universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Practical security and proof-of-principle implementation of quantum-digital payments“

verfasst von / submitted by

Esther Sztatecsny, BSc

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

Master of Science (MSc)

Wien, Juni 2023 / Vienna, June 2023

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 876 [2]
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Master Physics
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. Dr. Philip Walther
Mitbetreut von / Co-Supervisor:	Dr. Mathieu Bozzio

Abstract

The field of quantum cryptography has lead to the proposal of several interesting protocols in the last decades, such as quantum key distribution (QKD), quantum coin flipping, quantum bit commitment and unforgeable quantum money. While QKD has been successfully implemented multiple times, other protocols such as Wiesner's idea of hardcopy quantum money have remained infeasible until now. At the same time, classical digital payments have replaced physical banknotes in many aspects of our daily lives. They are easy to use, unique and tamper-resistant, but need to withstand digital attackers and data breaches. Current technology substitutes customers' sensitive data by randomized tokens, and secures the payment's uniqueness with a cryptographic function. However, computationally powerful attacks violate the security of these functions. Interestingly, schemes such as quantum money can provide security guarantees that rely solely on the no-cloning theorem instead of hardness assumptions. It must be noted, that current quantum tokenisation schemes are still facing some major practical obstacles, such as the need for long-term quantum storage or stringent space-time constraints in combination with several trusted agents to ensure flexible spending.

In this thesis I will present a protocol that relies neither on space-time nor quantum memory constraints — namely *quantum-digital payments*. This scheme constitutes the information-theoretically secure version of classical digital payments, which are used in everyday (online) transactions. This is achieved by compelling the user to commit to a specific merchant upon receiving a sequence of quantum states by measuring them in a certain basis. This basis choice is dictated by the output of a message authentication code (MAC) function, that uses the public Merchant ID and a secret token shared between Client and bank as inputs. The focus of my work lies on the derivation of the security proof – both of the classical MAC function and the quantum cryptographic commitment – as well as the experimental implementation. I will show that it is indeed feasible to securely implement our protocol over on urban fibre link while being robust against attacks.

Zusammenfassung

Quantenkryptographie hat in den letzten Jahren mehrere interessante Protokolle hervorgebracht, u.a. Quantum Key Distribution (QKD), Quantum Coin Flipping, Quantum Bit Commitment sowie fälschungssichere Geldscheine (Quantum Money). Während QKD bereits mehrfach erfolgreich implementiert wurde, sind andere Protokoll wie Quantum Money oder Bit Commitment nur schwer realisierbar.

Zeitgleich haben sich digitale Zahlungen in vielen Bereichen des täglichen Lebens etabliert und ersetzen zunehmend Banknoten als Zahlungsmittel. Digitale Zahlungen sind intuitiv zu verwenden, eindeutig und fälschungssicher, müssen aber gegen verschiedene (digitale) Attacken bestehen. In derzeitig eingesetzten Bezahlsystemen werden sensible Nutzerdaten durch zufällig generierte Token ersetzt und die Zahlung durch kryptographische Funktionen abgesichert. Die Sicherheit von quantenkryptographischen Protokollen wie Quantum Money stützt sich ausschließlich auf das *No-Cloning-Theorem* und nicht auf die unbewiesene Annahmen von schweren mathematischen Problemen – welche nicht effizient lösbar sind. Allerdings sind aktuelle Vorschläge zu quantensicheren Tokens mit einigen großen technischen und praktischen Hindernissen konfrontiert, wie z.B. der Notwendigkeit von langlebigen Quantenspeichern oder strikten Raum-Zeit-Beschränkungen.

Diese Arbeit stellt ein Protokoll vor, das auf keine der erwähnten Einschränkungen angewiesen ist – sogenannte *quantum-digital payments*. Wir beschreiben eine informationstheoretisch sichere Version von klassischen digitalen Zahlungen, die bei alltäglichen (Online-) Transaktionen verwendet werden kann. Der Nutzer entscheidet sich beim Empfang einer Folge von Quantenzuständen – dem Quantentoken – durch Messung in einer bestimmten Basis für einen bestimmten Händler. Diese Basiswahl wird durch die Ergebnis einer MAC-Funktion (kurz für Message Authentication Code) bestimmt. Die nötigen Eingaben sind die öffentliche Händler-ID und ein geheimer Schlüssel, der zwischen Kunde und Bank ausgetauscht wird. Diese Arbeit zeigt nicht nur die Sicherheit dieses Protokolles, sondern demonstriert es zusätzlich experimentell. Dabei wird sowohl die Sicherheit der klassischen MAC-Funktion als auch die der quantenkryptographischen Funktion veranschaulicht.

Contents

Acknowledgements

First of all I would like to thank Philip Walther for giving me the opportunity to write my Master Thesis in his research group and especially on such an exciting and innovative project. I would also like to sincerely thank Mathieu 'Ma' Bozzio for supervising me throughout all these months and providing me with all the necessary input and support. My gratitude in this respect also expands to Tobias Guggemos, who joined our project later but added significant knowledge to the project itself and did a great job in introducing me to the field of classical cryptography as well as vegan cheese. I would also like to thank Julia Kalb for taking the time to introduce me to the experimental setup and Peter Schiansky for explaining the post-processing procedure as well as helping me with figures and any programming question that I had. Thanks to all the members of the Walther research group – the Sensegasse team in particular – for the fun times, the relaxed evenings and the interesting discussions. Last but not least I want to thank Lorenzo for the best espressi and occasional sweets I could have asked for (I will surely miss them)!

1 | Introduction

1.1 Quantum mechanics and information-theoretic security

Quantum mechanics and the 'peculiar' properties associated with it, have fascinated humans since their postulation at the beginning of the 20th century. During the last decades it has enabled many technical advances in a variety of fields, such as computing [1], microscopy [2], cryptography [3] and communication [4]. Undoubtedly two of the most famous fields of application are, however, quantum cryptography and quantum computing, which holds the promise of enhancing communication and computation primitives. Quantum computation especially focuses on making these primitives more efficient, and is in principle capable of shortening computation times drastically for specific tasks (e.g. [5, 6, 7]).
The development of quantum algorithms compromising modern cryptography has triggered a global research for stronger security levels: the security of current cryptographic schemes relies on computationally hard mathematical problems (known as *computational security*), which should be replaced by new quantum-resistant schemes. While research and standardization for such quantum-resistant solutions is blossoming, some of them have already been broken by computational attacks [8, 9, 10].
Quantum cryptography, on the other hand, has the potential to provide security against adversaries with unlimited computational power for some tasks [11, 12], known as *information-theoretic security (i.t.-security)*. This makes quantum cryptographic schemes the perfect candidates for securing communications, transaction etc. in the future, where ever stronger computational power threatens to compromise existing schemes.

1.2 Quantum cryptography beyond QKD

While a plethora of different quantum cryptographic schemes have been developed in the past, the most mature of these is unarguably Quantum Key Distribution (QKD): It enables two parties to securely distribute a secret key over a potentially eavesdropped quantum channel. Ever since its invention by Bennett and Brassard in 1984 [11], it has already established information-theoretic securitys (i.t.-securitys) connections over 500 km of optical fiber [13, 14] and $1,000$ km of free space using satellites [15, 16]. Despite its justified popularity, QKD is not without its flaws: Once the secret key is distributed and the integrity of the quantum channel has been verified, the key may be stored as a classical bit string for later use. From this moment on the key is prone to classical attacks such as device hacking or screen monitoring. Device-independent versions of QKD [17, 18, 19], which do not assume trusted quantum sources or detectors, are also inadequate, since the final

classical output is prone to the same attacks. Also due to this circumstance the last years saw the rise of other quantum information primitives such as coin flipping [20, 21], bit commitment [22, 23], quantum money [24, 25, 26], one-time programs [27] and digital signatures [28, 29]. While some of them have significant drawbacks of their own, what makes them nevertheless interesting is that they cannot be substituted or simplified by QKD, i.e. they have quantum advantages *beyond* QKD. For instance, while it is possible to construct i.t.-secure a bit commitment scheme based on a pre-shared key (distributed via QKD), this relies on trust assumptions between the involved parties. However, many network applications necessitate interacting with potential adversaries.

The present work focuses on two of the above mentioned primitives – quantum bit commitment and quantum money – and combines them to create a new quantum cryptography application: quantum digital payments. As the name suggests this constitutes the information-theoretically secure version of classical digital payments, which became a cornerstone of financial transactions over the last decades. While the security of these schemes is usually based on the hardness of inverting a specific computational function (mostly hash-functions), our scheme proposes security that relies on the quantum no cloning principle, which is physically impossible to circumvent.

1.3 Contributions and thesis outline

In this thesis, we show how quantum light can provide practical security advantages over classical methods in everyday digital payments. One significant threat occuring in such payment schemes, is when customers interact with untrusted merchants, who may not have sufficient means to protect against external hackers, or may be malicious themselves [30]. In that case, a binding commitment between the customer, the merchant and the bank or payment-network is required to guarantee the validity of a transaction. Such a bond usually comes in the form of a cryptogram [31, 32], which is the output of a hash function that guarantees the one-time nature of each purchase. Since not all parties involved are trusted, Quantum Key Distribution (QKD) is (as mentioned above) not suitable to provide i.t. security here, and other quantum solutions need to be established. Interestingly, it is possible to implement our scheme under the assumption that all intermediate channels, networks and parties to be untrusted. Only one authenticated communication (between the client and their payment provider) has to take place at an arbitrary prior point in time. The concealment of the customers' sensitive information is guaranteed by an i.t.-securitys function, and the commitment to the purchase is guaranteed by the laws of quantum mechanics. Our implementation is performed over a 641m urban fiber link, and can withstand the full spectrum of noise and loss-dependent attacks, including those exploiting reporting strategies [33].

1.3.1 Contributions

The project was designed and initiated prior to this thesis by Mathieu Bozzio, Peter Schiansky, Julia Kalb and Alessandro Trenti. Since the experimental setup was almost built when I joined, my practical tasks were mainly optimising the setup, by implementing small changes (e.g. switching from the initial OTPs to BB84 states) and taking the final measurement data as well as finishing the setup characterisation. Additionally I derived the loss- and noise-tolerant security proof using semi-definite programs, both numerically and analytically. This quantum analysis was merged with classical cryptography techniques, building on a Message Authentication Code (MAC). I

was also involved in finalising the use case and developing the digital-payment use-case of our scheme.

1.3.2 Thesis outline

This thesis is structured as follows

- Chapter 2 focuses on the necessary basics of quantum mechanics, quantum cryptography and quantum optics.
- Chapter 3 introduces our scheme of quantum-digital payments, as well as the previous notions it builds upon.
- Chapter 4 is dedicated to the rigorous mathematical proof of the security of our protocol.
- Chapter 5 presents the experimental protocol implementation and the ensuing results.
- Chapter 6 closes the thesis with a short discussion and conclusion.

1.3.3 Publication

The results presented in the following paper (accepted for publication in Nature Communications): *P. Schiansky, J. Kalb, E. Sztatecsny, M.-C. Roehsner, T. Guggemos, A. Trenti, M. Bozzio, and P. Walther, "Demonstration of quantum-digital payments," 2023. arXiv:2305.14504*

2 | Preliminaries

This introductory chapter focuses on several topics and concepts that are crucial to understanding our quantum-digital payment protocol as well as its experimental implementation. These topics are divided into three categories: classical cryptography, quantum cryptography and quantum information in general and quantum optics.

2.1 Classical cryptography

While classical cryptography is mostly disregarded in works focusing on quantum information protocols, we will take the time to explain a few classical cryptographic primitives. This is done for demonstration purposes as well as due to the fact, that one of these primitives is crucial for our protocol, namely Message Authentication Code (MAC). Another important concept explained in this section is the definition of information-theoretic security (i.t.-security) in comparison to computational security.

2.1.1 The goals of cryptography

Cryptography is generally viewed as the art of securing information (or messages) against unauthorized or malicious third parties. One of the goals of cryptography is to achieve some or all of the following properties [34]:

1. **Confidentiality.** Ensures that the message is not disclosed to unauthorized third parties. This is achieved by encrypting the message.
2. **Integrity.** Ensures that the information or message was not modified or destroyed in an unauthorized manner. This can be achieved e.g. by hashing the message.
3. **Authenticity.** The message has to be genuine and able to be verified/trusted. For this usually digital signatures are employed.

In the following we will focus each of these goals in more detail, while discussing different examples for cryptographic primitives.

Confidentiality

In principle, encryption always requires some form of *key*, that turns the message (henceforth referred to as plaintext P) into a ciphertext C and then back into the original plaintext. This can be done

using symmetric or asymmetric algorithms: In the first case both sender and receiver share the same *private* key κ that is used for both en- and decryption:

$$P \xrightarrow{\kappa} C \xrightarrow{\kappa} P$$

In the asymmetric case there are two different keys, a public key k and a private key κ. These two keys are dependent on one another but connected through a mathematical one-way function (i.e. a function that is very hard to invert). This one-way function maps the private key, onto a public key, meaning it is very easy to retrieve the public key from the private key, but near impossible to derive the private key from the public key. The public key is then used for encryption, while the private key is used for decryption:

$$P \xrightarrow{k} C \xrightarrow{\kappa} P$$

One-time pads
One-time pad (OTP) is a special symmetric encryption protocol in which a secret key κ is shared between two parties. This key (sometimes also referred to as OTP) is then used to en- and decrypt a plaintext via $C = P \oplus \kappa$ and $P = C \oplus \kappa$, where $\oplus$ denotes bit-wise XOR. Thus κ has to be at least as long as the plaintext P in question, and to be secure it can only be used once (hence the name). If the key is uniformly distributed, OTP can provide unconditional security (see Subsection 2.1.2), but becomes fairly impractical: Not only is κ required to be as least as long as the plaintext, but also a new κ has to be securely distributed for every bit of the message.

Integrity

Integrity of a message is achieved when the receiver can verify that the message has not been altered by another unauthorised third party. Note that this does in general not mean, that the third party is not able to learn the message or impersonate party A. It follows that integrity is only useful if one assumes a trusted channel, i.e. if one can guarantee that party A is really the sender of the message. One way to achieve this constraint is via hash-functions.

Hash-functions
A hash function H maps an input of arbitrary length to an output of fixed length n. The important property of this mapping $H : 0, 1^* \to 0, 1^n$, is that any change in the input string, however small, has to lead to a sufficiently different output. In order for a hash-function to be *cryptographically secure* it has to fulfill the requirement of collision resistance: It should be computationally infeasible to find two inputs m and n, where $m \neq n$ such that $H(m) = H(n)$. This means that given m it is infeasible to find another input n that leads to the same output of the Hash-function.
Since it is very hard to find two plaintexts P and P' that lead to the same output, this can be used to ensure that the message has not been altered, if $H(P)$ is sent along with P.

Authenticity

Authenticity ensures that the message received by party B was sent by party A. It thus protects against impersonation attacks of untrusted third parties. Often (but not always) it also ensures that the plaintext itself has not been altered, thereby also achieving integrity as defined above. While dititial signatures are a common way to authenticate the sender, we will – for reasons that will become apparent later – focus on another example: message authentication codes, which are usually used to authenticate the message.

Message authentication codes

A message authentication code (MAC) is used to achieve *authenticity* and *integrity* of a message. Note that it does per se not ensure *confidentiality* of the message. In formal terms, a MAC can be defined as a function that takes a touple of key κ and message M and returns a tag T, i.e. $\text{MAC}(\kappa, M) \rightarrow T$. If T is sent along the message M, an honest verifier knowing the secret key κ can ascertain the *authenticity* and *integrity* of the message by checking that $T = \text{MAC}(\kappa, M)$.
In general a MAC is considered secure if it is existentially unforgeable against chosen message attacks. This means that an attacker is unable to generate a valid tag T, without knowing the secret key κ, and it is impossible for them to obtain tags on other messages.

HMAC Keyed-hash message authentication codes (HMACs) are a special form of MACs that are based on a hash-function H. Formally, they are defined similar to other MACs as a function that maps a message M and a secret key κ onto a tag T. The only difference is the precise implementation under usage of the hash-function: $\text{MAC}(\kappa, m) = H(\kappa \oplus \text{opad} \parallel H(\kappa \oplus \text{ipad} \parallel M))$. Here opad and ipad are public strings with a fixed length, $\oplus$ is a bit-wise XOR and $\parallel$ means concatenation. If the used hash-function is collision resistant, the corresponding HMAC is considered secure.

2.1.2 Computational versus i.t.-security

The security of a cryptographic primitive can be either be computational or i.t.-secure. Here computational means that the security relies on the *hardness* of breaking the primitve – but breaking it is per se not impossible. This also implies that the security is dependent on the computational power (or lack thereof) of the adversary. I.t.-security, on the other hand, refers to the fact, that no matter how strong the adversary is, it is (nearly) impossible to circumvent the security measure. This is also often referred to as *unconditional* security. It is therefore independent of the computational power of the adversary. This is especially interesting, since computers (and quantum computers) are becoming more and more powerful, thus threatening to break conventional security protocols. As mentioned in the introduction of this thesis, quantum protocols usually fall into the latter category which makes them promising candidates for the future of cryptography.

A useful theorem for determining whether a cipher can be considered information theoretically secure or not is given by a variant of Shannon's theorem [35]:

Theorem 2.1.1 (Shannons's theorem)**.** *If the probability distribution $D_{\mathcal{K}}$ on $\mathcal{K}$ of a cipher is the uniform distribution, and for every plaintext $P \in \mathcal{P}$ and every ciphertext $C \in \mathcal{C}$, there is exactly one key $\kappa \in \mathcal{K}$, s.t. $Enc_\kappa(P) = C$, then the cipher is perfectly secret, i.e. i.t.-secure.*

This holds true for e.g. OTPs as discussed above. One of the problems of OTPs is, however, how to distribute the key between the trusting interacting parties, while ensuring that no third party intercepts them. This problem has lead to the introduction of classical (Diffie-Hellman key exchange) as well as quantum (QKD) protocols, ensuring 'save' distribution of secret keys.

In contrast, a problem is referred to as *computationally hard* or *secure*, if it is not possible to solve this problem in polynomial time. A famous example of such a problem is prime factorisation which is used for example in the RSA scheme [36]: given an integer N find the prime numbers q and p such that $N = q \cdot p$. Another cryptographic protocol which falls into this category is the above mentioned Diffie-Hellman key exchange protocol which exploits the discrete logarithm problem, which describes

the problem of finding the integer x, when given g and $a = g^x \mod N$, where g is the generator of a cyclic group G [37]. In principle we distinguish between two types of computationally secure protocols:

1. Protocols that are in principle already broken by algorithms such as Shor's algorithm [5] and Grovers search algorithm [38]. Both prime factorisation and the discrete logarithm problem can be broken by Shor's algorithm. Grover's search algorithm on the other hand poses a threat to schemes, where the best cheating strategy is searching through a key space. However, the corresponding cryptographic schemes are still en-use, since the quantum algorithms that can break them are as of yet not fully implementable.

2. Protocols that as of yet have not been broken, even in principle. Among these are lattice-based cryptographic protocols [39] and hash-based signatures [40]. Note, however, that there is no guarantee that it is impossible to find an algorithm (classical or quantum) to break these schemes. In fact more and more *post-quantum* schemes are currently being discarded as they are found to be insecure.

Generally speaking we say that a protocol is computationally secure, if it has an underlying mathematical structure, that can be exploited to increase the cheating probability above the probabiliy of *guessing* or *brute-forcing* the correct key, message, etc. On the other hand, we refer to a protocol as being i.t.-secure, if there is no such underlying structure, and no cheating strategy that would yield better results than guessing.

2.1.3 i.t.-secure MAC

A very interesting version of MACs are those for which i.t.-security holds. We will follow the description given in [41]. This is the case, when it is secure against: 1.) **impersonation attacks**, where the attacker may produce a message and a tag that are valid under the used key and 2.) **substitution attacks**, where the attacker intercepts a valid tag-message touple (T, M) and replaces it with another valid tag-message touple (T', M'). This further implies that it should be impossible to find $\mathrm{MAC}(\kappa', M) = \mathrm{MAC}(\kappa, M)$, for a secret key κ.

For demonstration we will look at a simple example of a so called *authentication matrix*, displaying the different output tags corresponding to a certain key-message pair (see Table 2.1).

Using this example let us take a closer look at the two possible attacks.
For an impersonation attack it is necessary to pick a message M, i.e. either 0,1 or 2 and then guess the correct output tag under the private (and thus unknown) key in use. Now the probability of actually guessing the correct tag is exactly 1/3, and the success probability is purely probabilistic, meaning that there is no underlying logic that may be exploited (as long as the key remains unknown). When the key and message spaces grow, this probability decreases further.
Now assume an impersonation attack, where a valid tag-message combination (T, M) is intercepted, and should be replaced with another combination (T', M'), that is valid under the key in use. Now in our example it is easy to see that for every M there are exactly three different κ's that lead to the same output tag T. Thus the probability of successfully guessing the correct T' for M' is again 1/3. If we, like in the example above, assume that the size $|\kappa|$ of the key space κ is the square of the size

Table 2.1: Simple version of an authentication matrix: Depending on the key κ and the message M the tag T takes on different values. Note, that the same value of the tag can arise from different key-message pairs. This makes guessing the secret key probabilistic, even if the message is public. Example taken from [41].

M/κ	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
0	0	1	2	0	1	2	0	1	2
1	0	1	2	1	2	0	2	0	1
2	0	1	2	2	0	1	1	2	0

of the message space $|M|$, i.e. $|\kappa| = |M|^2$ and $|T| = |M|$ we get a cheating probability of:

$$p_c = \frac{1}{|T|} = \frac{|M|}{|\kappa|} = \frac{1}{\sqrt{|\kappa|}} \tag{2.1}$$

2.2 Quantum mechanics basics

In this section we will quickly cover theoretical basics of quantum mechanics, such as superposition, entanglement, evolution of quantum states, measurements, etc. This is by no means meant to be a complete description of quantum mechanics as a whole, but is aimed to explain the concepts that are most important to our protocol and experiment.

2.2.1 Quantum states

What distinguishes quantum particles from classical particles is their ability to be in a *superposition* of states. This property of not having 'to decide' where to be or which property to exhibit leads to a variety of interesting effects, especially the capability of quantum states to interfere with themselves. Often it is sufficient to describe quantum states using linear algebra, where quantum states are written as complex vectors and operations as unitary or hermitian matrices. For convenience we will henceforth use the so called bra-ket notation, where any pure quantum state and its complex conjugate can be written as

$$\begin{pmatrix} a \\ b \\ c \\ ... \end{pmatrix} \hat{=} |\psi\rangle\,, \quad \begin{pmatrix} a^* & b^* & c^* & ... \end{pmatrix} \hat{=} \langle\psi| \tag{2.2}$$

This notation allows to calculate and define certain values very easily and fast, such as the scalar product

$$\langle\psi|\psi\rangle = \begin{pmatrix} a^* & b^* & c^* & ... \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ ... \end{pmatrix} = a \cdot a^* + b \cdot b^* + c \cdot c^* + ... \tag{2.3}$$

or the tensor product:

$$|\psi\rangle\langle\psi| = \begin{pmatrix} a \\ b \\ c \\ ... \end{pmatrix} \cdot \begin{pmatrix} a^* & b^* & c^* & ... \end{pmatrix} = \begin{pmatrix} aa^* & ab^* & ac^* & ... \\ ba^* & bb^* & bc^* & ... \\ ca^* & cb^* & cc^* & ... \\ ... & ... & ... & ... \end{pmatrix} \tag{2.4}$$

For example we can use this notation to describe a photon being absent/present in a specific spatial mode:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.5}$$

Their complex conjugates can be defined as:

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix} \tag{2.6}$$

Note that this is a very abstract way of describing quantum particles and it is also possible to assign intrinsic values of particles to these states. E.g. we can describe the polarisation of a horizontally/vertically polarised photon by $|H\rangle/|V\rangle$ and assign the same vector notations to them, i.e.

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.7}$$

In this formalism it is possible to 'concatenate' quantum particles in different spatial modes in a simple manner, e.g. two empty spatial modes can be written as $|00\rangle$ etc. Note that in reality this corresponds to a tensor product $|0\rangle \otimes |0\rangle$ of two vectors living in two different Hilbert spaces.

Since we use linear algebra to describe quantum states, it is always possible to use different bases to describe the same state. For example, one might instead use the basis states

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{2.8}$$

Creation and annihilation operators

Another convenient way to describe quantum states are the *creation and annihilation operators*. As their name suggests they describe the abstract operation of creating or annihilating a photon in a given mode, i.e.

$$a^\dagger |0\rangle = |1\rangle \tag{2.9}$$
$$a |1\rangle = |0\rangle \tag{2.10}$$

For the case of more than one photon these two operators can be generalised to

$$a^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{2.11}$$
$$a |n\rangle = \sqrt{n}\,|n-1\rangle \tag{2.12}$$

The advantage of using these operators rather than the notation used previously, is mathematical simplicity, since these operators come with the intrinsic property of conserving normalisation in most cases. This makes the computation of multiple operations in succession simple, as there is often no need to renormalise the state by hand after every step. In the case of multiple modes and/or polarisations, it is necessary to label the creation and annihilation operators accordingly, e.g.

$$\begin{aligned} a^\dagger_{1_H} |00\rangle &= |H0\rangle \\ a^\dagger_{1_V} |00\rangle &= |V0\rangle \\ a^\dagger_{2_V} |00\rangle &= |0V\rangle \\ a^\dagger_{1_H 2_V} |00\rangle &= |HV\rangle \\ &\text{etc.} \end{aligned} \tag{2.13}$$

2.2.2 Measurements

Just like classical states, quantum states also evolve in time. This can happen in one of two ways: continuously (corresponding to a unitary operation) or in form of a so called 'collapse'. Conventional measurements are usually part of the second category, meaning they are instantaneous and irreversible. Mathematically they are described by hermitian operators H, which correspond to a projection or *collapse* of the wavefunction. Thus they always satisfy $H^\dagger{=}H$, ensuring that the eigenvalues of these operators are always real, since these values will correspond to the possible measurement outcomes in the real world. Let A denote one of these *measurement operators*. Furthermore these operators, often referred to as *observables* can be decomposed into their spectral decomposition

$$\hat{A} = \sum_i \lambda_i |\lambda_i\rangle \langle\lambda_i| \tag{2.14}$$

where A is the name of the observable λ_i denotes its eigenvalues and $|\lambda_i\rangle$ denotes its eigenstates. After the measurement the quantum state will collapse into one of these eigenstates and the measurement outcome will be given by the corresponding eigenvalue. The expectation value of a measurement on a quantum state is given by

$$\langle\psi| \hat{A} |\psi\rangle = \sum_i \lambda_i \langle\psi|\lambda_i\rangle \langle\lambda_i|\psi\rangle \tag{2.15}$$

Measurements can be expanded to multiple particles in a very straightforward manner:

$$\hat{A}_1 \otimes \hat{A}_2 \left|\psi_1\right\rangle \otimes \left|\psi_2\right\rangle = \sum_i \lambda_{1i} \left\langle\psi_1|\lambda_{1i}\right\rangle \left\langle\lambda_{1i}|\psi_1\right\rangle \otimes \sum_j \lambda_{2j} \left\langle\psi_2|\lambda_{2j}\right\rangle \left\langle\lambda_{2j}|\psi_2\right\rangle \tag{2.16}$$

Pauli operators

$$\begin{aligned} \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{2.17}$$

These operators correspond to a measurement in the x, y and z-basis respectively.

The conceptually important thing to note is that quantum measurements are always *irreversible*, i.e. after a measurement it is impossible to tell what the original quantum state looked like. This is, important for many quantum cryptographic concepts, discussed below.

2.2.3 Base complementarity

In quantum mechanics states can be described by different but equitable bases. For example the state

$$\left|\psi\right\rangle = \left|H\right\rangle \tag{2.18}$$

can also be described as a superposition in the diagonal

$$\left|\psi\right\rangle = \frac{1}{\sqrt{2}}(\left|+\right\rangle + \left|-\right\rangle) \tag{2.19}$$

or the circular basis[1]

$$\left|\psi\right\rangle = \frac{1}{\sqrt{2}}(\left|L\right\rangle + \left|R\right\rangle) \tag{2.20}$$

These three bases are called *mutually unbiased* or *complementary*, meaning that measuring in a different basis than the one in which the state was prepared, will lead to completely random outcomes. Note that these three bases correspond to the Pauli matrices mentioned earlier eq. 2.17. E.g. our state $\left|\psi\right\rangle$ as defined above is encoded in the computational basis and measuring it in this basis would always yield the result H or 0. Measuring the state in the diagonal or circular basis would, however, leads to randomly distributed outcomes. This fact is often used in quantum cryptography and is strongly connected to the no-cloning theorem (see Subsection 2.3.2). To see why, assume two parties Alice and Bob. Alice prepares a quantum state in a basis of her liking,

[1] Here and henceforth the following convention is used: $\left|L\right\rangle = \frac{1}{\sqrt{2}}(\left|H\right\rangle + i\left|V\right\rangle)$, $\left|R\right\rangle = \frac{1}{\sqrt{2}}(\left|H\right\rangle - i\left|V\right\rangle)$

e.g. the diagonal basis and sends this state to Bob. If Bob is unaware which basis Alice used, he is unable to determine what state Alice encoded. If he knew however, what basis Alice used, he could always read out her input, i.e. determine whether the photon is H or V polarised. This can be used to securely transmit messages from Alice to Bob, if they are the only ones knowing the basis to encode the message in. A third potentially malicious party E intercepting the quantum state would be unable to conclusively decode the message.

2.2.4 Entanglement and passive state preparation

Entanglement is another interesting property, only exhibited by quantum states. In general terms, it describes the ability of quantum states to be correlated with one another, in a way that is not achievable classically.
A quantum state is called entangled, iff it cannot be decomposed into two single particle states, i.e. when

$$|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \tag{2.21}$$

If this is the case these entangled quantum particles will be correlated such that if we measure the state of one of them, the state of the other particle will show correlations. The two particle states that exhibit the highest degree of entanglement, are the so called Bell states

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle) \end{aligned} \tag{2.22}$$

These states were famously used to proof Bell's theorem [42], which demonstrates that quantum mechanics cannot be explained by local hidden variables.

Apart from its philosophical implications entanglement is also useful for different experimental implementations: from quantum imaging cite to quantum computing with cluster states cite cite, etc. The application we are most interested in is *passive state preparation*. Here the properties of an entangled photon pair is exploited to set the value of a certain degree of freedom – e.g. polarization – of one of the photons, by measuring the other.

For example consider an entangled photon pair in the state $|\phi^-\rangle$. If one of the two photons is measured to be in the state $|H\rangle$, the other photon will also be found to be in this state. If, however, the measurement is done in the diagonal basis and the first photon is found to be in the state $|+\rangle$, the second photon will be measured to be in the state $|-\rangle$. We say the state $|\phi^-\rangle$ is *correlated* in the z-basis and *anti-correlated* in the x-basis. For the content of this thesis it is important to note that the state $|\psi^-\rangle$ is anti-correlated in every basis, meaning that no matter the measurement and outcome of one of the photons, the other photon will always be 'prepared' in the orthogonal state.

2.3 Quantum cryptography

Quantum cryptography makes use of the intrinsic properties of quantum states and employs them for cryptographic tasks. Often it is possible to achieve i.t.-security this way (see Subsection 2.1.2). We will briefly discuss qubits, the so called no cloning theorem – which lies at the heart of most

quantum cryptography schemes – as well as Quantum Key Distribution (QKD), one of the first installments of quantum cryptography, which also displays how i.t.-security can be achieved with quantum states.

2.3.1 Qubits

In classical computation a bit can take on either the value '0' or '1'. In the realm of quantum mechanics, however, a state cannot only be in a definite state but in a superposition of states. This could in principle allow to run the same algorithm in parallel for different input bits, without needing any additional resources. Of course it is not possible to retrieve both outcomes at the same time, only one will be displayed once the quantum particle gets destroyed. However, there is an additional degree of freedom in qubits impossible to achieve with classical bits: coherence. This allows to combine the two different outcomes and retrieve some shared information about them. This can then be used to obtain a quantum advantage for certain computational tasks. A well known example is Shor's algorithm that would allow for a significant advantage in prime factorization [5].

Often one refers to quantum states as qubits, whenever they are used to encode logical information, i.e. when they are used in the realm of quantum information or quantum cryptography. In this sense any degree of freedom of a quantum system can be a qubit – the polarisation or spatial mode of a photon, the spin of an electron etc – in this work, however, we will focus on polarisation, as this is the degree of freedom we use in the experimental implementation.

2.3.2 The no-cloning theorem

The no cloning theorem was first described by Wootters and Zurek [43] and states that a single quantum state cannot be cloned without failure. The proof is fairly simple and will thus be briefly demonstrated. Assume some unitary operator U_{clone} that is capable of cloning any quantum state in the computational basis. Its action can thus be described as:

$$\begin{aligned} U_{clone} |0\rangle |0\rangle &= |0\rangle |0\rangle \\ U_{clone} |1\rangle |0\rangle &= |1\rangle |1\rangle \end{aligned} \tag{2.23}$$

This same operator should of course also be able to clone quantum states in other bases e.g. the diagonal basis

$$\begin{aligned} U_{clone} |+\rangle |0\rangle &= U_{clone} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle \\ &= \frac{1}{\sqrt{2}} (|0\rangle |0\rangle + |1\rangle |1\rangle) \\ &\neq |+\rangle |+\rangle \end{aligned}$$

From this it is evident that such cloning operators always work for one specific basis only, e.g. the computational basis, and have unwanted effects on the states of any other basis.[2] It is thus impossible to clone an *unknown* quantum state. This has also consequences for quantum cryptography as it makes sure that a malicious party cannot circumvent the constriction imposed by mutually unbiased

[2] Interestingly, the cloning operator defined in eq. (2.23) is identical to the Controlled-Not gate, often used in quantum computing.

bases by simply cloning the quantum states. Note, however, that conjugate coding and the no cloning theorem are interconnected, although they might seem to be different concepts at first glance: if it is impossible to identify an unknown state, it is also impossible to duplicate it and vice-versa.

2.3.3 Quantum Key Distribution

As mentioned before, base complementarity (or the no-cloning theorem) can be used in cryptographic tasks enabling i.t.-security. Probably the most famous of those is Quantum Key Distribution (QKD). The first version of this scheme was proposed in 1984 by Bennett and Brassard [11] known as the *BB84 protocol*. Assume the following situation: Two parties (Alice and Bob) want to share a secret key, but can only do so remotely. Alice could simply send the key to Bob, however, then a third party intercepting the key, could copy it and then forward it to Bob. Alice and Bob would then, unsuspectingly, use this key to encrypt their messages, which the malicious third party could easily decode. As mentioned in Section 2.1 there are various classical encryption schemes, that are computationally hard but not inherently impossible to crack. In order to overcome the threat of an almighty malicious third party (that is still bound to the laws of physics), Alice and Bob instead exploit quantum mechanics, in particular the no-cloning theorem.

The BB84 protocol proceeds as follows: Alice sends a series of quantum states, choosing randomly between two possible bases for encryption, H/V or $+/-$. Bob then also chooses randomly in which basis to measure each qubit. Later Alice and Bob publicly declare what measurement basis they used for encryption and measurement respectively. By only keeping those bits for which their basis choices are identical, they ensure that Bob retrieves the same bit, that Alice encoded. This step is called 'sifting'. Since they only declare the basis choice and not the encoded bits, only Alice and Bob are now in possession of the secret key. However, it is of course possible for a malicious third-party (referred to as Eve) to intercept the quantum states sent by Alice and send randomly generated quantum states to Bob. She could then wait for the declaration of the basis-choice and use the attained classical measurement outcomes to decrypt the secret message. In order to avert this vulnerability of the protocol, Alice and Bob can compare some of their encoded and decoded bits, to assure that Bob did indeed receive Alice's states and not states that were randomly generated by a third party. The probability of successful cheating thus therefore decrease exponentially with the number n of qubits sent:

$$p_{\text{cheat}}(n) = \left(\frac{3}{4}\right)^n \tag{2.24}$$

Evidently this probability is independent of the computational power of the adversary, meaning that the corresponding protocol is i.t.-secure.

2.4 Quantum optics

Since the experimental implementation of our protocol is done with single photons, this section will recap a few basic properties of light as well as the working principles of optical elements (i.e. objects that are used to alter or determine the properties of light). While these include both classical and quantum processes, we will mainly focus on a specific property of light, namely polarisation. Additionally we will briefly discuss *spontaneous parametric down conversion*, which is one way of realising a single and/or entangled photon source.

2.4.1 Polarisation of light

As mentioned before, one important property of light is its *polarisation*. It describes how the electromagnetic field is oriented in the plain perpendicular to the direction of propagation. Two important examples are linear or circular polarisation of light. In the first case the orientation of the field stays constant in a specific direction relative to a reference frame, e.g. horizontally polarised with respect to the experimental setup, while in the latter case this direction changes circularly. Depending on the direction of this change we distinguish between left and right circularly polarised light. The polarisation of light or single photons can be changed fairly easy, but will remain unchanged if the light is kept sufficiently isolated. This makes polarisation a good choice for encoding information, since it is easy to manipulate but comparatively stable if left untouched.

Optical elements

In the following we will briefly explain the optical elements that are needed to manipulate the polarisation of light. We will only do a quick description of the properties of these elements, for an extensive explanation on the working principle see e.g. [44].

Polarisers
In order to turn unpolarised light into polarised light, so called polarisers are used. These only let a certain polarisation pass, effectively filtering out the unwanted parts. This is particularly important, when working with coherent sources, that most often do not emit light in a predefined polarisation. When working with single photons, polarisers are vital for setup calibration and characterisation.

Waveplates
Waveplates are optical elements that can change the polarisation of light or single photons without altering their path. This is done by retarding one of the polarisation components of the light with respect to the perpendicular component, i.e. they introduce a phase shift between these two components. We differentiate between *half wave plates* (HWP) and *quarter wave plates* (QWP). Both are made of a birefringent material, but differ in their thickness, always in respect to the wavelength of the targeted photons. HWP are used to turn linearly polarised light of any orientation, into linearly polarised light of any other polarisation depending on the precise setting. Additionally they are used to turn left into right circularly polarised light and vice versa. QWP on the other hand, are used to transition from linearly to circularly polarised light and vice versa. Since waveplates always have a fast and a slow axis, the way they act on light is always dependent on their angular setting. For example setting a HWP to an angle off 45° will turn horizontally polarised light into vertically polarised light and vice versa, while a HWP set to 0° won't alter the orientation of linearly polarised light at all.

(Polarising) Beamsplitters
A beamsplitter (BS) is a partially reflective and transmissive optical element, meaning that a certain percentage of the light that impinges on it is either reflected (at a 45° angle) while the other photons simply traverses them. If a single photon impinges on such a BS it is therefore either reflected or transmitted with a certain probability (conventionally 50%) . This makes a BS ideal to prepare a single photon in a superposition of two spatial modes, as – before the measurement – it is not possible to tell which path the photon took. While this 'normal' type of BS does not differentiate between different photons, it is also possible to construct a BS that reflect or transmit the photon

based on their polarisation: a so-called polarising beamsplitter (PBS). A PBS will thus always reflect photons of a specific polarisation (e.g H polarised photons) and transmit photons of the perpendicular polarisation (e.g. V polarised photons). This makes polarising beamsplitters ideal to seperate photons of different polarisations, which is necessary for e.g. building a polarisation resolving measurement aparatus.

2.4.2 Non-linear optics and single photon sources

In order to perform most quantum experiments a single photon source is of the essence. In the most ideal case the states produced by these sources can be described by the number state $|n = 1\rangle$, meaning there are no coherences in number basis or multiphoton emissions. While there are multiple ways how to implement such a source we will focus on *spontaneous parametric down conversion* (SPDC) sources which rely on non-linear processes within a $\chi^{(2)}$ nonlinear crystal. The following explanation is only meant as a broad overwiev and makes no claim at being thorough. We will describe the full mathematics and mechanics of the precise source we used in a later chapter (see Section 5.1).

Generally speaking non-linear optics describe processes in which the light interacts with nonlinear media. In this case the polarisation density of the material reacts in a nonlinear way to the electric field of the impinging light. Depending on the precise properties of the material, this can result in interesting effects, where the properties of the light, such as frequency, polarisation, spatial mode etc. get altered by the material in a nonlinear way, leading to a large variety of interesting optical effects. Some of these effects may be purely classical, e.g. sum-frequency generation (SFG), while others can only be explained in the context of quantum physics, e.g. spontaneous parametric down-conversion (SPDC). In SFG two photons of the impingent (laser-) light are destroyed, while a photon with the sum of the two frequencies is created.

SPDC on the othercand describes the opposite process, where a single (*pump*) photon of the laser light *downconverts* into two photons, often referred to as *idler* and *signal* photon respectively. As a physical process SPDC must satisfy conservation of energy as well as momentum. The first law thus dictates that

$$\nu_{pump} = \nu_{signal} + \nu_{idler} \tag{2.25}$$

meaning that signal and idler photons have a different frequency than the pump photon (most commonly the two resulting photons both have half the frequency of the impingent one). Conservation of momentum results in the exiting photons to be emitted into specific spatial modes. In the most common realisation with Beta Barium Borate (BBO) crystals these modes correspond to cones. By preparing the crytal and setup accordingly, these two cones can be made to intersect making the photons collected at these intersection points polarisation entangled. Thus SPDC processes are good candidates for single as well as entangled photon sources. In most cases one of the two photons is used to herald the existence of the other photon, which is in turn used for the actual experiment. Often the idler photon is used for passive state preparation of the signal photon: by measuring the polarisation of the idler, we 'force' a specifically correlated polarisation on the signal. For example, if the SPDC process results in the two photons being in the state $|\psi^-\rangle$, measuring the idler photon in the H/V basis and finding it to be H polarised will result in the signal photon to be V polarised. We call this kind of state preparation *passive*, since there is no way to *influence* the polarisation the

photon will eventually have, but only to *assess* it. It is nonetheless useful as it allows us to prepare the signal photons in an accountable way.

Multiphoton emission and g_2

One of the most problematic properties of SPDC sources is that, depending on the pump power, it might happen that multiple photon pairs are created simultaneously. As such they will also be enter the setup and be prepared in the same way. This can pose a problem for many reasons, the most important for us, however, is the threat it poses with respect to a cheating party. Suppose e.g. a QKD protocol as described above (Subsection 2.3.3) where the used source creates multiple identical photons in the same way. This would introduce a new version of eavesdropping, as the malicious third party could separate these identical photons from one another, forward one to Bob and measure the other one themselves, potentially doing so undetected. Thus it is important to know the amount of multiphoton emissions from the used source, to quantify these undetectable cheating/eavesdropping events.

Put simply, this multiphoton emission can be measured by statistically separating the emitted photons (e.g. with a 50/50 BS) and measuring the number of coincidences, i.e. the number of times two photons exit this BS through the two different spatial modes simultaneously. However, there are multiple different conventions on how to define the precise value of multiphoton emission. For the normalisation convention used in our experiment see Subsection 5.4.3.

2.5 Mathematical tools

In this section of the introductory chapter, we introduce different mathematical tools and definitions, that are needed for the rigorous security analysis of our scheme.

2.5.1 The quantum de Finetti theorem

We will use the quantum de Finetti theorem to simplify our security proof. In general terms, this theorem enables the approximation of permutation invariant states by *independent and identically distributed* (i.i.d.) subsystems. The ensuing explanation will closely follow [45].

Let π be the permutation on n qubits living in the Hilbert space $\mathscr{H}_2^{\otimes n}$. The corresponding permutation operator $P_d(\pi)$ is then given by:

$$P_d(\pi) = \sum_{m_n} \left|m_{\pi(1)}, m_{\pi(2)}, ..., m_{\pi(n),}\right\rangle \langle m_1, m_2, ..., m_n| \tag{2.26}$$

where $\langle m_1, m_2, ..., m_n|$ is a series of unpermutated quantum states and $\left|m_{\pi(1)}, m_{\pi(2)}, ..., m_{\pi(n),}\right\rangle$ represents the series of the same quantum states after applying the permutation π_i. Thus the permutation operator maps each series of quantum states onto the corresponding permutated series of quantum states.
A quantum state $|\psi\rangle \in \mathscr{H}_2^{\otimes n}$ is defined as n-exchangeable, iff

$$P_d(\pi) |\psi\rangle \langle\psi| P_d(\pi) = |\psi\rangle \langle\psi| \tag{2.27}$$

In general terms, a *measure* μ can be regarded as a function that assigns a value to some given subset of a set. The quantum de Finetti theorem then states that there exists such a measure μ such that

$$\begin{aligned} ||\mathrm{Tr}_{n-k}[\rho] - \int \sigma^{\otimes k} d\mu(\sigma)||_1 \leq \frac{2k \cdot (k+d)}{n+d}, \quad \forall k \leq n \\ \text{where } \rho = |\psi\rangle \langle\psi| \end{aligned} \tag{2.28}$$

This means that the density matrix of the multipartite quantum state ψ can be approximated by a convex combination of density operators, which are of the type $\sigma^{\otimes}k$ in most subsystems.

2.5.2 Semi-definite programming

A semi-definite program (SDP) is a tool to solve convex optimisation problems, involving semi-definite positive matrices as variables. The definitions here follow closely the description given in [46]. A primal SDP typically consists of an objective function (first line) that one tries to optimize, and one or multiple linear constraints (all other lines):

$$\begin{aligned} \sup \langle A, X\rangle = \sup \mathrm{Tr}[A^\dagger \cdot X] \\ \text{subject to: } \Phi(X) = B \\ X \geq 0 \end{aligned} \tag{2.29}$$

where Φ is a given trace-preserving, linear map, A and B are given hermitian operators, X is the positive semi-definite optimisation variable and 'sup' is short for *supremum*. We define the *optimal primal value* of this SDP as:

$$\alpha = \sup \mathrm{Tr}[A \cdot X] \tag{2.30}$$

Semidefinite programs present a dual structure, which makes it possible to associates a dual minimization problem to each primal maximization problem. Here, the new variable(s) Y of the dual problem can be understood as the Lagrange multipliers associated with the constraints of the primal problem (one for each constraint). Thus for the primal SDP above we can derive a dual problem

$$\begin{aligned} \inf \langle B, Y\rangle = \mathrm{Tr}[B \cdot Y] \\ \text{subject to: } \Phi^*(Y) \geq A \\ Y = Y^\dagger \end{aligned} \tag{2.31}$$

where we also define an *optimal dual value*:

$$\beta = \inf \mathrm{Tr}[B \cdot Y] \tag{2.32}$$

Note that what we define as primal and dual SDP is of course arbitrary – the primal SDP could also be used to find an infimum, while the dual is used to find the corresponding supremum.

Weak and strong duality

Weak duality states that $\alpha \leq \beta$ for every SDP. This means that the optimal solution of the dual problem upper bounds the optimal solution of the primal problem. Interestingly this also means that

$$\langle A, X\rangle \leq \alpha \leq \beta \leq \langle B, Y\rangle \tag{2.33}$$

implying, that if we find a X and Y such that $\langle A, X\rangle = \langle B, Y\rangle$ the optimal primal and dual values are attained.

2.5.3 Chernoff-Hoeffding bounds

Sometimes it may be necessary to consider statistics arising from finite sample sizes. For example it might happen that an honest party introduces more errors or losses than initially estimated, or that by chance a dishonest party introduces less errors than assumed. In order to estimate the likelihood of these events we utilize the notion of Chernoff-Hoeffding bounds as described in [47]. Assume a set of n random variables X_i, which can take on the values 0 or 1. To be precise $X_i = 1$ with probability p_i and $X_i = 0$ with probability $1 - p_i$. As per usual we denote the expectation value by $\mu = \sum_{i=0}^{n-1} p_i$. As we assume an equal error probability for all photons, we are specifically interested in the case where all n variables X_i have identical probabilities p_i, i.e. where $\mu = p_i \cdot n$. Then the probability that the mean value $X = \sum_{i=0}^{n-1} X_i$ is larger than the expectation value by more than some $\delta \in [0, 1]$ is upper bounded by the *upper tail*:

$$P[X \geq (1+\delta) \cdot p_i \cdot n] \leq e^{\frac{\delta^2}{3} \cdot p_i \cdot n} \tag{2.34}$$

Similarly the probability that the mean value is lower than the expectation value by more than some $\delta \in [0, 1]$ is lower bounded by the *lower tail*:

$$P[X \leq (1-\delta) \cdot p_i \cdot n] \leq e^{\frac{\delta^2}{2} \cdot p_i \cdot n} \tag{2.35}$$

2.5.4 The Choi-Jamiolkowski isomorphism

For our security proof it will be necessary to find a linear map that brings quantum states states living in the Hilbert space $\mathscr{H}_q$ to the joined Hilbert space of two classical states $\mathscr{H}_c \otimes \mathscr{H}_c$ ($\Lambda : \mathscr{H}_q \to \mathscr{H}_c \otimes \mathscr{H}_c$). In order to be able to ensure that this map really corresponds to physically implementable operations – i.e. that Λ is (1.) completely positive and (2.) trace preserving – it is convenient to find a corresponding density matrix, living in the tensor product space $\mathscr{H}_c \otimes \mathscr{H}_c \otimes \mathscr{H}_q$. The Choi-Jamialkowsi isomorphism (as described e.g. in [48]) provides a way to calculate the *Choi-matrix* of the map Λ:

$$C_\Lambda = \sum_{k,l=0}^{d-1} \Lambda\Big(|k\rangle \langle l| \Big) \otimes |k\rangle \langle l| \tag{2.36}$$

where $|k\rangle, |l\rangle$ are basis vectors for the Hilbert space $\mathscr{H}_q$ and $d = \dim(\mathscr{H}_q)$. Furthermore it holds that

$$\langle\phi| \Lambda\Big(|\psi\rangle \langle\psi| \Big) |\phi\rangle = \langle\phi| \otimes \langle\psi^*| C_\Lambda |\phi\rangle \otimes |\psi^*\rangle \tag{2.37}$$

or equivalently

$$\mathrm{Tr}\Big(|\phi\rangle \langle\phi| \Lambda\Big(|\psi\rangle \langle\psi| \Big) \Big) = \mathrm{Tr}\Big(|\phi\rangle \otimes |\psi\rangle \langle\phi| \otimes \langle\psi| \cdot C_\Lambda \Big) \tag{2.38}$$

where $|\psi\rangle \in \mathscr{H}_q$, $|\phi\rangle \in \mathscr{H}_c \otimes \mathscr{H}_c$ and $|\psi^*\rangle$ is the complex conjugate of $|\psi\rangle$.

Once the matrix C_Λ is found its properties can be used to gain information about Λ itself. In particular, we want to ascertain that Λ is (1.) completely positive and (2.) trace preserving, i.e.

that Λ is a physical map. These requirements are met iff C_Λ is (1.) positive semi-definite and (2.) $\mathrm{Tr}_{\mathscr{H}_c \otimes \mathscr{H}_c}[C_\Lambda] = \mathbb{1}_{\mathscr{H}_q}$.

3 | Quantum-digital payments

After discussing the theoretical and experimental basics necessary we enter the one of the main parts of this thesis, namely our notion of 'quantum digital payments'. This protocol relies heavily on previous schemes of quantum money or tokenization (which will also be discussed briefly) but overcomes the constraints these previous schemes faced. Remarkably it does so while still exhibiting an important advantage compared to its classical counterpart, namely i.t.-security in the presence of potentially corrupted communication channels and malicious Clients.

3.1 Classical counterpart and state-of-the-art quantum schemes

In this section we will briefly discuss the notion of classical digital payments as well as previous quantum money schemes. Until now these schemes faced major technological challenges – either the need for reliable quantum memory or the introduction of rigorous space-time constraints – which made the practical implementation impossible with the current state of the art.

3.1.1 Classical digital payments

Any quantum scheme can only truly claim to be advantageous if it is compared to a classical counterpart. For our protocol this counterpart is the notion of '(classical) digital payments', which describes the process of securing any kind of financial transaction that is relying on digital means. For the sake of simplicity we will follow the descriptions given in [32, 31], although the actual implementation in real life may vary. Usually the User or Client sets up an account at a Trusted Token Provider (TTP), which might be their bank, credit card provider or another trusted company. During this account creation the Client shares their sensitive credit card information (if necessary) and is assigned a *Client token* (C), which functions as a secret and unique identification number. At a later point when the Client wants to make a transaction at a specific Merchant M they will receive a randomly generated *payment token* (P), which is usually dependent on M. With these two numbers their device creates a *cryptogram* $\kappa(C, P, M)$. In most cases this cryptogram is a hash function or some other computationally secure function. In this respect the procedure can be viewed as an implementation of *challenge-response*.

For simplicity the general protocol may be summarised in the following steps:

0. The Client sets up an account with the TTP and shares their sensitive (credit card) information with them. During this initial step the Client also receives a unique identification token C -

either via some encrypted and authenticated channel. This information is privately shared only between TTP and Client.

1. At a later point, when the Client wants to make a purchase, they receive another random *payment* token P, either from the TTP or directly from the Merchant. The Clients device now uses a predefined operation to create the cryptogram $\kappa(C, M, P)$. Here P may or may not be a function of M (if this is the case κ is only indirectly dependent on M).
2. The Client sends $\kappa(C, M, P)$ to the Merchant, who forwards it to the TTP.
3. The TTP ensures that $\kappa(C, M, P)$ is indeed compatible with the Client's secret ID C and the sent payment token P and the Merchant ID M. If this is not the case the protocol is aborted.

3.1.2 State-of-the-art quantum money schemes

Motivated by the no-cloning property of quantum mechanics, previous works have investigated the potentials and drawbacks of using quantum light in the prevention of banknote counterfeiting [24, 49, 50] and double-spending with tokens or credit cards [51, 52, 53, 54, 55]. The first version of such a quantum money scheme was introduced by Wiesner in the 1970s [24], where he proposed to store quantum states on banknotes to prevent counterfeiting. Put simply, the bank holds a secret classical description k of the quantum states stored on the banknote it is about to issue. Since the classical description tells the bank which states were encoded in which basis, they are able to check the authenticity of the banknote, whenever needed. Again, the no-cloning theorem ensures that it is impossible for a malicious party that does not hold a classical description of the quantum states, to determine the stored states and duplicate the banknote. Introducing this fundamentally new type of money to everyday scenarios is, however, technologically challenging: quantum states must be stored over days or months to ensure flexible spending. This is far beyond state-of-the-art quantum storage times, which range from a few microseconds to a few minutes [56, 57, 58].

Quantum money without memories

Another quantum money proposal, that admittedly circumvents the drawbacks of quantum storage, is based on bit commitment. While quantum bit commitment [25] as such is impossible to implement in the strict sense, its basic working principle is still key to the protocol in question. In bit commitment one party (Bob) commits himself to a certain bit. While he will eventually reveal this bit to the other party (Alice), he wants his decision to stay private for a certain amount of time. Meanwhile Alice wants to be sure, that Bob made his decision at a certain time t_0 and was unable to change his mind till the revelation of the bit at time t_r. In the simplest case Bob can decide between committing to bit 0 or bit 1.

The *quantum* bit commitment scheme to this protocol then proceeds as follows: Alice prepares a sequence of n BB84 states according to a secret key of length $2n$, distinctly describing the quantum states. She sends these states to Bob who receives them at time t_0 and measures the whole sequence of quantum states either in the H/V-basis (commitment to bit 0) or in the $+/-$-basis (commitment to bit 1). Afterwards he sends the classical outcomes of the measurements to Alice, such that she receives them at time t_r. Since Bob does not know which quantum states Alice sent (and is unable to clone them), his commitment is *binding*, i.e. he cannot change his mind after the measurement. Furthermore, it is *hidden*, since Alice can by definition not know what bit Bob committed to until she

receives the measurement outcomes. The tricky part is in ensuring the exact moment of commitment, i.e. force Bob to make his decision at t_0. This can only be achieved if each party is split into three individuals: the 'original' Alice and Bob each have two accomplices, that are placed at two locations, that are light like separated from the starting point. Now Bob has to send his measurement results to both of his accomplices who will then hand them over to Alice's partners. Afterwards these partners compare with Alice whether they got the same classical bit string at the correct moment t_r and which commitment this corresponds to. Notice, that in this scenario Bob cannot postpone his decision.

From a practical standpoint, this approach presents new drawbacks, as customers and online shoppers do not have the means to securely set up complex trust networks for everyday transactions. Furthermore, accurately monitoring the spatial and temporal coordinates of verifiers requires a trusted Global Positioning System (GPS), which opens the door to undesired spoofing-type attacks [59]. By relaxing the condition on the exact moment of commitment, however, it is possible to receive another useful scheme (also introduced in [26]), called *quantum bit coordination*. This protocol has, one crucial advantage, that makes it suitable for real world applications - there is no need for space-time constraints. This 'weaker' version of commitment is also used in our protocol.

3.2 Quantum protocol

As discussed in Subsection 3.1.2, conventional quantum money schemes suffer from rather strict constraints, which usually make their implementation with the current state of the art photonic devices impractical. We, however, propose a quantum digital payment protocol, which relies on both these principles while avoiding their restrictions.

The change we make compared to the classical version of digital payments is fairly simple. Instead of sending the payment token P in the form of a classical bit string, the TTP creates a sequence of quantum states $|P\rangle$ which are then measured by the Client in a specific basis, to ensure their commitment to the corresponding Merchant. This 'quantum' part of the protocol is fairly similar to quantum bit coordination, as described above. However, instead of using the coordinate or identification number of the Merchant, the Client has to measure $|P\rangle$ in a basis dictated by $\mathrm{MAC}(C, M)$, where MACis the function described in item 2.1.1. The precise reason for this is related to the concealment of the Client identification number, and will be explained in more detail in a later section. The results of this measurement constitutes now the cryptogram κ which depends now explicitly on C, M and P. This cryptogram is then again send first to the Merchant and subsequently to the TTP for verification. Formally the protocol can be summarized in the following steps (see also Figure 3.1):

0. The Client sets up an account with the TTP and shares their sensitive information. During this step the Client receives a unique identification token C via QKD or another i.t.-secure way.

1. When the Client decides where to make a purchase they request a payment token from the TTP, who randomly generates a classical description (β, b) and prepares the corresponding sequence $|P\rangle$ of quantum states, which is sent to the Client. Here β corresponds to a basis choice, either H/V or $+/-$, and b corresponds to the encoded classical bit – either 0 or 1.

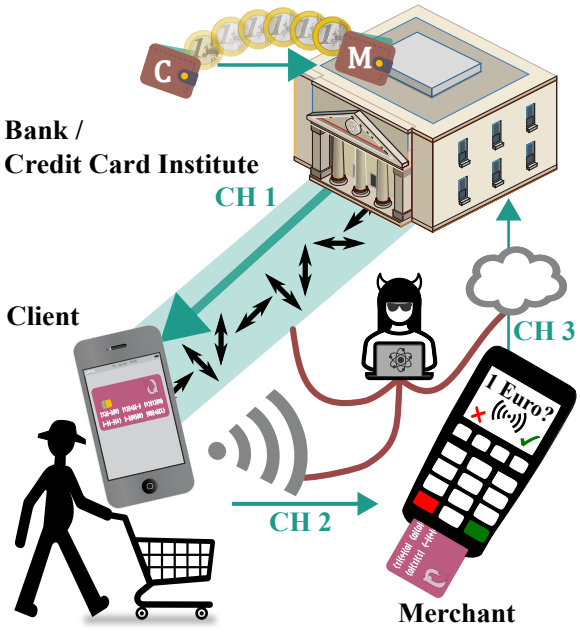


Figure 3.1: Simplified representation of quantum-digital payments. As in classical payments, we consider three parties: a Client, a Merchant and a Bank/TTP. In contrast to [26], we do not assume any quantum or classical communication channel to be trusted (i.e. CH 1, CH 2 and CH 3 are insecure), except an initial prior step between the Bank and Client for an account creation. The only trusted party is the Bank/TTP. During a payment, the Bank sends a set of quantum states to the Client, who measures them and transforms them into a quantum-secured *cryptogram*. The Client uses this cryptogram to pay at the Merchant, who then asks the Bank for payment verification. If the payment is accepted, the money is transferred from the Client's account to the Merchant's.

2. Upon receipt, the Client measures $|P\rangle$ in a sequence of bases dictated by $m_i = \mathrm{MAC}(C, M_i)$, where M_i is the identification number of the Merchant the Client wants to spend at. The results of this measurement $\kappa_i \xleftarrow{m_i} |P\rangle$ serve as the cryptogram for the ensuing transaction.

3. The Client sends κ_i to the Merchant, thereby making their choice M_i public, who forwards it to the TTP and asks for verification.

4. The TTP calculates $\mathrm{MAC}(C, M)$ and ensures that κ_i matches with the classical description (β, b) of the issued quantum token measured in m_i.

In this way we achieve two different levels of security, which will be discussed in detail in the next section: protection against interfering third parties, and protection against potentially malicious Clients and/or Merchants. Note especially that we achieve this level of protection under the assumption of *potentially untrusted communication channels* (see Figure 3.1). The only unconditionally trusted part of our scheme is the TTP or bank itself.

An important figure of merit regarding our scheme and its security is the length of the used quantum token, since we eventually we will have multiple quantum states measured in the same basis, to ensure protection against double spending. Note that as 'double spending' we define the attack where two *distinct but correct* cryptograms are generated from one quantum token $|P\rangle$. The entire length of the quantum token will be given by $\lambda = N \cdot ||m||$, where N is the sub-token length and $||m||$ denotes the bit-length of the MAC output.

3.3 Protection against potential attacks

In the following we will discuss the potential attacks our protocol protects against, and en passant explain which part of our scheme serves which precise purpose. Note that the following is only an intuitive explanation of security, while the next chapter will focus on the exact mathematical proof of these explanations.

Compromising classical channels
If we assume untrusted classical communication channels, we have to assume that it is possible for a malicious third party (Eve) to intercept the cryptogram κ at any point of its way from Client to TTP , with the goal of making purchases in the name of the Client. So Eve's goal is to either spend the intercepted κ in a wrongful way, or retrieve the Client's secret ID C. However, due to the quantum measurements κ is committed to one specific Merchant only and it is unfeasible for Eve to spend it at any other Merchant.
At the same time it is impossible for Eve to determine C since she does not know the classical description of the quantum token used, and is thus unable to even determine the measurement basis m_i in which it was measured.

Compromising the quantum channel
A significant advantage of our scheme is that it is preferable but *not necessary* to authenticate the quantum channel used to distribute $|P\rangle$. Suppose Eve intercepts the quantum states $|P\rangle$ from the TTP and sends their own quantum states $|P'\rangle$ to the Client instead.
After the Client measures these quantum states in the basis $MAC(C, M_i)$ they will hold the cryptogram $\kappa' = \kappa(C, M_i, |P'\rangle)$. If κ' reaches the TTP, the transaction will be declined since $\kappa(C, M_i, |P'\rangle) \neq \kappa(C, M_i, |P\rangle)$. This means, that the Client as well as the TTP will be able to detect that the quantum states have been tampered with and that precautions should be taken.
All the while Eve might try to use the quantum token herself and measure it in another basis than the Client had intended. However, we assume that she does not know C, since it was securely distibuted only between Client and TTP, and is thus unable to determine any measurement basis m_j that will be accepted at any Merchant with certainty.

Compromising both channels
Assume now the situation where Eve is again attacking the quantum channel, intercepts $|P\rangle$ and replaces it with another quantum token $|P\rangle$. The malicious party, however, could now also intercept the cryptogram and try to determine the secret Client token C. If the Client would measure $|P\rangle$ in a basis that is dependent on C in a simple way, e.g. $m_i = M_i \oplus C$, the malicious third party could easily determine C and use it in multiple ensuing transactions. This is why we us an MAC instead: Even if the malicious third party gets hold of κ' and, by knowing $|P'\rangle$, deduces the measurement

basis m_i, they are unable to retrieve C, because of the information theoretically secure nature of the used MAC (see Subsection 2.1.3), i.e. because the number of collision ensures that no cheating stategy would be better than guessing. Thus again, the TTP (and subsequently the Client) realise that something is wrong, while the secret Client token C remains hidden. Depending on the nature of the MAC the token C may resist a certain amount of failures, before it has to be exchanged. In this case C may also be used to encrypt the new client token C'.
This is a clear advantage compared to classical schemes, where a malicious third party could intercept multiple κs in succession and subsequently determine C by brute-forcing, while remaining undetected by the TTP and Client.

Malicious Clients
What a malicious Client (or third party) might do is try to double spend a single token at multiple Merchants. This is, however, forbidden by the Client having to choose which Merchant they want to spend at and the ensuing commitment.

Summary
We conclude with a quick summary of the protective properties of the quantum token and the MAC. While the quantum token mainly protects against double spending of the same token, it also acts as an alert system, that some malicious party is tampering with the payment scheme. The MAC, on the other hand, ensures that it is impossible for a third party to impersonate an honest Client.

3.4 Relation to other quantum primitives

Finally it is interesting to see how our scheme is related to and differs from other quantum primitives, such as QKD, previous quantum money schemes and digital signatures.

Contrary to QKD our scheme assumes only *one* trusted party – namely the TTP – while all other parties, like Clients and unknown third parties are allowed to behave maliciously. In such a scenario QKD is not sufficient, as it always assumes two parties unconditionally trusting each other. Nonetheless, QKD could be useful to establish the first initial step, namely the distribution of the secret Client token C. From a more technical perspective, our scheme differs from QKD as the choice of the measurement basis is neither random – but chosen according to a specific commitment – nor publicly revealed.

The main difference to other quantum money schemes is on one hand the fact that we do not rely on memories as the original scheme by Wiesner [24]. On the other hand, contrary to [26] we do not rely on tight space-time constraints, since we don't rely on such a high level of flexibility, nor the assumption of authenticated encrypted channels to protect against third parties, since our scheme intrinsically protects against any interfering from unauthorised parties.

Previous quantum digital signature schemes, [28, 29] could provide i.t.-security against the above mentioned attacks. However, they typically require QKD channels and classical authentication between all three parties, while our scheme only requires one authenticated channel at an arbitrary point in time.

4 | Security Proof

As mentioned above the security of our protocol is two-fold: While the quantum properties of the payment token $|P\rangle$ mainly protect against double spending, the information theoretically secure MAC conceals the measurement basis, i.e. protects against malicious third parties. Thus, we will also split the ensuing security proof in these two parts: First we will investigate in detail how the no-cloning property of quantum states ensures the impossibility of double spending, even in realistic (i.e. experimentally feasible) scenarios. Secondly, we will briefly demonstrate how the addition of an i.t.-secure MAC protects the payment from intervening malicious third parties.

4.1 Quantum states protecting against double spending

We stated above that our protocol protects against double spending a token with information theoretic security. This is, of course, only correct in the ideal case of no experimental shortcomings, like errors, losses or multiphoton emissions. Since the protocol should not abort for an honest but *imperfect* Client, the TTP is forced to allow for a certain amount of errors and/or losses according to the experimental deficiencies. This allowance, however, could also be exploited by a cheating Client or intercepting third party, that tries to *double spend*, i.e. use the quantum token to generate more than one committed token.
In the following section we will show that for our protocol collective attacks are the most efficient and derive a region in terms of allowed errors and losses in which the protocol still remains secure. This is done using the concept of semi-definite programming, which will be introduced shortly, to derive an optimal cheating strategy. In particular, we try to find a completely positive trace preserving (CPTP) 'cloning' map Λ which maps the quantum token onto two classical committed tokens with as little errors and losses as possible. To be secure even against an all-powerful cheating Client, we assume that they have a setup with perfect links and perfect detectors, i.e. they do not introduce any errors or losses by mistake, only deliberately.
Additionally we also extend this proof to the case of a large but finite number of quantum states, utilising the notion of Chernoff-Hoeffding bounds to define lower/upper bounds for honest and dishonest success probabilities respectively.

4.1.1 Collective versus coherent attacks

This section closely follows an argument stated in [60]. First we need to determine what kind of attack a malicious Client or third party would best resort to. Since the token consists of many quantum states the two main options are collective or coherent attacks. While coherent attacks make

use of all quantum states by making combined measurements and/or entangling them, collective attacks describe a strategy where the same attack is performed on each state individually.

As we see from the description of our protocol, the sequence of qubits used is random and it is possible to interchange any of the states, without changing the overall procedure. Therefore we can assume that the overall quantum token is *permutational invariant*, i.e. the exact order of the qubits does not matter. As we saw before, the quantum de Finetti theorem introduced in section 2.5.1, allows us to approximate the density matrix of our *token state* by a density matrix that has i.i.d. structure $\sigma^{\otimes k}$ in most subsystems. Consequently, the Client 'sees' a string of identical quantum states, namely the completely mixed polarisation state $\rho = \frac{1}{n}\mathbb{1}_n$, making coherent attacks ineffective. Thus we conclude that the most efficient attack a malicious party may use is of the *collective* type.

4.1.2 Security for $n = 1$ – Semi definite program

To outline the security proof we will first focus on the case of a single qubit, i.e. a quantum token of length 1. While this scenario is of course unsuited for any practical implementation, as it the Client would be able to just *guess* the correct value, it suffices to demonstrate the optimal cheating strategy and subsequent countermeasures. We will thus derive a cloning map $\Lambda(.)$ that a malicious Client may use to accomplish the highest cheating success probability.

4.1.3 Loss and error operators

In order to find the perfect cloning map, we need to first clarify how the TTP is able to determine losses and errors. This is done by defining loss and error operators. For this we utilise the linear cloning map Λ a malicious Client may use, and the corresponding Choi-operator C_Λ, as defined in eq. 2.36.

First we re-label our 4 different quantum states, living in the two-dimensional Hilbert space $\mathscr{H}_q$

$$\begin{aligned} |\psi_{00}\rangle &\equiv |H\rangle \\ |\psi_{01}\rangle &\equiv |V\rangle \\ |\psi_{10}\rangle &\equiv |+\rangle \\ |\psi_{11}\rangle &\equiv |-\rangle \end{aligned} \tag{4.1}$$

Note that the first digit in the subscript always refers to the basis ($0 = H/V$, $1 = +/-$) while the second digit refers to the encoded bit.

The classical outcomes of the measurements, which constitute the committed token are orhtogonal to each other and span the three-dimensional Hilbert space $\mathscr{H}_c$

$$\begin{aligned} |0\rangle &\ldots \text{ declare the classical outcome '0'} \\ |1\rangle &\ldots \text{ declare the classical outcome '1'} \\ |\oslash\rangle &\ldots \text{ declare 'the quantum state was lost' or 'flag'} \end{aligned} \tag{4.2}$$

Since we know which outcomes the TTP expects for which quantum states we can assign 'correct' $|a^c_{xx}\rangle$ and 'erroneous' $|a^\varepsilon_{xx}\rangle$ classical outcomes to any quantum state $|\psi_{xx}\rangle$

$$\begin{aligned} |\psi_{x0}\rangle : |a^c_{x0}\rangle = |0\rangle \,, |a^\varepsilon_{x0}\rangle = |1\rangle \\ |\psi_{x1}\rangle : |a^c_{x1}\rangle = |1\rangle \,, |a^\varepsilon_{x1}\rangle = |0\rangle \end{aligned} \tag{4.3}$$

As the quantum states the TTP sends to the Client are randomly chosen, any single quantum token state the Client receives can be expressed as:

$$\rho_{qt} = \frac{1}{4} \sum_{k,l=0}^{1} |\psi_{kl}\rangle \langle\psi_{kl}| = \frac{1}{2} \cdot \mathbb{1}_2 \tag{4.4}$$

i.e. what the Client 'sees' is a classical mixture of all four possible quantum states, also called *the completely mixed state*. As mentioned above, the fact that the Client never knows which quantum state he is receiving restricts the best cheating strategy.

The probability that the TTP detects a flag when it receives the committed token via Merchant M_0 is equal to the probability that the clients maps the received quantum state onto the state 'flag' in the corresponding Hilbert space:

$$p^l_0 = \mathrm{Tr}\Big[\Big(|\oslash\rangle\langle\oslash| \otimes \mathbb{1}_3\Big) \cdot \Lambda\Big(\rho_{qt}\Big)\Big] = \mathrm{Tr}[L_0 \cdot C_\Lambda] \tag{4.5}$$

Note that in the last step we made use of eq. 2.38 and defined the *loss operator*

$$L_0 = \frac{1}{4} \sum_{k,l=0}^{1} |\oslash\rangle\langle\oslash| \otimes \mathbb{1}_3 \otimes |\psi_{kl}\rangle\langle\psi_{kl}| = \frac{1}{2} |\oslash\rangle\langle\oslash| \otimes \mathbb{1}_3 \otimes \mathbb{1}_2 \tag{4.6}$$

Thus the TTP is able to discern a flag whenever the Client declares one. The probability of detecting a loss and the loss operator for a token, committed to M_1 are defined equivalently:

$$p^l_1 = \mathrm{Tr}\Big[\Big(\mathbb{1}_3 \otimes |\oslash\rangle\langle\oslash|\Big) \cdot \Lambda\Big(\rho_{qt}\Big)\Big] = \mathrm{Tr}[L_1 \cdot C_\Lambda] \tag{4.7}$$

$$L_1 = \frac{1}{2}\mathbb{1}_3 \otimes |\oslash\rangle\langle\oslash| \otimes \mathbb{1}_2 \tag{4.8}$$

where we simply switch the first and second Hilbert-space.

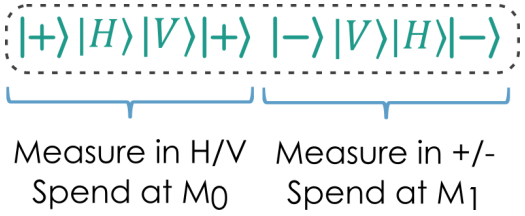
The probability that the TTP detects an error, when assuming a commitment to M_0 is then the probability that the Client maps the quantum state onto the wrong outcome in the corresponding Hilbert space:

$$p^\varepsilon_0 = \mathrm{Tr}\Big[\frac{1}{4} \sum_{k=0}^{1} \Big(|a^\varepsilon_{0k}\rangle\langle a^\varepsilon_{0k}| \otimes \mathbb{1}_3\Big) \cdot \Lambda\Big(|\psi_{0k}\rangle\langle\psi_{0k}|\Big)\Big] = \mathrm{Tr}[E_0 \cdot C_\Lambda] \tag{4.9}$$

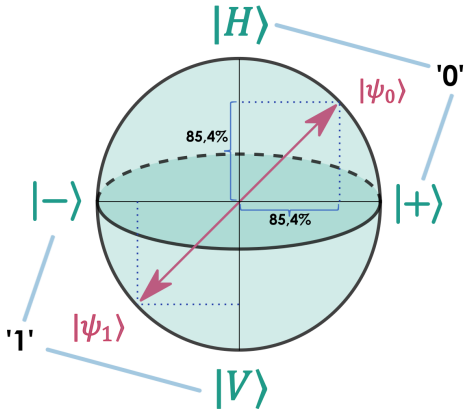
with the error operator

$$E_0 = \frac{1}{4} \sum_{k=0}^{1} |a^\varepsilon_{0k}\rangle\langle a^\varepsilon_{0k}| \otimes \mathbb{1}_3 \otimes |\psi_{0k}\rangle\langle\psi_{0k}| \tag{4.10}$$

This reflects the fact that the TTP is only able to detect errors that were introduced on quantum states encoded in the H/V basis and not in the $+/-$ basis, since they have to assume that the



(a) Zero errors The quantum token is split in two, and each part is measured in a different basis corresponding to one Merchant.



(b) Zero losses. Each state of the quantum token is measured in the basis $|\psi_0\rangle/|\psi_1\rangle$ and sent to both Merchants.

Figure 4.1: Optimal cheating strategies. A potential malicious Client may use a mixture of these two cheating strategies, in order to successfully spend the token at two Merchants.

quantum token was measured in this basis. Thus, if the errors are distributed evenly over the entire committed token, it can be assumed that the TTP is only capable of spotting half of the overall errors. Similarly, the probability of detecting an error when receiving the committed token via M_1 and the corresponding error operator are:

$$p_1^{\varepsilon} = \mathrm{Tr}\Big[\frac{1}{4}\sum_{k=0}^{1}\Big(\mathbb{1}_3 \otimes |a_{1k}^{\varepsilon}\rangle\langle a_{1k}^{\varepsilon}|\Big)\cdot\Lambda\Big(|\psi_{1k}\rangle\langle\psi_{1k}|\Big)\Big] = \mathrm{Tr}[E_1 \cdot C_\Lambda] \tag{4.11}$$

$$E_1 = \frac{1}{4}\sum_{k=0}^{1}\mathbb{1}_3 \otimes |a_{1k}^{\varepsilon}\rangle\langle a_{1k}^{\varepsilon}| \otimes |\psi_{1k}\rangle\langle\psi_{1k}| \tag{4.12}$$

4.1.4 Optimal cheating strategies

Instead of computationally solving the SDP (which would yield a Choi-matrix C_Λ, from which it may be hard to derive the optimal cheating strategy) we analytically solve the SDP by heuristically constructing the optimal cheating strategy. For simplicity we may first consider two extreme cases: (1) zero losses introduced, (2) zero errors introduced. Although these cases are not that important in practice (since the TTP will always allow a certain amount of errors as well as losses), they help to understand the optimal cheating behaviour of a malicious Client. Once the strategies for the two extreme cases are established, a generalisation to arbitrary cases is straightforward, as the cheating Client may simply perform a mixture of the two strategies.

Zero errors: The Client tries to generate two valid committed tokens from a single quantum token, without introducing a single error on either of them. The only way to deterministically introduce zero errors on a committed token, however, is to measure it in the correct corresponding basis. The Client would thus have to split the token in two parts and commit them separately to the two

different merchant, leading to minimum losses of 50% at each spending point.

Zero losses: If the malicious Client is not allowed to introduce any losses, they inevitably have to link all the states of the quantum states to the classical outcomes '0' and '1' one way or another. Their best choice would be to measure in a basis that is 'halfway between' the BB84 states, i.e. the basis $|\psi_0\rangle / |\psi_1\rangle$, where

$$|\psi_0\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|H\rangle + |+\rangle)$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|V\rangle - |-\rangle)$$

The probabilities for arriving at the correct outcomes using this measurement operator are given by:

$$\begin{aligned} p^{corr}_{0/H} &= |\langle\psi_0|H\rangle|^2 = \frac{2+\sqrt{2}}{4} = 0.85355... \\ p^{corr}_{0/+} &= |\langle\psi_0|+\rangle|^2 = \frac{2+\sqrt{2}}{4} = 0.85355... \\ p^{corr}_{1/V} &= |\langle\psi_1|V\rangle|^2 = \frac{2+\sqrt{2}}{4} = 0.85355... \\ p^{corr}_{1/-} &= |\langle\psi_1|-\rangle|^2 = \frac{2+\sqrt{2}}{4} = 0.85355... \end{aligned} \tag{4.13}$$

which corresponds to introducing $\sim 14.6\%$ errors on the overall committed token. The TTP, however, is only able to detect half of these errors with certainty, since they can only check for the states that were encoded in the basis, they have to assume the token was measured in (see also the definition of the error operators, eq. 4.10 and eq. 4.11). For example assume that the TTP receives the committed token via M_0, then they can only detect errors on those bits that were encoded in the H/V-basis. If the token is sufficiently large, this will be approximately half of the token.

Generalisation: In general the Client will use a combination of those two strategies – l % of the time they will declare a loss at either Merchant and measure the qubit in the measurement basis corresponding to the other merchant, and $(100 - 2l)$ % of the time they will measure the qubit in the basis $|\psi_0\rangle / |\psi_1\rangle$.

4.1.5 Primal SDP for minimising errors

We now mathematically define the cloning map from $\mathscr{H}_q$ to $\mathscr{H}_c \otimes \mathscr{H}_c$ corresponding to the cheating strategies defined above and prove that it is indeed the optimal one. This is related to the amount of losses the Client has to declare as well as the errors they will inevitably introduce on the two classical bit strings, i.e. the error and losses operators defined in Subsection 4.1.3.
We can formulate the corresponding SDP (see Subsection 2.5.2) either as a function of losses and try to minimise the errors or vice-versa. Since it is easier to define the cloning map as a function of losses we chose the former option. Note, however, that the two SDPs are equivalent and yield the

exact same outcome. The SDP is given by the following objective function and set of constraints:

$$\begin{aligned} &\inf \mathrm{Tr}[E_0 \cdot C_\Lambda] \\ &\text{s.t. } \mathrm{Tr}[E_0 \cdot C_\Lambda] \geq \mathrm{Tr}[E_1 \cdot C_\Lambda] \\ &\mathrm{Tr}[L_0 \cdot C_\Lambda] \leq l_0 \\ &\mathrm{Tr}[L_1 \cdot C_\Lambda] \leq l_1 \\ &C_\Lambda \geq 0 \\ &\mathrm{Tr}_{\mathscr{H}_c \otimes \mathscr{H}_c}[C_\Lambda] = \mathbb{1}_{\mathscr{H}_q} \end{aligned} \tag{4.14}$$

Here the objective is to minimise the propability of an error occurring in the bit string sent to the merchant M_0, while ensuring that the probability of an error occurring on the bit string sent to merchant M_1, should not exceed this value (first constraint). Furthermore the losses on the first and second bit string should not exceed the values l_0 or l_1 respectively. For symmetry, we will from now on assume $l_0 = l_1 = l$. The last two constraints ensure that C_Λ is a CPTP map.
In order to provide an analytical solution to this problem, we first have to study the action of the cloning map Λ on the states of our quantum token, which we can derive from the heuristic optimal cheating strategies above:

$$\begin{aligned} \Lambda\Big(|H\rangle\langle H|\Big) = &\overbrace{l\,|\oslash\rangle\langle\oslash| \otimes \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big)}^{\text{Flag at } M_0 \text{ and random outcome for } M_1} + \overbrace{l\,|0\rangle\langle 0| \otimes |\oslash\rangle\langle\oslash|}^{\text{Correct outcome for } M_0 \text{ and flag at } M_1} \\ &\underbrace{+\Big(1-2l\Big)\cdot\Big[\Big(\frac{2+\sqrt{2}}{4}\Big)|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{4+2\sqrt{2}}|1\rangle\langle 1| \otimes |1\rangle\langle 1|\Big]}_{\text{Measurement in} |\psi_0\rangle/|\psi_1\rangle \text{ , yields the right outcome with a probability of } \sim 85.4\%} \end{aligned} \tag{4.15}$$

and equivalently for the other parts of the density matrix ρ_{qt}:

$$\begin{aligned} \Lambda\Big(|V\rangle\langle V|\Big) =& l\,|\oslash\rangle\langle\oslash| \otimes \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big) + l\,|1\rangle\langle 1| \otimes |\oslash\rangle\langle\oslash| \\ &+ \Big(1-2l\Big)\cdot\Big[\Big(\frac{2+\sqrt{2}}{4}\Big)|1\rangle\langle 1| \otimes |1\rangle\langle 1| + \frac{1}{4+2\sqrt{2}}|0\rangle\langle 0| \otimes |0\rangle\langle 0|\Big] \\ \Lambda\Big(|+\rangle\langle +|\Big) =& l\frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big) \otimes |\oslash\rangle\langle\oslash| + l\,|\oslash\rangle\langle\oslash| \otimes |0\rangle\langle 0| \\ &+ \Big(1-2l\Big)\cdot\Big[\Big(\frac{2+\sqrt{2}}{4}\Big)|0\rangle\langle 0| \otimes |0\rangle\langle 0| + \frac{1}{4+2\sqrt{2}}|1\rangle\langle 1| \otimes |1\rangle\langle 1|\Big] \\ \Lambda\Big(|-\rangle\langle -|\Big) =& l\frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big) \otimes |\oslash\rangle\langle\oslash| + l\,|\oslash\rangle\langle\oslash| \otimes |1\rangle\langle 1| \\ &+ \Big(1-2l\Big)\cdot\Big[\Big(\frac{2+\sqrt{2}}{4}\Big)|1\rangle\langle 1| \otimes |1\rangle\langle 1| + \frac{1}{4+2\sqrt{2}}|0\rangle\langle 0| \otimes |0\rangle\langle 0|\Big] \end{aligned} \tag{4.16}$$

From this we can easily calculate the corresponding Choi-matrix (as introduced in Subsection 2.5.4) according to eq. 2.36:

$$\begin{aligned} C_\Lambda =& \Lambda\Big(|H\rangle\langle H|\Big) \otimes |H\rangle\langle H| + \Lambda\Big(|V\rangle\langle V|\Big) \otimes |V\rangle\langle V| \\ &+ \Big(\Lambda\Big(|+\rangle\langle +|\Big) - \Lambda\Big(|-\rangle\langle -|\Big)\Big) \otimes \Big(|H\rangle\langle V| + |V\rangle\langle H|\Big) \end{aligned} \tag{4.17}$$

where we used the fact that $|+\rangle\langle+| - |-\rangle\langle-| = |H\rangle\langle V| + |V\rangle\langle H|$ and that Λ is a linear map, i.e. $\Lambda(x+y) = \Lambda(x) + \Lambda(y)$. Furthermore note that we choose $\Lambda(|H\rangle\langle V|) = \Lambda(|V\rangle\langle H|)$.

This matrix satisfies all constraints, set by the SDP in eq. 4.14 and gives as analytical value of the objective function:

$$\mathrm{Tr}[E_0 \cdot C_\Lambda] = \frac{0.5}{4+2\sqrt{2}} - \frac{1}{4+2\sqrt{2}} \cdot l \equiv \varepsilon^d_{\mathrm{SDP}}(l) \tag{4.18}$$

In the last step we define the value of the objective as the amount of errors, that a dishonest party has to introduce in order to double spend, given a specific amount of declared losses. Note in particular that, since the last two constraints of the SDP are satisfied, the map defined above is fact completely positive and trace preserving, as required (see Subsection 2.5.4).

4.1.6 Dual SDP for minimising errors

In order to prove that that the solution found in the previous section is optimal, we also need to solve the corresponding dual SDP, which is given by the following objective function and constraint:

$$\begin{aligned} &\sup\ [\mathrm{Tr}[X_1] + l \cdot (x_2 + x_3)] \\ &\text{s.t. } [\mathbb{1}_9 \otimes X_1 + L_0^\dagger \cdot x_2 + L_1^\dagger \cdot x_3 + (E_1 - E_0)^\dagger \cdot x_4 - E_0^\dagger] \leq 0 \\ &\quad \text{where } X_1 \text{ is a hermitian } 2 \times 2 \text{ matrix} \\ &\quad x_2, x_3, x_4 \in \mathbb{R} \end{aligned} \tag{4.19}$$

Note that the error and loss operators are indeed hermitian, i.e. $L_x^\dagger = L_x$ and $E_x^\dagger = E_x$. Strong duality holds if we can find the same optimal value for the dual problem as for the primal problem. The easiest way is thus to assume that we can reach this value with the objective function and then show, that the constraint is satisfied. We therefore equate the objective of the dual SDP with the optimal value of the primal SDP:

$$\sup\ [\mathrm{Tr}[X_1] + l \cdot (x_2 + x_3)] = \frac{0.5}{4+2\sqrt{2}} - \frac{1}{4+2\sqrt{2}} \cdot l \tag{4.20}$$

From this we may presume the value of the ocurring variables:

$$\begin{aligned} X_1 &= \frac{0.25}{4+2\sqrt{2}} \cdot \mathbb{1}_2 \\ x_2 = x_3 &= -\frac{0.5}{4+2\sqrt{2}} \end{aligned} \tag{4.21}$$

We now choose $x_4 = -0.5$ (to symmetrize the constraint in respect to the error operators), which leads to

$$[\mathbb{1}_9 \otimes \frac{0.25}{4+2\sqrt{2}} \cdot \mathbb{1}_2 - \frac{0.5}{4+2\sqrt{2}} \cdot (L_0 + L_1) - 0.5 \cdot (E_1 + E_0)] \leq 0 \tag{4.22}$$

which can indeed be shown to hold. Thus our solution is tight, and the derived cloning map is optimal.

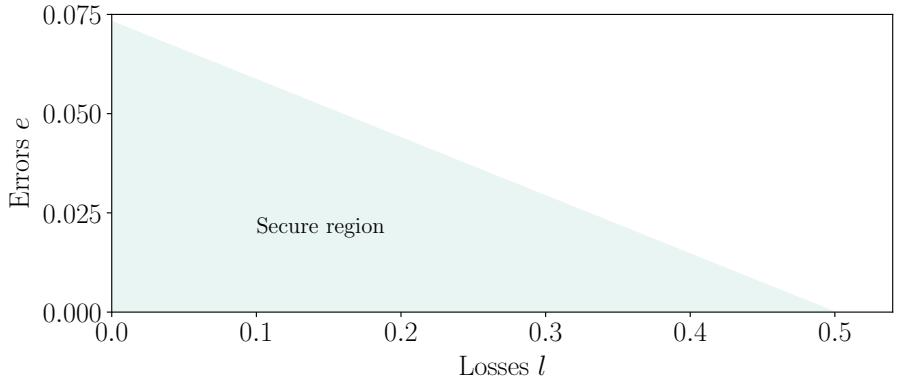


Figure 4.2: Secure region. The amount of errors and losses a TTP can allow without comprising the information theoretical security of the protocol.

4.1.7 Secure region

As shown above the optimal solution for minimising errors is given by

$$\varepsilon^d_{\mathrm{SDP}}(l) = -\frac{1}{4+2\sqrt{2}} \cdot l + \frac{1}{8+4\sqrt{2}} \tag{4.23}$$

which is a function of losses. Here we denote l^h as 'honest losses', since this would be the amount of losses the TTP has to expect from an honest Client and $\varepsilon^d_{\mathrm{SDP}}$ as 'dishonest errors', since they could have been introduced by a malicious Client. We can therefore easily determine how many errors a malicious Client has to introduce in order to comply to a certain constraint on losses and still double spend.
Equivalently, through simple inversion of this equation, we can determine the amount of losses needed for successful cheating given the amount of declared errors ε:

$$l^d_{\mathrm{SDP}}(\varepsilon) = -(4+2\sqrt{2}) \cdot \varepsilon + 0.5 \tag{4.24}$$

These two equations define the secure region, i.e. the region of losses and errors a TTP can allow, without compromising the information theoretical security of the protocol (see also Figure 4.2). For simplicity, we define a new parameter $\mathcal{M}(\varepsilon, l)$ which is a parameter for the overall amount of *mishaps* (i.e. any combination of errors and losses) a TTP might receive from a client. By upper bounding this function we can easily specify the secure region:

$$\mathcal{M}(\varepsilon, l) = (4+2\sqrt{2}) \cdot \varepsilon + l < 0.5 \tag{4.25}$$

4.1.8 Multiphoton emission

Besides the experimental imperfections at the side of the honest Client, we also have to account for imperfections at the TTP, i.e. the state preparation. While losses are negligible here, since the TTP only uses those quantum states for verification that were successfully prepared, i.e. detected on their side, multiphoton emission can be a serious threat to security. Assume for example that

the Client is able to perform a non-destructive photon number measurement and can subsequently separate the photons that were prepared in the same way. They could simply measure one of these photons in the H/V basis and the other one in the $+/-$ basis and subsequently introduce neither losses nor errors for this bit on both committed tokens (or all of them, if we assume more than two Merchants). In order to close this security loophole, the TTP needs to determine the probability of multiphoton emission of their source ($p_{>2}$) and assume that the Client can cheat perfectly for half of this percentage of photons. The reason for this is that on average only half of the photons that are being emitted simultaneously from the SPDC source will be prepared in the same way by the TTP, since the choice of measurement basis is made randomly with a BS and the photons do not necessarily leave it through the same output port.
Since the photon states produced by SPDC sources do not exhibit coherence in the number basis, the probability of multiphoton emissions can easily be incorporated in the SDP solutions:

$$\begin{aligned} l^d_{\mathrm{SDP}}(\varepsilon) &= \Big[-(4+2\sqrt{2}) \cdot \frac{\varepsilon}{1-\frac{p_{\geq 2}}{2}} + 0.5 \Big] \cdot (1 - \frac{p_{>2}}{2}) = -(4+2\sqrt{2}) \cdot \varepsilon + 0.5 \cdot (1 - \frac{p_{>2}}{2}) \\ \varepsilon^d_{\mathrm{SDP}}(l) &= -\frac{1}{4+2\sqrt{2}} \cdot l + \frac{1-\frac{p_{\geq 2}}{2}}{8+4\sqrt{2}} \end{aligned} \tag{4.26}$$

Note that here the cheating client exploits the photon-number measurement and subsequent state discrimination to decrease the amount of losses as well as errors.

Accordingly the constraint on mishaps gets slightly more tight:

$$\mathcal{M}(\varepsilon, l) = (4+2\sqrt{2}) \cdot \varepsilon + l < 0.5 \cdot (1 - \frac{p_{>2}}{2}) \tag{4.27}$$

4.1.9 Security for n finite – Chernoff-Hoeffding bounds

Correctness of the protocol

While the TTP allows for a certain amount of losses and errors, in order for the protocol to work in a realistic, i.e. imperfect scenario, there is still some probability, that the honest client actually introduces more than the allowed number of errors and/or losses. Since this would lead to an 'honest abort' or failure of the protocol, we denote this probability as p^h_{fail}. It is possible to derive a corresponding Chernoff bound in terms of the overall mishaps $\mathcal{M}(\varepsilon, l)$:

$$p^h_{\mathrm{fail}}(n) = P[\mathcal{M}(\varepsilon^h_{\mathrm{act}}, l_{\mathrm{act}}) \geq \mathcal{M}(\varepsilon^h, l^h) \cdot (1+\delta^h)] \leq e^{-\frac{(\delta^h)^2}{3} \cdot \mathcal{M}(\varepsilon^h, l^h) \cdot n} \tag{4.28}$$

that is the probability that the protocol aborts, if the TTP allows for mishaps that deviate by more than δ^h from the expected value $\mathcal{M}(\varepsilon^h, l^h)$.

The correctness c^h or honest success probability p_h of the protocol is then defined as the probability that the protocol does *not* abort, if the client is honest. Therefore it can be expressed as:

$$c^h(n) = p_h(n) = 1 - p^h_{\mathrm{fail}}(n) \geq 1 - e^{-\frac{(\delta^h)^2}{3} \cdot \mathcal{M}(\varepsilon^h, l^h) \cdot n} \tag{4.29}$$

As is apparent, the correctness would increase exponentially with δ. However, since the TTP has to allow for more errors and losses with increasing δ^h, it is more vulnerable to potentially cheating clients. Thus we need to ensure that

$$\mathcal{M}(\varepsilon^h, l^h) \cdot (1 + \delta^h) \leq 0.5 \cdot (1 - \frac{p_{>2}}{2}) \tag{4.30}$$

This inequality subsequently upper bounds the permissible value of δ^h without jeopardizing the information theoretical security of the protocol.

Cheating probability

In real world scenarios it might be possible for a cheating client to introduce less errors and losses than theoretically needed to double spend, i.e. they could double spend, while not violating the constraints set by the TTP. However, it is possible to derive an upper bound for this successful double spending probability using the Chernoff inequalities:

$$p_d(n) = P[\mathcal{M}(\varepsilon^d_{\text{act}}, l^d_{\text{act}}) \leq 0.5 \cdot (1 - \frac{p_{>2}}{2}) \cdot (1 - \delta^d)] \leq e^{-\frac{(\delta^d)^2}{2} \cdot 0.5 \cdot (1 - \frac{p_{>2}}{2}) \cdot n} \tag{4.31}$$

i.e. the probability that the combination of errors and losses *actually* introduced by the malicious client ($\mathcal{M}(\varepsilon^d_{\text{act}}, l^d_{\text{act}})$) are smaller than what the TTP would expect for successful cheating. However in order for this not to clash with the constraint we set for the correctness, we have to consider:

$$0.5 \cdot (1 - \frac{p_{>2}}{2}) \cdot (1 - \delta^d) \geq \mathcal{M}(\varepsilon^h, l^h) \cdot (1 + \delta^h) \tag{4.32}$$

Since this is the amount of mishaps the TTP allows for in order to assure the correctness of the protocol.

4.2 Classical security of the MAC concealing the Client ID

While the security against double spending is solely guaranteed by the laws of quantum mechanics, the protection against malicious third parties is achieved by a combination of this quantum commitment and classical security. To be precise the information theoretical security of the used MAC, since, as described above, this guarantees that a malicious third party is not capable of determining C even if they corrupt all communication channels, including the quantum one. As mentioned above, the malicious third party could intercept the quantum states from the TTP, discard them and send their own states to the Client. After the Client did their measurements and send the corresponding cryptogram to the Merchant of their choice, said third party may also intercept the cryptogram. Now, since they know the quantum states they received from the Client and the measurement outcomes they are able to determine the measurement basis which will correspond to $\text{MAC}(C, M)$.

The probability that Eve is capable of extracting C from this is given by eq. 2.1 and is thus strongly dependent on the actual length of the message (i.e. the public Merchant ID) and the key (given by the secret Client ID). For our protocol it would make sense to choose the cheating probability p_t of Eve to have the same value as that of a cheating Client that tries to double spend p_d. Thus we choose the size of the key space such that:

$$\frac{1}{\sqrt{|C|}} = p_t = p_d \tag{4.33}$$

4.3 Summary

As previously mentioned, our protocol is designed to withstand corrupted communication channels – classical as well as quantum. In this section we provided a concise proof of this claim, especially with respect to experimental imperfections such as losses or errors. We find that the protocol remains secure for certain amounts of experimental *mishaps* $\mathcal{M}(e^h, l^h)$, restricted by the multiphoton emission of the used source and the length N of the sub-token. Thus the cheating probability for double spending is intrinsically determined by experimental parameters. On the other hand the cheating probability for dishonestly retrieving C is dependent only on the length of C and M and can thus be easily adjusted by increasing the length λ of the entire token until the desired security level is achieved. Eventually in the actual implementation of our protocol there will be a trade-of between speed (i.e. sub- and total token length) and security.

5 | Experimental demonstration of the protocol security

This chapter focuses on the experimental proof of principle implementation of our protocol and the subsequent security proof using the acquired data. It is important to note that the experimental implementation is mainly used to demonstrate that it is possible to securely execute our protocol with current sources and devices. Thus the interesting experimental results are the losses of certain setup parts, the errors introduced when executing the protocol honestly as well as the multiphoton emission of the source.

5.1 Source

For the creation of the entangled photon pairs we use the collinear double-downconversion (CDDC) source, introduced in [61]. Thus the ensuing description will closely follow this publication. Contrary to conventional SPDC-sources (see Subsection 2.4.2) the photons created in this source, all exit the crystal in the same spatial mode in the direction of the pump beam. Furthermore the two photons of an entangled pair do not necessarily have the same but different wavelengths. This is achieved with quasi phase matching (QPM) in a periodically poled potassium titanyl phosphate (ppKTP) crystal.

In a normal, i.e. unpoled, KTP crystal the pump, signal and idler field would interfere destructively, due to a non-zero momentum difference vector

$$\Delta k = k_p - k_s - k_i = \frac{2\pi n_p}{\lambda_p} - \frac{2\pi n_s}{\lambda_s} - \frac{2\pi n_i}{\lambda_i} \tag{5.1}$$

where the underscores p, s and i mark the pump, signal and idler photons/fields respectively and n refers to the refractive indices.
Now, by poling the crystal in a periodical way, and thus alternating d_{eff}, it is possible to avoid the above mentioned destructive interference, leading to a positive energy transfer from the pump field to the signal and idler fields. This ferro-magnetical poling of the crystal happens in such a way that the nonlinearity coefficient d_{eff} changes from negative to positive values in multiples of the length of the poling periodicity Λ.

The downconversion amplitude inside a crystal of length L – assuming that pump, signal and

idler photon propagate along the same axis – is then given by:

$$|\psi\rangle = NL \int_0^\infty \int_0^\infty d_{\text{eff}}(\lambda_s, \lambda_i)\mu(\lambda_p)\psi(\lambda_s, \lambda_i)a_s^\dagger(\lambda_s)a_i^\dagger(\lambda_i)\ d\lambda_s d\lambda_i\,|0\rangle \tag{5.2}$$

Here N is some normalisation constant, $a_{s/i}^\dagger$ are the creation operators of signal and idler photons respectively. Furthermore,

$$\mu(\lambda_p) = \exp\left(\frac{-(\lambda_p - \lambda_{p0})^2}{2\sigma^2}\right) \tag{5.3}$$

is the pump envelope amplitude with $\lambda_p = (\frac{1}{\lambda_S} + \frac{1}{\lambda_i})^{-1}$ and λ_{p0} being the main pump wavelength and the quasi-phase matching amplitude ψ is defined as

$$\begin{aligned} \psi(\lambda_s, \lambda_i) &= e^{i\Delta k_m \frac{L}{2}} \text{sinc}(\frac{\Delta k_m}{2}) \\ \text{where } \Delta k_m &= \Delta k - \frac{2\pi m}{\Lambda} \end{aligned} \tag{5.4}$$

where Δk_m is the so-called phase-mismatch vector and m refers to the QPM order – a positive or negative *odd* integer.

Now, quasi phase matching is achieved when $\psi(\lambda,\lambda_i)$ is maximised, i.e. when

$$\Lambda = m\frac{2\pi}{\Delta k} \tag{5.5}$$

Since the momentum difference vector Δk can be both positive and negative, m also takes on positive or negative values, in order to ensure that Λ remains positive. This furthermore implies that the QPM amplitude reads:

$$\psi(\lambda_s, \lambda_i) = e^{i\Delta k_{m_+} \cdot \frac{L}{2}} \text{sinc}(\frac{\Delta k_{m_+}}{2}) + e^{i\Delta k_{m_-} \cdot \frac{L}{2}} \text{sinc}(\frac{\Delta k_{m_-}}{2}) = \psi_+(\lambda_s, \lambda_i) + \psi_-(\lambda_s, \lambda_i) \tag{5.6}$$

Accordingly the downconversion amplitude can be rewritten as

$$\begin{aligned} |\psi\rangle &= NL \int_0^\infty \int_0^\infty d_{\text{eff}}\ \mu\ \psi_+ a_s^\dagger a_i^\dagger\ d\lambda_s d\lambda_i\,|0\rangle + NL \int_0^\infty \int_0^\infty d_{\text{eff}}\ \mu\ \psi_- a_s^\dagger a_i^\dagger\ d\lambda_s d\lambda_i\,|0\rangle \\ &= \alpha\,|\psi_+\rangle + \beta\,|\psi_-\rangle \end{aligned} \tag{5.7}$$

While in most configurations only one of these two terms will lead to an output, there are specific experimental setups, where both processes will contribute to the downconversion amplitude. In a source such as ours it is in fact possible to phase-match two different SPDC processes that have the same Δk but with different signs. Notably, these processes can have distinct wavelength pairs. This is called collinear double-downconversion (CDDC).

The probability of a specific signal an idler wavelength pair being emitted is given by the joint spectral intensity (JSI), which is itself the square of the product of the phase-matching and pump envelope amplitudes:

$$\text{JSI} = |\mu(\lambda_p)\psi(\lambda_s, \lambda_i)|^2 \tag{5.8}$$

If the used crystal allows for phase matching with both positive and negative Δk the setup will allow for two JSI's corresponding to photons with four different wavelengths: one process with JSI_+ corresponding to the wavelengths λ_{s_+} and λ_{i_+} and one process with JSI_- and wavelengths λ_{s_-} and λ_{s_-} respectively. Now without loss of generality assume that the signal photons are horizontally polarised and idler photons are vertically polarised. Choosing the right parameters and configurations it is possible to make the center wavelength of one of these processes match the center wavelengths of the polarisation counterparts of the other process, i.e.:

$$\begin{aligned} \lambda_{H+} &= \lambda_{V-} \\ \lambda_{V+} &= \lambda_{H-} \end{aligned} \tag{5.9}$$

As the two wavelength of the two processes can no longer be told apart this leads to entanglement as it is no longer apparent from which process the photon originates. In fact the produced state can be written as:

$$|\psi\rangle = \alpha\,|HV\rangle \otimes |SL\rangle + \beta\,|HV\rangle \otimes |LS\rangle \tag{5.10}$$

where we denote by S the short wavelength and by L the long wavelength respectively. This state can now be reduced to be either wavelength entangled, or (as is used for our experiment) polarisation entangled, i.e. :

$$|\psi\rangle = (\alpha\,|H_1V_2\rangle + \beta\,|V_1H_2\rangle) \otimes |SL\rangle \tag{5.11}$$

In practice polarisation entanglement is achieved by making the photons pass through a dichroic mirror, that separates the two wavelengths into two different spatial modes (where the short wavelength photon is assumed to be in spatial mode 1 and the long wavelength photon in spatial mode 2). Our setup is configured such that the produced photons are polarisation entangled in the $|\psi^-\rangle$ state, i.e.:

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \otimes |SL\rangle \tag{5.12}$$

5.2 Setup

A simplified sketch of our setup is depicted in Figure 5.1. A pump beam with a wavelength of 515 nm impinges on the 20 mm long ppKTP crystal after traversing through a lens and a polariser. This pump beam can be rapidly turned on and off by a remotely controlled shutter placed in front of the polariser (not shown). The polariser ensures that the laser light reaching the crystal is vertically polarised, which is necessary for the correct downconversion process. The entangled photon pairs leaving the ppKTP pass through a pump filter, that ensures that no large quantities of laser light pollute the ensuing setup. The second KTP crystal is unpoled and used for walkoff compensation. Note that both crystals are placed in separate ovens, which are used to adjust the length of the crystals by altering their temperatures. In order to transition from wavelength to spatial modes the entangled photons pass a dichroic mirror, which reflects the 785 nm photons while transmitting the 1500 nm photons.
From there on the short wavelength photons pass through a lens and a quarter wave plate, which allows additional control of the relative phase between the two photons, to prepare the singlet state $|\psi^-\rangle$. Before being coupled into the passive state preparation device, they pass another filter, which ensures that only the photons with the desired wavelengths pass (i.e. no pump or stray light). The passive state preparation device itself consists of one conventional 50/50 beamsplitter, followed by

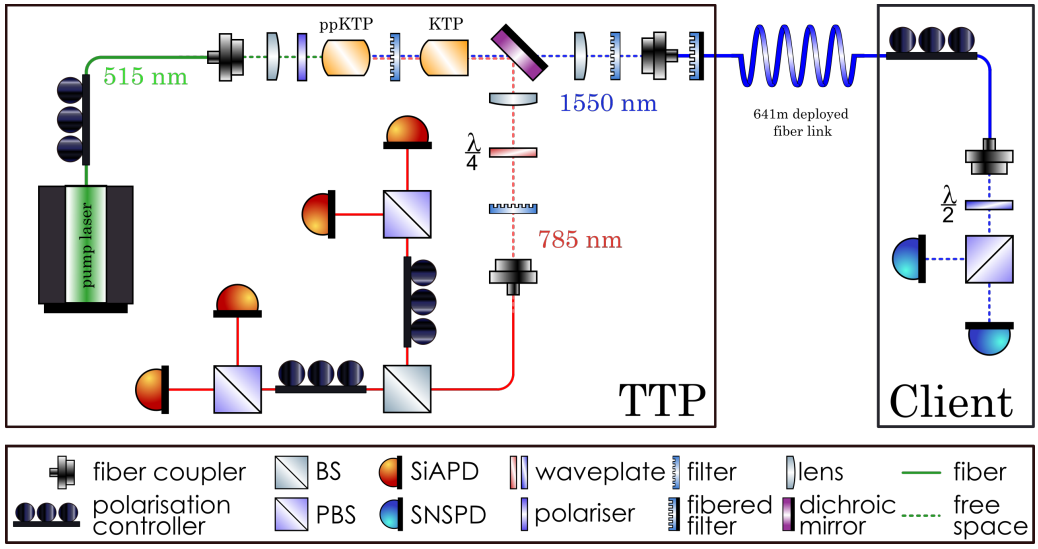


Figure 5.1: Setup for the quantum token transmission: For simplicity this figure only contains the optical elements necessary for transmitting and measuring the quantum token $|P\rangle$, but no purely classical agents, postprocessing etc.

two polarisation controllers and PBSs. The photons subsequently get projected either into the H/V or +/- basis, effectively preparing the other photon in the state orthogonal to the one measured. For detecting photons in this wavelength we used silicon avalanche photodiodes (SiAPD's).
Before the long wave photons travers through the fibre link connecting the two buildings, the pass a tunable fibred narrow band-pass filter. This filter is necessary to avoid spectral distinguishability of the photons created by the QPM source (see Section 5.1). Once the photons reach the other building and passed another polarisation controller, they couple out of the fibre into a free space setup for the measurement. The photons pass a HWP before impinging again on a polarising BS, followed by two detectors. Depending on the angle of the HWP the photons are all either measured in the H/V or the +/- basis using superconducting nanowire single-photon detectors (SNSPD's). Here all photon detectors located in the same building are connected to the same time tagger and subsequent computer. The two computers in the different buildings are connected via ethernet to one another, which is important for the actual execution of the protocol (see Subsection 5.3.2).

A more generic version of the setup (along with a depiction of the link connecting the two buildings) is shown in Figure 5.2. Here we opted to include a fictitious third party – the Merchant – which as such does not exist in our experiment. However the only task of this merchant is to forward the measurement results along with their own identification number.

5.3 Proceeding

In this section we describe the preparation steps of the experiment, its actual execution along with other technicalities, like necessary post-processing, etc.

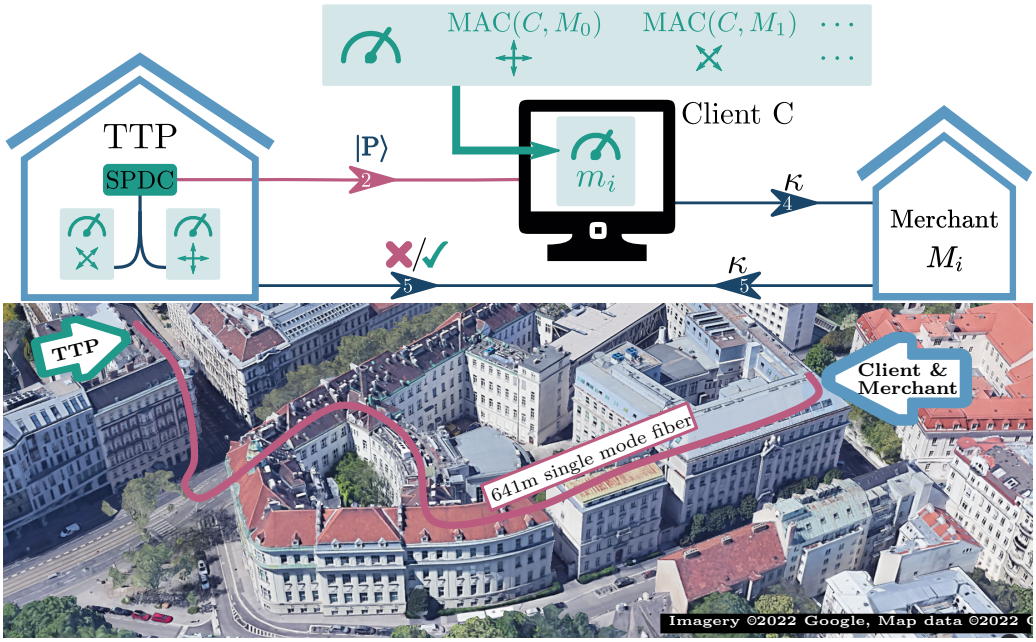


Figure 5.2: Experimental demonstration. a) The Trusted Token Provider (TTP) creates entangled photon pairs using a Spontaneous Parametric Down Conversion (SPDC) source. One photon's polarization is randomly measured by the TTP in either the linear or diagonal basis, creating the classical description $(b, \mathcal{B})$, which remotely prepares the quantum token $|P\rangle$ on the second photon. The latter is sent to the Client through a 641m long optical fiber link, who measures its polarization in a basis $m_i = MAC(C, M_i)$ specified by a Message Authentication Code (MAC) of the Merchant's ID M_i and the Client's private token C, and thereby obtains the *cryptogram* that is $\kappa_i \xleftarrow{m_i} |P\rangle$. Classical communication between the TTP, Client and Merchant is used to verify the compatibility of κ, M_i and C with $(b, \mathcal{B})$. Red (blue) lines indicate quantum (classical) channels. **b)** Satellite image of the two buildings housing the TTP, Client and Merchant. A 641 m optical fiber link connects the parties.

5.3.1 State preparation

Before the start of the experiment, it is of the essence to check and readjust the polarisation controllers (and thereby the measurement apparatuses) in both setup parts. For this we use additional pre-callibrated and automatised polarises, which can be slid into the setup (between the last free-space filter and coupler for both the TTP and Client respectively). These polarisers are set to specific angle (e.g. H polarisation) and used to rotate the polarisation controllers until the detections in the H detector are maximised (meaning the counts in the V detector are minimised). Ideally the number of the detection events in the + and - detector are approximately evened out. After this is achieved the polariser is rotated to another setting, e.g. + and the procedure is repeated. In the end the measurement setup of the TTP is ready to use. The polarisation controller on the Client's side is prepared in a similar fashion: the polariser is inserted into the photons path, set to a certain polarisation (e.g. H) and then the Clients polarisation controller is set such that the counts in the H detector are maximised (here the HWP is set to 0°). The same is done with the + and - polarisations, with the HWP set to 22.5°.

5.3.2 Execution of the experiment

Each run of the experiment was automatised to simplify the postprocessing. This procedure (along with the post-processing) was heavily inspired and based on the work of Marie-Christine Röhsner, described in her PhD thesis [62]. Each run takes 30 seconds in total, the beginning is marked by the shutter being opened for a very short amount of time, closed and then opened again, for the actual data acquisition. This initial short opening period is necessary to simplify the postprocessing (see Subsection 5.3.3). During these 30 seconds the clicks of all four TTP detectors along with their time bins are recorded on the corresponding computer, while the same happens in the other building for the Client's detection events. Once the 30 seconds are over the shutter closes again and the computers stop recording the detection events. During these measurements the wave-plate on the Client's side stays fixed either at 0° or 45° such that all states are measured in the H/V or +/- basis respectively. This is repeated multiple times to gather necessary statistics on bit flip errors.

5.3.3 Postprocessing and evaluation of the measurement data

One of the biggest challenges of having a spatially distant Client, is finding the coincidences of detections between two different TTMs. Since a nearly identical experimental setup was used by Marie-Christine Roehsner in her PhD thesis [62], we were able to use most of the code written and used by her to also conduct our experiment. Since this code is explained in detail in Roehsners work, we will only give a genera description. Using the initial seconds of signal before the actual measurement it is possible to find the rough offset between the two modules, by determining the point in time for which the signal starts at both measurement setups. Using this initial offset the two strings of actual data are shifted with respect to one another to a point at which the program finds the most coincidences between the two TTMs. Another problem is that the two internal clocks of the two TTMs may have a different drift with respect to one another. This drift, if not taken into account, can lead to coincidences decreasing over time, since the initially determined offset is no longer correct for all data points. In order to counteract this effect the program recalculates the exact offset multiple times within the 30 seconds of data.

The success probability of receiving the correct measurement outcome, when measuring in the correct basis is given by:

$$p_{corr.}^{n/m} = \frac{1}{2}\frac{N_{nm}}{N_{nn}+N_{nm}} + \frac{1}{2}\frac{N_{mn}}{N_{mm}+N_{mn}} \tag{5.13}$$

where n and m are the orthogonal states of a basis, i.e. either H/V or $+/-$, and N_{nm} refers to the number of photon pairs triggering the measurement outcome n on Alice's side and m on Bob's side. The factors $\frac{1}{2}$ are used to average over the two possible detection events for each basis.

5.4 Results: honest losses, errors and multiphoton emission

The main goal of the experiment is to show that it is possible to implement our protocol with i.t.-security. This means we need to characterise all honest errors and losses, as well as the multiphoton emission, which could be used to undermine the security of the protocol.

Table 5.1: Transmission and corresponding losses of the experimental setup. The uncertainties of these values stem from the uncertainties of the used power meter (for fibre link and Client setup), the Poisson distribution of detection events (for Detector 1 and 2) and subsequent Gaussian error propagation.

Setup part	Transmission	Losses
Fibre link	93.4 (± 1.5) %	6.9 (± 1.5) %
Client setup	89.82 (± 0.57) %	10.18 (± 0.57) %
Detector 1	93.34 (± 0.75) %	6.66 (± 0.75) %
Detector 2	92.51 (± 0.78) %	7.49 (± 0.78) %
Overall	77.6 (± 1.5) %	22.4 (± 1.5) %

5.4.1 Losses

First, we determine the amount of losses that a Client will declare, due to experimental imperfections, if they obeyed the protocol honestly. These losses can be introduced in three different parts of the setup:

1. the fibre link leading from the TTP to the Client, i.e. from one building to the other
2. the free space measurement setup of the Client
3. the efficiencies of the two detectors used by the Client

Note that we only take those losses into account that are introduced after the photons leave the laboratory of the TTP, since those are the losses a perfect cheating client (or malicious third party) might be able to circumvent. Losses that are introduced in the laboratory of the TTP, on the other hand, cannot be exploited, since these photons will not be used for the validation at the end.

We measured the transmission/efficiency of all the relevant setup parts (see Table 5.1) and subsequently determined the corresponding overall 'honest' losses to be:

$$l^h = 22.4\ (\pm\ 1.5)\ \% \tag{5.14}$$

5.4.2 Errors

By postprocessing the obtained data (see Subsection 5.3.3), we determine the overall bit-flip errors of the honest Client to be

$$\begin{aligned} \varepsilon_{H/V} &= 1.4491\ (\pm\ 0.0083)\ \% \\ \varepsilon_{+/-} &= 3.278\ (\pm\ 0.013)\ \% \end{aligned} \tag{5.15}$$

in the computational and diagonal basis respectively. Note that the errors in the diagonal basis are considerably higher than in the computational basis. This is mainly due to the fact that our source was optimised in the computational basis. While it is in principle possible to calibrate the

source such that both bases exhibit the same amount of errors, we found this calibration to be disadvantageous, i.e. the overall error rate would have been higher.

To err on the side of caution we will henceforth assume that the Client always introduces the higher amount of errors, no matter which basis they actually measure in, i.e. we will always use the higher value for all calculations regarding the security proof.

5.4.3 Mutliphoton emission

To quantify the multiphoton emission of the source we measure its heralded second order correlation function $g_h^{(2)}$. This is done by sending the 785 nm photons through a fibred beamsplitter and connecting the output ports to the two detecors D_1 and D_2. The telecom photons are measured by D_i, the *idler* detector. By measuring the three-fold coincidences between the 1550 photons and the two BS output ports as a function of delay it is possible to determine the number of multiphoton emissions. If the delay is zero three-fold coincidences can only happen if two SPDC photon pairs were created simultaneously, i.e. if multiphoton emission occurs. We define the second order correlation function by

$$g_h^{(2)}(\tau) = \frac{N_i \cdot N_{i12}(\tau)}{N_{i1}(0) \cdot N_{i2}(\tau)}, \tag{5.16}$$

where N_i is the total number of events detected in the telecom detector during the measurement integration time; $N_{i1}(0)$ are the 2-fold coincidence events between the D_i and D_1 at 0 delay; $N_{i2}(\tau)$ are the 2-fold coincidence events between the D_i and D2 at delay τ; and $N_{i12}(\tau)$ are the 3-fold coincidences between all 3 detectors with a delay $\tau = 0$ between the D_i and D_1, and delay τ between D_i and D_2. A plot of this function using different coincidence windows is shown in figure Figure 5.3. In our experiment we used a coincidence window of ≈ 3 ns corresponding to a zero delay value of:

$$g_h^{(2)}(0) = 0.03010 \ (\pm\ 0.00014) \tag{5.17}$$

Following an argument from [63], the multiphoton emission probability p_m can be approximated by

$$p_m = p_{n>1} = \sum_{n=2}^{\inf} p_n \leq \frac{1}{2} \sum_{n=0}^{\infty} n(n-1) \cdot p_n = \frac{1}{2} \mu^2 g_h^{(2)}(0) \tag{5.18}$$

where μ is the mean photon number per pulse $\mu = p_1 + 2p_2 + 3p_3 + \ldots$. We now assume that $p_1 \gg p_2 \gg p_3 \gg \ldots$, which in most cases holds true for SPDC sources and that $p_1 \approx 1$, as the measured correlation function is heralded. This leads to

$$p_m \approx \frac{1}{2} \cdot g_h^{(2)}(0) = 1.5051 \ (\pm\ 0.0070)\ \% \tag{5.19}$$

As explained in the discussion of the security proof (see Subsection 4.1.8), the figure of merit in our experiment is only half of the multiphoton emission p_m, since only half the photons created simultaneously get prepared in the same way. This is due to the process being probabilistic (induced by a 50/50 BS) so on average only half the photons emitted simultaneously will be prepared in the same way.

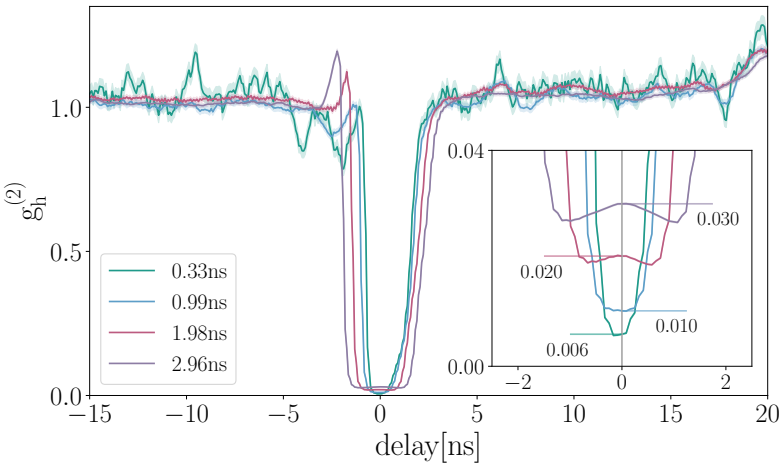


Figure 5.3: Heralded second order correlation function. We determine the second order correlation function for multiple different coincidence windows (0.33, 0.99, 1.98 and 2.96 ns). As can be seen the value of $g_h^{(2)}(0)$ increases considerably with the size of the coincidence window. For the run of our experiment we choose the largest of these coincidence windows, corresponding to $g_h^{(2)}(0) = 0.03010(\pm 0.00014)$.

5.5 Security

The main goal of our experimental results (displayed in Table 5.2) are used to demonstrate the security of our protocol in the presence of experimental imperfections. To do so we first calculate the experimental mishaps $\mathcal{M}(e, l)$ by plugging the obtained values of errors, losses into the left hand of eq. 4.27, while the bound of the secure region is determined by plugging the measured multiphoton emission into the right hand of equation eq. 4.27. As can be seen in Figure 5.4a our experimental values lie within this secure region. In order to determine the successfull double spending probability p_d and honest success probability p_h as functions of the sub-token length N we insert this value of mishaps into equations eq. 4.31 and eq. 4.29 respectively. As can be seen in Figure 5.4b p_d decreases exponentially with N while p_h increases. Since the sub-token length N in our experiment was approximately 4.5 mio states, we used this as an example to calculate the corresponding values of $p_h \approx 1$ and $p_d = 3.23 \cdot 10^{-49}$. Note that the tolerance for correctness and cheating, i.e. δ_h and δ_d were chosen to satisfy the constraints given by eq. 4.30 and eq. 4.32.
We thus demonstrate that it is possible to securely execute our experiment with the built setup with a sufficiently low double spending probability. However, since this probability depends on the length of the sub-token, it might be be more convenient to slightly increase this probability to speed up the token transmission procedure. This trade off between transmission time and security will be discussed in Section 6.1.

Table 5.2: Setup characterization and protocol performance. For clarity the results are split into three different categories: Experimental results, which stem immediately from measurements; SDP solutions, which are given by solving the SDP with the experimental results and Chernoff-Hoeffding bound solutions, which are likewise determined by inserting the measurement outcomes in the corresponding equations given in Section 4.1.

	Parameter name	Variable	Value
Experimental results	Losses	l_h	22.4 (± 1.5) %
	Errors H/V	$e_h^{H/V}$	1.4491 (± 0.0083) %
	Errors +/-	$e_h^{+/-}$	3.278 (± 0.013) %
	Mishaps	$\mathcal{M}(e_h^{+/-}, l_h)$	0.448 (± 0.016)
	Sub-token length	N	4 482 440 (± 1600)
	Qubit rate	$1/s$	14 298 (± 6) Hz
	Correlation function	$g_2(0)$	0.03010 (± 0.00014)
	Multiphoton emission	p_m	1.5051 (± 0.0070) %
SDP	Dishonest errors	$e_d(l_h)$	3.82 (± 0.22) %
	Dishonest losses H/V	$l_d(e_h^{H/V})$	38.600 (± 0.058) %
	Dishonest losses +/-	$l_d(e_h^{+/-})$	26.111 (± 0.090) %
C-H bounds	Allowed mishaps	$\mathcal{M}(e, l)$	0.496237 ± 0.000018
	Tolerance correctness	δ_h	0.031
	Honest success probability	p_h	~ 1
	Tolerance cheating	δ_d	0.01
	Double spending probability	p_d	$3.23 \cdot 10^{-49}$

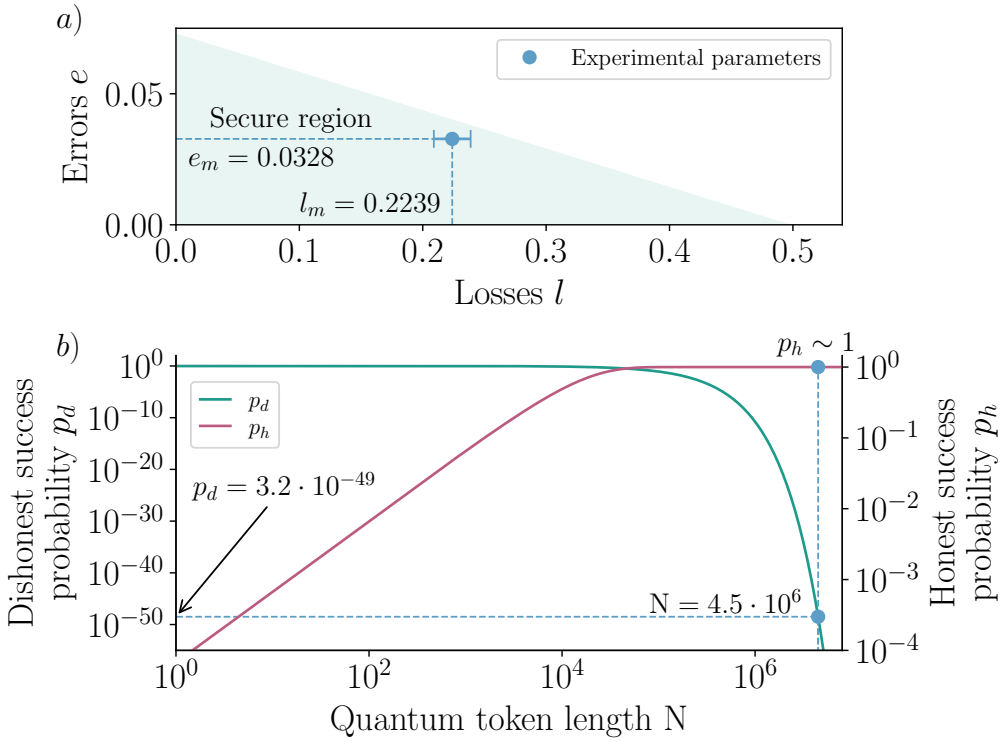


Figure 5.4: Security for experimental quantum cryptograms. a) The semidefinite programming framework extracts a secure region of operation (turquoise) as a function of errors and losses. Our honest experimental performance ($e_h = 0.0328 \pm 0.0001; l_h = 0.2239 \pm 0.015$) is indicated by the blue dot, and lies within the secure region. **b)** The double spending probability p_d (green, upper bound) and honest success probability p_h (red, lower bound) are displayed as a function of the number of quantum states N required to verify one bit of the cryptogram. These are derived using a Chernoff bound argument (see Subsection 4.1.9). As an example, an experimental token containing $\lambda = N = 4.5 \cdot 10^6$ quantum states (vertical blue dashed line) achieves an honest success probability very close to $p_h \sim 1$ and a dishonest success probability $p_d = 3.2 \cdot 10^{-49}$.

6 | Discussion and conclusion

In this thesis we proposed and demonstrated a new form of quantum payment that guarantees the one-time nature of purchases with i.t.-security. This is done by combining classical and quantum cryptographic schemes, namely i.t.-secure MAC functions and quantum bit coordination (introduced in [26]). The achieved scheme is proven to be experimentally feasible and secure over a deployed fibre link connecting two buildings. It is noteworthy that our scheme does not require any challenging technology on the side of the Client, apart from polarisation resolving single-photon detection setup.

While the cheating probability can be made arbitrarily close to zero by increasing the token length, the single photon generation and preparation efficiency (together with losses and errors) are also one of the most limiting factors.

6.1 Tradeoff between security and speed

Our scheme has a trade-off between quantum token length (or transmission time) and the security level, which is subject to the precise implementation. Depending on which level of security is desired, the transmission time has to be adjusted. As can be seen in Table 6.1 the transmission time increases with the level of security in a nonlinear way. Note that, for simplicity, we always assume that the two security parameters (i.e. p_d and p_t) are equal. While typical contactless payment delays are of the order of seconds, our quantum communication and verification provide i.t.-security within a few tens of minutes. These limitations are, however, only technological: quantum communication rates can be improved by using brighter quantum sources, while the verification delay originates from the correction of time-tagging drifts between the two buildings. Indeed, brighter sources of entangled photon pairs have already been demonstrated, which could decrease the quantum token transmission time to under a second [64].

6.2 Compromised payments

It is important to note that practical digital payment schemes must allow for rejected payments without compromising the Client's sensitive data. In our scheme, the adversary can compromise the payment token $|P\rangle$ sent over the quantum channel, the cryptogram sent over the classical channel or the Client's choice of M_i (as discussed in Section 3.3).
In the first two cases, quantum mechanics will ensure that the the TTP recognizes the malformed cryptogram and rejects the payment with arbitrarily high probability. The transaction may then be restarted. However, an i.t.-secure MAC must not re-use the key C, which is why we also propose the

Table 6.1: Token transmission time in dependence of the cheating probability. Depending on the tolerated cheating probability we list the Sub-token length N, the number of key and message bits, the total token lenght λ as well as the token transmission time, given our sources qubit rate of about 14300 per s. Note that these results are meant as estimations.

$p_d = p_t$	# key bits	# message bits	λ	N	token transmission time t
$5.4 \cdot 10^{-6}$	35	18	$9 \cdot 10^6$	$0.5 \cdot 10^6$	10.5 min
$2.9 \cdot 10^{-11}$	71	36	$36 \cdot 10^6$	10^6	42 min
$1.6 \cdot 10^{-16}$	105	53	$79.5 \cdot 10^6$	$1.5 \cdot 10^6$	93 min
$8.7 \cdot 10^{-22}$	140	70	$140 \cdot 10^6$	$2 \cdot 10^6$	163 min
$2.56 \cdot 10^{-32}$	210	105	$315 \cdot 10^6$	$3 \cdot 10^6$	367 min

use of n-time-secure Message Authentication Code (MAC) to overcome this obstacle. This allows re-using C as an input for the following payments, which imposes a finite, arbitrary bound on the number of purchases [65, 66]. When C is consumed, a new C, shared between Client and Trusted Token Provider (TTP), has to then be generated. Remarkably, we are able to amend our protocol such that the number of purchases is not bounded by the MAC function: the Client simply encrypts a new random key R with C, and forwards the result along with the cryptogram to the TTP. To protect against the third case, it must be ensured that the Client's choice of M_i is independent of any external bias. This can for example be guaranteed if a secure database of Merchants is initially distributed along with C and the Client chooses freely without any prior communication with the Merchant. Alternatively, the Merchant may send their ID to the Client, who uses the local database as a 2^{nd} factor authentication.

6.3 Final remarks

Our protocol's relaxed implementation requirements with respect to previous proposals, together with its error-tolerance, facilitate its deployment in mid-term quantum networks. Classical networks host applications beyond mere communication tasks. Similarly, a future quantum internet will necessitate the maturation of various quantum primitives and applications beyond QKD [67, 68]. Thus we believe that the presented scheme has the potential to advance the field of quantum payment schemes towards mid-term practical relevancy.

Bibliography

[1] S. Sahoo, A. Mandal, P. Samanta, I. Basu, and P. Roy, "A critical overview on quantum computing," *Journal of Quantum Computing*, vol. 2, pp. 181–192, 01 2020.

[2] D. Simon, G. Jaeger, and A. Sergienko, *Quantum Microscopy*, pp. 159–183. 11 2017.

[3] R. Renner and R. Wolf, "Quantum advantage in cryptography," *AIAA Journal*, vol. 61, pp. 1895–1910, may 2023.

[4] N. Gisin and R. Thew, "Quantum communication," *Nature Photonics*, vol. 1, pp. 165–171, mar 2007.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, oct 1997.

[6] 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, Sep 2021.

[7] 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. Photon.*, vol. 6, pp. 773–776, 2012.

[8] W. Beullens, "Breaking rainbow takes a weekend on a laptop." Cryptology ePrint Archive, Paper 2022/214, 2022. https://eprint.iacr.org/2022/214.

[9] W. Castryck and T. Decru, "An efficient key recovery attack on sidh (preliminary version)." Cryptology ePrint Archive, Paper 2022/975, 2022. https://eprint.iacr.org/2022/975.

[10] R. Perlner, J. Kelsey, and D. Cooper, "Breaking category five sphincs+ with sha-256." Cryptology ePrint Archive, Paper 2022/1061, 2022. https://eprint.iacr.org/2022/1061.

[11] C. Bennett and G. Brassard, "Withdrawn: Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science - TCS*, vol. 560, pp. 175–179, Jan 1984.

[12] 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, May 2020.

[13] 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. Photon.*, vol. 16, pp. 154–161, 2022.

[14] 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, Nov 2018.

[15] J. Yin, Y. Li, and S. e. a. Liao, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, p. 501, 2020.

[16] R. Bedington, J.-M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, p. 30, Aug 2017.

[17] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, "A device-independent quantum key distribution system for distant users," *Nature*, vol. 607, p. 687–691, 2022.

[18] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, "Experimental quantum key distribution certified by bell's theorem," *Nature*, vol. 607, p. 682–686, jul 2022.

[19] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, "Toward a photonic demonstration of device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 129, p. 050502, Jul 2022.

[20] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, "Quantum weak coin flipping with a single photon," *Physical Review A*, vol. 102, aug 2020.

[21] S. Neves, V. Yacoub, U. Chabaud, M. Bozzio, I. Kerenidis, and E. Diamanti, "Experimental cheat-sensitive quantum weak coin flipping," *Nature Communications*, vol. 14, apr 2023.

[22] 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, Nov 2013.

[23] E. Adlam and A. Kent, "Device-independent relativistic quantum bit commitment," *Physical Review A*, vol. 92, aug 2015.

[24] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, p. 78–88, Jan 1983.

[25] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Physical Review Letters*, vol. 109, Sep 2012.

[26] A. Kent and D. Pitalúa-García, "Flexible quantum tokens in spacetime," *Physical Review A*, vol. 101, Feb 2020.

[27] M.-C. Roehsner, J. Kettlewell, T. Batalhão, J. Fitzsimons, and P. Walther, "Quantum advantage for probabilistic one-time programs," *Nature Communications*, vol. 9, 12 2018.

[28] R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," *Phys. Rev. A*, vol. 93, p. 032325, Mar 2016.

[29] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, "Experimental quantum secure network with digital signatures and encryption," *Natl. Sci. Rev.*, 10 2022.

[30] PCI Security Standards Council (PCI SSC). https://www.pcisecuritystandards.org. Accessed: 2022-11-02.

[31] F. Corella and K. Lewison, "Interpreting the EMV tokenisation specification," *white paper*, 2014.

[32] EMVCo LLC, "EMV Payment Tokenisation Specification – Technical Reference," 2021.

[33] 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, Sep 2021.

[34] R. Shirey, "Internet security glossary, version 2." https://datatracker.ietf.org/doc/html/rfc4949, Aug 2007. Accessed: 2022-09-15.

[35] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[36] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, p. 120–126, feb 1978.

[37] K. S. McCurley, "The discrete logarithm problem," in *Proc. of Symp. in Applied Math*, vol. 42, pp. 49–74, USA, 1990.

[38] L. K. Grover, "A fast quantum mechanical algorithm for database search," 1996.

[39] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends® in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

[40] D. Butin, "Hash-based signatures: State of play," *IEEE Security amp; Privacy*, vol. 15, pp. 37–43, jul 2017.

[41] D. R. Stinson, *Cryptography: Theory and practice*. Discrete mathematics and its applications, Londen [etc.]: Chapman & Hall/CRC, 3rd ed. ed., 2006.

[42] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[43] W. K. Wootters and W. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[44] K. Sharma, *Optics: Principles and Applications*. Elsevier Science, 2006.

[45] T. Bohdanowicz, "Lecture 13: Quantum de finetti theorems." http://users.cms.caltech.edu/~vidick/teaching/286_qPCP/lecture13.pdf. Accessed: 2022-07-05.

[46] J. Watrous, "Lecture 7: Semidefinite programming." https://cs.uwaterloo.ca/~watrous/TQI-notes/TQI-notes.07.pdf, Oct 2011. Accessed: 2022-03-29.

[47] H. Chernoff, "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations," *The Annals of Mathematical Statistics*, vol. 23, no. 4, pp. 493 – 507, 1952.

[48] M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear Algebra and its Applications*, vol. 10, no. 3, pp. 285–290, 1975.

[49] S. Aaronson and P. Christiano, "Quantum money from hidden subspaces," *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, p. 41–60, 2012.

[50] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, "Experimental quantum forgery of quantum optical money," *npj Quantum Inf.*, vol. 3, p. 7, 2017.

[51] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, "Unforgeable noise-tolerant quantum tokens," *PNAS*, vol. 109, no. 40, pp. 16079–16082, 2012.

[52] M. Bozzio, A. Orieux, L. Trigo Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Inf.*, vol. 4, p. 5, Jan. 2018.

[53] 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.

[54] M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," *Physical Review A: General Physics*, vol. 99, p. 022336, Feb. 2019.

[55] K. Horodecki and M. Stankiewicz, "Semi-device-independent quantum money," *New J. Phys.*, vol. 22, p. 023007, feb 2020.

[56] Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, "One-hour coherent optical storage in an atomic frequency comb memory," *Nat. Commun.*, vol. 12, p. 2381, 2021.

[57] P. Vernaz-Gris, K. Huang, M. Cao, A. Sheremet, and J. Laurat, "Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble," *Nat. Commun.*, vol. 9, p. 363, 2018.

[58] K. Heshami, D. G. England, P. C. Humphreys, P. J. Bustard, V. M. Acosta, J. Nunn, and B. J. Sussman, "Quantum memories: emerging applications and recent advances," *J. Mod. Opt.*, vol. 63, no. 20, pp. 2005–2028, 2016.

[59] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," *Proc. of the 18th ACM Conference on Computer and Communications Security*, p. 75–86, 2011.

[60] R. Renner and J. I. Cirac, "de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Physical Review Letters*, vol. 102, Mar 2009.

[61] F. Laudenbach, S. Kalista, M. Hentschel, P. Walther, and H. Hübel, "A novel single-crystal & single-pass source for polarisation- and colour-entangled photon pairs," *Scientific Reports*, vol. 7, 12 2016.

[62] M.-C. Röhsner, "Experimental implementation of probabilistic one-time programs using quantum states," 2020.

[63] S. Polyakov, A. Migdall, J. Fan, and J. Bienfang, *Single-Photon Generation and Detection*. 12 2013.

[64] S. P. Neumann, M. Selimovic, M. Bohmann, and R. Ursin, "Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s," *Quantum*, vol. 6, p. 822, 2022.

[65] V. Fak, "Repeated use of codes which detect deception (Corresp.)," *IEEE Transactions on Information Theory*, vol. 25, no. 2, pp. 233–234, 1979.

[66] Rosenbaum, Ute, "A lower bound on authentication after having observed a sequence of messages," *Journal of Cryptology*, vol. 6, no. 3, pp. 135–156, 1993.

[67] L. Gyongyosi and S. Imre, "Advances in the quantum internet," *Commun. ACM*, vol. 65, p. 52–63, jul 2022.

[68] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.