^\dagger(t)\, \hat{a}^\dagger(t+\tau)\, \hat{a}(t+\tau)\, \hat{a}(t) \rangle \ . \tag{5.1-11}$$

First, we average over the entire pulse sequence to obtain the correlation function dependent only on the time delay argument τ

$$G^{(2)}(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_0^T dt\, G^{(2)}(t,\tau) \ . \tag{5.1-12}$$

Then, we integrate the peak-like structure around $\tau = 0$, which corresponds to the amount of multiphoton contribution within a single pulse of the pulse train, and normalize it to the first uncorrelated side peak. This results in the probability F_2 of having two or more photons during one pulse

$$F_2 = \frac{\int_{-T_{\mathrm{pulse}}/2}^{T_{\mathrm{pulse}}/2} d\tau\, G^{(2)}(\tau)}{\int_{T_{\mathrm{pulse}}/2}^{3T_{\mathrm{pulse}}/2} d\tau\, G^{(2)}(\tau)} \ , \tag{5.1-13}$$

where T_{pulse} is the separation of two subsequent pulse maxima within the excitation pulse train, which corresponds to the inverse repetition rate of the used pump laser. To estimate the probability of three or more photons emission we have to evaluate the third-order correlation function, which is defined as

$$G^{(3)}(t,\tau_1,\tau_2) = \langle \hat{a}^\dagger(t)\, \hat{a}^\dagger(t+\tau_1)\, \hat{a}^\dagger(t+\tau_1+\tau_2)\, \hat{a}(t+\tau_1+\tau_2)\, \hat{a}(t+\tau_1)\, \hat{a}(t) \rangle \ . \tag{5.1-14}$$

Similar to the second-order correlation function we now average over the pulse sequence and get

$$G^{(3)}(\tau_1,\tau_2) = \lim_{T\to\infty} \frac{1}{T} \int_0^T dt\, G^{(3)}(t,\tau_1,\tau_2) \ . \tag{5.1-15}$$

Then, the probability F_3 of having three or more photons during one pulse is calculated in close analogy with the previous as

$$F_3 = \frac{\int_{-T_{\mathrm{Pulse}}/2}^{T_{\mathrm{Pulse}}/2} d\tau_1 \int_{-T_{\mathrm{Pulse}}/2}^{T_{\mathrm{Pulse}}/2} d\tau_2\, G^{(3)}(\tau_1,\tau_2)}{\int_{T_{\mathrm{Pulse}}/2}^{3T_{\mathrm{Pulse}}/2} d\tau_1 \int_{T_{\mathrm{Pulse}}/2}^{3T_{\mathrm{Pulse}}/2} d\tau_2\, G^{(3)}(\tau_1,\tau_2)} \ . \tag{5.1-16}$$

Both $G^{(2)}(t,\tau)$ and $G^{(3)}(t,\tau_1,\tau_2)$ are then calculated numerically following the methods described in [262]. Finally, we define the unnormalized brightness of the QD as

$$\widetilde{\mathcal{B}} = \kappa \int_{t_0-T_{\mathrm{Pulse}}/2}^{t_0+T_{\mathrm{Pulse}}/2} dt\, \langle \hat{a}^\dagger(t) a(t) \rangle \ , \tag{5.1-17}$$

where t_0 is the centre time of the pulse. Just note here that the brightness counts all the emitted photons and is therefore not restricted to a value of 1.

To calculate the probabilities of n-photon emission, we used the following assumptions: $F_4 = 0$ for 2LS and $F_3 = 0$ for 3LS. These assumptions are based on n-photon generation probabilities which scale as $(\gamma T_{\mathrm{FWHM}})^{(n-1)}$ for 2LS [95] and $(\gamma T_{\mathrm{FWHM}})^{2(n-1)}$ for 3LS [96]. Using the correlation functions derived in Eq. 5.1-13 and Eq. 5.1-16, along with unnormalized brightness from Eq. 5.1-17, we inferred the emitted photon number populations $\{p_n\}$ as

$$\begin{aligned} p_1 &= \widetilde{\mathcal{B}} - 2(F_3 - F_2) - 3F_3 \ , \\ p_2 &= F_2 - F_3 \ , \\ p_3 &= F_3 \ , \\ p_{\geqslant 4} &= 0 \ , \\ p_0 &= 1 - p_1 - p_2 - p_3 - p_{\geqslant 4} \ . \end{aligned} \tag{5.1-18}$$

Now the normalized brightness and the single-photon purity can be calculated by standard expressions defined by Eq. 3.0-20 and Eq. 3.0-21, respectively.

5.1.4 Pumping schemes results

In this chapter, we will summarize the results of the QDC numerical simulation for the three main excitation schemes (RE, LA,TPE). To provide a straightforward reference, the outcomes for each excitation scheme are visually represented using a uniform colour code in Ch. 5 and Ch. 6: RE corresponds to BLUE, LA is indicated by YELLOW, and TPE is denoted by GREEN.

The photon number distributions corresponding to the assumed excitation schemes were determined through the numerical solution of the Liouville-von Neumann equations, employing the methods detailed in Ch. 5.1.3.1. The summarized results are shown in Fig. 5.2. In the case of RE, the observed behaviour aligns with expectations outlined in Ch. 3.2.2.1. As the pulse duration increases, the photon number statistics converge toward a Poisson distribution. Consequently, the component p_0 experiences growth, while the two-photon probability p_2 rises due to a more pronounced re-excitation process [95]. Ch. 3.2.2.3 demonstrated that the p_2 component in TPE scales quadratically with pulse length, in contrast to the linear scaling observed for RE [180]. This trend is also demonstrated by our numerical simulations. Previous theoretical expectations described an increase in the vacuum component p_0 with excitation pulse length for TPE, similar to RE [180]. However, our results show the opposite behaviour. We attribute this discrepancy with previous publications to a residual overlap with the X energy level for short pulses, which results in only a partial population of the XX level.

In the case of LA, the photon number probability behaviour is more intricate. For short pulses, the vacuum probability is decreasing and single-photon emission is increasing, which is a consequence of the population inversion boost by the adiabatic undressing process detailed in Ch. 3.2.2.2. Both probabilities reach their

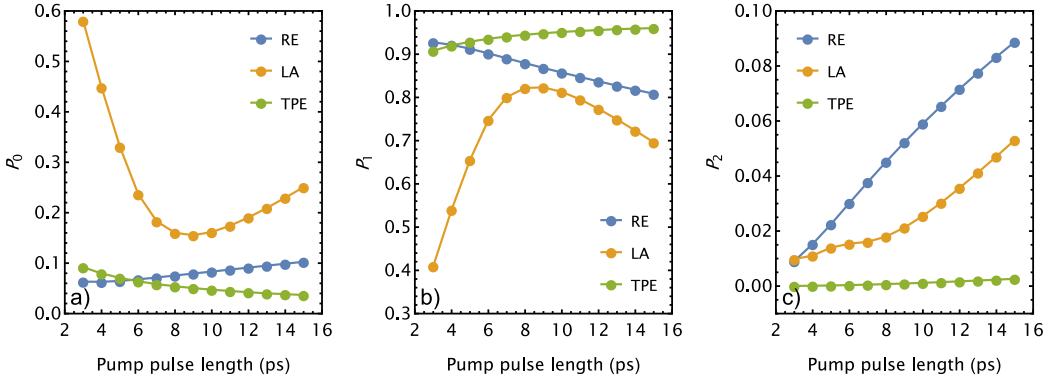


Figure 5.2: **Simulation of photon-number probabilities under different excitation schemes.** Photon-number probabilities for resonant excitation (RE), longitudinal acoustic phonon-assisted excitation (LA) and resonant two-photon excitation (TPE), where the $|X\rangle \rightarrow |G\rangle$ transition is assumed. **a)** vacuum probability p_0, **b)** single-photon probability p_1 and **c)** two-photon probability p_2.

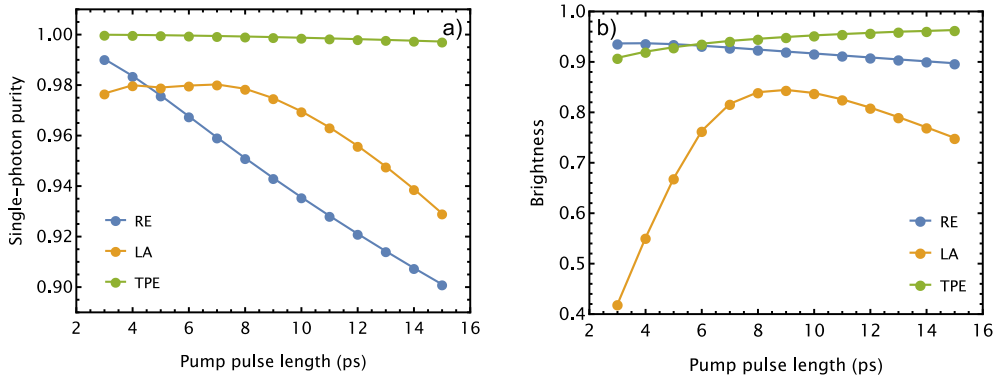


Figure 5.3: **Simulation of single-photon purity and brightness under different excitation schemes. a)** Single-photon purity and **b)** brightness for resonant excitation (RE), longitudinal acoustic phonon-assisted excitation (LA) and resonant two-photon excitation (TPE).

extremes around a pulse length of $\sim 9\,\mathrm{ps}$. With longer pulses, the efficiency of phonon excitation decreases due to lower pulse peak intensity under fixed pulse area conditions and, in general, reduced overlap with the phonon spectral density $J(\omega)$ [91].

The brightness and the single-photon purity can be computed from the photon-number probabilities, as illustrated in Fig. 5.3. Among the three considered excitation schemes, TPE achieves the highest single-photon purity, consistent with expectations from prior studies [180]. Additionally, there is evidence of the suppression of the re-excitation process by the adiabatic undressing in the case of LA, leading to a higher single-photon purity compared to RE. Both resonant schemes

(RE and TPE) attain brightness close to unity in their optimal operational conditions. However, the phonon excitation efficiency constrains the brightness of LA.

As detailed in Ch. 3.0.2.2, accessing photon number probabilities is experimentally challenging. Consequently, the single-photon purity is typically characterized using the second-order correlation function at the zero time delay. The $g^{(2)}(0)$ was calculated as defined by Eq. 3.0-22 from the calculated photon number probabilities, see Fig. 5.4.

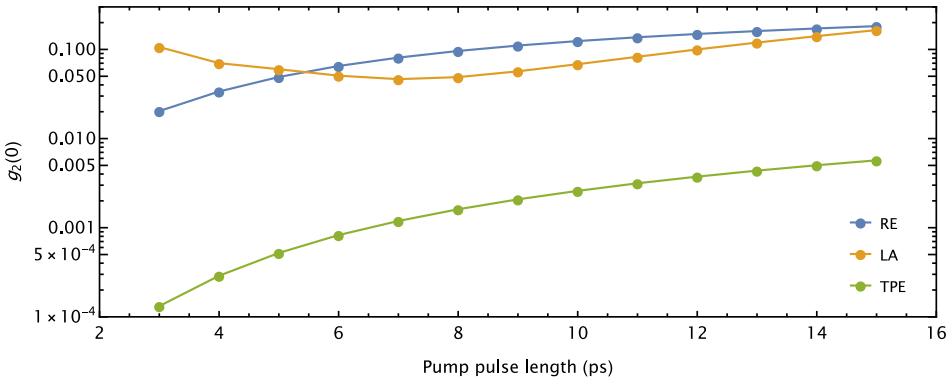


Figure 5.4: **Simulation of $g^{(2)}(0)$ under different excitation schemes.** The second-order correlation function at zero time delay for resonant excitation (RE), longitudinal acoustic phonon-assisted excitation (LA) and resonant two-photon excitation (TPE).

As discussed in Ch. 3.2.2, the excitation schemes also differ in terms of PNC. By tracing out the phonon and the cavity system from the solution of the Liouville-von Neumann equations, we obtain a reduced density matrix describing the generated photonic state, denoted as $\widetilde{\rho}$. In principle, this matrix can be directly used to calculate the state purity in the photon number bases. Unfortunately, in our case, normalizing the components of the reduced density matrix after tracing out the cavity system and summing up the numerical solutions in individual time steps proved challenging. Consequently, the p_n values were computed using correlation functions instead of using the diagonal elements of the reduced density matrix.

However, the relative difference in PNC between $|0\rangle$ and $|1\rangle$, characterized by the matrix element $\widetilde{\rho}_{01}$, can be observed from our numerical calculations. We normalized the element $\widetilde{\rho}_{01}$ by $\sqrt{p_0 p_1}$, where p_0 and p_1 represent photon number probabilities derived using the correlation function approach described in Ch. 5.1.3.1. The results, normalized to one, are summarized in Fig. 5.5.

For RE, the PNC is highest, as expected, and increases with longer excitation pulses. Spectrally narrower pulses exhibit less coupling to decoherence processes, here represented by acoustic phonons. In the case of LA, the coherence is higher for short pulses and then decreases as a consequence of a small spectral overlap between the excitation pulse and X energy level which partially pumps the transition

$|X\rangle \rightarrow |G\rangle$ resonantly. The second maximum is a result of increasing brightness, which consequently increases the error in $\widetilde{\rho}_{01}$ normalization. We assume that, in reality, the values are even lower due to the influence of other decoherence processes, which were not considered in our calculations [86, 263].

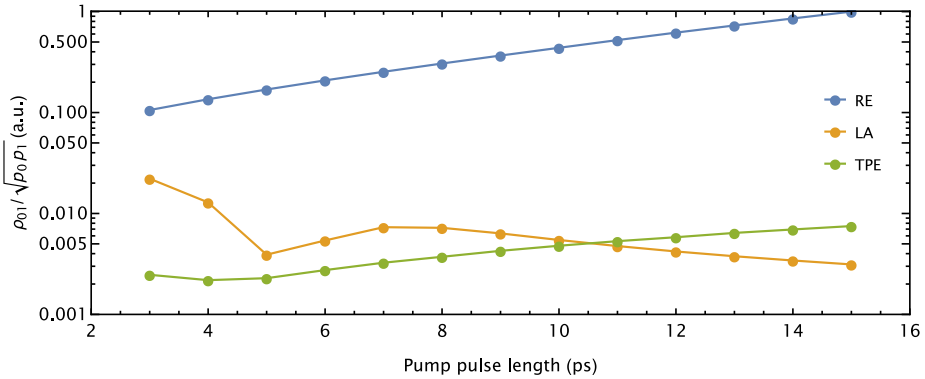


Figure 5.5: **Simulation of coherence between vacuum and single-photon component under different excitation schemes.** The off-diagonal element of reduced density matrix $\widetilde{\rho}_{01}$ normalized by $\sqrt{p_0 p_1}$, where p_0 and p_1 represent photon number probabilities derived using the correlation function approach. The off-diagonal element is plotted for resonant excitation (RE), longitudinal acoustic phonon-assisted excitation (LA) and resonant two-photon excitation (TPE).

		RE	**LA**	**TPE**
Pump pulse length	T_{FWHM}	3 ps	8 ps	12 ps
Pump pulse area	A	π_{RE}	$10\pi_{\mathrm{RE}}$	$\pi_{\mathrm{TPE}} \approx 6.8\pi_{\mathrm{RE}}$
Normalized brightness	B	0.9366	0.8399	0.9526
Single-photon purity	P	0.9903	0.9785	0.9988
Single-photon population	p_1	0.9275	0.8219	0.9514
Two-photon population	p_2	0.0091	0.0180	0.0012
Three-photon population	p_3	10^{-8}	10^{-7}	0

Table 5.2: **Optimal photon number populations for resonant excitation (RE), longitudinal acoustic phonon-assisted excitation (LA) and resonant two-photon excitation (TPE).**

The lowest PNC is observed for TPE, where photon number coherence between vacuum and single-photon contributions should be zero [94, 164]. Here, we assume that the values from short pulses fall below the precision of our normalization method, and the increase is attributed to a growing error with increasing brightness, which has a more pronounced impact at these small values. While our calculation, due to the limits of our normalization method, cannot serve as a

precise study of state purity in photon number bases, we can infer that the PNC between vacuum and single photon is at least two magnitudes lower for TPE and LA compared to RE. Therefore, in the following, we will consider RE photonic states to be maximally pure in number basis, expressed as $\sum_{n=0}^{\infty}\sqrt{p_n}\,|n\rangle$, while LA and TPE states are considered to be maximally mixed in number basis, expressed as diagonal states $\sum_{n=0}^{\infty} p_n\,|n\rangle\langle n|$.

For the following security proofs of quantum cryptographic primitives, an optimal operation point for each pumping scheme was selected based on its brightness and single-photon purity. The optimal photon number probabilities are summarized in Tab. 5.2.

5.1.5 Collection efficiency and state encoding

To evaluate the security of quantum cryptography primitives using realistic quantum light sources, it is essential to mathematically characterize the protocol states, typically the BB84, encoded within the quantum light states emitted by these sources. This chapter provides a summary of the mathematical description of state encoding for PDSs and QDs.

5.1.5.1 Collection efficiency and state encoding for Poisson distributed source

The state generated by PDSs can be modelled by coherent states, which were defined in Ch. 3.0.1.1. As was described in Ch. 2.2.3.4 the encoding of BB84 states in an arbitrary degree of freedom can be expressed by writing a coherent state in two-mode form

$$|\alpha_k\rangle = \left|\mathrm{e}^{i\theta}\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|\mathrm{e}^{i(\theta+\phi_k)}\frac{\alpha}{\sqrt{2}}\right\rangle \ , \tag{5.1-19}$$

where θ is a global phase and we will assume $\theta = 0$ and $\phi_k \in \{0, \frac{\pi}{2}, 2\pi, \frac{3\pi}{2}\}$ is the relative phase between the two modes, which can take one of four values depending on $k \in \{1,2,3,4\}$. The information is, therefore, encoded just with the value of the relative phase and the mapping of qubit states to the two-mode coherent state is given as [122]

$$\begin{aligned} |0\rangle \to |\alpha\rangle \otimes |v\rangle \ , \quad & |1\rangle \to |v\rangle \otimes |-\alpha\rangle \ , \\ |+\rangle \to \left|\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|\frac{\alpha}{\sqrt{2}}\right\rangle \ , \quad & |-\rangle \to \left|\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|-\frac{\alpha}{\sqrt{2}}\right\rangle \ , \\ |+i\rangle \to \left|\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|i\frac{\alpha}{\sqrt{2}}\right\rangle \ , \quad & |-i\rangle \to \left|\frac{\alpha}{\sqrt{2}}\right\rangle \otimes \left|-i\frac{\alpha}{\sqrt{2}}\right\rangle \ , \end{aligned} \tag{5.1-20}$$

where $|v\rangle$ donates the vacuum state. In the following, we will assume BB84 states encoded by the states $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$, which will allow us to focus only on the second mode which contains the relative phase ϕ_k, and thus rewrite these four encoded states as $|\widetilde{\alpha_k}\rangle = |\mathrm{e}^{i\phi_k}\frac{\alpha}{\sqrt{2}}\rangle$, with $k \in \{0,1,2,3\}$ [34, 122]. To avoid

truncating the infinite-dimensional Fock space in our state expressions, we notice that these four specific states may be expressed in a four-dimensional orthonormal basis $\{|b_i\rangle\}$ as

$$\begin{aligned}
|\widetilde{\alpha_0}\rangle &= B_0\,|b_0\rangle + B_1\,|b_1\rangle + B_2\,|b_2\rangle + B_3\,|b_3\rangle \ , \\
|\widetilde{\alpha_1}\rangle &= B_0\,|b_0\rangle + iB_1\,|b_1\rangle - B_2\,|b_2\rangle - iB_3\,|b_3\rangle \ , \\
|\widetilde{\alpha_2}\rangle &= B_0\,|b_0\rangle - B_1\,|b_1\rangle + B_2\,|b_2\rangle - B_3\,|b_3\rangle \ , \\
|\widetilde{\alpha_3}\rangle &= B_0\,|b_0\rangle - iB_1\,|b_1\rangle - B_2\,|b_2\rangle + iB_3\,|b_3\rangle \ ,
\end{aligned} \tag{5.1-21}$$

where the amplitudes B_i are given as

$$\begin{aligned}
B_0 &= \frac{\mathrm{e}^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\cosh\frac{\alpha^2}{2}+\cos\frac{\alpha^2}{2}} \ , \quad & B_1 &= \frac{\mathrm{e}^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\sinh\frac{\alpha^2}{2}+\sin\frac{\alpha^2}{2}} \ , \\
B_2 &= \frac{\mathrm{e}^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\cosh\frac{\alpha^2}{2}-\cos\frac{\alpha^2}{2}} \ , \quad & B_3 &= \frac{\mathrm{e}^{-\frac{|\alpha|^2}{4}}}{\sqrt{2}}\sqrt{\sinh\frac{\alpha^2}{2}-\sin\frac{\alpha^2}{2}} \ .
\end{aligned} \tag{5.1-22}$$

In the case of coherent states with randomly scrambled phase, which were defined in Ch. 2.2.3.4, the globe phase in Eq. 5.1-19 is allowed to take random values from $[0, 2\pi]$ instead of a single one. Therefore the assumption $\theta = 0$ cannot be used and we have to consider also the state $|\mathrm{e}^{i\theta}\frac{\alpha}{\sqrt{2}}\rangle$ in the two-mode representation of the coherent state. By integrating over all possible values of θ, the adversary sees a classical mixture of Fock states given by [264]

$$\frac{1}{2\pi}\int_0^{2\pi} |\sqrt{\mu}\mathrm{e}^{i\theta}\rangle\,\langle\sqrt{\mu}\mathrm{e}^{i\theta}|\,d\theta = \mathrm{e}^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\,|n\rangle\,\langle n| \ , \tag{5.1-23}$$

where we used the definition of the mean photon number $\mu :=| \alpha |^2$. Because the coherent superposition of number states disappears, quantum-cryptographic security proofs can straightforwardly follow the outcomes of quantum non-demolition photon number measurements. In the absence of photons in the state, there is no information content. With a single photon, the qubit security proof can be applied. If there are more than two photons in the wave packet, perfect cheating is assumed. Therefore the randomized coherent states $\hat{\rho}_k$ can be expressed in a 7-orthonormal basis $\{|v\rangle, |q_0\rangle, |q_1\rangle, |m_0\rangle, |m_1\rangle, |m_2\rangle, |m_3\rangle\}$, where $|v\rangle$ is the vacuum state, $|q_0\rangle$ and $|q_1\rangle$ span a qubit space, and $|m_i\rangle$ constitute the four orthogonal outcomes which materialize the four perfectly distinguishable states in the multiphoton subspace. Our four phase-randomized coherent states may then be written as the following density matrices

$$\begin{aligned}
\hat{\rho}_0 &= P_\mu(0)\ |v\rangle\langle v| + P_\mu(1)\ |+\rangle\langle +| + P_\mu(\geqslant 2)\ |m_0\rangle\langle m_0| \ , \\
\hat{\rho}_1 &= P_\mu(0)\ |v\rangle\langle v| + P_\mu(1)\ |+i\rangle\langle +i| + P_\mu(\geqslant 2)\ |m_1\rangle\langle m_1| \ , \\
\hat{\rho}_2 &= P_\mu(0)\ |v\rangle\langle v| + P_\mu(1)\ |-\rangle\langle -| + P_\mu(\geqslant 2)\ |m_2\rangle\langle m_2| \ , \\
\hat{\rho}_3 &= P_\mu(0)\ |v\rangle\langle v| + P_\mu(1)\ |-i\rangle\langle -i| + P_\mu(\geqslant 2)\ |m_3\rangle\langle m_3| \ ,
\end{aligned} \tag{5.1-24}$$

where $\{|+\rangle, |+i\rangle, |-\rangle, |-i\rangle\}$ are the usual $\hat{\sigma}_x$ and $\hat{\sigma}_y$ eigenstates in the qubit space spanned by $|q_i\rangle$, and the Poisson distribution coefficients $P_\mu(n)$ are given by

$$P_\mu(0) = \mathrm{e}^{-\mu} \ , \quad P_\mu(1) = \mu \mathrm{e}^{-\mu} \ , \quad P_\mu(\geqslant 2) = 1 - (1+\mu)\mathrm{e}^{-\mu} \ . \tag{5.1-25}$$

5.1.5.2 Collection efficiency and state encoding for quantum dots

As demonstrated in Ch. 5.1.4, the photon number probabilities in states emitted by QDs do not adhere to any specific mathematical distribution. Therefore, we cannot employ a direct mathematical expression for information encoding, as we did for PDSs. The QDs brightness and state encoding is here modelled by propagation through a setup consisting of one BS and a Mach-Zehnder interferometer, as shown in Fig. 5.6.

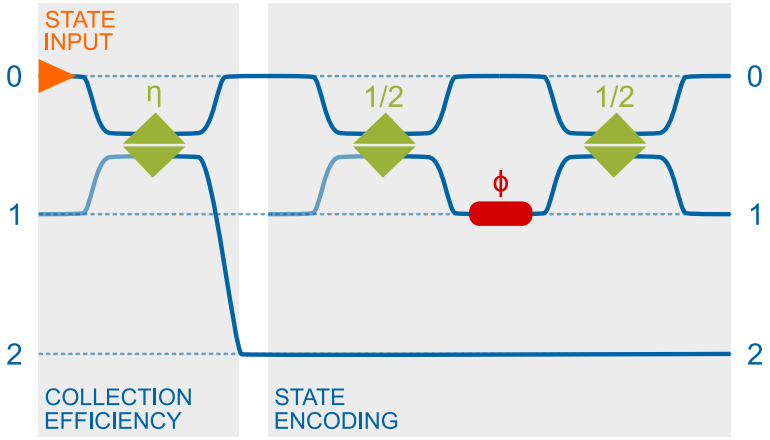


Figure 5.6: **Collection efficiency modelling and state encoding.** The collection efficiency of the quantum dot is modelled as a beamsplitter of reflection η, with two input spatial modes as 0 and 1. The quantum information is then encoded with a Mach-Zehnder interferometer, with tunable phase $\phi \in \{0, \pi\}$ for X eigenstates and $\phi \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ for Y eigenstates.

So far our simulation calculated the emission of almost ideal QDC, where the derived brightness is equal to quantum efficiency as it was defined in Ch. 3.0.2.1. Although the quantum efficiency of QDs is generally close to unity, the effective brightness is significantly constrained by the overall setup efficiency. This efficiency encompasses factors such as the collection efficiency of the emitted state or losses from excitation laser filtering. In our scenario, we modelled the QDs collection efficiency as a beamsplitter of reflectivity η, where the three input spatial modes are labelled as 0, 1 and 2. The standard four protocol states, such as BB84, are then encoded with a Mach-Zehnder interferometer, consisting of two beamsplitters and a tunable phase shifter in one of the interferometer's arms. The phase shift $\phi \in \{0, \pi\}$ corresponds to the Pauli X eigenstates in a two-dimensional Hilbert

space, and the phase shift $\phi \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$ corresponds to the Pauli Y eigenstates in a two-dimensional Hilbert space.

We start with a mathematical description of the building blocks of the model setup. The BS of reflectivity r acting on input modes (k, l) maps the input creation operators $\hat{a}_k^\dagger, \hat{a}_l^\dagger$ onto the output ones $\hat{b}_k^\dagger, \hat{b}_l^\dagger$ linearly as

$$\begin{pmatrix} \hat{b}_k^\dagger \\ \hat{b}_l^\dagger \end{pmatrix} = \hat{H}_{kl}^{(r)} \begin{pmatrix} \hat{a}_k^\dagger \\ \hat{a}_l^\dagger \end{pmatrix} , \tag{5.1-26}$$

where the transformation matrix $\hat{H}_{kl}^{(r)}$ is defined as

$$\hat{H}_{kl}^{(r)} = \begin{pmatrix} \sqrt{r} & \sqrt{1-r} \\ \sqrt{1-r} & -\sqrt{r} \end{pmatrix} . \tag{5.1-27}$$

Similarly, the transformation matrix describing the phase shift operation $\hat{P}_{kl}^{(\phi)}$ acting on input modes (k, l) is defined as:

$$\hat{P}_{kl}^{(\phi)} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\phi} \end{pmatrix} . \tag{5.1-28}$$

The model setup can be then described as a series of the following matrices $\hat{H}_{01}^{(\eta)}\, \hat{H}_{01}^{(\frac{1}{2})}\, \hat{P}_{01}^{(\phi)}\, \hat{H}_{01}^{(\frac{1}{2})}$, where the collection efficiency η model the setup losses and the phase shift ϕ encodes the state. Now, we can propagate the input state through the setup and calculate the output states, the full derivation can be found in the supplementary material of our paper [52]. A general photonic pure state with photon number distribution given by $\{p_n\}$ and input into the spatial mode 0 is defined as

$$|\psi\rangle_{in}^{(\mathbf{c})} = \sum_{n=0}^{\infty} \sqrt{\frac{p_n}{n!}} \left(\hat{a}_0^\dagger\right)^n |000\rangle_{012} , \tag{5.1-29}$$

where the **(c)** superscript denotes coherence in Fock basis for further convenience. The output-encoded state is then given as

$$|\psi_{\eta,\phi}\rangle_{012} = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \sum_{l=0}^{k} c_{nkl}(\eta, \phi) \left(\hat{a}_0^\dagger\right)^{k-l} \left(\hat{a}_1^\dagger\right)^l \left(\hat{a}_2^\dagger\right)^{n-k} |000\rangle_{012} , \tag{5.1-30}$$

where

$$c_{nkl}(\eta, \phi) = \sqrt{\frac{p_n}{n!}} \binom{n}{k} \binom{k}{l} \left(\frac{\eta}{4}\right)^{\frac{k}{2}} (1-\eta)^{\frac{n-k}{2}} \left(1 + \mathrm{e}^{i\phi}\right)^{k-l} \left(1 - \mathrm{e}^{i\phi}\right)^l . \tag{5.1-31}$$

In the following the $\{p_n\}$ take the values from Tab. 5.2 for each excitation scheme. To obtain the actual collected state $\hat{\rho}_{\eta,\phi}^{(\mathbf{c})}$ used in our security analyses, we simply trace out over spatial mode 2

$$\hat{\rho}^{(\mathbf{c})}_{\eta,\phi} = \mathrm{Tr}_2\left(|\psi_{\eta,\phi}\rangle_{012}\langle\psi_{\eta,\phi}|_{012}\right)$$
$$= \mathrm{Tr}_2\left(\sum_{n,m=0}^{\infty}\sum_{k=0}^{n}\sum_{l=0}^{k}\sum_{p=0}^{m}\sum_{q=0}^{p} c_{nkl}(\eta,\phi)c^*_{mpq}(\eta,\phi)\left(\hat{a}_0^\dagger\right)^{k-l}\left(\hat{a}_1^\dagger\right)^{l}\left(\hat{a}_2^\dagger\right)^{n-k}\right.$$
$$\left.|000\rangle_{012}\langle 000|_{012}\,\hat{a}_0^{p-q}\hat{a}_1^{q}\hat{a}_2^{m-p}\right). \tag{5.1-32}$$

Let's look now at a case, where the input state in the spatial mode 0 is mixed. If the photon number distribution of the mixed state is given by $\{p_n\}$ we can define the state as

$$\hat{\rho}^{(\mathbf{nc})}_{in} = \sum_{n=0}^{\infty}\frac{p_n}{n!}\left(\hat{a}_0^\dagger\right)^n|000\rangle_{012}\langle 000|_{012}\,\hat{a}_0^n\,, \tag{5.1-33}$$

where the superscript **(nc)** this time accounts for "no coherence" in Fock basis. The collected state for a mixed input state $\hat{\rho}^{(\mathbf{nc})}_{\eta,\phi}$ can be derived using the same procedure as was applied for the pure state. In essence, we set $n = m$ in Eq. 5.1 -32 and obtain the following state

$$\hat{\rho}^{(\mathbf{nc})}_{\eta,\phi} = \mathrm{Tr}_2\left(\sum_{n=0}^{\infty}\sum_{k=0}^{n}\sum_{l=0}^{k}\sum_{p=0}^{n}\sum_{q=0}^{p} c_{nkl}(\eta,\phi)c^*_{npq}(\eta,\phi)\left(\hat{a}_0^\dagger\right)^{k-l}\left(\hat{a}_1^\dagger\right)^{l}\left(\hat{a}_2^\dagger\right)^{n-k}\right.$$
$$\left.|000\rangle_{012}\langle 000|_{012}\,\hat{a}_0^{p-q}\hat{a}_1^{q}\hat{a}_2^{n-p}\right). \tag{5.1-34}$$

5.2 Quantum cryptography primitives with quantum dots

QDs hold a promise to be nearly ideal single-photon sources [55, 86]. However, their performance in the main quantum cryptography primitives had not been explored until our publication [52]. This chapter presents a summary of the results from the security analyses of the main quantum cryptography protocols for PDSs and QDs. Our primary objective is to compare the performance of QDs under various excitation schemes (RE, LA, and TPE) with the performance of the currently employed single-photon source technology, represented by PDSs (SPDC and WCS) [14]. It is important to note that the single-photon state generated by SPDC and WCS is in both cases mathematically described as a coherent state according to Eq. 2.2-24. Therefore, throughout the following discussions, we will not differentiate between these two technologies and will collectively refer to them as fixed-phase Poisson distributed sources (FP PDSs) when the global phase is fixed, allowing the state to be described by Eq. 2.2-24 as a pure state in the Fock

basis. Conversely, we will use the term randomized-phase Poisson distributed sources (RP PDSs) when the global phase is scrambled, leading to a state that can be described by Eq. 2.2-27 as a mixed state in the Fock basis.

Simulations for QDs under the three excitation schemes are based on methods outlined in Ch. 5.1. For the security analysis, the optimal operational point of each excitation scheme was selected, see Tab. 5.2. The modelling of collection efficiency and state encoding for both PDSs and QDs follows the procedures outlined in Ch. 5.1.5 and the detailed description of the utilized security analysis can be found in Appendix: A.

To be able to compare the performance of PDSs and QDs we define source efficiency

$$\begin{aligned} \eta^{(\mathrm{PDS})} &= 1 - e^{-\mu} \ , \\ \eta^{(\mathrm{QD})} &= 1 - \sum_{n=0}^{\infty} p_n (1-\eta)^n \ , \end{aligned} \tag{5.2-1}$$

where the source efficiency of PDSs, denoted as $\eta^{(\mathrm{PDS})}$, is dependent on the mean photon number μ and the source efficiency of QDs, denoted as $\eta^{(\mathrm{QD})}$, is dependent on the QDs collection efficiency η and photon number populations $\{p_n\}$, which are for each excitation scheme summarized in Tab. 5.2.

5.2.1 BB84 quantum key distribution

QKD is one of the most mature quantum-cryptographic primitives implemented so far [14]. In its simplest form, it allows two parties, Alice and Bob, to establish a secret key over a public quantum channel, provided that a public authenticated classical channel is available. The QKD protocol is described in detail in Ch. 2.2.2.1. To compare the performance of all sources for BB84 QKD, we study the protocol with and without the decoy state countermeasure, assuming one-way classical post-processing [265], refer to Ch. A.2.1 for more details. We fix the parameters of the BB84 QKD protocol as: alignment error rate $e_d = 2\,\%$, dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\,\%$, and error-correcting code inefficiency $f = 1.2$. To assess the protocol's performance as a function of communication distance, we consider a single-mode telecom fiber with standard losses of 0.21 dB/km.

For BB84 QKD without decoy states, we calculated the SKR per pulse using Eq. 2.2-30 and plotted it as a function of source efficiency, collection efficiency, and distance in Fig. 5.7. The graph shows that the SKR reaches a maximum for RP PDSs as a function of source efficiency, beyond which the multiphoton component becomes too significant. In contrast, for QDs, the key rate increases almost linearly with source efficiency, as the vacuum and single-photon components remain dominant across all source efficiencies. At zero communication distance, the SKR generated by QDs surpasses the theoretical maximum of the SKR generated by RP PDSs at threshold collection efficiencies of 32 % for TPE and 36 % for LA.

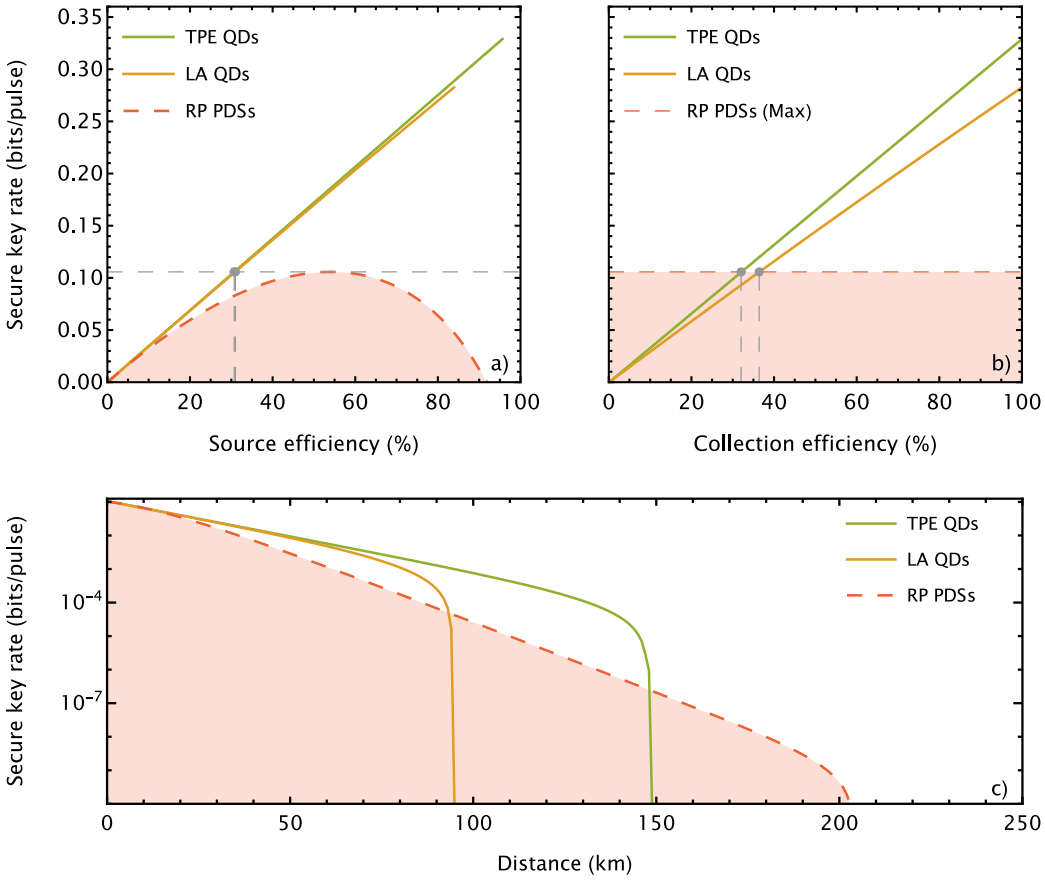


Figure 5.7: **Source comparison for BB84 QKD without decoy states. a)** Simulated secret key rates as a function of source efficiency for LA and TPE QDs, along with randomized-phase (RP) PDSs. **b)** Simulated secret key rates as a function of QDs collection efficiency, compared to the best performance of RP PDSs (dashed line). **c)** Simulated secret key rates as a function of distance. The QDs collection efficiencies were chosen as the intersection points from Fig **b)**.

If we set the collection efficiencies of QDs to their threshold values and examine how the SKR changes with increasing communication loss, we find that RP PDSs achieve longer communication distances compared to QDs. For RP PDSs, we optimize the average photon number μ to maximize the SKR at a given communication loss, as detailed in Ch.2.2.3.4. In contrast, the collection efficiency of QDs remains fixed, so the multiphoton component becomes too significant beyond a certain loss, leading to a fast decrease in SKR. This can be overcome by optimizing the collection efficiency of QDs to achieve the highest SKR at the given loss [63]. Additionally, TPE achieves longer distances than LA due to the higher single-photon purity of the emitted state, as shown in Tab.5.2.

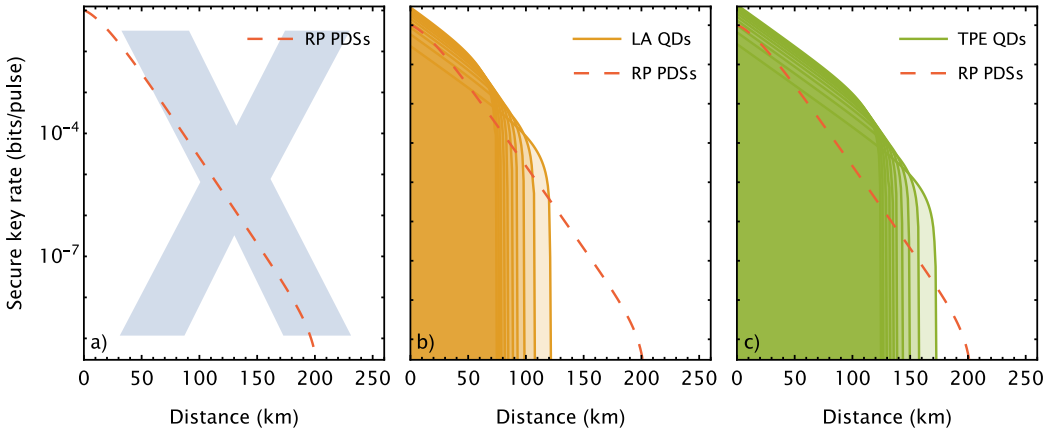


Figure 5.8: **Collection efficiency comparison for BB84 QKD without decoy states.** Simulated secret key rates as a function of distance for **a)** RE QDs **b)** LA QDs **c)** TPE QDs, with collection efficiencies ranging from $\eta = 10\,\%$ (bottom curves) to $\eta = 100\,\%$ (top curves), in steps of $10\,\%$. The optimal performance of randomized-phase (RP) PDSs is also plotted in dashed lines, in order to identify which QDs collection efficiencies are required to overcome PDSs for each pumping.

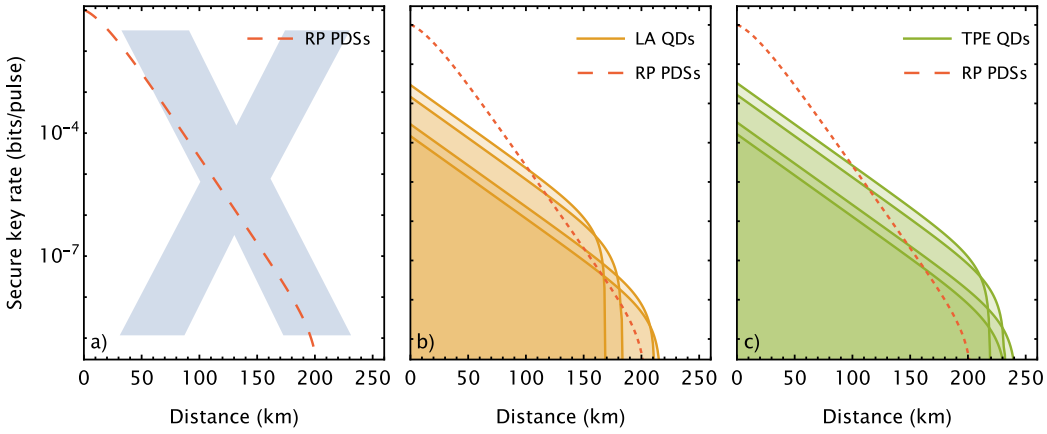


Figure 5.9: **Collection efficiency comparison for BB84 QKD without decoy states for low sources efficiencies $\eta \leq 1\,\%$.** Simulated secret key rates as a function of distance for **a)** RE QDs **b)** LA QDs **c)** TPE QDs, with collection efficiencies: $\eta = 0.05\,\%$ (bottom curves), $\eta = 0.1\,\%$, $\eta = 0.5\,\%$, $\eta = 1\,\%$ (top curves). The optimal performance of randomized-phase (RP) PDSs is also plotted in dashed lines, in order to identify which QDs collection efficiencies are required to overcome PDSs for each pumping.

To analyze how the SKR generated by QDs performs under varying communication losses, we plotted the performance of QDs excitation schemes for collection efficiencies ranging from $10\,\%$ to $100\,\%$ as a function of communication distance,

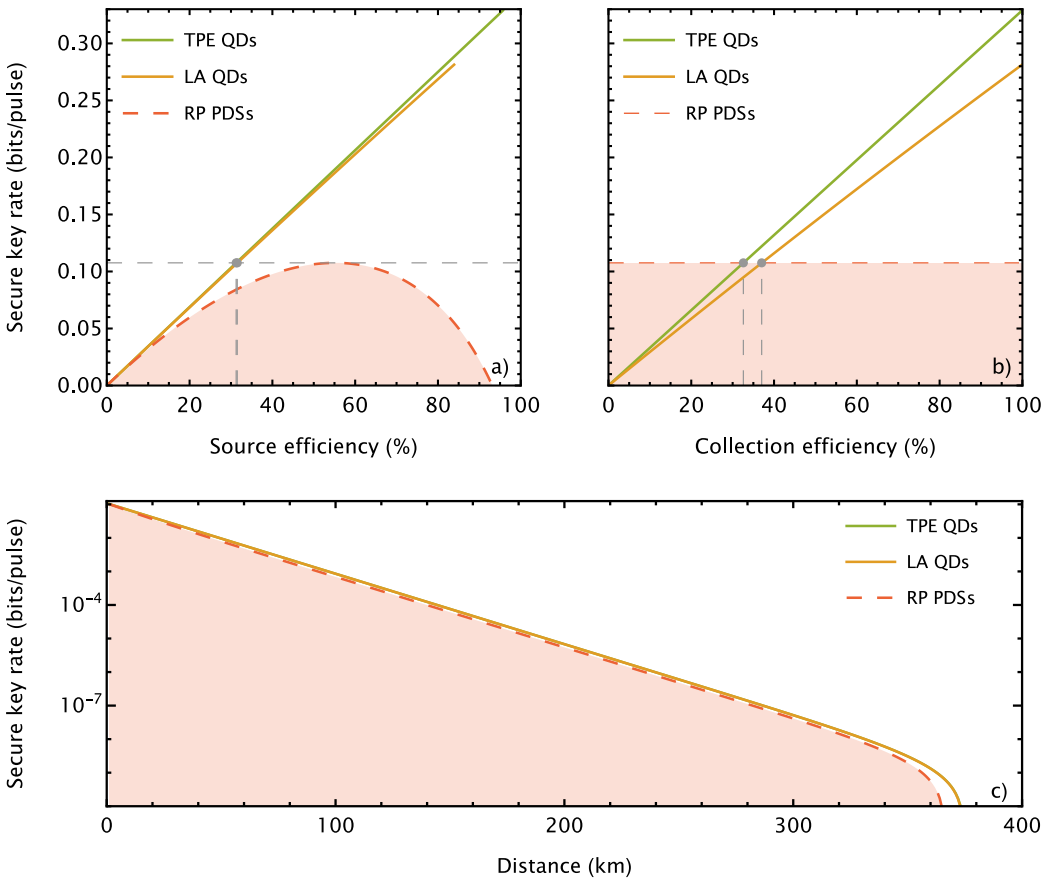


Figure 5.10: **Source comparison for BB84 QKD with decoy states. a)** Simulated secret key rates as a function of source efficiency for LA and TPE QDs, along with randomized-phase (RP) PDSs. **b)** Simulated secret key rates as a function of QDs collection efficiency, compared to the best performance of RP PDSs (dashed line). **c)** Simulated secret key rates as a function of distance. The QDs collection efficiencies were chosen as the intersection points from Fig **b)**.

and compared these results to the best performance of RP PDSs, as shown in Fig. 5.8. We observe that QDs with lower collection efficiencies can achieve longer communication distances because collection losses reduce the multi-photon component. Thus, similar to RP PDSs, optimizing the source efficiency of QDs is essential to maximize SKR at a given communication loss. Even with collection efficiencies as low as 10 %, QDs do not surpass the communication distances achieved by the optimum RP PDSs. However, when examining lower collection efficiencies below 1 %, QDs can surpass the maximum performance of RP PDSs, extending the maximum communication distance by up to 40 km for QDs under TPE. It is important to emphasize that if we optimize the QDs collection efficiency for each communication loss to achieve the maximum SKR, similar to how we optimized the average photon number μ for RP PDSs, then QDs will consistently outperform PDSs. This optimization is explored in our subsequent project [99]; for more information, see Ch. 8 and Appendix: B.

Next, we examined BB84 QKD with decoy states, assuming an infinite number of decoy states and neglecting losses associated with their preparation. We calculated the SKR using Eq. 2.2-37. First, we analyzed how the SKR varies with source efficiency, collection efficiency, and communication distance, as shown in Fig. 5.10. As observed previously, the optimal SKR generated by RP PDSs peaks at a source efficiency of approximately 55 % and then declines. In contrast, the SKR produced by QDs increases almost linearly with source efficiency and surpasses the maximum SKR of RP PDSs at threshold collection efficiencies of 33 % for TPE and 37 % for LA. Consequently, QDs can achieve an SKR up to three times higher than RP PDSs at zero communication distance.

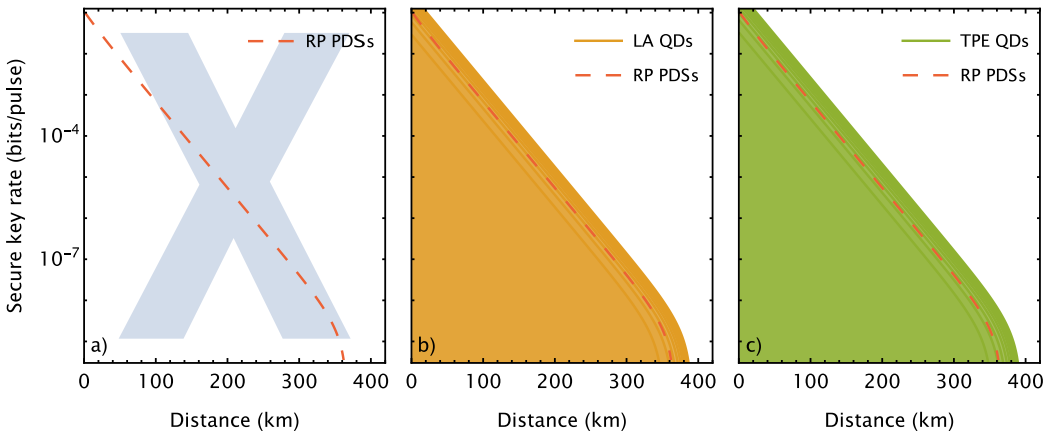


Figure 5.11: **Collection efficiency comparison for BB84 QKD with decoy states.** Simulated secret key rates as a function of distance for **a)** RE QDs **b)** LA QDs **c)** TPE QDs, with collection efficiencies ranging from $\eta = 10\,\%$ (bottom curves) to $\eta = 100\,\%$ (top curves), in steps of 10 %. The optimal performance of randomized-phase (RP) PDSs is also plotted in dashed lines, in order to identify which QDs collection efficiencies are required to overcome PDSs for each pumping.

The decoy-state method helps to mitigate the negative impact of multi-photon contributions on the SKR over communication distance, as discussed in Ch. 2.2.3.5. As a result, QDs do not achieve a significant advantage over RP PDSs in terms of reachable communication distance, despite their high single-photon purity, as shown in Fig. 5.11.

In our analysis, we assumed an infinite number of decoy states and zero preparation losses. However, comparing BB84 QKD with and without decoy states for QDs in a realistic setting is more complex. We aimed to address this comparison and explore whether the decoy-state method can enhance the performance of QD-based QKD protocols in our follow-up work, see Ch. 8.

5.2.2 Twin-field quantum key distribution

TF-QKD was proposed as a new QKD protocol configuration to overcome the repeater-less rate-distance limit of the standard QKD given by Eq. 2.2-3 [115]. This protocol introduces a third untrusted party, Charlie, positioned halfway between Alice and Bob, such that the optical fields sent by each party travel only half of the standard QKD communication distance. As the key bits are extracted from the resulting single-photon interference at Charlie's station, the SKR scales with the square root of the channel transmittance instead of linearly. The security analysis for TF-QKD is detailed in Ch. A.2.2. Here we assume the setup alignment error $e_d = 2\,\%$, duty cycle $d = 1$, number of phase slices $m = 16$, the error due to phase slicing is $e_s = 1.275\,\%$ [115], dark count probability $Y_0 = 10^{-9}$, detection efficiency $\eta_d = 100\,\%$, and error-correcting code inefficiency $f = 1.2$.

To compare the performance of all sources for TF-QKD, we plot the SKR from Eq. A.2-3 as a function of source efficiency, collection efficiency, and distance in Fig. 5.12. Subsequently, in Fig. 5.13, we illustrate the performance of RE QDs across collection efficiencies ranging from 1 % to 100 % and compare these outcomes to the optimal performance achieved by RP PDSs.

It is important to note here that RE is the only excitation scheme suitable for TF-QKD because of the need for global phase reference between Alice and Bob. The other two excitation schemes (LA and TPE) generate a mixed state in photon number bases and therefore the global phase is naturally randomized, see Ch. 3.2.2. Same as for BB84 QKD with decoy states, QDs is not reaching a significant security advantage over RP PDSs with distance if the performance of both sources at zero losses is comparable. Only if RE QDs cross the threshold collection efficiency 29 % the security advantage over RP PDSs is gained.

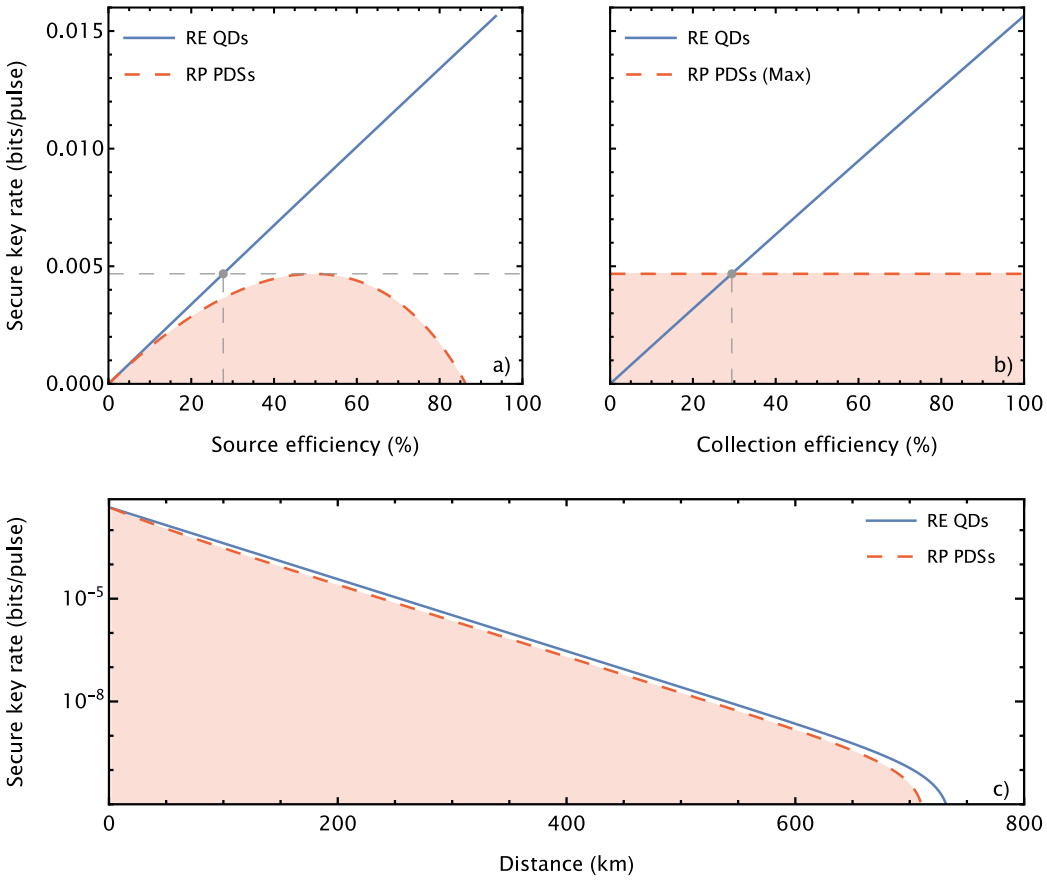


Figure 5.12: **Source comparison for twin-field QKD. a)** Simulated secret key rates as a function of source efficiency for RE QDs, along with randomized-phase (RP) PDSs. **b)** Simulated secret key rates as a function of QDs collection efficiency, compared to the best performance of RP PDSs (dashed line). **c)** Simulated secret key rates as a function of distance. The QDs collection efficiencies were chosen as the intersection points from Fig **b)**.

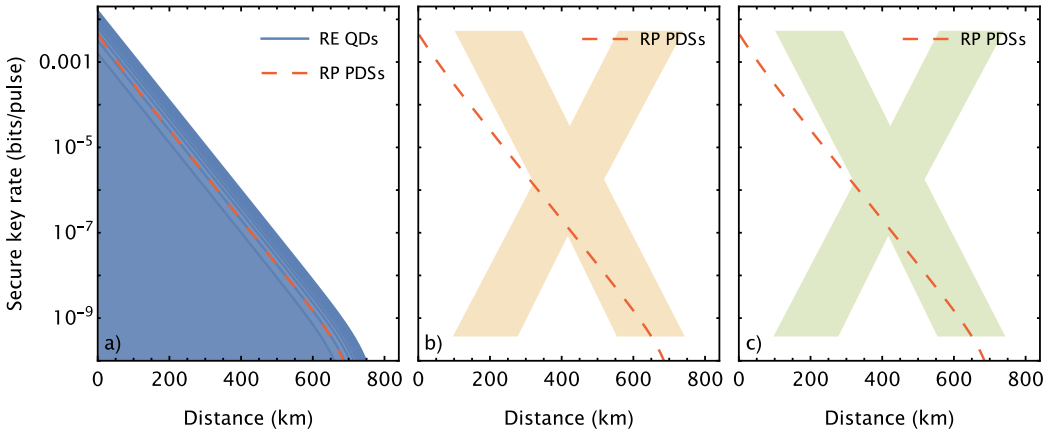


Figure 5.13: **Collection efficiency comparison for twin-field QKD.** Simulated secret key rates as a function of distance for **a)** RE QDs **b)** LA QDs **c)** TPE QDs, with collection efficiencies ranging from $\eta = 10\,\%$ (bottom curves) to $\eta = 100\,\%$ (top curves), in steps of $10\,\%$. The optimal performance of randomized-phase (RP) PDSs is also plotted in dashed lines, to identify which QDs collection efficiencies are required to overcome PDSs for each pumping.

5.2.3 Unforgeable quantum tokens

We consider here the unforgeable QT protocol as described in [122], and we extend its security analysis to the QDs framework in Ch. A.2.3.

To compare the performance of all sources for unforgeable QTs, we numerically solve the problem defined by Eq. A.2-14. In this way, we plot the noise tolerance evolution as a function of source efficiency, collection efficiency, and distance in Fig. 5.14. For PDSs, we observe a peak noise tolerance at source efficiencies around $63\,\%$, corresponding to the average photon number $\mu \approx 1$, before dropping again as the multiphoton contribution becomes significant.

In the case of QDs, we notice a striking difference between schemes with coherence (RE) and those without (LA and TPE). Despite LA having lower quantum efficiency and single-photon purity compared to TPE (as indicated in Tab. 5.2), the noise tolerance as a function of source efficiency is nearly the same in these two cases. This suggests that, in this specific application, PNC is a more critical parameter than brightness or single-photon purity. However, the performance disparity between LA and TPE becomes evident in Fig. 5.14 c), where the noise tolerance is plotted against the collection efficiency. Due to the lower quantum efficiency of LA, this excitation scheme needs a higher efficiency in the collection setup than TPE to surpass the performance of RP PDSs.

Fig. 5.15 compares the performance of each source as a function of distance. Once again, the difference between LA/TPE and RE is significant due to the coherence feature. We notice here that the maximal distance for all sources is much shorter than in QKD schemes since our selected QT scheme bears a maximal

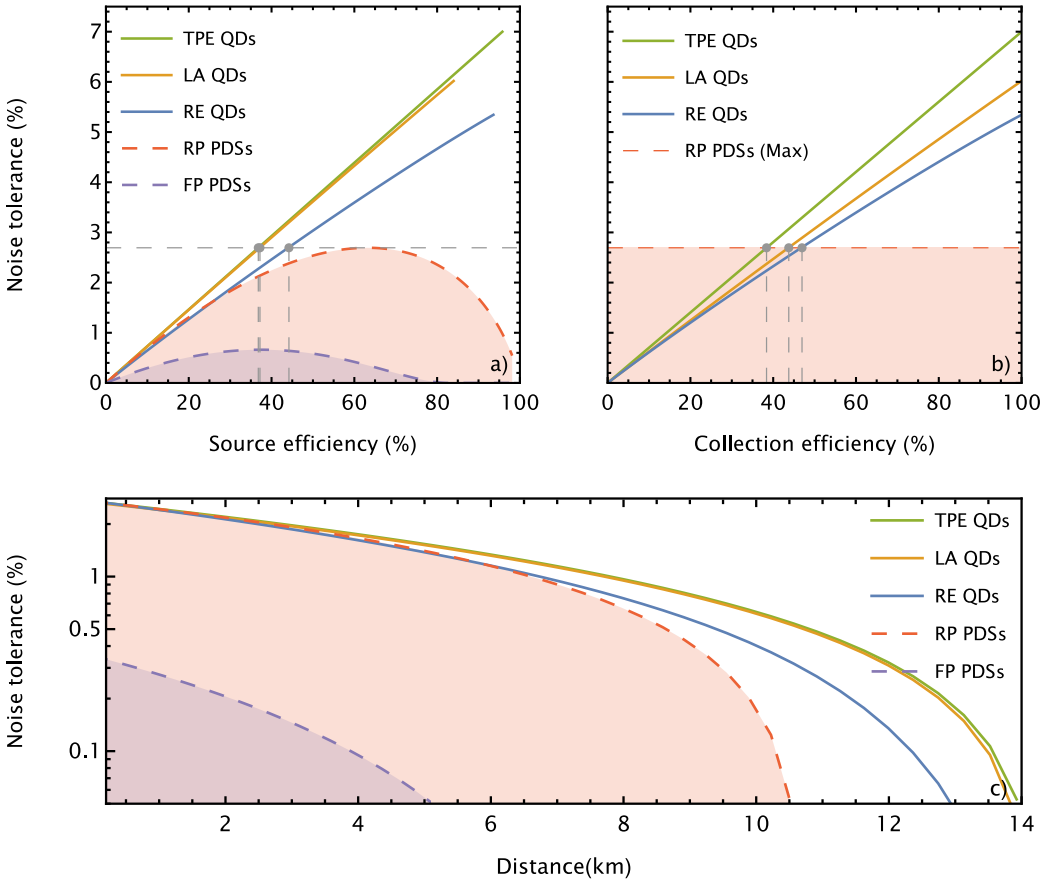


Figure 5.14: **Source comparison for unforgeable quantum tokens. a)** Numerical optimal noise tolerance from Eq. (A.2-14) as a function of source efficiency for RE, LA and TPE QDs, along with fixed-phase (FP) and randomized-phase (RP) PDSs. **b)** Numerical noise tolerance as a function of QDs collection efficiency, compared to the best performance of PDSs (dashed line). **c)** Numerical noise tolerance plotted as a function of distance. The QDs collection efficiencies were chosen as the intersection points from Fig **b)**.

loss tolerance of 50 %, above this limit, an adversary can clone the QT without introducing any errors [122].

The unforgeable QT protocol showcases the clear impact of PNC on its security. This is why we chose it as the model protocol to exemplify the differences in the performance of QDs excitation schemes in our publication [52]. For a more in-depth discussion of these results, refer to Chapter 6, which contains a reprint of the publication.

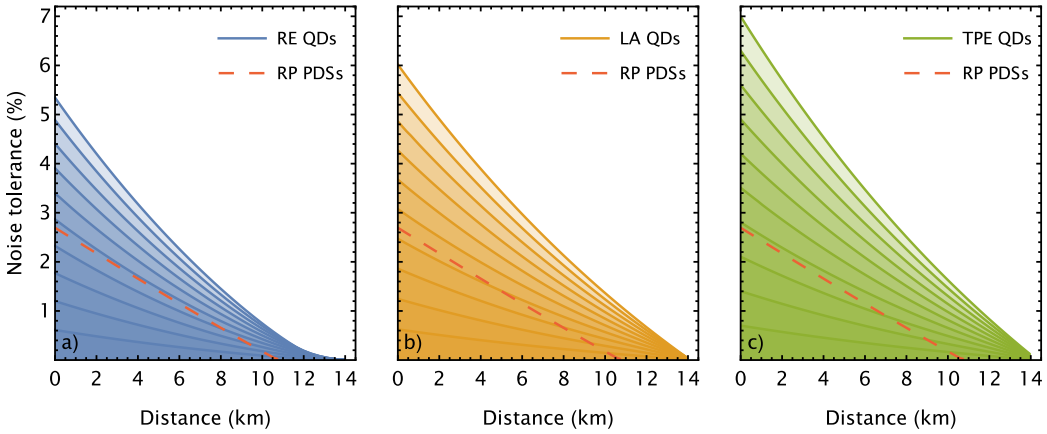


Figure 5.15: **Collection efficiency comparison for unforgeable quantum tokens.** Numerical optimal noise tolerance from Eq. (A.2-14) as a function of distance for **a)** RE QDs **b)** LA QDs **c)** TPE QDs, with collection efficiencies ranging from $\eta = 10\,\%$ (bottom curves) to $\eta = 100\,\%$ (top curves), in steps of $10\,\%$. The optimal performance of randomized-phase (RP) PDSs is also plotted in dashed lines, in order to identify which QDs collection efficiencies are required to overcome PDSs for each pumping. Single-mode telecom fiber losses of 0.21 dB/km are assumed.

5.2.4 Quantum strong coin flipping

We assume here the strong QCF protocol described in [32], we explore the impact of photon number coherence on the protocol's bias within the security proof, see Ch. A.2.4 for details.

In Fig. 5.16 we show how the cheating probability evolves as a function of source and collection efficiencies in a balanced protocol, a protocol where Alice and Bob have equal cheating probabilities. For this example, we fix the number of states to $N = 1000$ and a quantum error rate of $e = 1.5\,\%$, and calculate the subsequent honest abort probability as

$$\mathcal{P}_{ab} = Z + (1 - Z)\,\frac{e}{2}, \tag{5.2-2}$$

where Z is the probability that honest Bob does not register any click after N states have been sent by Alice. To determine where QDs and PDSs reach quantum advantage in terms of cheating probability, we define the optimal classical bound for a balanced strong coin-flipping protocol as [127, 266]

$$\mathcal{P}_c = 1 - \sqrt{\frac{\mathcal{P}_{ab}}{2}}\,. \tag{5.2-3}$$

The cheating probability for RE is likely under-estimated, as our security proof only considers a specific discrimination attack, as detailed in Chapter A.2.4. Conversely, the bounds for excitation schemes without PNC (LA/TPE) are over-estimated, since we relied on the framework from [32], which does not provide

tight bounds on cheating probability. As a result, RE appears to outperform LA, as shown in Fig. 5.16. However, this does not allow us to directly conclude that LA performs worse than RE. For comparable brightness and purity, LA should theoretically perform better than RE, given that optimal attacks in strong QCF protocols typically involve some form of discrimination, which is more effective in the presence of PNC.

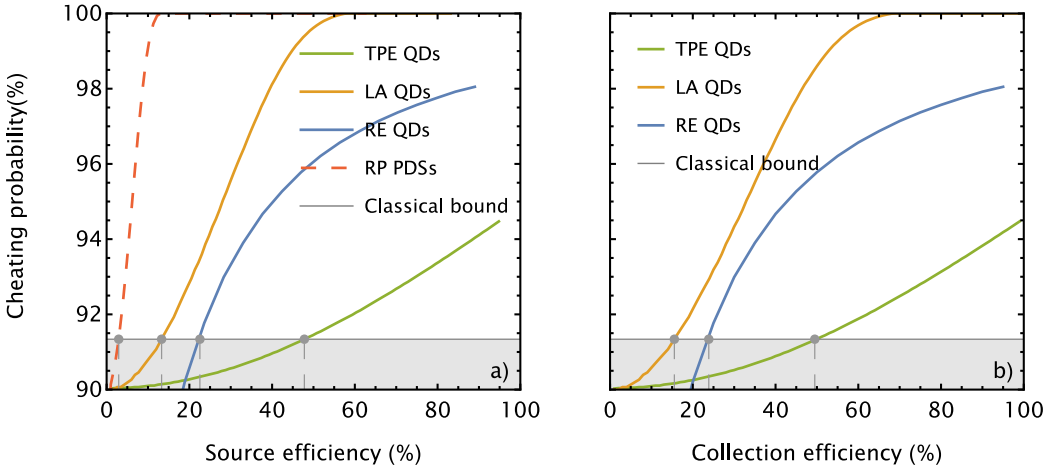


Figure 5.16: **Source comparison for quantum strong coin flipping.** Cheating probability as a function of **a)** source efficiency and **b)** collection efficiency for a balanced protocol with the number of states $N = 1000$, using RE, LA, TPE QDs, and randomized-phase (RP) PDSs. The best achievable classical is plotted in grey dashed lines. As discussed in Ch. A.2.4, note that the upper bounds on the cheating probability for LA and TPE are general and may be over-estimated, while the upper bound for RE considers a specific attack only (i.e., the cheating probability may be higher).

Note that we have not plotted the curves for FP PDSs. For LA, TPE, and RE QDs, the dimension of the Hilbert space is upper-bounded (since $p_n = 0$ for $n >= 3$). For RP PDSs, the required dimension is also upper-bounded, since perfect cheating is assumed for higher photon number terms as defined by Eq. 5.1 -24. On the other hand, deriving the bounds for FP PDSs would imply solving the semidefinite program from Eq. A.2-18 in an infinite-dimensional Hilbert space.

In Fig. 5.17, we show how the cheating probability evolves as a function of distance for various collection efficiencies and a fixed honest abort probability of $\mathcal{P}_{ab} = 2.5\,\%$ (of which $1.5\,\%$ come from the error rate). Since, for PDSs, a given abort probability can be achieved by varying either the number of states N or the average photon number per pulse μ, we choose N to be equal to the number of states required for the best performing QD scheme (TPE). Essentially, the number of states N at a fixed repetition rate defines the time duration of the protocol. Therefore the plots compare QDs to PDSs performance for a fixed protocol duration, and fixed abort probability.

Here, we note the striking feature that QDs performs better at lower collection efficiencies in strong QCF, due to a lower multiphoton component. This is in contrast with other mistrustful quantum cryptography primitives, such as QT, in which the trade-off between brightness and single-photon purity is more crucial.

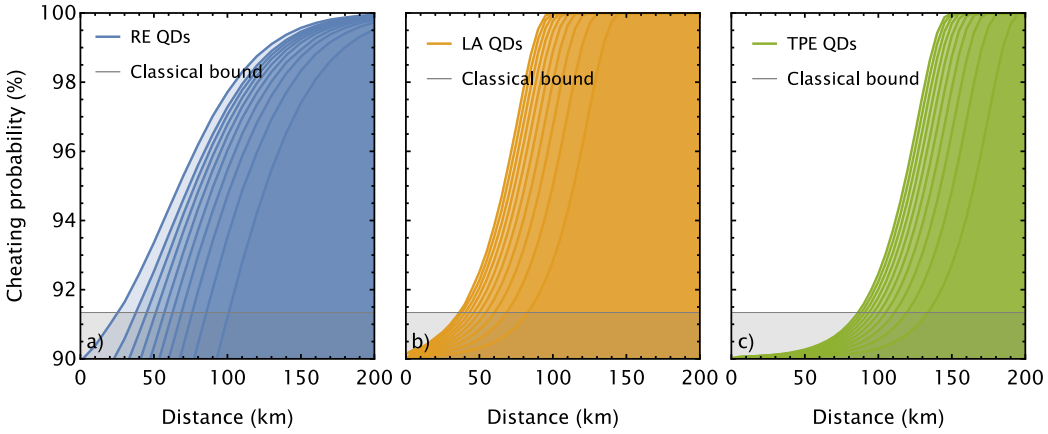


Figure 5.17: **Collection efficiency comparison for quantum strong coin flipping.** Cheating probability as a function of distance for a balanced protocol using **a)** RE QDs, **b)** LA QDs, and **c)** TPE QDs. Where the number of states N are varied for each point to achieve $\mathcal{P}_{ab} = 2.5\,\%$. The best achievable classical bound is plotted in grey dashed lines. Collection efficiencies ranging from $\eta = 10\,\%$ to $\eta = 100\,\%$ are plotted from right to left, in steps of $10\,\%$.

5.2.5 Quantum bit commitment

We assume the QBC protocol from [16], which is secure under a bounded storage assumption. A detailed protocol description can be found in Ch. 2.2.2.4. In Fig. 5.18 and Fig. 5.19, we plot the security condition based on Eq. A.2-22. Following a similar approach to [16], we consider that Alice transmits $N = 10^8$ states, and dishonest Bob's storage size is $S = 972$. Additionally, we assume an error rate of $e = 2\,\%$, detection efficiency of $\eta_d = 100\,\%$, and specific free parameters for Eq. A.2-22 as $\epsilon = 2 \times 10^{-5}$, $\beta = 0.007$, and $\gamma = 0.008$. The security threshold is defined by the zero value of the security parameter.

Once again, the security condition as a function of source efficiency peaks for PDSs, beyond which the multiphoton component becomes excessively significant. In contrast, for QDs, the condition evolves almost linearly with source efficiency because the vacuum and single-photon components dominate at all levels of source efficiency. To surpass PDSs in the QBC protocol, QDs only requires relatively low collection efficiencies compared to other quantum primitives, specifically $17\,\%$ for TPE and $19\,\%$ for LA.

For the QBC protocol, QDs also reaches an interesting distance advantage. If we assume TPE QDs with the threshold collection efficiency $17\,\%$ the QBC will

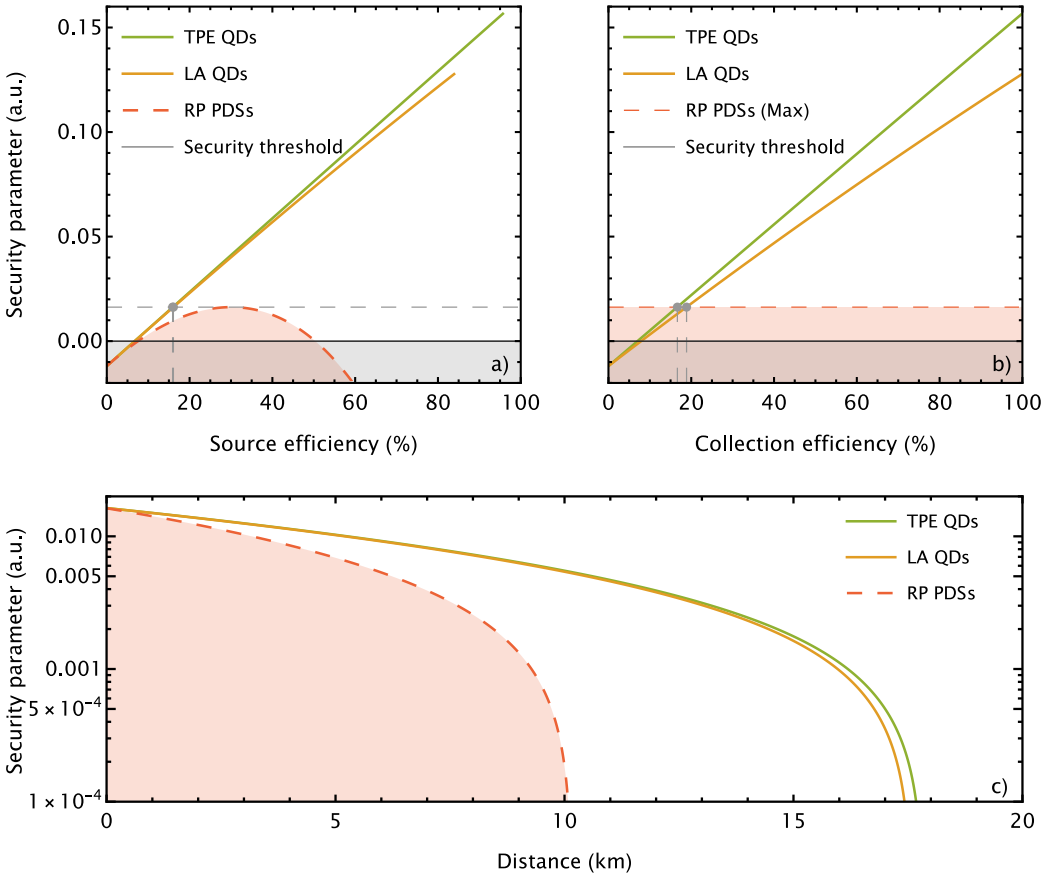


Figure 5.18: **Source comparison for quantum bit commitment under the bounded storage assumption. a)** Security condition as a function of source efficiency for LA and TPE QDs, along with randomized-phase (RP) PDSs. **b)** Security condition as a function of QDs collection efficiency, compared to the best performance of RP PDSs (dashed line). **c)** Security condition as a function of distance. The QDs collection efficiencies were chosen as the intersection points from Fig **b)**.

be secured for distances up to 18 km and at a collection efficiency equal to unity it will be secure up to 53 km. PDSs on the other hand, achieves at best only 10 km of secure operation. Therefore, QBC could be one of the first protocols where QDs will experimentally demonstrate a strong advantage over PDSs.

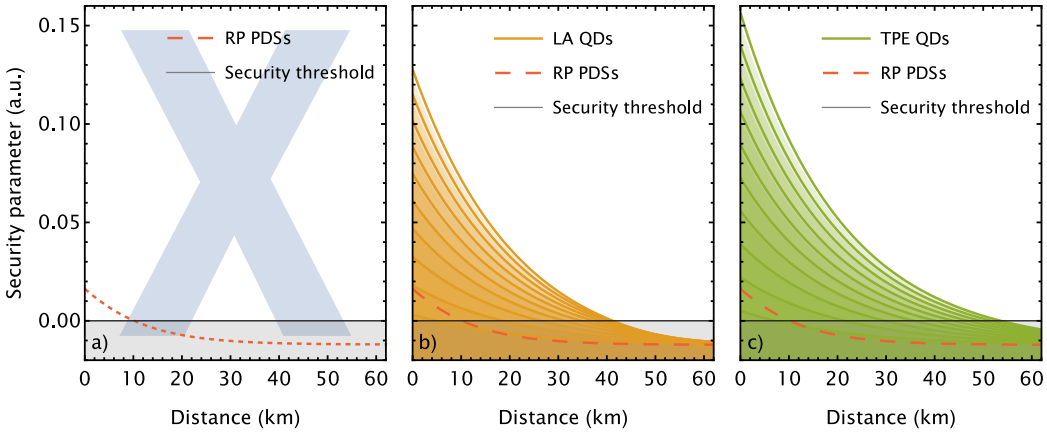


Figure 5.19: **Collection efficiency comparison for quantum bit commitment under the bounded storage assumption.** Security condition from Eq. (A.2-22) as a function of distance for **a)** RE QDs **b)** LA QDs **c)** TPE QDs, with collection efficiencies ranging from $\eta = 10\,\%$ (bottom curves) to $\eta = 100\,\%$ (top curves), in steps of $10\,\%$. The optimal performance of randomized-phase (RP) PDSs is also plotted in dashed lines, to identify which QDs collection efficiencies are required to overcome PDSs for each pumping.

6

Reprint of "Enhancing quantum cryptography with quantum dot single-photon sources"

Quantum cryptography harnesses quantum light, in particular single photons, to provide security guarantees that cannot be reached by classical means. For each cryptographic task, the security feature of interest is directly related to the photons' non-classical properties. Quantum dot-based single-photon sources are remarkable candidates, as they can in principle emit deterministically, with high brightness and low multiphoton contribution. Here, we show that these sources provide additional security benefits, thanks to the tunability of coherence in the emitted photon-number states. We identify the optimal optical pumping scheme for the main quantum-cryptographic primitives and benchmark their performance with respect to Poisson-distributed sources such as attenuated laser states and down-conversion sources. In particular, we elaborate on the advantage of using phonon-assisted and two-photon excitation rather than resonant excitation for quantum key distribution and other primitives. The presented results will guide future developments in solid-state and quantum information science for photon sources that are tailored to quantum communication tasks.

6.1 Introduction

With the rise of quantum algorithms capable of breaking modern encryption schemes, there follows a global response to search for stronger security levels [8–10]. While the security of most current schemes relies on the complexity of solving difficult mathematical problems, quantum-mechanical laws can provide security against adversaries endowed with unlimited computational power for some tasks [14, 267]. This type of security, known as information-theoretic security, motivates research towards a quantum internet [27].

Modern communication networks rely on a handful of fundamental building blocks, or cryptographic primitives [13, 268]. These can be combined with one another to provide security in various applications such as message encryption, electronic voting, digital signatures, online banking, anonymous messaging, and

software licensing, to name a few. In order to reach information-theoretic security through quantum primitives, information is typically encoded onto quantum properties of light, such as photonic path, time-bin, polarization, and photon number [14]. In the quantum realm, the uncertainty principle then ensures that any eavesdropper attempting to access quantum-encoded information, while unaware of the preparation basis, will alter the quantum states in a way that is detectable by the honest parties [113, 267].

For such quantum primitives, it is expected that QDs-based single-photon sources can excel by generating photons on-demand, with high brightness and low multiphoton contribution [86, 269]. In fact, source brightness is crucial in achieving high-speed quantum communication [29, 270], while low multiphoton contribution minimizes information leakage to a malicious eavesdropper [30]. In contrast to these on-demand single-photon sources, widely used PDSs, such as attenuated laser states [14] and spontaneous parametric down-conversion [35], suffer from a stringent trade-off between high brightness and low multiphoton emission. Despite elaborate countermeasures proposed to overcome this trade-off [15, 132], the distance and rate of secure quantum communication can be increased using on-demand single-photon sources.

Some pioneering works have already implemented instances of QKD employing QDs [63–69, 271, 272] or other single-photon sources [50, 273], comparing their performance to PDSs in terms of SKR. In these works, brightness and purity are the sole figures of merit used to establish a comparison, while the additional tuning capabilities of QDs and their role in quantum cryptography have not yet been investigated.

In this work, we explore novel features of QDs to enhance the performance and security of quantum-cryptographic primitives, with an emphasis on telecom wavelengths. We first optimize and compare the brightness and single-photon purity of three main optical pumping schemes, using realistic intra-cavity simulations of QD dynamics. We then show how PNC generated from QDs, experimentally demonstrated in [97], can be erased or preserved to boost the performance of practical QKD, and match its fundamental security requirements [132, 274]. We further explain how the field of mistrustful quantum cryptography [13, 268], not yet implemented with QDs, can significantly benefit from this new feature. Our findings are designed to bridge the gap between the quantum dot and quantum cryptography communities: we optimize and benchmark QDs optical pumping schemes for four main quantum cryptographic primitives, exploiting the combined advantage of brightness, single-photon purity, and photon-number coherence. The studied primitives include quantum key distribution (standard BB84, decoy and twin-field) [14, 15, 114, 115], unforgeable quantum tokens [18, 31, 116], quantum strong coin flipping [19, 32, 117], and quantum bit commitment [16, 17, 36] under storage assumptions.

6.2 Results

6.2.1 Comparison of pumping schemes

Solid-state single-photon sources can be excited under different optical pumping schemes, and we aim to provide a fair comparison of their performance for quantum cryptography. Using realistic intra-cavity simulations for GaAs-based QD, we calculate the emitted photon-number occupations up to three photons for RE, LA and TPE. In Fig. 6.1, we then compare each scheme's brightness and single-photon purity, and estimate the full-width-at-half-maximum excitation pulse length which maximizes both properties (marked with black symbols).

RE schemes are based on resonant excitation of a 2LS [87, 177, 275]. The spectral degeneracy of the excitation laser and the emitted photons usually imposes separation based on polarization filtering, which may cause significant collection losses of around 50 % [189,275]. Other methods, exploiting dichromatic pumping or trion recombination in asymmetric cavities however, can overcome such limitations [187,188]. Since RE exhibits Rabi oscillations of the excitonic state populations, its brightness and single-photon purity are susceptible to pump power fluctuations—thus presenting challenges for quantum network applications [276]. As we show in Fig. 6.1. (a)., for a fixed RE π-pulse area, single-photon purity decreases with pulse length due to re-excitation processes, while brightness decreases as the emission statistics tend to a Poisson distribution [95, 96].

The main limitations of RE may be overcome by using LA excitation schemes. Here, the pump energy is slightly higher than the relevant excitonic transition, and the fast emission of a longitudinal acoustic phonon precedes the population of the excited state. Due to this additional incoherent step, Rabi oscillations vanish, and the purity of the emitted single photons becomes less sensitive to small pump power fluctuations [277]. Recently, it was shown that LA excitation can reach even smaller multiphoton components than its RE counterpart [91], while still enabling spectral filtering of the pump [90, 278]. As regards to brightness, Fig. 6.1. (b). displays an increase with pulse length, as was experimentally demonstrated in [90]. With longer pulses, however, the peak intensity decreases for a fixed pulse area, thus lowering the efficiency of the phonon excitation process.

RE and LA multiphoton contributions can be greatly reduced by addressing the exciton-biexciton cascade through TPE schemes, usually employed to generate spectrally-separated entangled photon pairs. Here, the re-excitation probability scales quadratically with the pulse length, as opposed to linearly in the resonantly-driven RE scheme [96], which can reduce multiphoton emission by several orders of magnitude [279]. Moreover, TPE offers the possibility to overcome the collection efficiency limitations of RE: the spectral separation of the generated photons allows for frequency filtering of the pump laser [182], avoiding the polarisation filtering losses. We show in Fig. 6.1. (c). that the brightness is low for short pulse lengths, due to a remaining overlap with the exciton transition, causing the biexciton level to be only partially populated. Although the emitted exciton polarization

is random, which would limit the brightness to half the values of Fig. 6.1. (c)., recent works have shown the possibility of deterministically preparing the exciton polarization with near-unit brightness by adding a stimulated biexciton excitation after the original two-photon excitation [93, 280, 281].

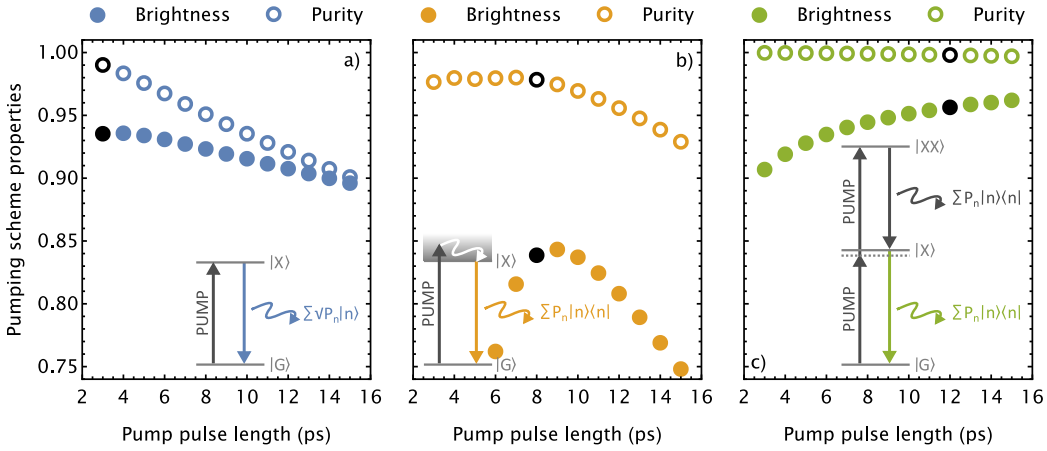


Figure 6.1: **Simulation of emission properties under different pumping schemes.** Simulated brightness and single-photon purity for individual pumping schemes calculated from our numerical model (see Methods) for (a) resonant excitation (RE) between ground $|G\rangle$ and exciton $|X\rangle$ states, (b) longitudinal phonon-assisted excitation (LA) (c) two-photon excitation (TPE) between ground $|G\rangle$ and biexciton $|XX\rangle$ states. Insets show a schematic representation of each pumping scheme (the upper grey area in the LA sketch represents the vibrational quasi-continuum of the exciton state). Optimal FWHM pulse lengths are marked with black disks and circles, chosen pulse areas for maximum population inversion are π_{RE} for RE and π_{TPE} for TPE, while we choose $10\pi_{\mathrm{RE}}$ for LA. Simulation parameters are: dot-cavity coupling $\hbar g = 50\,\mu\mathrm{eV}$, radiative decay rate $\hbar\gamma = 0.66\,\mu\mathrm{eV}$, cavity loss rate $\hbar\kappa = 379\,\mu\mathrm{eV}$ (yielding a Purcell factor of $P = 10$), initial system temperature $T = 4.2\,\mathrm{K}$, electron confinement length 3 nm, and material properties typical for GaAs. Throughout the paper, we assume that photonic states are maximally pure in the photon-number basis for RE, i.e. expressed as $\sum_{n=0}^{\infty}\sqrt{p_n}\,|n\rangle$, while they are expressed as diagonal states for LA and TPE, i.e. as $\sum_{n=0}^{\infty} p_n\,|n\rangle\langle n|$.

6.2.2 Photon-number coherence

We now discuss the presence of coherence in the photon-number basis, a usually disregarded feature of interest, under each excitation scheme. For PDSs such as attenuated laser states, this quantity refers to a fixed phase relationship between the various Poisson-distributed number states. For QDs, this will materialize as a coherent superposition of vacuum, single and two-photon states.

In RE, it was experimentally demonstrated in [97] that the coherently-driven Rabi oscillations translate into emitted PNC: values of coherence purity as high as 96 % for π-pulse areas were measured. On the other hand, this coherence can gradually vanish as the pump is detuned from resonance in LA schemes, along with

the vanishing of Rabi oscillations [91, 98]. Our QD dynamics simulations support these findings: for the optimal pulse lengths of Fig. 6.1, the normalized off-diagonal density matrix elements of LA between the vacuum and single-photon components are around 10 times smaller than the RE ones. Accordingly, we will assume in this work that states emitted under RE are pure in photon-number basis, while those emitted under LA present vanishing off-diagonal elements.

In TPE, our simulation results display off-diagonal elements around 20 times smaller than the RE ones. Although the biexciton level follows Rabi oscillations under resonant TPE [182, 279], loss of coherence arises from a radiative decay between the biexciton to exciton state, which creates a timing jitter similar to the phonon-induced jitter in LA schemes. We will therefore also assume that states emitted under TPE present vanishing off-diagonal elements. Note that this assumption is expected to hold for the stimulated schemes discussed in [93, 280, 281], since the remaining jitter due to the biexciton-exciton transition is significantly larger than the jitter responsible for coherence erasure.

6.2.3 Practical sources and security

We now discuss the role of brightness, single-photon purity and PNC in quantum primitives involving two parties, exchanging a sequence of classical and quantum (photonic) messages that do not rely on quantum entanglement. Each of these primitives achieves a different functionality within quantum networks, and thus also requires its own security figure of merit.

The main efficiency limitations of PDSs may be understood upon inspection of the generated state $\sum_{n=0}^{\infty} C_\mu(n)|n\rangle$, where the $P_\mu(n) = |C_\mu(n)|^2$ coefficients follow a Poisson distribution with average photon number μ, and $\{|n\rangle\}$ span the photon-number basis. Increasing the source brightness (i.e., increasing μ) comes at the cost of increasing the multiphoton components $n \geqslant 2$, which renders the respective quantum primitive vulnerable to attacks involving photon number splitting on lossy channels [30]. Thus, μ is typically kept very low in quantum-cryptographic implementations, in the range $\mu{\sim}0.005{-}0.5$ [14, 31, 32, 36], which limits the communication rate. On the other hand, single-photon purity in QDs can be increased without an intrinsic penalty on the multiphoton component. Achieving higher QDs brightness is then ultimately a technological challenge, limited by the collection efficiency of the source [188, 269], and not a fundamental limitation as in the case of PDSs.

In contrast to their PDSs counterparts, QDs have not yet been optimized to suit the security requirements of quantum primitives. Most importantly, a main assumption behind the implementation of decoy QKD and other primitives is that the global phase of PDSs must be actively scrambled, to effectively destroy the coherence in the number basis [132, 274]:

$$\sum_{n=0}^{\infty} C_\mu(n)|n\rangle \xrightarrow[\text{scrambling}]{\text{phase}} \sum_{n=0}^{\infty} P_\mu(n)|n\rangle\langle n|\,. \tag{6.2-1}$$

Under this assumption, the adversary's cheating strategy is restricted to performing an attack conditioned on the photon-number content of each pulse. Many works rely on this feature to prove the security of quantum primitive implementations [14, 15, 31, 32, 115].

Achieving phase randomization with active phase modulation or laser gain switching imposes practical limitations of a few GHz on repetition rates [29, 51]. These limitations, combined with the low values of μ required due to fundamental PDSs source statistics, can bring effective communication rates down to a few MHz. Unwanted remnants of coherence in the number basis, furthermore, can be exploited for a large spectrum of attacks, using USD for instance [33, 34]. In contrast, as discussed in this work, QDs can be excited in such a way that this coherence is intrinsically suppressed, thus circumventing the need for active phase scrambling. With demonstrated Purcell-enhanced photon lifetimes of tens of picoseconds [188, 282] and source efficiencies now beyond the 50 % level [188], QDs have the potential to enable secure communication rates of tens of GHz [270], i.e. around 3 orders of magnitude higher than effective PDSs communication rates. This is not only true for QKD but for many quantum primitives as shown in the following sections.

6.2.4 Quantum key distribution

A few decades after the birth of QKD [267], experimentalists started demonstrating that QDs with low collection efficiencies can already outperform PDSs in terms of SKR [63–66]. We first show that, while this is true for standard QKD implemented *without* the decoy-state countermeasure, beating PDSs with decoy states [15] requires much higher QDs collection efficiencies at an equal repetition rate. Our results, based on the optimal performance of pumping schemes in Fig. 6.1, are displayed in Fig. 6.2: without decoy states (a), QDs with collection efficiency 1 % are enough to outperform PDSs after 100 km, while infinite decoy schemes (b) require at least 30 %. We should emphasize, however, that this benchmark must be scaled by a repetition rate factor for QDs which could achieve considerably higher repetition rates than phase-randomized PDSs. Any state preparation losses, including modulator losses, can be absorbed in the QDs collection efficiency, and the resulting key rate inferred from Fig. 6.2. Comparisons can also be established using a finite (and different) number of decoy intensities for QDs and PDSs.

The optimal pumping scheme for QKD then follows from Eq. 6.2-1: the states' global phase must be uniformly randomized [132, 274], which implies that standard and decoy-state QKD should only be implemented with LA and TPE. Any remaining PNC will lead to a decrease in the SKR, as shown in [274].

TF-QKD, on the other hand, requires two states, generated by Alice and Bob, to interfere on an untrusted party's beamsplitter [114, 115]. This forces Alice and Bob to scramble the global phase of their states in an active manner (using a modulator for instance), such that they can record their original fixed phase en-

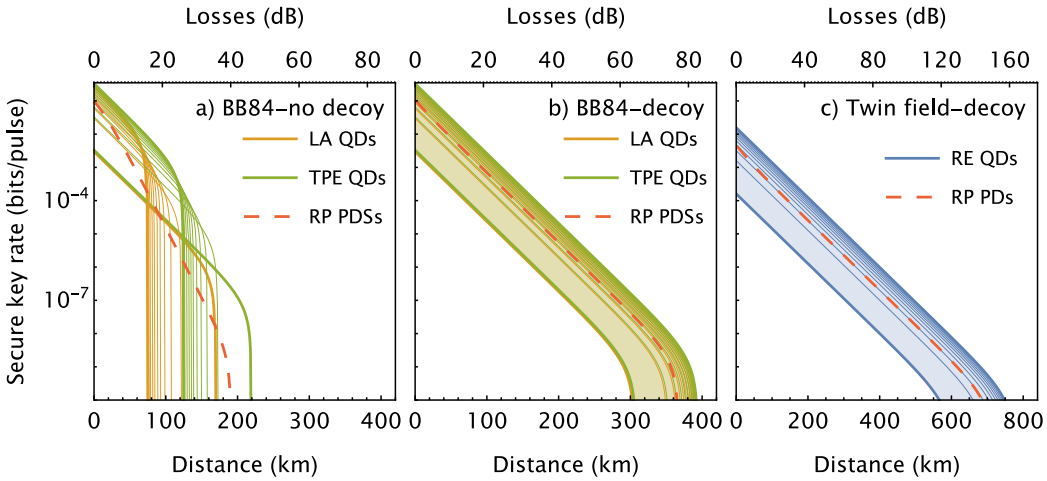


Figure 6.2: **Source comparison for three main QKD schemes.** Simulated secret key rates using one-way classical post-processing [265,283] for (a) BB84 without decoy states, (b) BB84 with infinite decoy states, (c) twin-field with infinite decoy states. The continuum in each plot shows the attainable key rates for QDs ranging from 1 to 100 % collection efficiencies, with intermediate curves showing steps of 10 %. The dashed line indicates the optimal performance of randomized-phase (RP) PDSs. For QDs, pulse lengths were chosen to simultaneously maximize the brightness and single-photon purities from Fig. 6.1: 3 ps for RE, 8 ps ps for LA, 12 ps ps for TPE. Chosen pulse areas: π_{RE} for RE, $10\pi_{\mathrm{RE}}$ for LA, π_{TPE} for TPE. photon-number populations $\{p_n\}$ up to $n = 3$ were inferred from the subsequent values of brightness and single-photon purity. Parameters for all plots are: $e = 2\,\%$ single photon error rate, 0.21 dB/km single mode telecom fiber losses, $Y_0 = 10^{-9}$ dark count probability, unit detection efficiency, and error-correcting code inefficiency $f = 1.2$.

coding. We therefore argue that twin-field schemes must be implemented with RE QDs, in order to provide the two parties with a shared phase reference before the scrambling. We simulate the protocol performance of [115] under these conditions in Fig. 6.2. (c), assuming the implementation of decoy states. We note that performing TF-QKD with a perfect single photon source (RE π-pulse and unit single-photon purity) is impossible, since there is no accessible phase to encode the key information. However, by decreasing the pulse area a little below π, in the same manner as [97], it is possible to create a coherent superposition of vacuum and single-photon, thus providing an accessible phase to perform the protocol.

Our results are focused on QKD implemented with discrete degrees of freedom, such as polarization or time-bin. For completeness, we note the existence of QKD protocols optimized for continuous degrees of freedom of PDSs, such as phase and amplitude [284]. These can actually compete with discrete-variable QKD over metropolitan distances, using simpler technology, but are sensitive to larger attenuations due to heavier post-selection and noise estimation techniques [285, 286].

6.2.5 Quantum primitives beyond QKD

Quantum cryptography presents a broad spectrum of other primitives, many of which belong to the branch of *mistrustful cryptography* [13,268]: unlike in QKD, Alice and Bob are not collaborators, but adversaries wishing to compute a common function. Decoy-state methods are then more challenging to apply (although not impossible for all protocols), since Alice and Bob do not trust each other.

Remarkably, the desired security properties for such primitives can be very sensitive to PNC. In this instance, substituting PDSs by appropriately optimized QDs can yield even more benefits than in QKD. To show this, we extend the practical security analyses of three mistrustful quantum primitives [16, 31, 32] to the QDs framework, and estimate the QDs collection efficiencies required to outperform PDSs for the relevant security figures of merit. Our performance results are summarized in Fig. 6.3 for all primitives.

We display the performance of QDs and PDSs for one example primitive in Fig. 6.4: unforgeable quantum tokens. This primitive allows a central authority to issue tokens, comprised of quantum states, whose unforgeability is intrinsically guaranteed by the no-cloning theorem, thus requiring no hardware assumptions. One famous application is quantum money, which, in its private-key form, can prevent banknote forgery [113], double-spending with credit cards [31, 122] and guarantee features such as user privacy [116].

In Fig. 6.4 (a)., we compare the noise tolerance of the QT scheme from [122] for PDSs and QDs as a function of source efficiency. Noise tolerance indicates how much experimental error rate can be tolerated such that the unforgeability property holds, while source efficiency is the probability that a threshold single-photon detector will click in a lossless setting. Naturally, PDSs reach a maximal noise tolerance for source efficiencies around 63 %, corresponding to $\mu \approx 1$, before dropping again when the multiphoton contribution becomes too significant. For QDs, we notice a striking difference between schemes with coherence (RE) and those without (LA and TPE): the letters give an overhead of almost 2 % on the noise tolerance with respect to RE at high source efficiencies. This difference is crucial in making implementations feasible, since boosting the fidelity of quantum state preparation and quantum storage by a few percent can be extremely challenging. These differences are also reflected in Fig. 6.4 (b)., which identifies the collection efficiencies at which QDs can outperform the best PDSs performance: while LA and TPE require 44 % and 38 %, respectively, RE must be pushed to 47 % to beat PDSs. For information purposes, we also select three state-of-the-art experimental QDs, and show how they would perform in such a beyond-QKD protocol with their reported values of brightness and single-photon purity.

Fig. 6.4 (c). finally compares the performance of each source as a function of distance. Once again, the difference between LA/TPE and RE is significant due to the coherence feature. We notice here that the maximal distance for all sources is much shorter than in QKD schemes since our selected QT scheme bears a maximal loss tolerance of 50 %: above this limit, an adversary can clone the QT without

introducing any errors [122].

Our work showcases the importance of engineering optical pumping schemes towards specific primitives. Fig. 6.3 displays non-trivial requirements for quantum strong coin flipping for instance: unlike with decoy-state QKD and QT, QDs perform better at lower collection efficiencies, thus rendering state-of-the art QDs already capable of providing quantum advantage in such mistrustful primitives. Furthermore, the absence of photon number coherence in LA and TPE allows these schemes to reach quantum advantage over significantly longer distances than RE schemes: for the selected protocol from [32], these values read 86 km and 36 km for TPE and LA, respectively, vs. 25 km for RE.

Primitive	Description Applications	Figure of merit	Optimal pumping	Zero distance Threshold collection T%	Zero distance QDs 100%/ Max PDSs	Distance Loss tolerance - km (dB) QDs T%	 QDs 100%	 PDSs
Key distribution BB84 -no decoy	Alice and Bob wish to establish a secret key over a public channel. message encryption, digital signatures, channel authentication.	secret key rate	TPE LA	32 36	3.3 2.9	149 (31) 95 (20) ⚠ lower collections perform better than higher ones	125 (26) 75 (17)	190 (40)
BB84 -decoy			TPE LA	33 37	3.1 2.6	375 (79) 375 (79)	393 (83) 390 (82)	366 (77)
Twin field -decoy			RE	29	3.3	738 (155)	778 (163)	714 (150)
Unforgeable tokens	Alice issues a token to Bob, such that he may use it only once. unforgeable money, license/copy protection, one-time programs.	noise tolerance	TPE LA RE	38 44 47	2.6 2.2 2.0	14 (3) 13.7 (2.9) 12.9 (2.8)	14 (3) 14 (3) 14 (3)	11 (2.3)
Coin flipping	Alice and Bob wish to remotely toss a fair coin, such that none of the two parties can bias the outcome towards their preferred value. multiparty computing, leader election/e-voting, secure online gaming.	quantum advantage (for bias)	TPE LA RE	49 16 <24 for 1000 states and 1.5% honest abort	N/A N/A N/A	100 (21) 73 (10) <82 (17) ⚠ lower collections perform better than higher ones	86 (18) 36 (8) <25 (5)	N/A
Bit commitment (under bounded storage)	Alice sends a bit to Bob, such that: 1) Alice cannot change the bit after committing to its value, 2) Bob cannot discover the value until she reveals it. multiparty computing, zero-knowledge proofs, verifiable secret sharing.	security threshold	TPE LA	17 19	9.6 7.9	17.9 (3.9) 17.6 (3.9)	53.5 (11.8) 41.0 (9)	10.2 (2.2)

Figure 6.3: **QDs performance for the main quantum primitives.** A description of each primitive is provided, along with its main network applications, and our chosen security figure of merit. In each case, we summarize the various QDs pumping scheme performances and the threshold collection efficiencies T required to outperform PDSs in a lossless setting. We then display the performance ratio of QDs with 100 % collection over the best PDSs at zero distance (note that this ratio has to be scaled for QDs achieving higher repetition rates than PDSs). We then calculate the loss tolerance, both in terms of distance (in km) assuming single-mode telecom fiber losses of 0.21 dB/km, and in terms of absolute losses (in dB) for QDs reaching T% collection, QDs reaching 100 % collection, and randomized-phase PDSs. All the relevant protocol descriptions, security analyses, and simulation results are provided in Ch. 5.2.

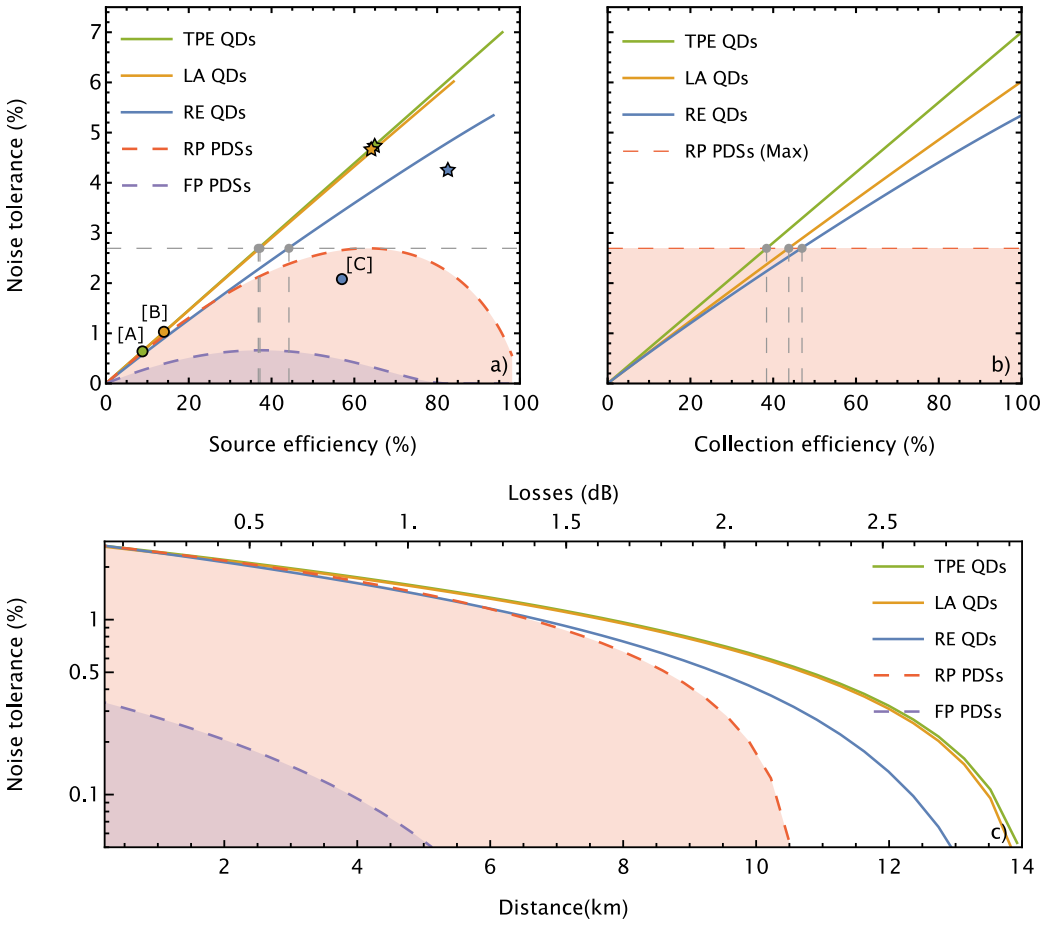


Figure 6.4: **Source comparison for unforgeable quantum tokens (quantum verification protocol from [122]).** (a) Numerical noise tolerance as a function of source efficiency for RE, LA and TPE QDs, along with fixed-phase (FP) and randomized-phase (RP) PDSs. Source efficiency is defined as $1-e^{-\mu}$ for PDSs and $1-\sum_{n=0}^{\infty} p_n(1-\eta)^n$ for QDs, where η is the QDs collection efficiency. Photon-number populations $\{p_n\}$ emitted under different QDs excitation schemes were obtained from the brightness and single-photon purity results of Fig. 6.1, assuming the optimal pulse lengths marked in black. RE photonic states are assumed to be maximally pure in number basis, expressed as $\sum_{n=0}^{\infty}\sqrt{p_n}\,|n\rangle$, while LA states were expressed as diagonal states $\sum_{n=0}^{\infty} p_n\,|n\rangle\langle n|$. Colored circles indicate the performance of three state-of-the-art quantum dots, inferred from the experimental brightness and purity values reported in [A]= [192], [B]= [287], [C]= [188], corrected to unit detector efficiency. Stars indicate the potential of these quantum dots assuming the reported collection losses, but no setup losses. (b) Numerical noise tolerance as a function of QDs collection efficiency, compared to the best performance of PDSs sources (dashed line). (c) Numerical noise tolerance plotted as a function of distance, assuming single mode telecom fiber losses of 0.21 dB/km. The QDs collection efficiencies were chosen as the intersection points from (b), also summarized in Fig. 6.3.

6.3 Discussion

We have estimated threshold collection efficiencies for which GaAs-based QD photon sources can outperform Poisson-distributed-based implementations in four main quantum-cryptographic primitives. The estimations include the combined effect of brightness, single-photon purity, and photon-number coherence. We have shown in particular that resonant excitation should be used for twin-field QKD, but not for decoy QKD and other quantum primitives due to the unwanted presence of photon-number coherence that violates practical security assumptions.

We believe that these results will provide a benchmark for future achievements in quantum dot cavity structures, especially at telecom wavelengths [60, 270, 288, 289]. Although state-of-the-art dot-cavity simulation frameworks cannot account for all characteristics of quantum dots emitting in the telecom range, current telecom performance [235,270,290] shows good agreement with our 900 nm framework: the brightness and purities are not strongly dependent on the emission wavelength. Furthermore, frequency conversion of 900 nm photons to telecom photons can currently reach efficiencies up to 57 % [291]. These extra losses can be absorbed in our collection efficiency quantity.

We wish to encourage future QKD experiments with optimal pumping schemes, taking into account the security assumptions provided by the quantum cryptography community. Finally, we hope to stimulate experiments that explore the full potential of QD-based single-photon sources for other quantum network primitives like unforgeable tokens [18, 31, 116], coin flipping [32, 117] and bit commitment [16, 17, 36]. We believe our analysis can be extended in future works to multipartite entanglement-based quantum network primitives, such as secret sharing [266] and anonymous messaging [292].

6.4 Methods

Our GaAs-based QD, driven by a pulsed pump laser, is modelled either as a 2LS or a 3LS coupled to a single-mode microcavity in the Jaynes-Cummings manner. The interaction of the QD with phonons is treated by the standard pure-dephasing Hamiltonian [251–253,255]. In this way, we solve for the dynamics of the dot-cavity system by employing a numerically exact path-integral formalism [257, 259, 262]. The derivation of the photon number populations, along with all practical security analyses, are detailed in Ch. 5.1.

7

Methods for "Robust excitation of C-band quantum dots for quantum communication"

The following two chapters introduce the paper titled "Robust Excitation of C-band Quantum Dots for Quantum Communication" [99] and provide a more detailed context for it. The experiment was part of a close collaboration with Prof. Peter Michler's group from the University of Stuttgart, which supplied the QDs sample emitting in the telecommunication C-band. The LA was considered as an intriguing excitation scheme for real-life quantum networks due to its robustness and strong performance in quantum cryptographic protocols [52, 276]. However, it was known that the brightness and single-photon purity are nontrivially dependent on pump power and the pump wavelength detuning from the excitonic level [91]. Therefore, we conducted this in-depth experimental study in the context of QKD applications.

My contribution: *Together with Cornelius Nawrath, I designed the setup for quantum dot excitation and the collection of emitted single photons. I constructed the setup in Vienna, included the spectral filtering of single photons and did the characterization of the first QDs. Alongside Mathieu Bozzio and Lennart Jehle, I defined the project, and together with Lennart Jehle, I collected the experimental data. Additionally, I supported Lennart Jehle in processing the data.*

In the paper titled *"Robust excitation of C-band quantum dots for quantum communication"*, we experimentally investigate LA QD as a remarkable candidate for long-distance single-photon quantum cryptography [99]. This scheme has already displayed high robustness against environmental fluctuations present in real-life communication networks [276]. We described how to tailor the QD's photon-number statistics for QKD protocol, while simultaneously exploiting the new security features enabled by incoherent phonon decay.

We experimentally investigated recently developed QDs emitting single photons in the telecommunication C-band [293], which is highly appealing for future quantum network implementations. The brightness and single-photon purity of

emitted state by LA-pumped telecom C-band QD were measured for detunings between 0.9 nm and 3.7 nm form X energy level and for pump powers from 0 to well beyond saturation. The obtained data were utilized to simulate the performance of QKD protocols with and without decoy states. We also identified optimal pumping conditions, maximizing the SKR, accounting for various protocol losses.

This chapter provides a description of the experimental setup and the investigated QDs sample. Additionally, it outlines the introduction to data processing methods and summarizes the adapted QKD theory for QDs.

7.1 Experimental Setup

The scheme of the experimental setup is displayed in Fig. 7.1. We use an Er-doped fiber pulsed mode-locked laser at a repetition rate of $\nu_{\text{rep}} = 75.95\,\text{MHz}$ to excite the QD. A spectral filter with 1 nm bandwidth inside the laser cavity stretches the generated pulses to a pulse width of 10.1 ps (spectral width FWHM 400 pm, the pulses are not Fourier-limited). The laser provides tunability of wavelength between 1530 nm and 1560 nm at an average output power 200 mW.

The laser pulses are then stretched by a free space pulse shaper in 4-f arrangement, which is based on a reflective grating (1200 lines/mm, blaze at 1550 nm) with efficiency $\approx 90\,\%$, C-coated lens with a focal length of 400 mm and tunable filtering slit. The pulses after the pulse shaper have a pulse width of 17(1) ps.

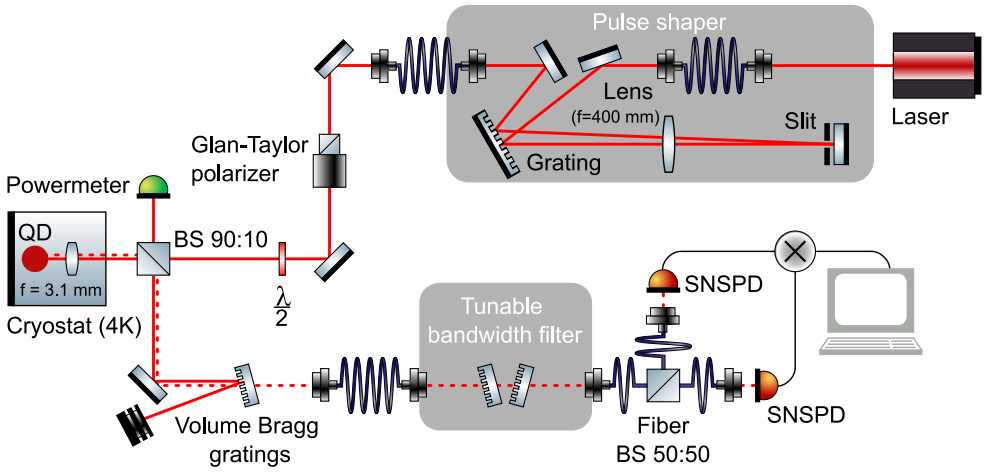


Figure 7.1: **Scheme of the experimental setup.** A schematic representation of the main building blocks of the experimental setup, such as excitation pulse laser, pulse shaper, excitation of the QD sample, filtering of the QD transition spectral line and detection.

The pulse-shaped excitation laser beam is coupled to single-mode fiber and then collimated by an 8 mm lens collimator. A Glan-Taylor polarizer sets the

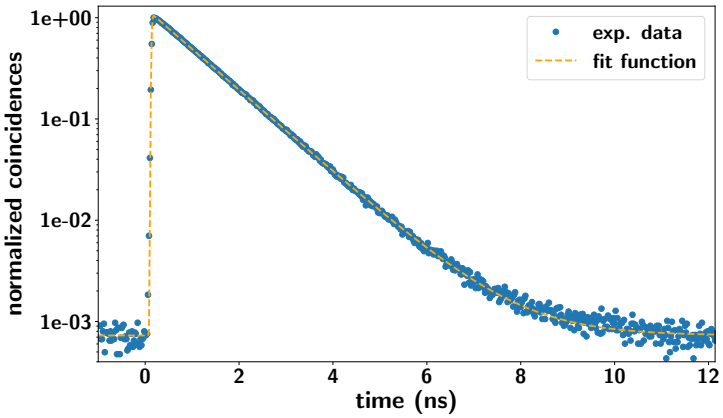


Figure 7.2: **Time-resolved fluorescence measurement.** In this measurement, the excitation laser was spectrally detunend by 1.5 nm and a pump power of 0.89 a.u. was used. The mono-exponential fit function (dashed line) yields a decay time of 1.07(2) ns.

excitation beam to linear polarization and the angle of the polarization is then adjustable by a HWP. Just before the cryostat chamber, a 90 : 10 BS is placed to separate the incoming excitation beam and single photons emitted by the QD. Approximately 90 % of the excitation beam (depending on its polarization state) is reflected by the BS to a power meter, which is used to control the QD excitation power, only $\approx 10\,\%$ of the laser power is guided to the cryostat chamber, where the QD sample is placed.

The sample design [294] features a bottom-DBR where the distance between the 23 pairs of AlAs/GaAs constituting the reflector and the semiconductor/vacuum interface corresponds to a nominal, weak λ cavity, where the QD layer is situated in its anti-node. The attribution of the QD transition to a positive trion, is based on power- and polarization-resolved μ-PL measurements, as well as previous experimental and theoretical investigations [234, 236, 294, 295] on similar samples. Fig. 7.2 displays a time-resolved fluorescence measurement in a semi-logarithmic scale where an excitation power of 0.89 a.u. and spectral detuning of 1.5 nm was used. The mono-exponential fit function yields a decay time of 1.07(2) ns.

The emission is collected by a lens ($f = 3.1\,\mathrm{mm}$) with an NA of 0.68. The excitation laser suppression is realized based on two volume Bragg gratings (VBGs) notch filters which block a spectral bandwidth (FWHM) 1.2 nm and reach an individual suppression OD6. The QD emission is coupled by a $f = 8\,\mathrm{mm}$ lens collimator. For precise filtering of the QD transition line, we use a fiber-coupled bandwidth tunable filter based on VBGs with set filtering spectral bandwidth (FWHM) 150 pm, approximately corresponding to the QD-transition linewidth.

The full setup exhibits an efficiency of $\eta_{\mathrm{setup}} = 0.13$. The measurements of $g^{(2)}(\tau)$ are acquired with a fiber-based symmetric beam splitter in a HBT configuration, see Fig. 3.3, using SNSPDs with an efficiency of $\eta_{\mathrm{d}} = 0.86$ each and a

time tagging device. The detection exhibits a temporal resolution of 34 ps, given as FWHM of the system response function. The dark counts of the used detectors are 130 Hz for the first detector and 180 Hz for the second one.

7.1.1 Evaluation of measured time tags

For each laser detuning and excitation power, time tags from both of the detectors in the HBT setup were saved. For enough statistics in the auto-correlation data, each measurement is stopped once the coincidence counts of the uncorrelated side peaks of the measured second-order correlation function exceed a threshold value 700 counts at 100 ps bin width.

To determine the actual source brightness, simply adding the detection events from both detectors is not sufficient. Doing so would result in the double counting of contributions from multi-photon occurrences given as

$$\tilde{B} = B + \sum_{k \geqslant 2} p_k \left(1 - \frac{1}{2^{k-1}}\right) = B + \frac{1}{2} p_2 + \frac{3}{4} p_3 \ , \tag{7.1-1}$$

where we assume that $p_{\geq 4} = 0$. To correct the over-counting we subtract the number of coincidence events occurring within a single repetition period $\frac{1}{\nu_{\mathrm{rep}}}$. Now multi-photons contribute to the final brightness with the same weighting as single photons, which follows the original definition of brightness given by Eq. 3.0-20. Such that the corrected brightness reads as

$$B = \frac{1}{\nu_{\mathrm{rep}} \eta_{\mathrm{setup}} \eta_{\mathrm{d}}} \Big(R_1 + R_2 - CC_{1,2}(t_{\mathrm{coinc}} = \frac{1}{\nu_{\mathrm{rep}}}) \Big) \ , \tag{7.1-2}$$

where R_i is the raw count rate of the $i-$th detector and CC is the coincidence count rate. The brightness is normalized to the setup efficiency η_{setup} and the detector efficiency η_{d}. As a result, the brightness expressed in Eq. 7.1-2 is referred to as the first lens brightness, as explained in Ch. 3.0.2.1.

For source applications in quantum cryptography, it is crucial to consider the full repetition period when calculating the source's single-photon purity since an adversary has access to all the information leaving Alice's secure laboratory. Therefore we don't apply any time filtering and assume only a simple background subtraction based on the expected coincidences arising from a dark count in at least one of the channels computed given as

$$CC^{\mathrm{d}}_{1,2} = R_1 R^{\mathrm{d}}_2 + R_2 R^{\mathrm{d}}_1 + R^{\mathrm{d}}_1 R^{\mathrm{d}}_2 \ , \tag{7.1-3}$$

where R^{d}_1 (R^{d}_2) is dark count rate at the 1st (2nd) detector.

7.2 Parameter Estimation for Quantum Key Distribution with Quantum Dots

For LA QDs, the emitted photon states bear very little PNC [52,98] and therefore it is fair to assume that the emitted state is mixed stated in photon number bases. Under this assumption, we can use standard practical security analysis for QKD protocol as described in Ch. 2.2.3.4 and Ch. 2.2.3.5.

We calculate SKR based on Eq. 2.2-30, respectively Eq. 2.2-37 for the decoy the state protocol. Following the underlying theory, only single-photon states contribute positively to secure-key generation, whereas multi-photon states contain redundantly encoded information. To describe the protocol security with QDs we aim to assess the contribution of multi-photon states from brightness and single-photon purity, which are indeed the main source parameters conveniently measurable by Alice. For this, we used our theory framework described in Ch. 3.0.2.2, which upper bound the multi-photon contribution $p_{\mathrm{m}} = \sum_{k \geqslant 2} p_k$ as

$$p_{\mathrm{m}} \leq \frac{1 - Bg^{(2)}(0) - \sqrt{1 - 2Bg^{(2)}(0)}}{g^{(2)}(0)} \ . \tag{7.2-1}$$

In contrast to the security analysis of QKD with decoy states, outlined in Ch. 5.2.1, our approach here assumes only two decoy states. As for QDs, the multi-photon component $p_{n \geq 4}$ can be neglected and two decoy states are sufficient to compute the yields and error rates, $\{Y_k, e_k\}$, exactly.

7.2.1 Maximum QKD-distance approximation from experimental measures

One of the main advantages of QDs over PDSs is reaching longer communication distances in quantum cryptography protocols as was demonstrated by Ch. 5.2.1 and Ch. 6. Therefore, estimating the maximum achievable communication distance $d_{\max}$ of QKD protocol for a specified source is crucial for practical applications. However, solving Eq. 2.2-30 analytically for the channel transmission η_{ch} is challenging due to its complexity. Even the precision of the numerical solution for a given photon-number distribution of Eq. 2.2-30 is limited as we have to estimate additional protocol parameters. These parameters include single-photon detection error, detection efficiency, dark-count probability, and inefficiencies in error correction codes. Consequently, an analytical approximation for $d_{\max}$ can offer distinct advantages, particularly when the requisite parameters are readily accessible.

The detailed derivation of the maximal QKD-distance approximation is available in the supplementary material of [99]. Here, we provide an overview of the primary logical steps. We start by establishing an upper bound for Eq. 2.2-30 as follows

$$SKR \leq \frac{1}{2} Q_1 (1 - H_2(\epsilon_1)) \ . \tag{7.2-2}$$

As the cost for this upper bounding, we have to assume that the error correction term, $fQ_\mu H_2(\epsilon_{E_\mu})$, is strictly positive. The maximum attainable distance $d_{\max}$ is formalised as the minimal channel efficiency $\eta_{\text{ch}}^{\min}$ for which $SKR > \delta$.

Assume that δ is small then we are studying a situation where $SKR \to 0$. This can happen if the single-photon gain Q_1 goes to zero or $H_2(\epsilon_1) \to 0$. As we assume a long-distance communication approximation where η_{ch} is low, we can focus only on the case $Q_1 \to 0$. From Eq. 2.2-29 and Eq. 2.2-31 we can estimate the single-photon gain as

$$Q_1 = p_{\text{m}} \left(\frac{p_1}{p_{\text{m}}} Y_1 + Y_2 - 1 \right) \geq 0 \ . \tag{7.2-3}$$

Since $p_{\text{m}} \geqslant 0$ for a realistic source, the expression inside the bracket has to tend to zero to cause $Q_1 \to 0$. By assuming $Y_0 \ll \eta_{\text{ch}}$ we can simplify Eq. 2.2-28 to $Y_1 = \eta_{\text{ch}}$ and $Y_2 = 2\eta_{\text{ch}} - \eta_{\text{ch}}^2$. Thus, Eq. 7.2-3 for $Q_1 \geq 0$ becomes

$$1 \leq \eta_{\text{ch}} \left(\frac{p_1}{p_{\text{m}}} + 2 - \eta_{\text{ch}} \right). \tag{7.2-4}$$

In the long-distance communication approximation, we can assume just the linear terms of η_{ch}. Then we can write the equation as

$$\eta_{\text{ch}} \geq \frac{1}{\dfrac{p_1}{p_{\text{m}}} + 2} \ . \tag{7.2-5}$$

Finally, we use the multiphoton estimation given by the Eq. 7.2-1, express the single-photon probability as $p_1 = B - p_m$ and estimate $\eta_{\text{ch}}^{\min}$ by the fist fist term of Tylor series of Eq. 7.2-5

$$\eta_{\text{ch}}^{\min} \approx \frac{B g^{(2)}(0)}{2}. \tag{7.2-6}$$

Considering the complexity of Eq. 2.2-30, the approximation is strikingly simple and follows directly from the fundamental source parameters. However, in contrast to the precise numerical solution, Eq. 7.2-6 consistently provides an overestimation of the maximum distance. This systematic error originates from the approximation's derivation as an upper bound, mainly due to neglecting the error correction term in Eq. 2.2-30. Generally, the overestimation tends to be in the range of $25 - 35\,\text{km}$.

8

Reprint of "Robust excitation of C-band quantum dots for quantum communication"

Building a quantum internet requires efficient and reliable quantum hardware, from photonic sources to quantum repeaters and detectors, ideally operating at telecommunication wavelengths. Thanks to their high brightness and single-photon purity, QD sources hold the promise to achieve high communication rates for quantum-secured network applications. Furthermore, it was recently shown that excitation schemes such as LA provide security benefits by scrambling the coherence between the emitted photon-number states. In this work, we investigate further advantages of LA-pumped quantum dots with emission in the telecom C-band as a core hardware component of the quantum internet. We experimentally demonstrate how varying the pump power and spectral detuning with respect to the excitonic transition can improve quantum-secured communication rates and provide stable emission statistics regardless of network-environment fluctuations. These findings have significant implications for general implementations of QD single-photon sources in practical quantum communication networks.

8.1 Introduction

The emergence of practical quantum technology paves the way to a quantum internet – a network of connected quantum computers capable of reaching computational speed-ups in various tasks such as prime factoring [10], machine learning [40] and the verification of NP-complete problems with limited information [296]. Although such schemes are appealing, most are technologically challenging, while the security advantages provided by quantum cryptography are more tangible [14, 29, 297]. A broad range of quantum-cryptographic primitives including QKD [14, 29, 297], quantum coin flipping [32, 117, 298], unforgeable quantum tokens [18, 116, 299], and quantum bit commitment [16, 17, 36] have been developed to demonstrate some security advantage over their classical counterparts. The success of a future quantum internet then relies on the development of fundamental quantum hardware (sources, repeaters and detectors) which should adhere

to these primitives' security standards, provide high communication rates, and operate reliably in a real-world environment [26].

Non-classical light sources such as SPDC [38, 300], nitrogen-vacancy centers [301] and trapped atoms [302], have been used as hardware for the first quantum networks. In recent years, semiconductor QDs have materialized as highly versatile and quality single-photon sources [75, 76, 303–305], with outstanding end-to-end efficiencies overcoming 57 % and the potential to reach repetition rates of tens of GHz [304]. Such emission properties of QDs have led to the implementation of complex network building blocks relying on quantum teleportation [73, 306] and quantum entanglement swapping [75, 76, 307]. Regarding the emission wavelength, the spectral regime of the telecom C-band (1530 nm to 1565 nm) is highly appealing, due to its global absorption minimum in standard silica fibers, the possibility to implement daylight satellite communication [39] and the compatibility with the mature silicon photonic platforms [200]. QDs with emission wavelengths in and around the C-band are available on indium phosphide (InP) [28, 308, 309] and gallium arsenide (GaAs) material system [237, 293, 294], and circumvent the technical overhead and losses of quantum frequency conversion [310]. Embedded in circular Bragg cavities, QDs based on the well-established GaAs platform have simultaneously demonstrated high brightness and high purity values recently [293].

Previous works have investigated the advantages and drawbacks of various optical pumping schemes (resonant, phonon-assisted and two-photon excitation) in terms of efficiency, single-photon purity and indistinguishability [178, 276, 311]. On the other hand, it was recently shown that such schemes must be carefully tuned to satisfy the security assumptions of each quantum-cryptographic application [52]. Crucially, quantum coherences between the emitted photon-number components must be scrambled for optimal performance, which is inherently provided by some optical pumping schemes such as LA and TPE [52]. On top of their intrinsic security benefits, LA schemes are fairly insensitive to pump instabilities like power or polarization fluctuations, making them suitable for real-life communication networks [276, 311]. These excitation schemes are also beneficial for QDs with a complex charge environment, while other pumping schemes such as TPE can typically only address charge-neutral transitions. Moreover, unlike for neutral transitions, charged excitons can enhance polarized emission in polarized cavities, an important feature for most applications [304]. Finally, LA schemes do not require challenging single-photon polarization filtering (contrary to the resonant counterpart), and thus promise an experimentally straightforward way to obtain simultaneously high brightness and purity with high reproducibility in QD fabrication and experimental setups [311].

In this work, we combine all aforementioned advantages of LA in the C-band, and exploit its tunable parameters to investigate the complex dependence of brightness and purity on pump power and spectral detuning. We illustrate how this non-trivial behavior affects the security of quantum-cryptographic primitives with the example of single-photon QKD, and how the optimal operation conditions de-

pend on the communication distance. In agreement with theoretical findings [91], our results show that the characteristics of LA excitation can be tuned to achieve the ideal photon-number statistics. This optimization is reminiscent of the mean-photon adjustment required in WCS implementations [134].

8.2 Results

8.2.1 Excitation parameter investigation

To start investigating and optimizing our excitation parameters, it is important to note that most quantum-secured applications rely on a few trusted parameters that are typically not all experimentally accessible. Here, we infer the photon-number probabilities $\{p_k\}$ from two measurements, the brightness $B = \sum_{k=1}^{\infty} p_k$ and the single-photon purity $P = 1 - g^{(2)}(0)$, where $g^{(2)}(0)$ is the second-order auto-correlation measurement evaluated at zero time delay. We use an InAs QD based on an InGaAs metamorphic buffer layer enabling emission in the telecommunication C-band [294]. The tunable excitation is provided by a mode-locked fiber laser with a pulse length of 17(1) ps and a FWHM spectral width of 210(20) pm. The QD transition line is filtered by a set of volume Bragg grating filters (FWHM = 0.2 nm). The total setup efficiency is determined to be 13 %. For more experimental details, see Ch. 7.1. The highest single-photon purity under pulsed LA excitation was measured as $P = 0.982$, the corresponding second-order auto-correlation measurement is shown in Fig. 8.1.

While scanning both the power and wavelength of the pump laser, we simultaneously measure the brightness B (experimentally evaluated according to Eq. 7.1 -2 and corresponding to first-lens brightness) and single-photon purity P. We then compile the results in 2D maps as shown in Fig. 8.2 (a) and (b), respectively. Due to the low phonon density at a sample temperature of $\sim 4\,\mathrm{K}$ we excite the QD only with positive detunings $\Delta = \hbar(\omega_{\mathrm{laser}} - \omega_{\mathrm{dot}}) > 0$. The brightness map features a single, broad maximum around $\Delta \approx 0.8\,\mathrm{meV}(\Delta\lambda \approx 1.5\,\mathrm{nm})$ agreeing with similar experimental findings [184,312] and theoretical studies [313,314]. LA excitation with sufficiently smooth pulses [191] achieves a population inversion of the QD ground and excited state if the effective Rabi splitting of the laser-dressed states, $\hbar\Omega_{\mathrm{eff}} = \sqrt{(\hbar\Omega)^2 + \Delta^2}$, ensures an efficient exciton-phonon coupling that is characterized by the spectral phonon density $J(\omega)$ [312, 313], for more details see Ch. 3.2.2.2. The robustness of this scheme against power and wavelength fluctuations of the excitation laser is demonstrated by the broad maximum of the brightness in Fig. 8.2 (a) and stems from the spectral width of $J(\omega)$. Thus, the large bandwidth of the phonon interaction directly benefits a stable operation of the QD source. Only for large detunings and weak fields, the phonon-induced relaxation to the exciton level fails and the brightness drops significantly. Similarly, for high powers, the effective Rabi splitting is no longer in resonance with the phonon interaction resulting in reduced brightness.

Besides emission efficiency, the single-photon purity of the quantum-light source

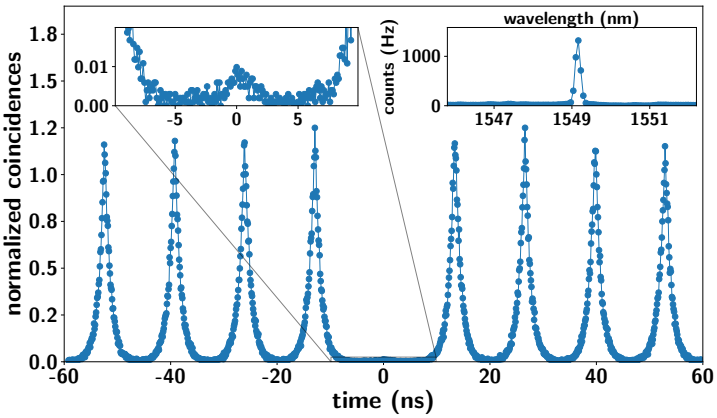


Figure 8.1: **Characterisation of the positively-charged exciton transition under pulsed LA excitation.** Second-order auto-correlation measurement $g^{(2)}(\tau)$ for an excitation field strength of 0.46 a.u. and a detuning of 1.5 nm. The well-suppressed peak at zero time delay confirms the high single-photon purity ($g^{(2)}(0) = 0.018\,(1)$). Further details on the analysis of $g^{(2)}(0)$ can be found in Ch. 7.1.1. The inset shows a micro photoluminescence (μ-PL) spectrum of the studied transition, including spectral suppression of the laser with an excitation field strength of 0.89 a.u. and a detuning of 1.5 nm from the QD resonance.

is crucial to the performance of cryptographic protocols [52]. Therefore, we analyze the purity P, depicted in Fig. 8.2 (b), for the same parameter range as the brightness. We identify a broad region of high purity at similar detunings but shifted towards lower powers. At large detunings, the purity degrades because the exciton state preparation via LA phonons becomes less efficient (evident by the low brightness in the same area of Fig. 8.2 (a)) and spurious contributions to the emission, including neighbouring QDs or a quasi-continuum of transitions, are no longer negligible. Considering a perfect two-level system, Ref. [91] predicts an enhanced purity for increasing excitation field strength because the phonon-induced level inversion is delayed until the end of the pulse. As a consequence, the a chance of a reexcitation event during the same pulse, as it is known for resonant pumping [180, 311], would be reduced. In our experiment, however, this process competes with, and is eventually out-weighed by, the aforementioned unintended emission decreasing the purity at high powers significantly.

Interestingly, our experimental findings imply the absence of a trivial set of optimal parameters (simultaneously maximizing brightness and single-photon purity), which confirms some of the complex behaviours predicted in previous theory works [52, 91]. Instead, a careful tuning of the excitation parameters is required for each quantum-cryptographic application. Depending on the desired security of merit, the correct weighting of the photon-number populations $\{p_k\}$ used for the optimization [52] must be defined. At the same time, fluctuations in the excitation parameters produce only small changes in photon-number populations.

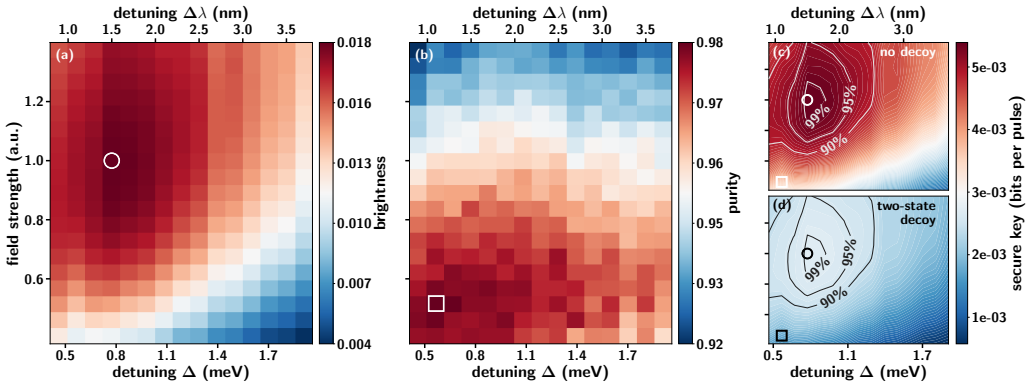


Figure 8.2: **Measured photon-number statistics and extrapolated QKD secure key bits per pulse for LA excitation.** Scanning the excitation parameters while simultaneously measuring (a) brightness $B = \sum_{k=1}^{\infty} p_k$ and (b) single-photon purity $P = 1 - g^{(2)}(0)$ of the QD emission. The white circle (square) marks the set of excitation parameters achieving the optimal brightness (purity). From the photon-number populations $\{p_k\}$, the secure key bits per pulse (SK) are calculated for zero distance based on the BB84 QKD protocol without (c) and with two decoy states (d). For more details on the parameter estimation see Ch. 7.2. The equipotential lines indicate where the SK has dropped to $\{99\,\%,\ 95\,\%,\ 90\,\%\}$ of their individual SK maxima. The SK was estimated in the asymptotic limit [283], $SK = \eta_{\mathrm{sif}}[Q_1(1 - H_2(E_1)) - f(E)Q_{\mathrm{tot}}H_2(E_{\mathrm{tot}})]$, where H_2 is the binary Shannon entropy and $\eta_{\mathrm{sif}} = 1/2$. Extrapolation for a two-state decoy includes an intensity modulator loss of 3 dB. Parameters for all plots are: single-photon detection error $e_{\mathrm{d}} = 0.02$, detection efficiency $\eta_{\mathrm{d}} = 0.86$, dark-count probability $Y_0 = 1.6 \cdot 10^{-6}$, error-correction code inefficiency $f = 1.2$.

Furthermore, optimal brightness and near-optimal purity are achieved for a pump pulse detuned by $\approx 1.5\,\mathrm{nm}$ from the QD transition that can be readily separated from the single-photon emission using efficient, off-the-shelf spectral filters. This simplifies source operation and optimizes brightness by removing the need for a cross-polarization setup, further underlining the practicality of LA excitation for network applications [14, 16–18, 29, 31, 32, 36, 116, 117, 297, 298]. In the following section, we experimentally show how to perform the excitation parameter optimization on the example of QKD, arguably the best-known primitive in quantum communication.

8.2.2 Quantum key distribution

QKD allows two parties to establish a secret key over an eavesdropped channel [14, 267]. In that sense, the most natural figure of merit is the number of secure bits communicated per round of the protocol. This quantity can be computed from two experimental parameters: the total gain Q_{tot}, corresponding to the probability of detecting at least one photon from a given pulse sent by Alice, and the total error rate E_{tot}, indicating the fraction of states for which the wrong (polarization)

detector clicks. Naturally, only the error-free single photon states contribute positively to the secure key, while the multi-photon contribution p_m leaks significant amounts of information. Starting from experimental data, one therefore needs to estimate the values of the single-photon gain Q_1 and the single-photon error rate E_1, which are not directly accessible. In Ch. 7.2, we infer these quantities in two ways: first by deriving an upper bound on the multi-photon emission probability

$$p_\mathrm{m} \leq \frac{1 - Bg^{(2)}(0) - \sqrt{1 - 2Bg^{(2)}(0)}}{g^{(2)}(0)} \tag{8.2-1}$$

and second by employing the two-state decoy approach [15,315]. Compared to previous work [316], Eq. 8.2-1 gives an explicit expression for p_m relying only on the experimentally accessible B and $g^{(2)}(0)$ and provides additional intuition to Ref. [317].

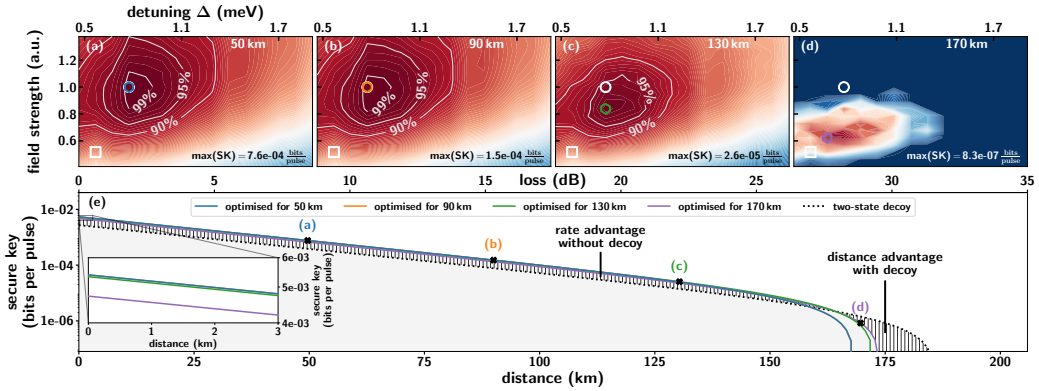


Figure 8.3: **Secure key rates of BB84 QKD for varying communication distances.** Secure key bits per pulse for the LA excitation parameter space in a standard BB84 QKD scenario for increasing channel length {50 km, 90 km, 130 km, 170 km} (a)-(d), where we assumed a fiber attenuation of $\alpha = 0.17\,\mathrm{dB/km}$, typical for the telecom C-band. The white circle (square) marks the set of excitation parameters achieving the optimal brightness (purity) as shown in Fig. 8.2, whereas the colored hexagon marks the trade-off between the two, optimizing the SK at the given distance. The color scale of each map is normalized to its maximum SK which is noted in the bottom right corner of each map. (e) Calculating the SK for each highlighted parameter set from (a)-(d) as a function transmission loss demonstrates how the tunability of LA excitation helps to adapt the emission statistics to the channel. The two-state decoy protocol reduces the SK by a factor of $\sim$ 3 at short and medium distances but performs better in the high-loss regime. The parameters used to calculate the SK are the same as for Fig. 8.2.

Following the parameter estimation, we calculate the attainable SK in the asymptotic regime for standard and decoy-state BB84 QKD for each set of excitation parameters as shown for zero communication distance in Fig. 8.2 (c) and (d), respectively. For the decoy protocol, we include a typical 3 dB loss for a

high-bandwidth intensity modulator required to produce the decoys. While the qualitative dependence of the SK is very similar for both protocols, the performance gap is evident in the absolute values. Decoy states have been introduced to handle the risk of multi-photon contributions p_{m}, but since these are inherently small for QDs, introducing the constant loss of the intensity modulator outweighs the effect of an exact bounding of p_{m}. Furthermore, recalling that quantum cryptography with off-resonantly or TPE QDs does not require any modulator for phase scrambling, adding an intensity modulator for decoy would increase the setup complexity. Comparing Fig. 8.2 finally shows that for zero distance the brightness (more accurately, p_1) dominates the SK map making a tight bounding of p_{m} even less relevant.

However, the impact of the multi-photon events on the SK comes into play for non-zero communication distances making the ideal set of $\{p_k\}$ no longer trivial but dependent on the channel loss. Computing SK maps at four distances, as depicted in Fig. 8.3 (a)-(d), visualizes the shift in source requirements. Short-distance transmissions benefit most from a bright source, whereas high-loss scenarios such as long-distance communication call for sources with high purity. Fig. 8.3 (e) then shows how these four ideal parameter sets behave over distances. The difference in performance underlines the potential of individually adjusting the excitation conditions with respect to the channel loss. Note that the joint optimization of $\{p_k\}$ by tuning the pump conditions is possible with RE or TPE but less performant.

The maximum distance for which the generation of a secure key is still possible is of great interest for applications. Since there is no analytical expression, we state the maximal communication distance as minimal channel transmission $\eta_{\mathrm{ch}}^{\mathrm{min}}$ and find that the approximation

$$\eta_{\mathrm{ch}}^{\mathrm{min}} \approx \frac{B g^{(2)}(0)}{2} + Y_0\,, \tag{8.2-2}$$

where Y_0 is the dark-count probability, captures the breakdown of secure key generation due to multi-photon contributions well under realistic assumptions. Due to its construction (effectively lower bounding $\eta_{\mathrm{ch}}^{\mathrm{min}}$), Eq. 8.2-2 always overestimates the distance by 30 km (see Ch. 7.2.1). Eq. 8.2-2 also implies that, within the limits of the approximation, a brighter source reduces the maximum communication distance. Counter-intuitive at first sight, this is readily explained as the multi-photon probability p_{m} increases with the source brightness if $g^{(2)}(0)$ is unchanged (see Eq. 8.2-1). While brighter QDs further improve the SK at short to medium distances, one must reduce the multi-photon component when communicating over large distances. For this purpose, simply attenuating the signal before launching it into the untrusted channel is sufficient [316]. Note how this approach resembles the mean-photon number optimization used for QKD with WCSs [134]. Considering a detector dark-count probability $Y_0 = 10^{-7}$, single-photon detection error $e_{\mathrm{d}} = 0.02$ and a highly pure source ($g^{(2)}(0) = 0.02$), our numerical analysis (see Appendix B) identifies the ideal brightness for maximum

distance as $B \approx 0.9\,\%$. This is well within the range of today's telecom C-band QD-technology.

Finally, we remark that implementing decoy states could be advantageous in the long-distance regime even for highly pure single-photon sources such as QDs, as reflected in Fig. 8.3 (e). However, for low to moderate loss, standard BB84 outperforms the decoy-state protocol.

In conclusion, we have investigated the benefits that phonon-assisted excitation of a telecom C-band QD provides for quantum-secured applications. Besides the convenient wavelength for communication applications, the InAs QDs provide a deep confinement potential, typically spanning over several hundred millielectron volts. As a consequence, their photon-number statistics are relatively insensitive to temperature fluctuations [236]. Moreover, the source can be operated at 25 K, which is feasible for a low-cost Stirling cryostat [293].

In addition to the previously simulated low photon-number coherence [52], the robustness to environmental fluctuations [276] and the efficient single-photon filtering, we have shown that LA excitation allows to effectively optimize the photon-number statistics with respect to the desired application. This feature originates from interaction with the phonon environment and is therefore not common to resonant excitation schemes but can be exploited by tailoring the LA pumping conditions. The complex implications of phonon interactions for brightness and single-photon purity have also been theoretically predicted for idealized systems [91]. Therefore, our observations can be generalized to other QD-based sources.

As a means of improving the emission statistics independently of the excitation mechanism, temporal filtering of the signal was proposed [318, 319] but requires special hardware and comes at the price of additional loss. Moreover, we show that optimizing $\{p_k\}$ using only the LA pump power is as efficient as temporal filtering with a fast and lossless modulator. Only at very large distances, temporal filtering performs better since it also reduces the source brightness and detector dark counts. For the calculation see the supplementary of the paper [99]

However, we note that TPE can simultaneously yield a higher brightness and purity than achievable for any parameter set using the LA scheme [180]. Nevertheless, TPE – being a resonant process – is sensitive to environmental fluctuations and thus less suitable for real-world implementations.

Furthermore, we found that even for quantum light sources with inherently low multi-photon contribution, decoy states can push the maximum attainable distance in QKD. Although, in consideration of the low SK at these distances and the experimental overhead involved, we believe that decoy states are not beneficial for QD implementations. Finally, we would like to stress that we optimized the photon-number statistics in LA excitation with respect to QKD as an example but the process is transferable to other quantum-secured applications [16–18, 32, 36, 116, 117, 298, 299] and prone to improve their performance.

9 Conclusion and future challenges

In recent years, QD-based single-photon sources have been steadily approaching the performance of ideal single-photon sources, with brightness recently reaching 71 % and single-photon purity close to unity [56]. Despite these advancements, QDs still struggle to outperform the currently commonly used PDSs in quantum cryptographic applications [52]. Techniques such as the decoy state protocol have partially mitigated the main limitation of PDSs in quantum cryptography, namely the trade-off between brightness and multi-photon emission [15, 50]. As a result, the performance of QKD is not heavily dependent on multi-photon contributions, allowing more affordable sources, such as attenuated lasers, rather than relying on high-performance single-photon sources. The example of decoy state protocols or optimizing the average photon number μ nicely illustrates how a good understanding of hardware, which is mostly imperfect, can improve the quantum algorithm performance [134].

9.1 The advantages of quantum dots in quantum cryptography

In this work, we have compared the performance of QDs and PDSs in the main QKD protocols, see the Ch. 5 and Ch. 6. In the standard BB84 QKD protocol without decoy states, QDs can outperform SKR achievable with PDSs for both low and high communication link losses, due to their high single-photon purity. In the high-losses scenario, QDs can achieve a SKR more than two orders of magnitude higher than what is attainable with PDSs. However, the situation changes significantly when decoy states are used. With decoy state protocols, the impact of multi-photon components on security is minimized, making QDs less advantageous compared to PDSs. Only QDs with high brightness (around 35 %) can achieve a higher SKR and an ideal QD with brightness close to unity can deliver SKR approximately three times higher than the theoretical limit of PDSs.

Given that the decoy-state method significantly enhances PDSs performance in QKD protocol, it was worth exploring whether similar benefits could be realized for QD-based implementations. We investigated this with InAs QD emitting in the telecommunication C-band, see the Ch. 7 and Ch. 8. Our findings indicate that decoy state protocols offer a minimal advantage for QD-based QKD systems. Under reasonable loss conditions (below $< 30\,\mathrm{dB}$), standard QKD protocols using

QDs achieve higher SKR than those using decoy states. This is caused by the additional losses from the variable attenuator. In the case of PDSs these losses can be easily compensated by increasing the average photon number, μ. However, QDs, being single-photon sources, do not allow for adjustments to the emitted photon-number statistics in the same way.

QDs can be excited by various coherent and incoherent excitation schemes, which differ in emitted single-photon statistics, brightness, photon indistinguishability, PNC, and other factors. Therefore, the performance of QDs in quantum cryptography protocols is highly dependent on the chosen excitation scheme, where the optimal scheme is determined by the specific protocol. One of the advantages of QDs in quantum cryptography is the possibility of generating mixed states in the Fock basis directly by the single-photon source. This allows the source to be used directly in protocols that require zero PNC in the generated photonic state, without a need for active phase scrambling. This holds the promise of achieving higher communication rates, which will not be limited by the speed of active phase scrambling methods combined with the low values of average photon number μ required due to fundamental PDSs photon-number statistics, but only by the single-photon sources, detectors, and control electronics. On the other hand, some excitation schemes, such as RE or sTPE, allow for the generation of pure states in the Fock basis and can be used in protocols where a phase reference is required, namely TF-QKD and MP-QKD.

Off-resonant excitation schemes, such as LA and LA-TPE, are highly appealing for the future implementation of QDs in deployed communication networks [276]. These schemes exhibit high robustness against environmental fluctuations and allow for efficient spectral filtering of the residual pump. We studied LA pumped InAs QD emitting in the telecommunication C-band as a source for the QKD protocol. Our results showed that the emitted photon number statistics can be tuned by adjusting the excitation power and the spectral detuning of the pump field from the excitonic level to maximize the SKR for given protocol losses, see the Ch. 8. A similar method is used in PDSs implementations, where the average photon number μ is adjusted according to the losses to maximize the SKR, as higher losses require lower multi-photon contributions [134].

Implementing QDs in QKD protocols presents challenges due to the necessity for an ideal excitation scheme, optimized pump conditions, and a QD with sufficient collection efficiency. Despite these challenges, QDs can surpass the theoretical SKR limit for PDSs and potentially achieve higher communication rates, that are limited by phase-scrambling modulators. One significant follow-up of our work was provided by Prof. Jian-Wei Pan group, in which they first experimentally overcame the maximal SKR for PDSs by implementing a QD in a QKD protocol [320]. The performance of QDs dramatically changes in quantum primitives based on parties that don't trust each other, such as QT, QBC, and QCF. In these protocols, implementing the decoy states technique is not always possible, making the minimal multiphoton component crucial for achieving high security.

In these scenarios, the excitation schemes do not generate PNC in the emitted photonic state, reaching higher performance. Generally, we stress the performance of TPE, which shows high single-photon brightness with an ultra-low multiphoton component and generates PNC only between even photon number components, produced as photon pairs from the exciton-biexciton cascade. Thus, if we use only one of these two photons, we obtain a mixed state in the Fock basis with single-photon purity almost equal to unity. The TPE scheme in our study outperforms all other studied excitation schemes (RE, LA) in all studied mistrustful quantum cryptography primitives, see the Ch. 6.

In the example of QT, we see basic characteristics that differentiate QDs from PDSs in security analyses for most quantum primitives. The security figure of merit, such as the protocol noise tolerance in QT, is almost linearly dependent on the source efficiency, unlike PDSs, where it reaches a maximum for ideal source efficiency and then starts decreasing. This allows us to run the protocols with highly efficient single-photon sources and achieve higher communication rates. In the case of QT, the noise tolerance achieved by a QD under TPE is more than twice as high as the maximum achieved by PDSs.

Even more outstanding performance of QDs can be observed in strong QCF and QBC protocols. In the case of strong QCF, QDs achieve a quantum advantage in terms of bias even for high source efficiencies, which can be sixteen times higher than the maximum usable efficiency of PDSs, maintaining this advantage over long communication distances up to 86 km of single-mode telecommunication fiber at 1550 nm. A significant increase in communication distance can also be achieved by implementing QDs in the noisy storage QBC protocol, where QDs can stay over the security threshold up to approximately 54 km, compared to PDSs, which maintain security only up to around 10 km of single-mode at 1550 nm.

9.2 Practical challenges in utilizing quantum dots as usable sources

In general, QDs enable high communication rates and long communication distances while maintaining a high level of security for individual quantum cryptographic primitives. This makes a compelling case for considering QDs as the core hardware for future long-distance quantum networks. Additionally, proper operation of many components of the coming quantum internet, such as all-optical quantum repeaters, quantum switches, and quantum memories requires high single-photon purity, which QDs straightforwardly provide.

On the other hand, PDSs offer high technological readiness, robustness against environmental fluctuations, room temperature operation, and low-cost deterministic production, making them the leading sources in modern quantum cryptography, despite not being ideal single-photon sources [14]. The recent progress in the deterministic production of QDs and effectively coupling the single-photon sources directly to single-mode fibre [83,84] or a photonic structure [55,56,78–82] is steadily

pushing QDs toward readiness for real-life applications. The biggest limitation of QDs is the need for cryogenic temperatures. However, the efficient fibre-coupled QD single-photon sources nowadays allow the operation of many of them within one cryostat. In such setups, QDs can be deterministically grown so that their wavelengths vary, enabling individual sources to occupy specific channels of spectral demultiplex channels in the future quantum network. Off-resonant excitation schemes, such as LA, will also allow efficient spectral filtering based on fiber Bragg gratings. Such a system can then serve as the core hardware in a data centre of the quantum internet, providing photonic qubits for the rest of the network. Another approach to surpassing the need for cryogenic temperatures is developing QDs that operate at higher temperatures, achievable by small and affordable Stirling coolers. InAs QDs based on an InGaAs metamorphic buffer layer emitting in the telecom C-band can be interesting sources for these applications, as they exhibit a deep confinement potential, typically spanning several hundreds of millielectron volts. Therefore, the emitted photon-number statistics are relatively insensitive to temperature fluctuations up to 30 K [61, 236].

9.3 Vision for quantum dots in future quantum networks

Nowadays, the quantum communication community often discusses the concept of a hybrid quantum internet, which combines different technologies tailored to the needs of individual users, integrated via quantum interconnections [27,321,322]. At first, we can simply divide the quantum internet into metropolitan networks and long-distance networks, with the latter serving as connections between metropolitan ones. Metropolitan networks are characterized by small communication distances and a high number of public users. To ensure accessibility of quantum internet to the general public, PDSs, such as attenuated lasers, are ideal sources for these metropolitan networks due to their good performance over short communication distances [14]. However, long-distance networks require high communication rates, long-distance reach, and compatibility with quantum repeaters, switches, memories, or quantum servers. For these applications, high-quality single-photon sources are essential, and QDs are considered a strong candidate for this role [307, 323].

The biggest challenge in the coming years will be developing efficient quantum interconnections [321] capable of connecting QDs, PDSs, and quantum memories to merge metropolitan networks and long-distance connections into a single, uniform quantum internet. These interconnections will need to align photons from different platforms in the spectral and temporal domains. Recent advancements in polarization-maintaining quantum frequency conversion [216, 217, 324, 325] and time lensing techniques [326–328] show significant progress toward achieving this goal. While QDs are unlikely to replace PDSs in metropolitan quantum communication applications, they will likely become a reliable building block of the future long-distance quantum internet.

A

APPENDIX: Mathematical tools for quantum cryptography

This appendix provides a concise overview of the mathematical tools and security analyses for quantum cryptography primitives with PDSs and QDs. The toolkit described here was used to derive results presented in Ch. 5 and Ch. 6. The text of the appendix is based on the supplementary material of our publication [52].

A.1 Semidefinite programming

Quantum theory relies on linear algebra. In quantum cryptography, security analyses frequently involve optimizing over semidefinite positive objects to identify the adversary's optimal cheating strategy. These objects often take the form of density matrices, measurement operators, or more broadly, completely positive trace-preserving (CPTP) maps. Semidefinite programming offers an appropriate framework for this task, enabling optimization over semidefinite positive variables while adhering to linear constraints.

A semidefinite program may be defined as a triple $\left(\Lambda, \hat{F}, \hat{C}\right)$ where Λ is a Hermitian-preserving CPTP map, and $\hat{F}$ and $\hat{C}$ are Hermitian operators defined in complex Hilbert spaces $\mathcal{H}_F$ and $\mathcal{H}_C$, respectively. We start by defining a maximization problem, which will serve as our primal problem. The primal problem maximizes a primal objective function defined as $\mathrm{Tr}\left(\hat{F}^\dagger \hat{X}\right)$, where $\hat{X}$ is positive semidefinite variable and the given set of linear constraints is expressed as a function of $\hat{C}$

$$\begin{aligned} \text{maximize} \quad & \mathrm{Tr}\left(\hat{F}^\dagger \hat{X}\right) \\ \text{s.t.} \quad & \Lambda(\hat{X}) = \hat{C} \\ & \hat{X} \geqslant 0 \ . \end{aligned} \tag{A.1-1}$$

The operator $\hat{X}$ which maximizes the primal objective function within given constraints is the primal optimal solution if it exists, and the corresponding value of $\mathrm{Tr}\left(\hat{F}^\dagger \hat{X}\right) := s_p$ is the primal optimal value.

In a semidefinite program, we can define a dual minimization problem associated with each primal maximization problem. Effectively, the new variable(s)

of the dual problem may be understood as the Lagrange multipliers for the constraints of the primal problem, where one variable of the dual problem is always associated with one constraint of the primal problem. The dual problem associated with (A.1-1) reads as

$$\begin{aligned} \text{minimize} \quad & \mathrm{Tr}\left(\hat{C}^\dagger \hat{Y}\right) \\ \text{s.t.} \quad & \Lambda^*(\hat{Y}) - \hat{F} \geqslant 0 \\ & \hat{Y} = \hat{Y}^\dagger \ . \end{aligned} \tag{A.1-2}$$

Similarly to the primal problem, the operator $\hat{Y}$ which minimizes the dual objective function $\mathrm{Tr}\left(\hat{C}^\dagger \hat{Y}\right)$ within the given constraints, if it exists, is the dual optimal solution, and the corresponding value of the dual objective function is the dual optimal value donated as s_d.

The Lagrange multiplier method enables the identification of local extrema for a constrained function. Consequently, the optimal value s_p of the primal problem serves as an upper bound for the optimal value s_d of the dual problem, while the optimal value of the dual problem serves as a lower bound for that of the primal. This property is known as weak duality and can be expressed as

$$s_p \leqslant s_d \ . \tag{A.1-3}$$

However, in many quantum-cryptographic applications, our goal is to verify that the upper bound derived in the primal problem is tight. This means ensuring that the local maximum is indeed a global maximum for the objective function. The dual problem will help to prove this when there exists a strong duality

$$s_p = s_d \ . \tag{A.1-4}$$

A.2 Security of quantum cryptography primitives

This chapter provides a comprehensive overview of security proofs for each quantum cryptography primitive. Initially, we will provide a summary of the established toolkit for PDSs, followed by the adaptation of security analysis for QDs. The updated security toolkit for QDs was developed and presented in our publication [52].

A.2.1 Security of BB84 quantum key distribution

A.2.1.1 With Poisson-distributed sources

We used practical security analysis of BB84 QKD protocol from [15, 134, 283] in versions with and without decoys states. All the equations to calculated gain, QBER and SKR are summarized in Ch. 2.2.3.4 and Ch. 2.2.3.5.

A.2.1.2 With quantum dot sources

For QDs with collection efficiency η, we simply replace the $P_\mu(k)$ photon number coefficients in Eqs. 2.2-29, 2.2-31, 2.2-35 and 2.2-36 by the following $P_\eta(k)$ coefficients

$$\begin{aligned} P_\eta(0) &= p_0 + p_1(1-\eta) + p_2(1-\eta)^2 \ , \\ P_\eta(1) &= p_1\eta + p_2\left[1-\eta^2-(1-\eta)^2\right] \ , \\ P_\eta(k\geqslant 2) &= 1 - P_\eta(0) - P_\eta(1) \ , \end{aligned} \tag{A.2-1}$$

where $\{p_n\}$ are the photon number populations from Eq. 5.1-18.

A.2.2 Security of twin-field quantum key distribution

A.2.2.1 With Poisson-distributed sources

The decoy method discussed in Ch. 2.2.3.5 can also be applied in TF-QKD, which implies that Alice and Bob must both randomize their pulses' global phase. However, a shared global phase reference must be established between the two parties at some point during the protocol without revealing any information to Charlie. In [115], the proposed method is for Alice and Bob to agree on a fixed number of global phase slices m, equally splitting the interval $[0, 2\pi)$, from which they uniformly sample a global phase for each state. After Charlie discloses the measurement outcomes, they reveal the chosen phase slice and sift the raw key in such a way that they keep only the elements for which their chosen phase slices match. Although this method may potentially leak information to eavesdroppers, alternative variants providing additional security measures have been proposed [329,330].

In this context, the SKR for TF-QKD is akin to that derived in Eq.2.2-30 for standard decoy QKD, with a few modifications. Firstly, the channel transmittance η_t in Eq.2.2-28 must be corrected to $\sqrt{\eta_t}$, since each optical pulse travels only half the distance between Alice and Bob. This gives the following expression for the yield

$$Y_k^{(TF)} = Y_0 + (1-Y_0)\left[1-(1-\eta_d\sqrt{\eta_t})^k\right]. \tag{A.2-2}$$

Then, an extra factor, dependent on the number of chosen phase slices m and the duty cycle d of quantum vs. classical signals, must be added to correct the key rate. This factor reads $\frac{d}{m}$. Finally, the intrinsic error rate e_s generated by the finite phase slicing must be taken into account on top of the overall setup alignment error e_d.This provides the following modified expression for the TF-QKD SKR [115]

$$SKR^{(TF)} \geqslant \frac{d}{2m}\left[Q_1^{(TF)}\left(1-H_2\left(e_1^{(TF)}\right)\right) - fQ_\mu^{(TF)}H_2\left(E_\mu^{(TF)}\right)\right], \tag{A.2-3}$$

where $H_2(x)$ is Shannon binary entropy as it was defined by Eq. 2.2-17 and the other variables are defined as follows

$$Q_k^{(TF)} = Y_k^{(TF)} P_\mu(k) \ , \tag{A.2-4}$$

$$Q_\mu^{(TF)} = \sum_{k=0}^{\infty} Q_k^{(TF)} \ , \tag{A.2-5}$$

$$e_k^{(TF)} = \frac{e_0 Y_0 + (e_d + e_s)\left[1 - \left(1 - \eta_d\sqrt{\eta_t}\right)^k\right]}{Y_k^{(TF)}} \ , \tag{A.2-6}$$

$$E_\mu^{(TF)} = \frac{1}{Q_\mu^{(TF)}} \sum_{k=0}^{\infty} e_k^{(TF)} Q_k^{(TF)} \ . \tag{A.2-7}$$

A.2.2.2 With quantum dot sources

Same as for BB84 QKD protocol, in the case of QDs with collection efficiency η, we simply replace the $P_\mu(k)$ photon number coefficients in Eq. A.2-3 by the following $P_\eta(k)$ coefficients:

$$\begin{aligned} P_\eta(0) &= p_0 + p_1(1-\eta) + p_2(1-\eta)^2 \ , \\ P_\eta(1) &= p_1\eta + p_2\left[1 - \eta^2 - (1-\eta)^2\right] \ , \\ P_\eta(k \geqslant 2) &= 1 - P_\eta(0) - P_\eta(1) \ , \end{aligned} \tag{A.2-8}$$

where $\{p_n\}$ are the photon number populations from Eq. 5.1-18.

A.2.3 Security of unforgeable quantum tokens

The security analysis of unforgeable quantum tokens is based on the semidefinite programming method described in Ch. A.1 followed by Choi's theorem on completely positive maps [331–333].

A.2.3.1 Unforgeability analysis for quantum tokens

We assume here quantum unforgeable token protocol as was described in [122], and we extend its security analysis to the QDs framework. A successful forging attack is one in which two copies of the QT state are simultaneously accepted at two spatially separated verification points, in the following analysis we will call these copies *token* 1 and *token* 2. Let Λ be the optimal adversarial map which produces two copies (defined in $\mathcal{H}_1 \otimes \mathcal{H}_2$) of the following original quantum token state living in $\mathcal{H}_{\text{ini}}$

$$\hat{\rho}_{\text{ini}} = \frac{1}{4} \sum_{k=0}^{3} \hat{\sigma}_k^{(\eta,\phi)} \ , \tag{A.2-9}$$

where the set $\{\hat{\sigma}(\eta,\phi)_k\}$ contains either the fixed-phase coherent states from Eq. 5.1 -21, the randomized phase coherent states given by Eq. 5.1-24, the QD states

exhibiting number coherence described by Eq. 5.1-32, or the quantum dot states without number coherence from Eq. 5.1-34. The superscripts (η, ϕ) serve as a reminder that these states depend on the PDS average photon number μ or QD collection efficiency η, and encoding phase ϕ.

This proof makes use of the existence of a squashing model for the measurement setup [334]. Essentially, it allows expressing the infinite-dimensional measurement operators in a 3-dimensional space spanned by $\{|0\rangle, |1\rangle, |\varnothing\rangle\}$, by imposing a condition on the terminal's postprocessing, consisting of assigning a random measurement outcome $|0\rangle$ or $|1\rangle$ to any double click, and declaring a $|\varnothing\rangle$ flag when no detection is registered. The probability that a verifier declares an incorrect measurement outcome for *token* 1 is given as

$$V_1 = \mathrm{Tr} \sum_{k=0}^{3} \left(\frac{1}{2} |\beta_k^{\perp}\rangle \langle \beta_k^{\perp}| \otimes \mathbb{1} \right) \Lambda \left(\frac{1}{4} \hat{\sigma}_k^{(\eta,\phi)} \right) , \tag{A.2-10}$$

while that for *token* 2 reads as

$$V_2 = \mathrm{Tr} \sum_{k=0}^{3} \left(\mathbb{1} \otimes \frac{1}{2} |\beta_k^{\perp}\rangle \langle \beta_k^{\perp}| \right) \Lambda \left(\frac{1}{4} \hat{\sigma}_k^{(\eta,\phi)} \right) , \tag{A.2-11}$$

where $|\beta_k\rangle$ is the squashed qubit associated with the original state $\sigma_k^{(\eta,\phi)}$, i.e. $|\beta_0\rangle = |+\rangle$, $|\beta_1\rangle = |+i\rangle$, $|\beta_2\rangle = |-\rangle$, $|\beta_3\rangle = |-i\rangle$, and $|\beta_k^{\perp}\rangle$ is its orthogonal qubit state. The factor $\frac{1}{4}$ indicates that each $\hat{\sigma}_k$ is equally likely to occur, while $\frac{1}{2}$ accounts for the verifier's random measurement basis choice. Using Choi's theorem, we may rewrite these expressions as $V_1 = \mathrm{Tr}\left(\hat{E}_1(\mu) J(\Lambda)\right)$ and $V_2 = \mathrm{Tr}\left(\hat{E}_2(\mu) J(\Lambda)\right)$, where $\hat{E}_1(\mu)$ and $\hat{E}_2(\mu)$ are the error operators defined by

$$\begin{aligned} \hat{E}_1(\mu) =& \frac{1}{4} \sum_{k=0}^{3} \frac{1}{2} |\beta_k^{\perp}\rangle \langle \beta_k^{\perp}| \otimes \mathbb{1} \otimes \overline{\hat{\sigma}_k^{(\eta,\phi)}} , \\ \hat{E}_2(\mu) =& \frac{1}{4} \sum_{k=0}^{3} \mathbb{1} \otimes \frac{1}{2} |\beta_k^{\perp}\rangle \langle \beta_k^{\perp}| \otimes \overline{\hat{\sigma}_k^{(\eta,\phi)}} . \end{aligned} \tag{A.2-12}$$

Following a similar method, the probability that verifier 1 (resp. 2) registers a no-detection event for a *token* 1 (resp. 2) reads $\mathrm{Tr}\left(\hat{L}_1(\mu) J(\Lambda)\right)$ (resp. $\mathrm{Tr}\left(\hat{L}_2(\mu) J(\Lambda)\right)$), where $\hat{L}_1(\mu)$ and $\hat{L}_2(\mu)$ are the loss operators, which contain the projection onto the state $|\varnothing\rangle$:

$$\begin{aligned} \hat{L}_1(\mu) &= \frac{1}{4} \sum_{k=0}^{3} |\varnothing\rangle \langle \varnothing| \otimes \mathbb{1} \otimes \overline{\hat{\sigma}_k^{(\eta,\phi)}}, \\ \hat{L}_2(\mu) &= \frac{1}{4} \sum_{k=0}^{3} \mathbb{1} \otimes |\varnothing\rangle \langle \varnothing| \otimes \overline{\hat{\sigma}_k^{(\eta,\phi)}}. \end{aligned} \tag{A.2-13}$$

We now search for the optimal cloning map Λ that minimizes the noise that the adversary must introduce for both tokens given a fixed combined channel and detection losses l. We cast this problem in the following semidefinite program for a card with a single state,

$$\begin{aligned} \min \quad & \mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right) \\ \text{s.t.} \quad & \mathrm{Tr}_{\mathcal{H}_1\otimes\mathcal{H}_2}\left(J(\Lambda)\right) = \mathbb{1}_{\mathcal{H}_{\mathrm{ini}}} \\ & \mathrm{Tr}\left(E_1(\mu)J(\Lambda)\right) \geqslant \mathrm{Tr}\left(E_2(\mu)J(\Lambda)\right) \\ & \mathrm{Tr}\left(\hat{L}_1(\mu)J(\Lambda)\right) \leqslant l \\ & \mathrm{Tr}\left(\hat{L}_2(\mu)J(\Lambda)\right) \leqslant l \\ & J(\Lambda) \geqslant 0 \ . \end{aligned} \tag{A.2-14}$$

The first constraint imposes that Λ is trace-preserving, the second imposes that the error rate measured for *token* 1 is at least equal to the one measured for *token* 2, the third and fourth impose that the losses measured for *tokens* 1 and 2 do not exceed the expected honest losses, and the fifth imposes that Λ is completely positive.

Using similar techniques to [122], it can be shown that this lower bound is in fact optimal, and that the adversary does not succeed better by performing a general attack on the full tensor product of the N states contained in the token.

A.2.4 Security of quantum strong coin flipping

We focus here on the quantum strong coin flipping protocol from [110], and additionally study the effect of photon number coherence on the protocol bias in the security proof.

A.2.4.1 Dishonest Alice

Since dishonest Alice can send any arbitrary quantum state to honest Bob, the corresponding security proof does not depend on the emitted PDS or QD state but depends only on the parameter encoding y imposed by the protocol, which was defined by Eq. 2.2-4. We assume here that Dishonest Alice aims to influence the coin flip outcome in favour of $x = 0$, aligning with $b = c$. Here, c represents a random bit encoded in the quantum state by Alice, and b is a random classical bit transmitted by Bob to Alice, as detailed in Chapter 2.2.2.3. Note that the security analysis proceeds similarly for outcome $x = 1$ with $b \neq c$.

From [110], dishonest Alice's optimal strategy consists of sending the state $|\Phi^{(y)}_{\alpha,c}\rangle$ that maximizes the average probability of revealing $(\alpha = 0, c = 0)$ and $(\alpha = 1, c = 1)$ or of revealing $(\alpha = 1, c = 0)$ and $(\alpha = 0, c = 1)$, where α denotes the encoding basis. Note that these four pairs yield a better cheating strategy than the other pairs, since the states in the pairs $\{|\Phi^{(y)}_{0,0}\rangle, |\Phi^{(y)}_{1,1}\rangle\}$ and $\{|\Phi^{(y)}_{1,0}\rangle, |\Phi^{(y)}_{0,1}\rangle\}$ have a larger overlap than the states in the pairs $\{|\Phi^{(y)}_{0,0}\rangle, |\Phi^{(y)}_{0,1}\rangle\}$

and $\{|\Phi_{1,0}^{(y)}\rangle, |\Phi_{1,1}^{(y)}\rangle\}$, for more intuition see the states' graphical representation at Fig. 2.4.

Following the arguments from [110, 126], dishonest Alice's optimal cheating strategy is to create an entangled state, of which she sends one half to Bob and saves the second half. She waits for his measurement and declaration of classical data and finally measures her part of the state to decide which outcome she reveals. This yields the following upper-bound on Alice's cheating probability

$$\mathcal{P}_A^{bias} \leqslant \frac{3}{4} + \frac{1}{2}\sqrt{y(1-y)}. \tag{A.2-15}$$

A.2.4.2 Dishonest Bob: without photon number coherence

In general, dishonest Bob's optimal cheating strategy involves some form of discrimination problem, in which he tries to identify which state was sent by Alice from a known and pre-agreed set of states. The works from [110,117,335] provided a practical security analysis for PDSs, with the crucial assumption that no coherence is present in the photon number basis. Consequently, we can apply these security assessments to RP PDSs, as well as to LA and TPE QD. However, for RE QDs, it becomes necessary to extend the security analysis to account for the presence of PNC in the states generated by Alice.

To upper bound Bob's cheating probability without PNC, we use the expression derived in [110], noting that it may not be a tight upper bound. However, this does not compromise the security of the protocol, as it only increases dishonest Bob's power. Similarly to dishonest Alice, we assume that dishonest Bob wishes to bias the flip outcome towards $x = 0$, corresponding to $b = c$. Note that the security analysis proceeds similarly for outcome $x = 1$ with $b \neq c$. As a brief summary, the cases in which Bob cannot perfectly cheat, considered in [110], are the following:

- A_1: Alice sends only vacuum states, with probability:
  $\mathcal{P}(A_1) = P_x^N(0)$.
- A_2: Alice sends at least one single-photon pulse, and vacuum states, with probability:
  $\mathcal{P}(A_2) = (P_x(0) + P_x(1))^N - P_x^N(0)$.
- A_3: Alice sends one two-photon pulse, and vacuum states, with probability:
  $\mathcal{P}(A_3) = NP_x(k \geqslant 2)P_x^{N-1}(0)$.
- A_4: Alice sends one two-photon pulse, at least one single-photon pulse, and vacuum states, with probability:
  $\mathcal{P}(A_4) = NP_x(k \geqslant 2)\left((P_x(0) + P_x(1))^{N-1} - P_x^{N-1}(0)\right)$

where $\{P_x(k)\}$ are the PDS coefficients from Eq. 5.1-25 for $x = \mu$ or the QD coefficients from Eq. (A.2-1) for $x = \eta$.

Assuming no coherence in photon number basis, Bob's cheating probability can be upper-bounded individually for each of the four cases [110]. In case A_1, Bob's optimal strategy involves declaring a random bit b', which will make him successfully bias the coin towards his desired outcome with probability $\mathcal{P}(b'|A_1) = 1/2$. In case A_2, Bob's optimal strategy consists of performing a Helstrom measurement to distinguish the quantum state, which is successful with probability $\mathcal{P}(b'|A_2) = y$. In case A_3, Bob's optimal cheating strategy also reads $\mathcal{P}(b'|A_3) = y$. In case A_4, an optimization must be performed to find the best set of discrimination measurement operators within the full spectrum of conclusive and inconclusive measurements. This allows to upper bound his cheating probability as $\mathcal{P}(b'|A_4) \leqslant -2y^2 + 4y - 1$ [110].

Summing the contributions from all four cases, and assuming that Bob can cheat with a probability 1 in all other cases, provides the final upper bound

$$\mathcal{P}_B^{bias} \leqslant \sum_{i=1}^{4} \mathcal{P}(A_i)\, \mathcal{P}\left(b'|A_i\right) + \left[1 - \sum_{i=1}^{4} \mathcal{P}(A_i)\right] \times 1. \tag{A.2-16}$$

A.2.4.3 Dishonest Bob: with photon number coherence

Extending the security proof to account for PNC in a photonic state generated by RE QDs is challenging. In contrast to the previous subsection, the security analysis cannot be broken down into independent components conditioned on the outcome of a photon number measurement. Dishonest Bob can exploit the presence of coherence to execute more comprehensive discrimination attacks.

We note that Bob's aim is to discriminate between the following two states sent by honest Alice with equal probabilities, in such a way that the outcome of the flip is optimally biased towards $x = 0$:

$$\begin{aligned} \hat{\sigma}_0^{(y,\eta,\phi)} &= \frac{1}{2}\left(\hat{\sigma}_{0,0}^{(y,\eta,\phi)} + \hat{\sigma}_{1,0}^{(y,\eta,\phi)}\right) \\ \hat{\sigma}_1^{(y,\eta,\phi)} &= \frac{1}{2}\left(\hat{\sigma}_{0,1}^{(y,\eta,\phi)} + \hat{\sigma}_{1,1}^{(y,\eta,\phi)}\right) . \end{aligned} \tag{A.2-17}$$

There exists a broad spectrum of discrimination measurements, which may be characterized by a set of parameters $\{p_{conc}, p_{corr}\}$ [126]. The first parameter, p_{conc}, represents the probability that implementing the POVM will result in a conclusive outcome, indicating that one state from the pre-agreed set was identified. The second parameter, p_{corr}, denotes the probability that this outcome is correct, confirming that the identified state is indeed the one which was sent by Alice. Fully conclusive measurements have $p_{conc} = 1$, but typically exhibit a non-unit probability of correctness $p_{corr} < 1$ (depending on the set of states). Other measurements may enhance p_{corr} by allowing some probability of inconclusive results $p_{conc} < 1$.

Of course, Bob's optimal discrimination strategy will involve optimizing over these parameters for all N states, which is beyond our scope. Nevertheless, we

show here how one powerful attack exploiting inconclusive measurement operators, known as USD [336,337], can already provide dishonest Bob with a cheating advantage over states which do not exhibit PNC. Intuitively, a USD POVM will return an outcome that is always correct ($p_{corr} = 1$), at the risk of getting an inconclusive outcome with some probability $p_{conc} < 1$. Since this attack yields inconclusive outcomes instead of erroneous ones, Bob can repeatedly perform the same attack on each state until the outcome is conclusive, in which case he has identified Alice's state without any error. If, after $(N-1)$ states, the attack is still inconclusive, he may then perform a conclusive minimum-error discrimination measurement on the last state, with $p_{corr} < 1$ and $p_{conc} = 1$, whose maximum success probability is given by the Helstrom bound [338].

To derive Bob's cheating probability in this case, we must first justify that USD is possible for our set of states. This entails confirming the existence of a USD attack that provides a non-zero probability of successfully identifying the state sent by Alice. For this, it suffices to note that the kernels associated with the states $\hat{\sigma}_0^{(y,\eta,\phi)}$ and $\hat{\sigma}_1^{(y,\eta,\phi)}$ living in the full photon space are both non-zero [336]. Although this is enough to derive an upper bound on the success of the USD measurement, i.e. on the value of p_{conc}, we must find a bound that is tight in order to provide a meaningful comparison with the over-estimated bounds from Eq. A.2-16. For this, we once again use the semidefinite programming techniques introduced in Ch. A.1. We extend the pure state treatment from [339] and the discrimination problem from [340] to recast dishonest Bob's search for the optimal USD strategy:

$$\begin{aligned} \max \quad & \frac{1}{2}\left[\mathrm{Tr}\left(\hat{M}_0\hat{\sigma}_0^{(y,\eta,\phi)}\right) + \mathrm{Tr}\left(\hat{M}_1\hat{\sigma}_1^{(y,\eta,\phi)}\right)\right] \\ \text{s.t.} \quad & \mathrm{Tr}\left(\hat{M}_0\hat{\sigma}_1^{(y,\eta,\phi)}\right) = 0 \\ & \mathrm{Tr}\left(\hat{M}_1\hat{\sigma}_0^{(y,\eta,\phi)}\right) = 0 \\ & \hat{M}_0 + \hat{M}_1 + \hat{M}_{inc} = \mathbb{1} \\ & \hat{M}_0, \hat{M}_1, \hat{M}_{inc} \geqslant 0 \ , \end{aligned} \tag{A.2-18}$$

where $\hat{M}_0$ and $\hat{M}_1$ are the POVM operators which identify the states $\hat{\sigma}_0^{(y,\eta,\phi)}$ and $\hat{\sigma}_1^{(y,\eta,\phi)}$, respectively, and $\hat{M}_{inc}$ is the POVM operator yielding an inconclusive outcome. All three operators serve as the optimization variables. The first two constraints ensure that the optimal POVM operators identify the correct state with zero error probability. Similarly to unforgeable quantum tokens, the tightness of this upper bound can be shown by using strong duality, see Ch. A.1 and [340].

We label Bob's optimal USD cheating probability coming from the solution of the semidefinite program given by Eq. A.2-18, as $\mathcal{P}_{USD}$. On the other hand, the probability of a successful Helstrom measurement is given by [338]

$$\mathcal{P}_{HEL} = \frac{1}{2} + \frac{1}{4}||\hat{\sigma}_0^{(y,\eta,\phi)} - \hat{\sigma}_1^{(y,\eta,\phi)}||_1 \ , \tag{A.2-19}$$

where $||\odot||_1$ denotes the Schatten 1-norm.

Since Bob performs the same USD based attack on each of the $(N-1)$ states sent by Alice, followed by a Helstrom measurement on the Nth state, we can finally upper-bound his cheating probability as

$$\mathcal{P}_B^{bias} \leqslant \left[1-(1-\mathcal{P}_{USD})^{N-1}\right] \times 1 + (1-\mathcal{P}_{USD})^{N-1} \times \mathcal{P}_{HEL} \ . \qquad \text{(A.2-20)}$$

A.2.5 Security of quantum bit commitment

We focus on the quantum bit commitment protocol from [16], under the bounded storage assumption. This assumption strategically sidesteps the no-go theorem for two-party computations [128,129] by imposing limitations on dishonest Bob's storage capabilities. Specifically, he is allowed to store only S out of the N quantum states transmitted by honest Alice, within a time frame not exceeding Δt. Similar to the BB84 QKD discussed in Chapter 2.2.3.4, the practical security analysis assumes that states emitted by honest Alice exhibit no coherence in the photon number basis. Consequently, we exclusively consider RP PDS and LA/TPE QD. In this context, we adopt here the conditions provided in the supplementary Information of [16] for a 3ϵ-secure quantum bit commitment implementation, where ϵ is a fixed parameter which upper-bounds the occurrence of bad events, governed by the Hoeffding inequality.

In a nutshell, the practical bit commitment protocol is constructed from a weak string erasure sub-routine with errors (WSEE) [341], which is defined by a set of parameters $(N, \lambda, \epsilon, e)$. WSEE provides Alice with a bit string X_N and Bob with a randomly chosen subset $I \in [N]$ and a substring $\widetilde{X}_I$. This substring is given by the substring X_I (the bits of X_N corresponding to the indices in I) passed through a binary symmetric channel that flips each bit of X_I with probability e. The security statements then read as follows:

- If Alice is honest, then the amount of information a Dishonest Bob holds about X_N is limited. Specifically, the ϵ-smooth min-entropy of X_N conditioned on a Dishonest Bob's information is lower bounded by a value λ.
- If Bob is honest, then Alice does not have any information I. That is, Alice does not learn which bits of X_N are known to Bob.

Essentially, losses allow Dishonest Bob to discard a fraction of single-photon detection events, and keep more multiphoton events so that his chance of guessing X_N correctly is increased. The resulting min-entropy rate λ can thereby be calculated as a function of experimental parameters $\{P_x(k)\}$ and $\{P_{(x\eta_c)}(k)\}$, where $\{P_x(k)\}$ are the PDS coefficients from Eq. (5.1-25) for $x = \mu$ or the QDcoefficients from Eq. (A.2-1) for $x = \eta$, and $\{P_{(x\eta_c)}(k)\}$ are defined similarly, only with an extra channel transmission factor η_c multiplying x to account for honest losses.

Following Lemma 12 from the Supplementary Information of [16], given an experimental error rate e, channel losses η_c, fixed parameters ϵ and $(\beta, \gamma) \in (0, 0.01]$,

and considering a Dishonest Bob with bounded storage size S, we define the following parameters

$$\begin{aligned}
m_2 &= P_x(1) - P_{(x\eta_c)}(0) + P_x(0) - 3\gamma \ , \\
m_3 &= 1 - P_{(x\eta_c)}(k) \ , \\
L' &= \max_{s\in(0,1]} -\frac{1}{s}\left[\log\left(1+2^s\right) - 1 - s\right] - \frac{3\epsilon}{s} \ , \\
\delta &= 2\,\frac{e + \frac{\beta}{\sqrt{1-2\beta}}}{1-4\sqrt{5}\beta} \ , \\
\lambda &= H_2(\delta) + 3\beta^2 \ , \\
M_1 &= \frac{1}{2\gamma^2}\log\frac{2}{\epsilon} \ , \\
M_2 &= \frac{\log\frac{1}{\epsilon}}{\epsilon\, m_2} \ , \\
M_3 &= \frac{\log\frac{2}{\epsilon}}{(m_3-\gamma)\,\beta^2} \ , \\
M_4 &= \frac{S}{m_2 L' - m_3\lambda} \ ,
\end{aligned} \tag{A.2-21}$$

where $H_2(x)$ is Shannon binary entropy defined for $0 < x \leqslant 1$ by Eq. 2.2-17. For security to hold in a practical implementation, the following condition must hold

$$m_2 L' - m_3\lambda > 0 \ . \tag{A.2-22}$$

If Eq. A.2-22 is true, then quantum bit commitment under the bounded storage model can be implemented 3ϵ-securely by using a randomly constructed error-correcting code, whenever the number of states sent by Alice

$$N > \max\{M_1, M_2, M_3, M_4\}. \tag{A.2-23}$$

B

APPENDIX: Photon-number optimization via variable attenuation

For QKD implementations using WCSs, the mean photon number must be optimized for each protocol efficiency to achieve the maximum possible SK [134]. In Chapter 2.2.3.4, we discussed that the optimal mean photon number is approximately equal to the protocol efficiency $\mu_{opt} \approx \eta$. Here, we will apply a similar approach to QDs, where the final source brightness can be controlled using a variable attenuator to optimize the achievable SK [316].

The equation to calculate the gain, QBER, and SK of the QKD protocol without decoy states were derived in Ch. 2.2.3.4, following the approaches in [134]. These calculations are based on the estimated photon-number probabilities p_k. To include the variable attenuation to our QD single-photon source we will use the approach of the variable BS, which was derived in Ch. 5.1.5.2 and Ch. A.2.1.2. The photon-number probabilities are then given as

$$\begin{aligned} p_0(\eta_{\mathrm{att}}) &= p_0 + p_1(1-\eta_{\mathrm{att}}) + p_{\mathrm{m}}(1-\eta_{\mathrm{att}})^2 \ , \\ p_1(\eta_{\mathrm{att}}) &= p_1\eta_{\mathrm{att}} + p_{\mathrm{m}}(1-\eta_{\mathrm{att}}^2 - (1-\eta_{\mathrm{att}})^2) \ , \\ p_{\mathrm{m}}(\eta_{\mathrm{att}}) &= 1 - p_0(\eta_{\mathrm{att}}) - p_1(\eta_{\mathrm{att}}) \ , \end{aligned} \tag{B.0-1}$$

where $p_m = p_{k>1}$ is multi-photon probability, η_{att} is the probability to transmit a photon and we assumed $p_2 \gg p_3$. Using the modified set of $p_k(\eta_{\mathrm{att}})$, we follow the approach outlined in Chapter 2.2.3.4 to calculate the SK. For each communication distance, we optimize the SK over η_{att} to evaluate the full potential of a given QD. The results, shown in Fig. B.1, compare the QD used in our publication [99] with the idealized QD single-photon source.

We see that for our source parameters ($B = 2.5\,\%$, $g^{(2)}(0) = 4.3\,\%$) as reported in [99], the SK achievable at the QD's maximum brightness closely aligns with the point-wise optimized SK. This is because the experimental brightness was already low, and further optimization through attenuation would decrease the effective brightness ($B_{\mathrm{eff}}(\eta_{\mathrm{att}}) = p_0(\eta_{\mathrm{att}}) + p_1(\eta_{\mathrm{att}}) + p_{\mathrm{m}}(\eta_{\mathrm{att}})$), therefore reduce the maximum communication distance and the SK at shorter distances.

However, if we consider a QD with ideal brightness ($B = 100\,\%$) and the same single-photon purity characterized by a second-order correlation function $g^{(2)}(0) = 4.3\,\%$, the advantages of adjusting attenuation according to channel loss become evident, as shown in Fig.B.1 (b). The enveloping curve, the point-wise

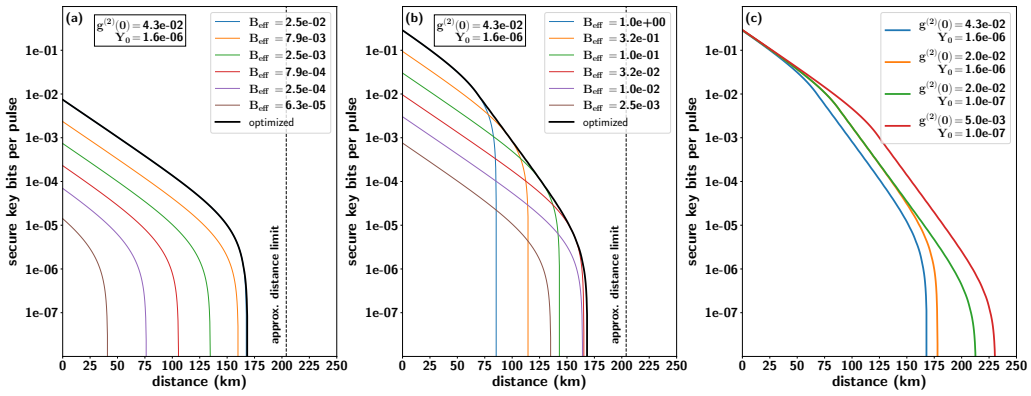


Figure B.1: **Secure key bits per pulse over distance for variable signal attenuation.** Including a variable attenuator in the sender's setup can improve the secure key bits per pulse at large distances. (a)-(b) The secure key bits per pulse as a function of distance is displayed for six effective brightness values, B_{eff}. The thick, black line represents the attainable secure key bits per pulse for a point-wise optimization of B_{eff}. The dotted vertical line indicates the approximated maximum distance according to Eq. 7.2-6. The dark-count probability $Y_0 = 1.6 \cdot 10^{-6}$ and purity of 95.7 % correspond to the experimental data at ideal brightness excitation conditions. For (a) the maximum brightness $B = 2.5\,\%$ corresponds to the experimental value whereas for (b) an ideal brightness, $B = 100\,\%$, is assumed. (c) Point-wise optimized curves for a set of $\{g^{(2)}(0), Y_0\}$ highlighting the different influences on the secure key bits per pulse. The parameters for all plots are: single-photon detection error $e_{\text{d}} = 2\,\%$, detection efficiency $\eta_{\text{d}} = 86\,\%$, error-correction code inefficiency $f = 1.2$, fiber attenuation $\alpha = 0.17\,\text{dB/km}$.

optimized SK, can now be divided into three regions. For short communication distances up to approximately 75 km, the highest SK is achieved with a non-attenuated QD, as at low protocol losses, the SK is primarily determined by p_1. In the next region, continuous balancing of $p_1(\eta_{\text{att}})$ and $p_{\text{m}}(\eta_{\text{att}})$ is required to achieve the optimal SK for a given communication distance. Finally, for long distances beyond approximately 170 km, further attenuation fails to extend the maximum distance, as the impact of dark counts becomes dominant.

In Fig. B.1 (a)-(b) we also identify the maximum communication distance calculated by Eq. 7.2-6 where the brightness corresponds to the ideal long-distance brightness. We see Eq. 7.2-6 overestimates the maximal distance over ~ 30 km as we discussed in Ch. 7.2.1.

We analyzed the impact of single-photon purity and detector dark-count probabilities Y_0 on the maximum SK, assuming an ideal QD brightness of $B = 100\,\%$. The attenuation-optimized SK for different parameter sets is presented in Fig.B.1 (c). The first inflection point is influenced by single-photon purity, given by the multi-photon probability p_{m}, see Eq. 3.0-25. Higher multi-photon probabilities cause the SK to drop at shorter communication distances because the information leakage from multi-photon events becomes too significant to extract a SK from the raw key. The point at which the SK drops a second time is influenced by both studied parameters: single-photon purity and detector dark counts. At this stage, the probability of signal clicks becomes comparable to that of dark-count clicks, leading to a high error rate ϵ_1. Overall, we observe that single-photon purity has minimal impact on SK at short communication distances but enhances SK at medium distances. When combined with a low dark-count probability, it also significantly increases the maximum achievable communication distance d_{max}.

Bibliography

[1] D. Castelvecchi, "Ibm releases first-ever 1, 000-qubit quantum chip," *Nature*, vol. 624, no. 7991, p. 238–238, 2023.

[2] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, "Superconducting qubits: Current state of play," *Annual Review of Condensed Matter Physics*, vol. 11, no. 1, p. 369–395, 2020.

[3] C. Q. Choi, "Ibm's quantum leap: The company will take quantum tech past the 1, 000-qubit mark in 2023," *IEEE Spectrum*, vol. 60, no. 1, p. 46–47, 2023.

[4] S. Patra, S. S. Jahromi, S. Singh, and R. Orús, "Efficient tensor network simulation of ibm's largest quantum processors," *Physical Review Research*, vol. 6, no. 1, 2024.

[5] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada, and J. Lavoie, "Quantum computational advantage with a programmable photonic processor," *Nature*, vol. 606, no. 7912, pp. 75–81, 2022.

[6] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, J. J. Renema, C.-Y. Lu, and J.-W. Pan, "Phase-programmable gaussian boson sampling using stimulated squeezed light," *Phys. Rev. Lett.*, vol. 127, p. 180502, 2021.

[7] K. Alexander, A. Bahgat, A. Benyamini, D. Black, D. Bonneau, S. Burgos, B. Burridge, G. Campbell, G. Catalano, A. Ceballos, C.-M. Chang, C. Chung, F. Danesh, T. Dauer, M. Davis, E. Dudley, P. Er-Xuan, J. Fargas, A. Farsi, C. Fenrich, J. Frazer, M. Fukami, Y. Ganesan, G. Gibson, M. Gimeno-Segovia, S. Goeldi, P. Goley, R. Haislmaier, S. Halimi, P. Hansen, S. Hardy, J. Horng, M. House, H. Hu, M. Jadidi, H. Johansson, T. Jones, V. Kamineni, N. Kelez, R. Koustuban, G. Kovall, P. Krogen, N. Kumar, Y. Liang, N. LiCausi, D. Llewellyn, K. Lokovic, M. Lovelady, V. Manfrinato, A. Melnichuk, M. Souza, G. Mendoza, B. Moores, S. Mukherjee, J. Munns, F.-X. Musalem, F. Najafi, J. L. O'Brien, J. E. Ortmann, S. Pai, B. Park, H.-T. Peng, N. Penthorn, B. Peterson, M. Poush, G. J. Pryde, T. Ramprasad,

G. Ray, A. Rodriguez, B. Roxworthy, T. Rudolph, D. J. Saunders, P. Shadbolt, D. Shah, H. Shin, J. Smith, B. Sohn, Y.-I. Sohn, G. Son, C. Sparrow, M. Staffaroni, C. Stavrakas, V. Sukumaran, D. Tamborini, M. G. Thompson, K. Tran, M. Triplet, M. Tung, A. Vert, M. D. Vidrighin, I. Vorobeichik, P. Weigel, M. Wingert, J. Wooding, and X. Zhou, "A manufacturable platform for photonic quantum computing," 2024.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[9] E. Gouzien and N. Sangouard, "Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory," *Phys. Rev. Lett.*, vol. 127, p. 140503, 2021.

[10] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, "Experimental realization of shor's quantum factoring algorithm using qubit recycling," *Nat. Photonics*, vol. 6, pp. 773–776, 2012.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[13] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, pp. 351–382, 2016.

[14] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, p. 025002, 2020.

[15] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, 2005.

[16] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, "Experimental implementation of bit commitment in the noisy-storage model," *Nature Communications*, vol. 3, no. 1, 2012.

[17] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li, H.-F. Zhang, Y. Zhao, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, "Experimental unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 112, p. 010504, 2014.

[18] J.-Y. Guan, J.-M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J.-W. Pan, "Experimental preparation and verification of quantum money," *Phys. Rev. A*, vol. 97, p. 032338, 2018.

[19] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, "Quantum weak coin flipping with a single photon," *Phys. Rev. A*, vol. 102, p. 022414, 2020.

[20] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, H.-F. Zhang, K. Cui, H. Liang, X.-G. Li, Y. Mao, L.-J. Wang, S.-B. Feng, Q. Chen, Q. Zhang, L. Li, N.-L. Liu, C.-Z. Peng, X. Ma, Y. Zhao, and J.-W. Pan, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Information*, vol. 7, no. 1, 2021.

[21] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[22] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network," in *SPIE Proceedings* (E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds.), SPIE, 2005.

[23] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[24] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4, 600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[25] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, vol. 120, no. 3, 2018.

[26] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[27] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[28] M. Anderson, T. Müller, J. Skiba-Szymanska, A. B. Krysa, J. Huwer, R. M. Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields, "Gigahertz-Clocked Teleportation of Time-Bin Qubits with a Quantum Dot in the Telecommunication C Band," *Physical Review Applied*, vol. 13, no. 5, p. 054052, 2020.

[29] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, p. 190502, 2018.

[30] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, 2000.

[31] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Inf.*, vol. 4, p. 5, 2018.

[32] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, "Experimental plug and play quantum coin flipping," *Nat. Commun.*, p. 3717.

[33] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, p. 022308, 2013.

[34] M. Duvsek, M. Jahma, and N.Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A*, vol. 62, p. 022306, 2000.

[35] J. Schneeloch, S. H. Knarr, D. F. Bogorin, M. L. Levangie, C. C. Tison, R. Frank, G. A. Howland, M. L. Fanto, and P. M. Alsing, "Introduction

to the absolute brightness and number statistics in spontaneous parametric down-conversion," *J. Opt.*, vol. 21, no. 4, p. 043501, 2019.

[36] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, "Experimental bit commitment based on quantum communication and special relativity," *Phys. Rev. Lett.*, vol. 111, p. 180504, 2013.

[37] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, p. 210801, 2023.

[38] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, 2017.

[39] S. K. Liao, H. L. Yong, C. Liu, G. L. Shentu, D. D. Li, J. Lin, H. Dai, S. Q. Zhao, B. Li, J. Y. Guan, W. Chen, Y. H. Gong, Y. Li, Z. H. Lin, G. S. Pan, J. S. Pelc, M. M. Fejer, W. Z. Zhang, W. Y. Liu, J. Yin, J. G. Ren, X. B. Wang, Q. Zhang, C. Z. Peng, and J. W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photon.*, vol. 11, no. 8, pp. 509–513, 2017.

[40] V. Saggio, B. E. Asenbeck, A. Hamann, T. Strömberg, P. Schiansky, V. Dunjko, N. Friis, N. C. Harris, M. Hochberg, D. Englund, S. Wölk, H. J. Briegel, and P. Walther, "Experimental quantum speed-up in reinforcement learning agents," *Nature*, vol. 591, no. 7849, pp. 229–233, 2021.

[41] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, p. 1460–1463, 2020.

[42] J. C. Adcock, C. Vigliar, R. Santagati, J. W. Silverstone, and M. G. Thompson, "Programmable four-photon graph states on a silicon chip," *Nature Communications*, vol. 10, no. 1, 2019.

[43] A. Aspuru-Guzik and P. Walther, "Photonic quantum simulators," *Nature Physics*, vol. 8, no. 4, p. 285–291, 2012.

[44] G. Brida, M. Genovese, and I. Ruo Berchera, "Experimental realization of sub-shot-noise quantum imaging," *Nature Photonics*, vol. 4, no. 4, p. 227–230, 2010.

[45] G. B. Lemos, V. Borish, G. D. Cole, S. Ramelow, R. Lapkiewicz, and A. Zeilinger, "Quantum imaging with undetected photons," *Nature*, vol. 512, no. 7515, p. 409–412, 2014.

[46] R. Tenne, U. Rossman, B. Rephael, Y. Israel, A. Krupinski-Ptaszek, R. Lapkiewicz, Y. Silberberg, and D. Oron, "Super-resolution enhancement by quantum image scanning microscopy," *Nature Photonics*, vol. 13, no. 2, p. 116–122, 2018.

[47] L.-Z. Liu, Y.-Z. Zhang, Z.-D. Li, R. Zhang, X.-F. Yin, Y.-Y. Fei, L. Li, N.-L. Liu, F. Xu, Y.-A. Chen, and J.-W. Pan, "Distributed quantum phase estimation with entangled photons," *Nature Photonics*, vol. 15, no. 2, p. 137–142, 2020.

[48] E. Meyer-Scott, C. Silberhorn, and A. Migdall, "Single-photon sources: Approaching the ideal through multiplexing," *Review of Scientific Instruments*, vol. 91, no. 4, 2020.

[49] F. Kaneda and P. G. Kwiat, "High-efficiency single-photon generation via large-scale active time multiplexing," *Sci. Adv.*, vol. 5, no. 10, p. eaaw8586, 2019.

[50] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, "Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source," *Phys. Rev. Lett.*, vol. 100, p. 090501, 2008.

[51] T. Kobayashi, A. Tomita, and A. Okamoto, "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser," *Phys. Rev. A*, vol. 90, p. 032320, 2014.

[52] M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler, and P. Walther, "Enhancing quantum cryptography with quantum dot single-photon sources," *npj Quantum Inf.*, vol. 8, p. 104, 2022.

[53] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, *et al.*, "Experimental quantum repeater without quantum memory," *Nature photonics*, vol. 13, no. 9, pp. 644–648, 2019.

[54] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, no. 1, 2015.

[55] P. Senellart, G. Solomon, and A. White, "High-performance semiconductor quantum-dot single-photon sources," *Nature nanotechnology*, vol. 12, no. 11, pp. 1026–1039, 2017.

[56] X. Ding, Y.-P. Guo, M.-C. Xu, R.-Z. Liu, G.-Y. Zou, J.-Y. Zhao, Z.-X. Ge, Q.-H. Zhang, H.-L. Liu, L.-J. Wang, M.-C. Chen, H. Wang, Y.-M. He, Y.-H. Huo, C.-Y. Lu, and J.-W. Pan, "High-efficiency single-photon source above the loss-tolerant threshold for efficient linear optical quantum computing," 2023.

[57] M. Sartison, L. Engel, S. Kolatschek, F. Olbrich, C. Nawrath, S. Hepp, M. Jetter, P. Michler, and S. L. Portalupi, "Deterministic integration and optical characterization of telecom o-band quantum dots embedded into wet-chemically etched gaussian-shaped microlenses," *Applied Physics Letters*, vol. 113, no. 3, 2018.

[58] S. Kolatschek, C. Nawrath, S. Bauer, J. Huang, J. Fischer, R. Sittig, M. Jetter, S. L. Portalupi, and P. Michler, "Bright purcell enhanced single-photon source in the telecom o-band based on a quantum dot in a circular bragg grating," *Nano Letters*, vol. 21, no. 18, p. 7740–7745, 2021.

[59] C. Nawrath, F. Olbrich, M. Paul, S. L. Portalupi, M. Jetter, and P. Michler, "Coherence and indistinguishability of highly pure single photons from non-resonantly and resonantly excited telecom c-band quantum dots," *Applied Physics Letters*, vol. 115, no. 2, 2019.

[60] C. Nawrath, H. Vural, J. Fischer, R. Schaber, S. L. Portalupi, M. Jetter, and P. Michler, "Resonance fluorescence of single in(ga)as quantum dots emitting in the telecom c-band," *Appl. Phys. Lett.*, vol. 118, no. 24, p. 244002, 2021.

[61] C. Nawrath, R. Joos, S. Kolatschek, S. Bauer, P. Pruy, F. Hornung, J. Fischer, J. Huang, P. Vijayan, R. Sittig, M. Jetter, S. L. Portalupi, and P. Michler, "Bright source of purcell-enhanced, triggered, single photons in the telecom c-band," *Advanced Quantum Technologies*, vol. 6, no. 11, 2023.

[62] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, Z. Wang, C. Schneider, J. J. Renema, S. Höfling, C.-Y. Lu, and J.-W. Pan, "Boson sampling with 20 input photons and a 60-mode interferometer in a 10^{14}-dimensional hilbert space," *Phys. Rev. Lett.*, vol. 123, p. 250503, 2019.

[63] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, "Quantum cryptography with a photon turnstile," *Nature*, vol. 420, p. 762, 2002.

[64] R. J. Collins, P. J. Clarke, V. Fernández, K. J. Gordon, M. N. Makhonin, J. A. Timpson, A. Tahraoui, M. Hopkinson, A. M. Fox, M. S. Skolnick, and

G. S. Buller, "Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source," *J. Appl. Phys.*, vol. 107, no. 7, p. 073102, 2010.

[65] P. Intallura, M. Ward, O. Karimov, Z. Yuan, P. See, P. Atkinson, D. Ritchie, and A. Shields, "Quantum communication using single photons from a semiconductor quantum dot emitting at a telecommunication wavelength," *Journal of Optics A: Pure and Applied Optics*, vol. 11, p. 5, 2009.

[66] T. Heindel, C. A. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W.-M. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth, M. Lermer, H. Weier, M. Jetter, M. Kamp, S. Reitzenstein, S. Höfling, P. Michler, H. Weinfurter, and A. Forchel, "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New J. Phys.*, vol. 14, no. 8, p. 083001, 2012.

[67] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120km using ultrahigh purity single-photon source and superconducting single-photon detectors," *Sci. Rep.*, vol. 5, p. 14383, 2015.

[68] C. Schimpf, M. Reindl, D. Huber, B. Lehner, S. F. C. D. Silva, S. Manna, M. Vyvlecka, P. Walther, and A. Rastelli, "Quantum cryptography with highly entangled photons from semiconductor quantum dots," *Sci. Adv.*, vol. 7, p. 16, 2021.

[69] F. B. Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta, "Quantum key distribution with entangled photons generated on demand by a quantum dot," *Sci. Adv.*, vol. 7, p. 12, 2021.

[70] M. Zahidy, M. T. Mikkelsen, R. Müller, B. Da Lio, M. Krehbiel, Y. Wang, N. Bart, A. D. Wieck, A. Ludwig, M. Galili, S. Forchhammer, P. Lodahl, L. K. Oxenløwe, D. Bacco, and L. Midolo, "Quantum key distribution using deterministic single-photon sources over a field-installed fibre link," 2023.

[71] J. Yang, Z. Jiang, F. Benthin, J. Hanel, T. Fandrich, R. Joos, S. Bauer, S. Kolatschek, A. Hreibi, E. P. Rugeramigabo, M. Jetter, S. L. Portalupi, M. Zopf, P. Michler, S. Kück, and F. Ding, "High-rate intercity quantum key distribution with a semiconductor single-photon source," 2023.

[72] D. Huber, M. Reindl, S. F. Covre da Silva, C. Schimpf, J. Martín-Sánchez, H. Huang, G. Piredda, J. Edlinger, A. Rastelli, and R. Trotta, "Strain-tunable gaas quantum dot: A nearly dephasing-free source of entangled photon pairs on demand," *Phys. Rev. Lett.*, vol. 121, p. 033902, 2018.

[73] F. B. Basset, F. Salusti, L. Schweickert, M. B. Rota, D. Tedeschi, S. F. C. da Silva, E. Roccia, V. Zwiller, K. D. Jöns, A. Rastelli, and R. Trotta, "Quantum teleportation with imperfect quantum dots," *npj Quantum Inf.*, vol. 7, p. 7, 2021.

[74] M. Reindl, D. Huber, C. Schimpf, S. F. C. da Silva, M. B. Rota, H. Huang, V. Zwiller, K. D. Jöns, A. Rastelli, and R. Trotta, "All-photonic quantum teleportation using on-demand solid-state quantum emitters," *Sci. Adv.*, vol. 4, no. 12, 2018.

[75] F. Basso Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. Covre da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli, and R. Trotta, "Entanglement Swapping with Photons Generated on Demand by a Quantum Dot," *Phys. Rev. Lett.*, vol. 123, no. 16, p. 160501, 2019.

[76] M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding, and O. G. Schmidt, "Entanglement Swapping with Semiconductor-Generated Photons Violates Bell's Inequality," *Phys. Rev. Lett.*, vol. 123, no. 16, p. 160502, 2019.

[77] S. E. Thomas, L. Wagner, R. Joos, R. Sittig, C. Nawrath, P. Burdekin, T. Huber-Loyola, S. Sagona-Stophel, S. Höfling, M. Jetter, P. Michler, I. A. Walmsley, S. L. Portalupi, and P. M. Ledingham, "Deterministic storage and retrieval of telecom quantum dot photons interfaced with an atomic quantum memory," 2023.

[78] J. Liu, R. Su, Y. Wei, B. Yao, S. F. C. d. Silva, Y. Yu, J. Iles-Smith, K. Srinivasan, A. Rastelli, J. Li, *et al.*, "A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability," *Nature nanotechnology*, vol. 14, no. 6, pp. 586–593, 2019.

[79] N. Somaschi, V. Giesz, L. De Santis, J. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, *et al.*, "Near-optimal single-photon sources in the solid state," *Nature Photonics*, vol. 10, no. 5, pp. 340–345, 2016.

[80] N. Tomm, A. Javadi, N. O. Antoniadis, D. Najer, M. C. Löbl, A. R. Korsch, R. Schott, S. R. Valentin, A. D. Wieck, A. Ludwig, *et al.*, "A bright and fast source of coherent single photons," *Nature Nanotechnology*, vol. 16, no. 4, pp. 399–403, 2021.

[81] P. Lodahl, A. Floris van Driel, I. S. Nikolaev, A. Irman, K. Overgaag, D. Vanmaekelbergh, and W. L. Vos, "Controlling the dynamics of spontaneous emission from quantum dots by photonic crystals," *Nature*, vol. 430, no. 7000, p. 654–657, 2004.

[82] A. Faraon, A. Majumdar, D. Englund, E. Kim, M. Bajcsy, and J. Vučković, "Integrated quantum optical networks based on quantum dots and photonic crystals," *New Journal of Physics*, vol. 13, no. 5, p. 055025, 2011.

[83] R. S. Daveau, K. C. Balram, T. Pregnolato, J. Liu, E. H. Lee, J. D. Song, V. Verma, R. Mirin, S. W. Nam, L. Midolo, S. Stobbe, K. Srinivasan, and P. Lodahl, "Efficient fiber-coupled single-photon source based on quantum dots in a photonic-crystal waveguide," *Optica*, vol. 4, no. 2, p. 178, 2017.

[84] L. Bremer, K. Weber, S. Fischbach, S. Thiele, M. Schmidt, A. Kaganskiy, S. Rodt, A. Herkommer, M. Sartison, S. L. Portalupi, P. Michler, H. Giessen, and S. Reitzenstein, "Quantum dot single-photon emission coupled into single-mode fibers with 3d printed micro-objectives," *APL Photonics*, vol. 5, no. 10, 2020.

[85] R. Trivedi, K. A. Fischer, J. Vučković, and K. Müller, "Generation of non-classical light using semiconductor quantum dots," *Advanced Quantum Technologies*, vol. 3, no. 1, p. 1900007, 2020.

[86] P. Michler, *Quantum Dots for Quantum Information Technologies*. Springer International Publishing, 2017.

[87] R. Uppu, F. T. Pedersen, Y. Wang, C. T. Olesen, C. Papon, X. Zhou, L. Midolo, S. Scholz, A. D. Wieck, A. Ludwig, and P. Lodahl, "Scalable integrated single-photon source," *Sci. Adv.*, vol. 6, no. 50, p. eabc8268, 2020.

[88] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaítre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart, "Near-optimal single-photon sources in the solid state," *Nat. Photonics*, vol. 10, p. 340, 2016.

[89] Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu, and J.-W. Pan, "On-demand semiconductor single-photon source with near-unity indistinguishability," *Nat. Nanotechnol.*, vol. 8, p. 213, 2013.

[90] S. E. Thomas, M. Billard, N. Coste, S. C. Wein, Priya, H. Ollivier, O. Krebs, L. Tazaïrt, A. Harouri, A. Lemaitre, I. Sagnes, C. Anton, L. Lanco, N. Somaschi, J. C. Loredo, and P. Senellart, "Bright polarized single-photon source based on a linear dipole," *Phys. Rev. Lett.*, vol. 126, p. 233601, 2021.

[91] M. Cosacchi, F. Ungar, M. Cygorek, A. Vagov, and V. M. Axt, "Emission-frequency separated high quality single-photon sources enabled by phonons," *Phys. Rev. Lett.*, vol. 123, p. 017403, 2019.

[92] I. A. Akimov, J. T. Andrews, and F. Henneberger, "Stimulated emission from the biexciton in a single self-assembled ii-vi quantum dot," *Phys. Rev. Lett.*, vol. 96, p. 067401, 2006.

[93] F. Sbresny, L. Hanschke, E. Schöll, W. Rauhaus, B. Scaparra, K. Boos, E. Zubizarreta Casalengua, H. Riedl, E. del Valle, J. J. Finley, K. D. Jöns, and K. Müller, "Stimulated generation of indistinguishable single photons from a quantum ladder system," *Phys. Rev. Lett.*, vol. 128, p. 093603, 2022.

[94] Y. Karli, D. A. Vajner, F. Kappe, P. C. A. Hagen, L. M. Hansen, R. Schwarz, T. K. Bracht, C. Schimpf, S. F. Covre da Silva, P. Walther, A. Rastelli, V. M. Axt, J. C. Loredo, V. Remesh, T. Heindel, D. E. Reiter, and G. Weihs, "Controlling the photon number coherence of solid-state quantum light sources for quantum cryptography," *npj Quantum Information*, vol. 10, no. 1, 2024.

[95] K. A. Fischer, L. Hanschke, M. Kremser, J. J. Finley, K. Müller, and J. Vučković, "Pulsed rabi oscillations in quantum two-level systems: beyond the area theorem," *Quantum Sci. Technol.*, vol. 3, no. 1, p. 014006, 2017.

[96] L. Hanschke, K. A. Fischer, S. Appel, D. Lukin, J. Wierzbowski, S. Sun, R. Trivedi, J. Vučković, J. J. Finley, and K. Müller, "Quantum dot single-photon sources with ultra-low multi-photon probability," *npj Quantum Inf.*, vol. 4, no. 1, 2018.

[97] J. C. Loredo, C. Antón, B. Reznychenko, P. Hilaire, A. Harouri, C. Millet, H. Ollivier, N. Somaschi, L. De Santis, A. Lemaître, and et al., "Generation of non-classical light in a photon-number superposition," *Nat. Photonics*, vol. 13, no. 11, pp. 803–808, 2019.

[98] C. Schimpf, "Quantum communication with semiconductor quantum dots," 2022.

[99] M. Vyvlecka, L. Jehle, C. Nawrath, F. Giorgino, M. Bozzio, R. Sittig, M. Jetter, S. L. Portalupi, P. Michler, and P. Walther, "Robust excitation of c-band quantum dots for quantum communication," *Applied Physics Letters*, vol. 123, no. 17, 2023.

[100] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, p. 379–423, 1948.

[101] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, p. 145, 2002.

[102] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, 2020.

[103] J. L. O'Brien, "Optical quantum computing," *Science*, vol. 318, no. 5856, p. 1567–1570, 2007.

[104] A. Steane, "Quantum computing," *Reports on Progress in Physics*, vol. 61, no. 2, p. 117–173, 1998.

[105] D. Gottesman, "Theory of fault-tolerant quantum computation," *Physical Review A*, vol. 57, no. 1, p. 127–137, 1998.

[106] N. Peters, J. Altepeter, E. Jeffrey, D. Branning, and P. Kwiat, "Precise creation, characterization, and manipulation of single optical qubits," *Quantum Information and Computation*, vol. 3, no. special, pp. 503–517, 2003.

[107] R. Simon and N. Mukunda, "Universal su(2) gadget for polarization optics," *Physics Letters A*, vol. 138, no. 9, p. 474–480, 1989.

[108] R. Simon and N. Mukunda, "Minimal three-component su(2) gadget for polarization optics," *Physics Letters A*, vol. 143, no. 4–5, p. 165–169, 1990.

[109] J. Altepeter, E. Jeffrey, and P. Kwiat, *Photonic State Tomography*, p. 105–159. Elsevier, 2005.

[110] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, "Experimental plug and play quantum coin flipping," *Nat. Commun.*, vol. 5, p. 3717, 2014.

[111] W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802, 1982.

[112] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[113] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, p. 78, 1983.

[114] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Z. Wei Chen, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," *Nat. Photonics*, vol. 16, pp. 154–161, 2022.

[115] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, p. 400–403, 2018.

[116] A. Kent, D. Lowndes, D. Pitalúa-García, and J. Rarity *npj Quantum Inf.*, vol. 8, no. 1, 2022.

[117] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, "Experimental loss-tolerant quantum coin flipping," *Nat. Commun.*, vol. 2, p. 561, 2011.

[118] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, no. 1, 2017.

[119] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022.

[120] P. Zeng, H. Zhou, W. Wu, and X. Ma, "Mode-pairing quantum key distribution," *Nature Communications*, vol. 13, no. 1, 2022.

[121] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, and J.-W. Pan, "Twin-field quantum key distribution without phase locking," *Phys. Rev. Lett.*, vol. 130, p. 250802, 2023.

[122] M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," *Phys. Rev. A*, vol. 99, p. 022336, 2019.

[123] A. Kent and D. Pitalúa-García, "Flexible quantum tokens in spacetime," *Phys. Rev. A*, vol. 101, p. 022309, 2020.

[124] A. Kitaev, "Quantum coin flipping," *6th Workshop on Quantum Information Processing*, 2003.

[125] A. Chailloux and I. Kerenidis, "Optimal quantum strong coin flipping," *50th Annual IEEE Symposium on Foundations of Computer Science*, pp. 527–533, 2009.

[126] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, "Fair loss-tolerant quantum coin flipping," *Phys. Rev. A*, vol. 80, p. 062321, 2009.

[127] E. Hänggi and J. Wullschleger, "Tight bounds for classical and quantum coin flipping," *Proceedings of TCC*, pp. 468–485, 2011.

[128] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, pp. 3414–3417, 1997.

[129] H.-K. Lo and H. F. Chau, "Is quantum bit commitment really possible?," *Phys. Rev. Lett.*, vol. 78, pp. 3410–3413, 1997.

[130] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000.

[131] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, p. 475–478, 2014.

[132] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Info. Comput.*, vol. 7, no. 5, p. 431–458, 2007.

[133] S.-H. Sun, M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, "Partially random phase attack to the practical two-way quantum-key-distribution system," *Physical Review A*, vol. 85, no. 3, 2012.

[134] X. Ma, "Quantum cryptography: theory and practice," 2008.

[135] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, 2000.

[136] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003.

[137] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, no. 3, pp. 366–387, 2016.

[138] Y. Zhao, B. Qi, and H.-K. Lo, "Experimental quantum key distribution with active phase randomization," *Appl. Phys. Lett.*, vol. 90, p. 044106, 2007.

[139] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, "Effect of source tampering in the security of quantum cryptography," *Phys. Rev. A*, vol. 92, p. 022304, 2015.

[140] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics*, vol. 48, no. 13, pp. 2023–2038, 2001.

[141] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, no. 6, p. 065003, 2009.

[142] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[143] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New Journal of Physics*, vol. 13, no. 11, p. 113042, 2011.

[144] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, 2006.

[145] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, 2008.

[146] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Robust countermeasure against detector control attack in a practical quantum key distribution system," *Optica*, vol. 6, no. 9, pp. 1178–1184, 2019.

[147] J. P. Dowling and G. J. Milburn, "Quantum technology: the second quantum revolution," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[148] J. L. O'Brien, A. Furusawa, and J. Vučković, "Photonic quantum technologies," *Nature Photonics*, vol. 3, no. 12, pp. 687–695, 2009.

[149] B. J. Lawrie, P. D. Lett, A. M. Marino, and R. C. Pooser, "Quantum sensing with squeezed light," *ACS Photonics*, vol. 6, no. 6, pp. 1307–1318, 2019.

[150] M. Perarnau-Llobet, A. González-Tudela, and J. I. Cirac, "Multimode fock states with large photon number: effective descriptions and applications in quantum metrology," *Quantum Science and Technology*, vol. 5, no. 2, p. 025003, 2020.

[151] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, "Dynamically protected cat-qubits: a new paradigm for universal quantum computation," *New J. Phys.*, vol. 16, no. 4, p. 045014, 2014.

[152] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, "Experimental one-way quantum computing," *Nature*, vol. 434, no. 7030, pp. 169–176, 2005.

[153] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, "Entangled photon-pair sources based on three-wave mixing in bulk crystals," *Review of Scientific Instruments*, vol. 92, no. 4, 2021.

[154] A. Beveratos, S. Kühn, R. Brouri, T. Gacoin, J.-P. Poizat, and P. Grangier, "Room temperature stable single-photon source," *The European Physical Journal D - Atomic, Molecular and Optical Physics*, vol. 18, no. 2, pp. 191–196, 2002.

[155] D. B. Higginbottom, L. Slodička, G. Araneda, L. Lachman, R. Filip, M. Hennrich, and R. Blatt, "Pure single photons from a trapped atom source," *New Journal of Physics*, vol. 18, no. 9, p. 093038, 2016.

[156] C. Toninelli, I. Gerhardt, A. S. Clark, A. Reserbat-Plantey, S. Götzinger, Z. Ristanović, M. Colautti, P. Lombardi, K. D. Major, I. Deperasińska, W. H. Pernice, F. H. L. Koppens, B. Kozankiewicz, A. Gourdon, V. Sandoghdar, and M. Orrit, "Single organic molecules for photonic quantum technologies," *Nature Materials*, vol. 20, no. 12, pp. 1615–1628, 2021.

[157] R. Loudon, *The quantum theory of light*. London, England: Oxford University Press, 3 ed., 2000.

[158] R. J. Glauber, "The quantum theory of optical coherence," *Physical Review*, vol. 130, no. 6, pp. 2529–2539, 1963.

[159] R. H. Brown and R. Q. Twiss, "Correlation between photons in two coherent beams of light," *Nature*, vol. 177, no. 4497, pp. 27–29, 1956.

[160] P. Grünwald, "Effective second-order correlation function and single-photon detection," *New Journal of Physics*, vol. 21, no. 9, p. 093003, 2019.

[161] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, pp. 2044–2046, 1987.

[162] C. Eichler, D. Bozyigit, C. Lang, L. Steffen, J. Fink, and A. Wallraff, "Experimental state tomography of itinerant single microwave photons," *Phys. Rev. Lett.*, vol. 106, p. 220503, 2011.

[163] C. Eichler, D. Bozyigit, and A. Wallraff, "Characterizing quantum microwave radiation and its entanglement with superconducting qubits using linear detectors," *Phys. Rev. A*, vol. 86, p. 032106, 2012.

[164] S. Gasparinetti, M. Pechal, J.-C. Besse, M. Mondal, C. Eichler, and A. Wallraff, "Correlations and entanglement of microwave photons emitted in a cascade decay," *Phys. Rev. Lett.*, vol. 119, p. 140504, 2017.

[165] H. Paul, "Interference between independent photons," *Rev. Mod. Phys.*, vol. 58, pp. 209–231, 1986.

[166] T. F. da Silva, D. Vitoreti, G. Xavier, G. T. ao, and J. P. von der Weid, "Long-distance bell-state analysis of fully independentpolarization weak coherent states," *J. Lightwave Technol.*, vol. 31, no. 17, pp. 2881–2887, 2013.

[167] R. W. Boyd, *Nonlinear Optics*. Elsevier, 2008.

[168] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, 1995.

[169] I. N. Stranski and L. Krastanow, "Zur theorie der orientierten ausscheidung von ionenkristallen aufeinander," *Monatshefte für Chemie und verwandte Teile anderer Wissenschaften*, vol. 71, no. 1, pp. 351–364, 1937.

[170] L. Goldstein, F. Glas, J. Y. Marzin, M. N. Charasse, and G. Le Roux, "Growth by molecular beam epitaxy and characterization of InAs/GaAs strained-layer superlattices," *Applied Physics Letters*, vol. 47, no. 10, pp. 1099–1101, 1985.

[171] Y. H. Huo, A. Rastelli, and O. G. Schmidt, "Ultra-small excitonic fine structure splitting in highly symmetric quantum dots on gaas (001) substrate," *Applied Physics Letters*, vol. 102, no. 15, 2013.

[172] D. Huber, M. Reindl, Y. Huo, H. Huang, J. S. Wildmann, O. G. Schmidt, A. Rastelli, and R. Trotta, "Highly indistinguishable and strongly entangled photons from symmetric gaas quantum dots," *Nature Communications*, vol. 8, no. 1, 2017.

[173] T. Kuroda, T. Mano, N. Ha, H. Nakajima, H. Kumano, B. Urbaszek, M. Jo, M. Abbarchi, Y. Sakuma, K. Sakoda, I. Suemune, X. Marie, and T. Amand, "Symmetric quantum dots as efficient sources of highly entangled photons: Violation of bell's inequality without spectral and temporal filtering," *Phys. Rev. B*, vol. 88, p. 041306, 2013.

[174] K. Watanabe, N. Koguchi, and Y. Gotoh, "Fabrication of gaas quantum dots by modified droplet epitaxy," *Japanese Journal of Applied Physics*, vol. 39, no. 2A, p. L79, 2000.

[175] M. Gurioli, Z. Wang, A. Rastelli, T. Kuroda, and S. Sanguinetti, "Droplet epitaxy of semiconductor nanostructures for quantum photonic devices," *Nature Materials*, vol. 18, no. 8, p. 799–810, 2019.

[176] A. V. Kuhlmann, J. H. Prechtel, J. Houel, A. Ludwig, D. Reuter, A. D. Wieck, and R. J. Warburton, "Transform-limited single photons from a single quantum dot," *Nature Communications*, vol. 6, no. 1, 2015.

[177] Y.-M. He, Y. He, Y.-J. Wei, D. Wu, M. Atatüre, C. Schneider, S. Höfling, M. Kamp, C.-Y. Lu, and J.-W. Pan, "On-demand semiconductor single-photon source with near-unity indistinguishability," *Nat. Nanotechnol.*, vol. 8, no. 3, pp. 213–217, 2013.

[178] M. Reindl, J. H. Weber, D. Huber, C. Schimpf, S. F. Covre da Silva, S. L. Portalupi, R. Trotta, P. Michler, and A. Rastelli, "Highly indistinguishable single photons from incoherently excited quantum dots," *Phys. Rev. B*, vol. 100, p. 155420, 2019.

[179] Y.-J. Wei, Y.-M. He, M.-C. Chen, Y.-N. Hu, Y. He, D. Wu, C. Schneider, M. Kamp, S. Höfling, C.-Y. Lu, and J.-W. Pan, "Deterministic and robust generation of single photons from a single quantum dot with 99.5% indistinguishability using adiabatic rapid passage," *Nano Lett.*, vol. 14, p. 6515, 2014.

[180] L. Hanschke, K. A. Fischer, S. Appel, D. Lukin, J. Wierzbowski, S. Sun, R. Trivedi, J. Vučković, J. J. Finley, and K. Müller, "Quantum dot single-photon sources with ultra-low multi-photon probability," *npj Quantum Information*, vol. 4, no. 1, 2018.

[181] T. Huber, L. Ostermann, M. Prilmüller, G. S. Solomon, H. Ritsch, G. Weihs, and A. Predojević, "Coherence and degree of time-bin entanglement from quantum dots," *Phys. Rev. B*, vol. 93, p. 201301, 2016.

[182] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, "On-demand generation of indistinguishable polarization-entangled photon pairs," *Nat. Photonics*, vol. 8, p. 224, 2014.

[183] E. Schöll, L. Schweickert, L. Hanschke, K. D. Zeuner, F. Sbresny, T. Lettner, R. Trivedi, M. Reindl, S. F. Covre da Silva, R. Trotta, J. J. Finley, J. Vučković, K. Müller, A. Rastelli, V. Zwiller, and K. D. Jöns, "Crux of using the cascaded emission of a three-level quantum ladder system to generate indistinguishable photons," *Phys. Rev. Lett.*, vol. 125, p. 233605, 2020.

[184] S. Bounouar, M. Müller, A. M. Barth, M. Glässl, V. M. Axt, and P. Michler, "Phonon-assisted robust and deterministic two-photon biexciton preparation in a quantum dot," *Phys. Rev. B*, vol. 91, p. 161302, 2015.

[185] M. Reindl, K. D. Jöns, D. Huber, C. Schimpf, Y. Huo, V. Zwiller, A. Rastelli, and R. Trotta, "Phonon-assisted two-photon interference from remote quantum emitters," *Nano Lett.*, vol. 17, no. 7, pp. 4090–4095, 2017.

[186] J. H. Quilter, A. J. Brash, F. Liu, M. Glässl, A. M. Barth, V. M. Axt, A. J. Ramsay, M. S. Skolnick, and A. M. Fox, "Phonon-Assisted Population Inversion of a Single InGaAs/GaAs Quantum Dot by Pulsed Laser Excitation," *Phys. Rev. Lett.*, vol. 114, p. 137401, 2015.

[187] Y.-M. He, H. Wang, C. Wang, M.-C. Chen, X. Ding, J. Qin, Z.-C. Duan, S. Chen, J.-P. Li, R.-Z. Liu, and et al., "Coherently driving a single quantum two-level system with dichromatic laser pulses," *Nat. Phys.*, vol. 15, no. 9, p. 941–946, 2019.

[188] N. Tomm, A. Javadi, N. O. Antoniadis, D. Najer, M. C. Löbl, A. R. Korsch, R. Schott, S. R. Valentin, A. D. Wieck, A. Ludwig, and et al., "A bright and fast source of coherent single photons," *Nat. Nanotechnol.*, vol. 16, no. 4, p. 399–403, 2021.

[189] M. Arcari, I. Söllner, A. Javadi, S. Lindskov Hansen, S. Mahmoodian, J. Liu, H. Thyrrestrup, E. H. Lee, J. D. Song, S. Stobbe, and P. Lodahl, "Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide," *Phys. Rev. Lett.*, vol. 113, p. 093603, 2014.

[190] C. Gustin and S. Hughes, "Pulsed excitation dynamics in quantum-dot–cavity systems: Limits to optimizing the fidelity of on-demand single-photon sources," *Phys. Rev. B*, vol. 98, p. 045309, 2018.

[191] A. M. Barth, S. Lüker, A. Vagov, D. E. Reiter, T. Kuhn, and V. M. Axt, "Fast and selective phonon-assisted state preparation of a quantum dot by adiabatic undressing," *Phys. Rev. B*, vol. 94, p. 045306, 2016.

[192] H. Wang, H. Hu, T.-H. Chung, J. Qin, X. Yang, J.-P. Li, R.-Z. Liu, H.-S. Zhong, Y.-M. He, X. Ding, Y.-H. Deng, Q. Dai, Y.-H. Huo, S. Höfling, C.-Y. Lu, and J.-W. Pan, "On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability," *Phys. Rev. Lett.*, vol. 122, p. 113602, 2019.

[193] T. Huber, A. Predojević, H. Zoubi, H. Jayakumar, G. S. Solomon, and G. Weihs, "Measurement and modification of biexciton-exciton time correlations," *Opt. Express*, vol. 21, no. 8, pp. 9890–9898, 2013.

[194] T. Seidelmann, C. Schimpf, T. K. Bracht, M. Cosacchi, A. Vagov, A. Rastelli, D. E. Reiter, and V. M. Axt, "Two-photon excitation sets limit to entangled photon pair generation from quantum emitters," *Phys. Rev. Lett.*, vol. 129, p. 193604, 2022.

[195] F. Basso Basset, M. B. Rota, M. Beccaceci, T. M. Krieger, Q. Buchinger, J. Neuwirth, H. Huet, S. Stroj, S. F. Covre da Silva, G. Ronco, C. Schimpf, S. Höfling, T. Huber-Loyola, A. Rastelli, and R. Trotta, "Signatures of the optical stark effect on entangled photon pairs from resonantly pumped quantum dots," *Phys. Rev. Lett.*, vol. 131, p. 166901, 2023.

[196] S. Varo, G. Juska, and E. Pelucchi, "An intuitive protocol for polarization-entanglement restoral of quantum dot photon sources with non-vanishing fine-structure splitting," *Scientific Reports*, vol. 12, no. 1, 2022.

[197] A. Fognini, A. Ahmadi, S. J. Daley, M. E. Reimer, and V. Zwiller, "Universal fine-structure eraser for quantum dots," *Opt. Express*, vol. 26, no. 19, pp. 24487–24496, 2018.

[198] Y. Yu, S. Liu, C.-M. Lee, P. Michler, S. Reitzenstein, K. Srinivasan, E. Waks, and J. Liu, "Telecom-band quantum dot technologies for long-distance quantum networks," *Nature Nanotechnology*, vol. 18, no. 12, p. 1389–1400, 2023.

[199] A. Ghatak and K. Thyagarajan, *Introduction to fiber optics*. Cambridge University Press, 1998.

[200] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," *Nat. Photon.*, vol. 14, no. 5, pp. 273–284, 2020.

[201] X. Qiang, X. Zhou, J. Wang, C. M. Wilkes, T. Loke, S. O'Gara, L. Kling, G. D. Marshall, R. Santagati, T. C. Ralph, J. B. Wang, J. L. O'Brien, M. G. Thompson, and J. C. F. Matthews, "Large-scale silicon quantum photonics implementing arbitrary two-qubit processing," *Nature Photonics*, vol. 12, no. 9, p. 534–539, 2018.

[202] C. Couteau, "Spontaneous parametric down-conversion," *Contemporary Physics*, vol. 59, no. 3, p. 291–304, 2018.

[203] O. Alibart, V. D'Auria, M. D. Micheli, F. Doutre, F. Kaiser, L. Labonté, T. Lunghi, Picholle, and S. Tanzilli, "Quantum photonics at telecom wavelengths based on lithium niobate waveguides," *Journal of Optics*, vol. 18, no. 10, p. 104001, 2016.

[204] X. Cao, M. Zopf, and F. Ding, "Telecom wavelength single photon sources," *Journal of Semiconductors*, vol. 40, no. 7, p. 071901, 2019.

[205] J. Wang, Y. Zhou, Z. Wang, A. Rasmita, J. Yang, X. Li, H. J. von Bardeleben, and W. Gao, "Bright room temperature single photon source at telecom range in cubic silicon carbide," *Nature Communications*, vol. 9, no. 1, 2018.

[206] G. Wolfowicz, C. P. Anderson, B. Diler, O. G. Poluektov, F. J. Heremans, and D. D. Awschalom, "Vanadium spin qubits as telecom quantum emitters in silicon carbide," *Sci. Adv.*, vol. 6, no. 18, 2020.

[207] X. He, N. F. Hartmann, X. Ma, Y. Kim, R. Ihly, J. L. Blackburn, W. Gao, J. Kono, Y. Yomogida, A. Hirano, T. Tanaka, H. Kataura, H. Htoon, and S. K. Doorn, "Tunable room-temperature single-photon emission at telecom wavelengths from sp3 defects in carbon nanotubes," *Nature Photonics*, vol. 11, no. 9, p. 577–582, 2017.

[208] Y. Zhou, Z. Wang, A. Rasmita, S. Kim, A. Berhane, Z. Bodrog, G. Adamo, A. Gali, I. Aharonovich, and W.-b. Gao, "Room temperature solid-state quantum emitters in the telecom range," *Sci. Adv.*, vol. 4, no. 3, 2018.

[209] A. M. Dibos, M. Raha, C. M. Phenicie, and J. D. Thompson, "Atomic source of single photons in the telecom band," *Phys. Rev. Lett.*, vol. 120, p. 243601, 2018.

[210] B. Merkel, A. Ulanowski, and A. Reiserer, "Coherent and purcell-enhanced emission from erbium dopants in a cryogenic high-q resonator," *Phys. Rev. X*, vol. 10, p. 041025, 2020.

[211] R. T. Willis, F. E. Becerra, L. A. Orozco, and S. L. Rolston, "Photon statistics and polarization correlations at telecommunications wavelengths from a warm atomic ensemble," *Opt. Express*, vol. 19, no. 15, pp. 14632–14641, 2011.

[212] J. Huang and P. Kumar, "Observation of quantum frequency conversion," *Phys. Rev. Lett.*, vol. 68, pp. 2153–2156, 1992.

[213] M. T. Rakher, L. Ma, O. Slattery, X. Tang, and K. Srinivasan, "Quantum transduction of telecommunications-band single photons from a quantum dot by frequency upconversion," *Nature Photonics*, vol. 4, no. 11, p. 786–791, 2010.

[214] J. H. Weber, B. Kambs, J. Kettler, S. Kern, J. Maisch, H. Vural, M. Jetter, S. L. Portalupi, C. Becher, and P. Michler, "Two-photon interference in the telecom c-band after frequency conversion of photons from remote quantum emitters," *Nature Nanotechnology*, vol. 14, no. 1, p. 23–26, 2018.

[215] B. Kambs, J. Kettler, M. Bock, J. N. Becker, C. Arend, A. Lenhard, S. L. Portalupi, M. Jetter, P. Michler, and C. Becher, "Low-noise quantum frequency down-conversion of indistinguishable photons," *Opt. Express*, vol. 24, no. 19, pp. 22250–22260, 2016.

[216] M. Bock, P. Eich, S. Kucera, M. Kreis, A. Lenhard, C. Becher, and J. Eschner, "High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion," *Nature Communications*, vol. 9, no. 1, 2018.

[217] T. van Leent, M. Bock, F. Fertig, R. Garthoff, S. Eppelt, Y. Zhou, P. Malik, M. Seubert, T. Bauer, W. Rosenfeld, W. Zhang, C. Becher, and H. Weinfurter, "Entangling single atoms over 33km telecom fibre," *Nature*, vol. 607, no. 7917, p. 69–73, 2022.

[218] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W.-M. Schulz, M. Jetter, P. Michler, and C. Becher, "Visible-to-telecom quantum frequency conversion of light from a single quantum emitter," *Phys. Rev. Lett.*, vol. 109, p. 147404, 2012.

[219] K. Takemoto, Y. Sakuma, S. Hirose, T. Usuki, and N. Yokoyama, "Observation of exciton transition in 1.3-1.55 μm band from single inas/inp quantum dots in mesa structure," *Japanese Journal of Applied Physics*, vol. 43, no. No. 3A, p. L349–L351, 2004.

[220] L. Seravalli and F. Sacconi, "Reviewing quantum dots for single-photon emission at 1.55 m: a quantitative comparison of materials," *Journal of Physics: Materials*, vol. 3, no. 4, p. 042005, 2020.

[221] M. Yacob, J. P. Reithmaier, and M. Benyoucef, "Low-density inp-based quantum dots emitting around the 1.5m telecom wavelength range," *Applied Physics Letters*, vol. 104, no. 2, 2014.

[222] Dusanowski, M. Syperek, W. Rudno-Rudziński, P. Mrowiński, G. Sk, J. Misiewicz, A. Somers, J. P. Reithmaier, S. Höfling, and A. Forchel, "Exciton and biexciton dynamics in single self-assembled inas/ingaalas/inp quantum dash emitting near 1.55m," *Applied Physics Letters*, vol. 103, no. 25, 2013.

[223] Dusanowski, M. Syperek, P. Mrowiński, W. Rudno-Rudziński, J. Misiewicz, A. Somers, S. Höfling, M. Kamp, J. P. Reithmaier, and G. Sek, "Single photon emission at 1.55m from charged and neutral exciton confined in a single quantum dash," *Applied Physics Letters*, vol. 105, no. 2, 2014.

[224] P. Mrowiński, M. Zieliński, M. Świderski, J. Misiewicz, A. Somers, J. P. Reithmaier, S. Höfling, and G. Sek, "Excitonic fine structure and binding energies of excitonic complexes in single inas quantum dashes," *Phys. Rev. B*, vol. 94, p. 115434, 2016.

[225] A. Musiał, P. Holewa, P. Wyborski, M. Syperek, A. Kors, J. P. Reithmaier, G. Sek, and M. Benyoucef, "High-purity triggered single-photon emission from symmetric single inas/inp quantum dots around the telecom c-band window," *Advanced Quantum Technologies*, vol. 3, no. 2, 2019.

[226] P. Holewa, M. Gawełczyk, C. Ciostek, P. Wyborski, S. Kadkhodazadeh, E. Semenova, and M. Syperek, "Optical and electronic properties of low-density inas/inp quantum-dot-like structures designed for single-photon emitters at telecom wavelengths," *Phys. Rev. B*, vol. 101, p. 195304, 2020.

[227] J. Skiba-Szymanska, R. M. Stevenson, C. Varnava, M. Felle, J. Huwer, T. Müller, A. J. Bennett, J. P. Lee, I. Farrer, A. B. Krysa, P. Spencer, L. E. Goff, D. A. Ritchie, J. Heffernan, and A. J. Shields, "Universal growth scheme for quantum dots with low fine-structure splitting at various emission wavelengths," *Phys. Rev. Appl.*, vol. 8, p. 014013, 2017.

[228] E. M. Sala, Y. I. Na, M. Godsland, A. Trapalis, and J. Heffernan, "Inas/inp quantum dots in etched pits by droplet epitaxy in metalorganic vapor phase epitaxy," *physica status solidi (RRL) – Rapid Research Letters*, vol. 14, no. 8, 2020.

[229] E. M. Sala, M. Godsland, Y. I. Na, A. Trapalis, and J. Heffernan, "Droplet epitaxy of inas/inp quantum dots via movpe by using an ingaas interlayer," *Nanotechnology*, vol. 33, no. 6, p. 065601, 2021.

[230] M. Paul, J. Kettler, K. Zeuner, C. Clausen, M. Jetter, and P. Michler, "Metal-organic vapor-phase epitaxy-grown ultra-low density ingaas/gaas

quantum dots exhibiting cascaded single-photon emission at 1.3m," *Applied Physics Letters*, vol. 106, no. 12, 2015.

[231] F. Olbrich, J. Kettler, M. Bayerbach, M. Paul, J. Höschele, S. L. Portalupi, M. Jetter, and P. Michler, "Temperature-dependent properties of single long-wavelength ingaas quantum dots embedded in a strain reducing layer," *Journal of Applied Physics*, vol. 121, no. 18, 2017.

[232] M. Zimmer, A. Trachtmann, M. Jetter, and P. Michler, "Movpe grown ingaas quantum dots with emission near 1.3 ¡mml:math xmlns:mml="http://www.w3.org/1998/math/mathml" altimg="si31.svg" display="inline" id="d1e75"¿¡mml:mi mathvariant="normal"¿¡/mml:mi¿¡/mml:math¿m for electrically driven single-photon sources," *Journal of Crystal Growth*, vol. 605, p. 127081, 2023.

[233] E. S. Semenova, R. Hostein, G. Patriarche, O. Mauguin, L. Largeau, I. Robert-Philip, A. Beveratos, and A. Lemaître, "Metamorphic approach to single quantum dot emission at 1.55m on gaas substrate," *Journal of Applied Physics*, vol. 103, no. 10, 2008.

[234] M. Paul, F. Olbrich, J. Höschele, S. Schreier, J. Kettler, S. L. Portalupi, M. Jetter, and P. Michler, "Single-photon emission at 1.55 μ m from MOVPE-grown InAs quantum dots on InGaAs/GaAs metamorphic buffers," *Applied Physics Letters*, vol. 111, no. 3, p. 033102, 2017.

[235] R. Sittig, C. Nawrath, S. Kolatschek, S. Bauer, R. Schaber, J. Huang, P. Vijayan, P. Pruy, S. L. Portalupi, M. Jetter, and P. Michler *Nanophotonics*, vol. 11, no. 6, pp. 1109–1116, 2022.

[236] C. Carmesin, F. Olbrich, T. Mehrtens, M. Florian, S. Michael, S. Schreier, C. Nawrath, M. Paul, J. Höschele, B. Gerken, J. Kettler, S. L. Portalupi, M. Jetter, P. Michler, A. Rosenauer, and F. Jahnke, "Structural and optical properties of InAs/(In)GaAs/GaAs quantum dots with single-photon emission in the telecom C-band up to 77 K," *Physical Review B*, vol. 98, no. 12, p. 125407, 2018.

[237] T. Lettner, S. Gyger, K. D. Zeuner, L. Schweickert, S. Steinhauer, C. Reuterskiöld Hedlund, S. Stroj, A. Rastelli, M. Hammar, R. Trotta, K. D. Jöns, and V. Zwiller, "Strain-Controlled Quantum Dot Fine Structure for Entangled Photon Generation at 1550 nm," *Nano Letters*, vol. 21, no. 24, pp. 10501–10506, 2021.

[238] K. D. Zeuner, M. Paul, T. Lettner, C. Reuterskiöld Hedlund, L. Schweickert, S. Steinhauer, L. Yang, J. Zichi, M. Hammar, K. D. Jöns, and V. Zwiller, "A stable wavelength-tunable triggered source of single photons and cascaded photon pairs at the telecom c-band," *Applied Physics Letters*, vol. 112, no. 17, 2018.

[239] S. L. Portalupi, M. Jetter, and P. Michler, "Inas quantum dots grown on metamorphic buffers as non-classical light sources at telecom c-band: a review," *Semiconductor Science and Technology*, vol. 34, no. 5, p. 053001, 2019.

[240] K. D. Zeuner, K. D. Jöns, L. Schweickert, C. Reuterskiöld Hedlund, C. Nuñez Lobato, T. Lettner, K. Wang, S. Gyger, E. Schöll, S. Steinhauer, M. Hammar, and V. Zwiller, "On-demand generation of entangled photon pairs in the telecom c-band with inas quantum dots," *ACS Photonics*, vol. 8, no. 8, p. 2337–2344, 2021.

[241] L. Schweickert, K. D. Jöns, K. D. Zeuner, S. F. Covre da Silva, H. Huang, T. Lettner, M. Reindl, J. Zichi, R. Trotta, A. Rastelli, and V. Zwiller, "On-demand generation of background-free single photons from a solid-state source," *Appl. Phys. Lett.*, vol. 112, no. 9, p. 093106, 2018.

[242] D. Huber, B. U. Lehner, D. Csontosová, M. Reindl, S. Schuler, S. F. Covre da Silva, P. Klenovský, and A. Rastelli, "Single-particle-picture breakdown in laterally weakly confining gaas quantum dots," *Phys. Rev. B*, vol. 100, p. 235425, 2019.

[243] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, p. 3–28, 1992.

[244] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, 1992.

[245] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, 2007.

[246] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.*, vol. 84, pp. 4729–4732, 2000.

[247] A. V. Kuhlmann, J. Houel, A. Ludwig, L. Greuter, D. Reuter, A. D. Wieck, M. Poggio, and R. J. Warburton, "Charge noise and spin noise in a semiconductor quantum device," *Nature Physics*, vol. 9, no. 9, p. 570–575, 2013.

[248] J.-P. Jahn, M. Munsch, L. Béguin, A. V. Kuhlmann, M. Renggli, Y. Huo, F. Ding, R. Trotta, M. Reindl, O. G. Schmidt, A. Rastelli, P. Treutlein, and R. J. Warburton, "An artificial rb atom in a semiconductor with lifetime-limited linewidth," *Phys. Rev. B*, vol. 92, p. 245439, 2015.

[249] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, p. 210–229, 1988.

[250] L. Zhai, M. C. Löbl, G. N. Nguyen, J. Ritzmann, A. Javadi, C. Spinnler, A. D. Wieck, A. Ludwig, and R. J. Warburton, "Low-noise gaas quantum dots for quantum photonics," *Nature Communications*, vol. 11, no. 1, 2020.

[251] D. E. Reiter, T. Kuhn, and V. M. Axt, "Distinctive characteristics of carrier-phonon interactions in optically driven semiconductor quantum dots," *Advances in Physics: X*, vol. 4, no. 1, p. 1655478, 2019.

[252] L. Besombes, K. Kheng, L. Marsal, and H. Mariette, "Acoustic phonon broadening mechanism in single quantum dot emission," *Phys. Rev. B*, vol. 63, p. 155307, 2001.

[253] P. Borri, W. Langbein, S. Schneider, U. Woggon, R. L. Sellin, D. Ouyang, and D. Bimberg, "Ultralong dephasing time in InGaAs quantum dots," *Phys. Rev. Lett.*, vol. 87, p. 157401, 2001.

[254] B. Krummheuer, V. M. Axt, and T. Kuhn, "Theory of pure dephasing and the resulting absorption line shape in semiconductor quantum dots," *Phys. Rev. B*, vol. 65, p. 195313, 2002.

[255] V. M. Axt, T. Kuhn, A. Vagov, and F. M. Peeters, "Phonon-induced pure dephasing in exciton-biexciton quantum dot systems driven by ultrafast laser pulse sequences," *Phys. Rev. B*, vol. 72, p. 125309, 2005.

[256] S. Lüker, T. Kuhn, and D. E. Reiter, "Phonon impact on optical control schemes of quantum dots: Role of quantum dot geometry and symmetry," *Phys. Rev. B*, vol. 96, p. 245306, 2017.

[257] A. Vagov, M. D. Croitoru, M. Glässl, V. M. Axt, and T. Kuhn, "Real-time path integrals for quantum dots: Quantum dissipative dynamics with superohmic environment coupling," *Phys. Rev. B*, vol. 83, p. 094303, 2011.

[258] A. M. Barth, A. Vagov, and V. M. Axt, "Path-integral description of combined Hamiltonian and non-Hamiltonian dynamics in quantum dissipative systems," *Phys. Rev. B*, vol. 94, p. 125439, 2016.

[259] M. Cygorek, A. M. Barth, F. Ungar, A. Vagov, and V. M. Axt, "Nonlinear cavity feeding and unconventional photon statistics in solid-state cavity QED revealed by many-level real-time path-integral calculations," *Phys. Rev. B*, vol. 96, p. 201201(R), 2017.

[260] T. Kaldewey, S. Lüker, A. V. Kuhlmann, S. R. Valentin, J.-M. Chauveau, A. Ludwig, A. D. Wieck, D. E. Reiter, T. Kuhn, and R. J. Warburton, "Demonstrating the decoupling regime of the electron-phonon interaction in a quantum dot using chirped optical excitation," *Phys. Rev.* B, vol. 95, no. 24, p. 241306, 2017.

[261] F. Ding, R. Singh, J. D. Plumhof, T. Zander, V. Křápek, Y. H. Chen, M. Benyoucef, V. Zwiller, K. Dörr, G. Bester, A. Rastelli, and O. G. Schmidt, "Tuning the Exciton Binding Energies in Single Self-Assembled InGaAs / GaAs Quantum Dots by Piezoelectric-Induced Biaxial Stress," *Phys. Rev. Lett.*, vol. 104, no. 6, p. 067405, 2010.

[262] M. Cosacchi, M. Cygorek, F. Ungar, A. M. Barth, A. Vagov, and V. M. Axt, "Path-integral approach for nonequilibrium multitime correlation functions of open quantum systems coupled to Markovian and non-Markovian environments," *Phys. Rev. B*, vol. 98, p. 125302, 2018.

[263] H. Vural, S. L. Portalupi, and P. Michler, "Perspective of self-assembled ingaas quantum-dots for multi-source quantum implementations," *Applied Physics Letters*, vol. 117, no. 3, 2020.

[264] H.-K. Lo and J. Preskill, "Phase randomization improves the security of quantum key distribution," no. CALT-68-2556, 2005.

[265] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," *Phys. Rev. Lett.*, vol. 95, p. 080501, 2005.

[266] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, "Experimental demonstration of graph-state quantum secret sharing," *Nat. Commun.*, vol. 5, no. 1, 2014.

[267] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, vol. 1, (Bangalore, India), pp. 175–179, 1984.

[268] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent, and D. Pitalúa-García, "Multiphoton and side-channel attacks in mistrustful quantum cryptography," *PRX Quantum*, vol. 2, p. 030338, 2021.

[269] P. Senellart, G. Solomon, and A. White, "High-performance semiconductor quantum-dot single-photon sources," *Nat. Nanotechnol.*, vol. 12, pp. 1026–1039, 2017.

[270] M. Anderson, T. Müller, J. Skiba-Szymanska, A. B. Krysa, J. Huwer, R. M. Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields, "Gigahertz-clocked teleportation of time-bin qubits with a quantum dot in the telecommunication *c* band," *Phys. Rev. Applied*, vol. 13, p. 054052, 2020.

[271] D. A. Vajner, L. Rickert, T. Gao, K. Kaymazlar, and T. Heindel, "Quantum communication using semiconductor quantum dots," *Adv. Quantum Technol.*, vol. 5, no. 7, p. 2100116, 2022.

[272] P. Chaiwongkhot, S. Hosseini, A. Ahmadi, B. L. Higgins, D. Dalacu, P. J. Poole, R. L. Williams, M. E. Reimer, and T. Jennewein, "Enhancing secure key rates of satellite qkd using a quantum dot single-photon source," 2020.

[273] G. Murtaza, M. Colautti, M. Hilke, P. Lombardi, F. S. Cataliotti, A. Zavatta, D. Bacco, and C. Toninelli, "Efficient room-temperature molecular single-photon sources for quantum key distribution. preprint at https://arxiv.org/abs/2202.12635," 2022.

[274] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New J. Phys.*, vol. 17, no. 5, p. 053014, 2015.

[275] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, and et al., "Near-optimal single-photon sources in the solid state," *Nat. Photonics*, vol. 10, no. 5, pp. 340–345, 2016.

[276] M. Reindl, K. D. Jöns, D. Huber, C. Schimpf, Y. Huo, V. Zwiller, A. Rastelli, and R. Trotta, "Phonon-assisted two-photon interference from remote quantum emitters," *Nano Lett.*, vol. 17, no. 7, pp. 4090–4095, 2017.

[277] S. Lüker and D. E. Reiter, "A review on optical excitation of semiconductor quantum dots under the influence of phonons," *Semicond. Sci. Technol.*, vol. 34, no. 6, p. 063002, 2019.

[278] X. Ding, Y. He, Z.-C. Duan, N. Gregersen, M.-C. Chen, S. Unsleber, S. Maier, C. Schneider, M. Kamp, S. Höfling, C.-Y. Lu, and J.-W. Pan, "On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar," *Phys. Rev. Lett.*, vol. 116, p. 020401, 2016.

[279] L. Schweickert, K. D. Jöns, K. D. Zeuner, S. F. Covre da Silva, H. Huang, T. Lettner, M. Reindl, J. Zichi, R. Trotta, A. Rastelli, and et al., "On-demand generation of background-free single photons from a solid-state source," *Appl. Phys. Lett.*, vol. 112, no. 9, p. 093106, 2018.

[280] Y. Wei, S. Liu, X. Li, Y. Yu, X. Su, S. Li, X. Shang, H. Liu, H. Hao, H. Ni, S. Yu, Z. Niu, J. Iles-Smith, J. Liu, and X. Wang *Nat. Nanotechnol.*, vol. 17, no. 5, pp. 470–476, 2022.

[281] J. Yan, S. Liu, X. Lin, Y. Ye, J. Yu, L. Wang, Y. Yu, Y. Zhao, Y. Meng, X. Hu, D.-W. Wang, C. Jin, and F. Liu *Nano Lett.*, vol. 22, no. 4, pp. 1483–1490, 2022.

[282] F. Liu, A. J. Brash, J. O'Hara, L. M. P. P. Martins, C. L. Phillips, R. J. Coles, B. Royall, E. Clarke, C. Bentham, N. Prtljaga, and et al., "High

purcell factor generation of indistinguishable on-chip single photons," *Nat. Nanotechnol.*, vol. 13, no. 9, pp. 835–840, 2018.

[283] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Info. Comput.*, vol. 4, no. 5, pp. 325–360, 2004.

[284] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, 2002.

[285] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[286] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," *Opt. Express*, vol. 28, no. 10, pp. 14547–14559, 2020.

[287] X. Ding, Y. He, Z.-C. Duan, N. Gregersen, M.-C. Chen, S. Unsleber, S. Maier, C. Schneider, M. Kamp, S. Höfling, C.-Y. Lu, and J.-W. Pan, "On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar," *Phys. Rev. Lett.*, vol. 116, p. 020401, 2016.

[288] S. Kolatschek, C. Nawrath, S. Bauer, J. Huang, J. Fischer, R. Sittig, M. Jetter, S. L. Portalupi, and P. Michler, "Bright purcell enhanced single-photon source in the telecom o-band based on a quantum dot in a circular bragg grating," *Nano Lett.*, vol. 21,18, p. 7740–7745, 2021.

[289] K. Takemoto, M. Takatsu, S. Hirose, and N. Yokoyama, "An optical horn structure for single-photon source using quantum dots at telecommunication wavelength," *J. Appl. Phys.*, vol. 101, p. 081720, 2007.

[290] T. Miyazawa, K. Takemoto, Y. Nambu, S. Miki, T. Yamashita, H. Terai, M. Fujiwara, M. Sasaki, Y. Sakuma, M. Takatsu, T. Yamamoto, and Y. Arakawa, "Single-photon emission at 1.5m from an inas/inp quantum dot with highly suppressed multi-photon emission probabilities," *Appl. Phys. Lett.*, vol. 109, no. 13, p. 132106, 2016.

[291] T. van Leent, M. Bock, R. Garthoff, K. Redeker, W. Zhang, T. Bauer, W. Rosenfeld, C. Becher, and H. Weinfurter, "Long-distance distribution of atom-photon entanglement at telecom wavelength," *Phys. Rev. Lett.*, vol. 124, p. 010510, 2020.

[292] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Phys. Rev. Lett.*, vol. 122, p. 240501, 2019.

[293] C. Nawrath, R. Joos, S. Kolatschek, S. Bauer, P. Pruy, F. Hornung, J. Fischer, J. Huang, P. Vijayan, R. Sittig, M. Jetter, S. L. Portalupi, and P. Michler, "High emission rate from a purcell-enhanced, triggered source of pure single photons in the telecom c-band," 2022.

[294] R. Sittig, C. Nawrath, S. Kolatschek, S. Bauer, R. Schaber, J. Huang, P. Vijayan, P. Pruy, S. L. Portalupi, M. Jetter, and P. Michler, "Thin-film InGaAs metamorphic buffer for telecom C-band InAs quantum dots and optical resonators on GaAs platform," *Nanophotonics*, vol. 11, no. 6, pp. 1109–1116, 2022.

[295] Ł. Dusanowski, C. Nawrath, S. L. Portalupi, M. Jetter, T. Huber, S. Klembt, P. Michler, and S. Höfling, "Optical charge injection and coherent control of a quantum-dot spin-qubit emitting at telecom wavelengths," *Nat. Commun.*, vol. 13, no. 1, p. 748, 2022.

[296] F. Centrone, N. Kumar, E. Diamanti, and I. Kerenidis, "Experimental demonstration of quantum advantage for NP verification with limited information," *Nat. Commun.*, vol. 12, no. 1, 2021.

[297] R. Bedington, J.-M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, p. 30, 2017.

[298] S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti, "Experimental cheat-sensitive quantum weak coin flipping," *Nat. Commun.*, vol. 14, p. 1855, 2023.

[299] P. Schiansky, J. Kalb, E. Sztatecsny, M.-C. Roehsner, T. Guggemos, A. Trenti, M. Bozzio, and P. Walther, "Demonstration of quantum-digital payments," *Nat. Commun.*, vol. 14, no. 1, 2023.

[300] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[301] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, pp. 682–686, 2015.

[302] S. Ritter, C. Nölleke, C. Hahn, A. Reiserer, A. Neuzner, M. Uphoff, M. Mücke, E. Figueroa, J. Bochmann, and G. Rempe, "An elementary quantum network of single atoms in optical cavities," *Nature*, vol. 484, no. 7393, pp. 195–200, 2012.

[303] H. Wang, Y. M. He, T. H. Chung, H. Hu, Y. Yu, S. Chen, X. Ding, M. C. Chen, J. Qin, X. Yang, R. Z. Liu, Z. C. Duan, J. P. Li, S. Gerhardt, K. Winkler, J. Jurkat, L. J. Wang, N. Gregersen, Y. H. Huo, Q. Dai, S. Yu, S. Höfling, C. Y. Lu, and J. W. Pan, "Towards optimal single-photon sources from polarized microcavities," *Nat. Photon.*, vol. 13, no. 11, pp. 770–775, 2019.

[304] N. Tomm, A. Javadi, N. O. Antoniadis, D. Najer, M. C. Löbl, A. R. Korsch, R. Schott, S. R. Valentin, A. D. Wieck, A. Ludwig, and R. J. Warburton, "A bright and fast source of coherent single photons," *Nat. Nanotechnol.*, 2021.

[305] L. Zhai, G. N. Nguyen, C. Spinnler, J. Ritzmann, M. C. Löbl, A. D. Wieck, A. Ludwig, A. Javadi, and R. J. Warburton, "Quantum interference of identical photons from remote GaAs quantum dots," *Nature Nanotechnology*, vol. 17, no. 8, pp. 829–833, 2022.

[306] M. Anderson, T. Müller, J. Huwer, J. Skiba-Szymanska, A. B. Krysa, R. M. Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields, "Quantum teleportation using highly coherent emission from telecom c-band quantum dots," *npj Quantum Inf.*, vol. 6, p. 14, 2020.

[307] P. Lodahl, "Quantum-dot based photonic quantum networks," *Quantum Science and Technology*, vol. 3, no. 1, p. 013001, 2017.

[308] T. Miyazawa, K. Takemoto, Y. Nambu, S. Miki, T. Yamashita, H. Terai, M. Fujiwara, M. Sasaki, Y. Sakuma, M. Takatsu, T. Yamamoto, and Y. Arakawa, "Single-photon emission at 1.5 μ m from an InAs/InP quantum dot with highly suppressed multi-photon emission probabilities," *Applied Physics Letters*, vol. 109, no. 13, p. 132106, 2016.

[309] G. Shooter, Z.-H. Xiang, J. R. A. Müller, J. Skiba-Szymanska, J. Huwer, J. Griffiths, T. Mitchell, M. Anderson, T. Müller, A. B. Krysa, R. Mark Stevenson, J. Heffernan, D. A. Ritchie, and A. J. Shields, "1GHz clocked distribution of electrically generated entangled photon pairs," *Optics Express*, vol. 28, no. 24, p. 36838, 2020.

[310] T. van Leent, M. Bock, R. Garthoff, K. Redeker, W. Zhang, T. Bauer, W. Rosenfeld, C. Becher, and H. Weinfurter, "Long-distance distribution of atom-photon entanglement at telecom wavelength," *Phys. Rev. Lett.*, vol. 124, p. 010510, 2020.

[311] S. E. Thomas, M. Billard, N. Coste, S. C. Wein, Priya, H. Ollivier, O. Krebs, L. Tazaïrt, A. Harouri, A. Lemaitre, I. Sagnes, C. Anton, L. Lanco, N. Somaschi, J. C. Loredo, and P. Senellart, "Bright polarized single-photon source based on a linear dipole," *Phys. Rev. Lett.*, vol. 126, p. 233601, 2021.

[312] J. H. Quilter, A. J. Brash, F. Liu, M. Glässl, A. M. Barth, V. M. Axt, A. J. Ramsay, M. S. Skolnick, and A. M. Fox, "Phonon-assisted population inversion of a single InGaAs/GaAs quantum dot by pulsed laser excitation," *Phys. Rev. Lett.*, vol. 114, p. 137401, 2015.

[313] M. Glässl, A. M. Barth, and V. M. Axt, "Proposed robust and high-fidelity preparation of excitons and biexcitons in semiconductor quantum dots making active use of phonons," *Phys. Rev. Lett.*, vol. 110, p. 147401, 2013.

[314] C. Gustin and S. Hughes, "Efficient pulse–excitation techniques for single photon sources from quantum dots in optical cavities," *Advanced Quantum Technologies*, vol. 3, no. 2, p. 1900073, 2019.

[315] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, p. 230503, 2005.

[316] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-poisson light," *Phys. Rev. A*, vol. 66, p. 042315, 2002.

[317] P. Grünwald, "Effective second-order correlation function and single-photon detection," *New Journal of Physics*, vol. 21, no. 9, p. 093003, 2019.

[318] S. Ates, I. Agha, A. Gulinatti, I. Rech, A. Badolato, and K. Srinivasan, "Improving the performance of bright quantum dot single photon sources using temporal filtering via amplitude modulation," *Scientific Reports*, vol. 3, no. 1, 2013.

[319] T. Kupko, M. von Helversen, L. Rickert, J.-H. Schulze, A. Strittmatter, M. Gschrey, S. Rodt, S. Reitzenstein, and T. Heindel, "Tools for the performance optimization of single-photon quantum key distribution," *npj Quantum Inf.*, vol. 6, no. 1, p. 29, 2020.

[320] Y. Zhang, X. Ding, Y. Li, L. Zhang, Y.-P. Guo, G.-Q. Wang, Z. Ning, M.-C. Xu, R.-Z. Liu, J.-Y. Zhao, G.-Y. Zou, H. Wang, Y. Cao, Y.-M. He, C.-Z. Peng, Y.-H. Huo, S.-K. Liao, C.-Y. Lu, F. Xu, and J.-W. Pan, "Experimental single-photon quantum key distribution surpassing the fundamental coherent-state rate limit," 2024.

[321] D. Awschalom, K. K. Berggren, H. Bernien, S. Bhave, L. D. Carr, P. Davids, S. E. Economou, D. Englund, A. Faraon, M. Fejer, S. Guha, M. V. Gustafsson, E. Hu, L. Jiang, J. Kim, B. Korzh, P. Kumar, P. G. Kwiat, M. Lončar, M. D. Lukin, D. A. Miller, C. Monroe, S. W. Nam, P. Narang, J. S. Orcutt, M. G. Raymer, A. H. Safavi-Naeini, M. Spiropulu, K. Srinivasan, S. Sun, J. Vučković, E. Waks, R. Walsworth, A. M. Weiner, and Z. Zhang, "Development of quantum interconnects (quics) for next-generation information technologies," *PRX Quantum*, vol. 2, no. 1, 2021.

[322] S. Wei, B. Jing, X. Zhang, J. Liao, C. Yuan, B. Fan, C. Lyu, D. Zhou, Y. Wang, G. Deng, H. Song, D. Oblak, G. Guo, and Q. Zhou, "Towards real-world quantum networks: A review," *Laser amp; Photonics Reviews*, vol. 16, no. 3, 2022.

[323] C.-Y. Lu and J.-W. Pan, "Quantum-dot single-photon sources for the quantum internet," *Nature Nanotechnology*, vol. 16, no. 12, pp. 1294–1296, 2021.

[324] E. Arensk̈otter, T. Bauer, S. Kucera, M. Bock, J. Eschner, and C. Becher, "Telecom quantum photonic interface for a 40ca+ single-ion quantum memory," *npj Quantum Information*, vol. 9, no. 1, 2023.

[325] T. Strobel, S. Kazmaier, T. Bauer, M. Schäfer, A. Choudhary, N. L. Sharma, R. Joos, C. Nawrath, J. H. Weber, W. Nie, G. Bhayani, L. Wagner, A. Bisquerra, M. Geitz, R.-P. Braun, C. Hopfmann, S. L. Portalupi, C. Becher, and P. Michler, "High fidelity distribution of triggered polarization-entangled telecom photons via a 36km intra-city fiber network," 2024.

[326] M. Karpiński, M. Jachura, L. J. Wright, and B. J. Smith, "Bandwidth manipulation of quantum light by an electro-optic time lens," *Nature Photonics*, vol. 11, no. 1, p. 53–57, 2016.

[327] F. Sośnicki, M. Mikołajczyk, A. Golestani, and M. Karpiński, "Interface between picosecond and nanosecond quantum light pulses," *Nature Photonics*, vol. 17, no. 9, p. 761–766, 2023.

[328] J. M. Donohue, "Fresnel time lens empowers quantum networks," *Nature Photonics*, vol. 17, no. 9, p. 738–739, 2023.

[329] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection," *Physical Review Applied*, vol. 11, no. 3, 2019.

[330] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Information*, vol. 5, no. 1, 2019.

[331] A. Molina, T. Vidick, and J. Watrous, "Optimal counterfeiting attacks and generalizations for wiesner's quantum money," in *TQC 2012: Theory of Quantum Computation, Communication, and Cryptography* (K. Iwama, Y. Kawano, and M. Murao, eds.), vol. 7582 of *Lecture Notes in Computer Science*, Springer, 2013.

[332] J. Watrous, *Semidefinite Programming*, ch. 7. University of Waterloo, 2011.

[333] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, no. 1, pp. 49–95, 1996.

[334] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing models for optical measurements in quantum communication," *Phys. Rev. Lett.*, vol. 101, p. 093601, 2008.

[335] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, "Experimental quantum coin tossing," *Phys. Rev. Lett.*, vol. 94, p. 040501, 2005.

[336] T. Rudolph, R. W. Spekkens, and P. S. Turner, "Unambiguous discrimination of mixed states," *Phys. Rev. A*, vol. 68, p. 010301, 2003.

[337] X. Lü, "Lower bounds on the failure probability of unambiguous discrimination," *Phys. Rev. A*, vol. 103, p. 022216, 2021.

[338] S. M. Barnett and S. Croke, "Quantum state discrimination," *Adv. Opt. Photon.*, vol. 1, no. 2, pp. 238–278, 2009.

[339] Y. Eldar, "A semidefinite programming approach to optimal unambiguous discrimination of quantum states," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 446–456, 2003.

[340] Y. Eldar, A. Megretski, and G. Verghese, "Designing optimal quantum detectors via semidefinite programming," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 1007–1012, 2003.

[341] R. Konig, S. Wehner, and J. Wullschleger, "Unconditional security from noisy quantum storage," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1962–1984, 2012.

Zusammenfassung

Quantenpunkt-basierte Einzelphotonenquellen sind von sehr hohem Interesse für Anwendungen im der Bereich Quanteninformation, da sie in der Lage sind einzelne Photonen auf Bedarf zu emittieren. Besonders in der Quantenkryoptographie ist diese Eigenschaft von großer Bedeutung, da dort die Sicherheit jedes einzelnen kryptographischen Primitivs direkt mit den nichtklassischen Eigenschaften der Photonen verbunden ist. Eine hohe Helligkeit der Quellenist dabei eine wesentliche Voraussetzung für sehr schnelle Quantenkommunikation, während eine nied-rige Wahrscheinlichkeit für Multiphotonen minimalen Informationsverlust an potentielle Abhörer sicherstellt.

Diese Arbeit fokussiert sich auf die Untersuchung von Quantenpunkten als Einzelphotonenquellen für Quantenkryptographie und das zukünftige Quanteninternet. Wir simulieren die Dynamik eines Quantenpunkts innerhalb eines optischen Resonators unter drei grundlegenden optischen Pumpmechanismen: resonante Anregung, LA Phononen-assistierte Anregung und Zwei-Photonen Anregung. Wir bestimmen den optimalen optischen Pumpprozess für die wichtigsten quantenkryptographischen Primitive und prüfen ihre Leistungsfähigkeit im Vergleich zu Poissonverteilten Quellen, wie etwa abgeschwächte Laser oder Systeme basierend auf parametrischer Fluoreszenz. Des Weiteren demonstrieren wir, dass Quantenpunkte durch die Einstellbarkeit der Kohärenz in den emittierten Fockzuständen zusätzliche zusätzliche Sicherheitsvorteile bieten.

Wir führen eine experimentelle Untersuchung der nicht-trivialen Abhängigkeit von Helligkeit und Reinheit vom spektralen Abstand sowie der Energie des Pumppulses durch. Die hier untersuchten C-Band Einzelphotonen wurden durch LA-Phononenassistierter Anregung von In(Ga)As Quantenpunkten erzeugt. Dieses Schema zeigt eine niedrige Sensitivität gegenüber umfeldbedingten Fluktuationen, wie Leistung, Polarisation und Wellenlänge der Anregung, und ermöglicht eine hocheffiziente spektrale Filterung des restlichen Pumppulses von den emittierten Einzelphotonen. Die emittierten Photonen zeigen eine niedrige Wahrscheinlichkeit für Multiphotonenevents, hohe Helligkeit und keine Kohärenz in den Fockzuständen. Deshalb ist LA Phononenassistierte Anregung vielversprechend für Implementierungen von Quantenpunkten in Quantennetzwerken unter Praxisbedingungen. Wir definieren die optimalen optischen Anregungsbedingungen für Quantenpunkte unter LA-Anregung, um die maximale sichere Schlüsselübertragungsrate für Quantenschlüsselaustausch mit Einzelphotonen zu erreichen, und zeigen, wie die optimalen Arbeitsbedingungen von den resultierenden Verlusten im Netzwerk abhängen.

Diese Arbeit fasst ebenso die Ergebnisse einer Implementierung des BBM92 Protokolls für Quantenschlüsselaustausch über eine 350m lange, unterirdisch verlegte Glasfaser zusammen, wobei verschränkte Photonenpaare verwendet werden, welche von GaAs Quantenpunkten, hergestellt durch Tröpfchenepitaxie, unter Zwei-Photonen Anregung emittiert werden. Dabei demonstrieren wir die Möglichkeit, Quantenpunkte für verschränkungsbasierte Protokolle zu verwenden, und machen einen wichtigen, ersten Schritt für die Integration von Quantenpunkten in zukünftige Quantenrepeaterschemata basierend auf Verschränkungsaustausch.

Wir unterstreichen die Notwendigkeit an die Anwendung angepasster Anregungsschemata bei der Verwendung von Halbleiterquantenpunkten. Diese richten sich vornehmlich nach deren Helligkeit, Einzelphotonenreinheit und Kohärenz in der Fockbasis. Wir stellen einen wichtigen Leitfaden für die Optimierung von Quantenpunkten bereit, um deren Potential als Einzelphotonenquellen für Quantenkryptographieprotokolle zu maximieren.