universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„A quantum-resistant zero-knowledge protocol for NP-complete“

verfasst von / submitted by

Rebecca Hofer, BSc

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

Master of Science (MSc)

Wien, September 2023 / Vienna, September 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

Acknowledgements

I want to start by saying thank you to Prof. Philip Walther for letting me be part of his research team. I've learned a lot in the past year thanks to this opportunity. I especially want to thank Mathieu Bozzio for introducing me to the world of quantum cryptography, and for all the interesting discussions, and guidance in writing this thesis. I also owe thanks to Tobias Guggemos for explaining classical cryptography to me and continuously pointing out important security issues that helped me in developing the protocol. I also want to thank everyone in the Walther group, especially the Sensengasse group, for making me feel welcome in their team. Lastly, a big thanks to my friends and family for supporting me as I worked on finishing and writing this thesis.

Abstract

In recent years, considerable progress has been made in the quantum cryptography field in developing and enhancing protocols such as quantum key distribution, quantum money, or quantum coin flipping and in bringing these concepts into practical applications. In contrast to classical cryptography, where security is commonly argued based on computational hardness assumptions, these protocols aim to elevate security through quantum means. Quantum key distribution, in particular, is a foundational cornerstone in this field, illustrating how quantum principles can achieve information-theoretic security.

However, it is well-recognized that quantum cryptography does have its limitations. Equally, achieving perfect bit commitment or weak coin flipping remains impossible, akin to their classical counterparts. A common alternative approach is introducing relativistic constraints into the protocols, which, while bypassing certain no-go theorems, necessitates establishing or assuming security and trust in other aspects or parties involved in the protocol.

This thesis will outline a quantum version of a zero-knowledge proof protocol that does not rely on such relativistic constraints or classical computational hardness assumptions. Instead, it offers an information-theoretic secure binding and quantum-computationally hiding commitment scheme, achieved utilizing the method of conjugate coding — a core element of many quantum cryptographic protocols, such as the BB84 quantum key distribution protocol.

Building on this quantum commitment scheme, our protocol provides a quantum-computationally secure zero-knowledge proof for NP-complete problems. While considerable research has already been conducted on classical and quantum zero-knowledge proofs, this work distinguishes itself by focusing on developing a theoretically sound, practically implementable, and robust protocol against classical and quantum attacks.

Kurzfassung

In den letzten Jahren wurden erhebliche Fortschritte auf dem Gebiet der Quantenkryptographie erzielt. So wurden Protokolle wie *Quantum key distribution (QKD)*, *Quantum money*, oder *Quantum coin flipping* entwickelt und verbessert und ebenso in praktische Anwendungen umgesetzt.

Klassische Kryptographie stüzt ihre Sicherheit in der Regel auf Annahmen zur schweren Lösbarkeit von mathematischen Problemen. Hier liegt auch der grundlegende Unterschied zu *Quantenkryptografischen Protokollen*: solche unbewiesenen mathematischen Annahmen sind nicht notwendig um die Sicherheit von Protokollen zu argumentieren, da diese auf Quantenmechanischen Prinzipien beruhen. Das BB84 Protokoll war eines der ersten das zeigen konnte, wie mit Quantenprinzipien informationstheoretische Sicherheit erreicht werden kann.

Es ist jedoch auch allgemein bekannt, dass Quantenkryptographie ihre Grenzen hat. So wurde gezeigt dass es, ebenso wie bei den klassischen Gegenstücken, unmöglich ist, eine perfektes *Quantum bit-commtiment* Protokoll oder ein perfektes *Quantum weak coin flipping* Protokoll zu erstellen.

Ein häufig alternativ gewählter Ansatz um trotzdem informationstheoretische Sicherheit erreichen zu können besteht darin, relativistische Einschränkungen in die Protokolle einzuführen, die zwar bestimmte No-Go-Theoreme umgehen, jedoch im Gegenzug erfordern, dass Sicherheit und Vertrauen in andere Aspekte oder Parteien im Protokoll angenommen werden.

In dieser Arbeit werde ich ein Zero-Knowledge-Protokoll vorstellen, das weder relativistische Raum-Zeit-Einschränkungen noch Annahmen zur Berechnungsschwierigkeit von mathematischen Problemen erfordert. Stattdessen basiert das Protokoll auf einem *commitment scheme* das informations-theoretisch *binding* und *quantum computationally hiding* ist. Dies wird durch die Methode *conjugate coding* erreicht - ein häufig verwendetes Prinzip in der Quantenkryptographie, welche auch ein Kernbestandteil des BB84-Protokolls ist.

Basierend auf dem *commitment scheme* ermöglicht unser Protokoll ein *quantum-computationally secure* zero-knowledge proof Protokoll für NP-complete Probleme. Während bereits erhebliche Forschung zu klassischen und quantenbasierten Zero-Knowledge-Beweisen durchgeführt wurde, war das primäre Ziel dieser Arbeit die Entwicklung eines sicheren, und vorallem praktisch umsetzbaren Protokolls, dass resilient ist gegenüber Angriffen von klassichen und Quantencomputern.

Contents

1 Introduction

1.1 Information-theoretic security via quantum information

Today's cryptography relies on computational hardness assumptions, i.e., mathematical problems that are hard to solve, such as prime factorization and one-way functions. This is also known as *computational security*. However, these schemes have faced new threats in recent decades, with Shor's algorithmic discovery [Sho97] and ongoing efforts to build quantum computers with increasing computing power. This makes widely used encryption schemes like RSA vulnerable, hence necessitating the exploration of new security approaches. In this regard, quantum information not only offers fundamentally new computing resources to break some of the existing encryption schemes but a fundamentally new way of securing information that relies on the laws of quantum mechanics. It exploits quantum phenomena like the no-cloning theorem and quantum superposition instead of computational assumptions [WZ82] [AB16] to achieve *information-theoretic security*, i.e. security against computationally unbounded adversaries.

A prime example of information-theoretic security using quantum is quantum key distribution (QKD), which enables the remote generation and sharing of cryptographic keys securely. Researchers have extensively studied QKD, implementing shared keys over long distances, up to 1000 kilometers [WYH22] [BBR$^+$18] [YLL20]. In classical cryptography, a malicious third party called an *eavesdropper* can intercept and copy the keys as they are sent from one party to another, but quantum mechanics prohibits this due to the no-cloning theorem. Any attempt to extract information from a key encoded as quantum states would alter the states, making the eavesdropping detectable.

While information-theoretic security sounds promising, practical challenges remain. These concern experimental imperfections such as imperfect single-photon sources or how to securely store the key once it is generated and shared over the quantum channel. To address these concerns, ongoing research efforts have focused on various aspects of quantum information and cryptography, exploring measurement device-independent QKD to counter side-channel attacks on detectors [WTC21], decoy state protocols to counter photon-number splitting attacks [LMC05] and studying Bell inequality tests to address security loopholes [HBD15], [DLY16].

Despite progress, there are still open questions, particularly regarding data transmission at practical rates beyond a few hundred kilometers [ELH$^+$21], and resolving these challenges is crucial for implementing information-theoretic secure quantum key sharing in practice.

1.2 Quantum cryptography beyond QKD

1.2.1 Quantum advantage for various primitives

Given the advantages of quantum information in cryptography, researchers have explored its applications outside key exchange. They have investigated the quantum counterparts of various cryptographic schemes and protocols, such as quantum money [Wie83], [BDG19], digital signatures [YFL22], weak coin flipping [BCKD20] [NYC+23], delegated quantum computation [SB12], and one-time programs [RKB+18]. These schemes leverage quantum properties to achieve security benefits that are not achievable classically. Many of these protocols are based on *conjugate coding* [Wie83], which is also the crucial ingredient of QKD [AB16]. Conjugate coding is based on the uncertainty principle: security is achieved by encoding a bit value in one of two conjugate bases. Since a measurement in one basis destroys the state's information in the other, the information is information-theoretical securely hidden from anyone who does not know the correct encoding basis [Boz19]. A more thorough introduction to conjugate coding will be provided later in this thesis.

However, along with revealing advantages, the study of quantum cryptography has also shed light on its limitations. For example, certain cryptographic primitives, like information-theoretically secure quantum bit commitment and two-party computation, are proven to be impossible using only quantum resources [AB16]. To circumvent these constraints, an avenue that has been pursued involves leveraging the principles established by the second fundamental theory of physics, namely relativity. By imposing temporal and spatial restrictions on interacting parties, efforts have been made to reintroduce the feasibility of implementing information-theoretic bit commitment or zero-knowledge proof protocols with perfect security [LKB+15], [ABC+21]. However, a critical drawback arises as these protocols rely on trusted elements like GPS or third-party involvement, introducing potential vulnerabilities that undermine claims of unconditional security. This highlights the ongoing necessity for research regarding enhancing security for cryptographic protocols. It furthermore presents a subjective choice: whether one is inclined to anchor security on trusted devices under the framework of relativity, adopt and trust the assumption of the existence of one-way functions as in classical scenarios, or leverage methods offered by quantum mechanics and limit arising protocol vulnerabilities through binding the potential for dishonest behavior among participating parties.

1.2.2 (Quantum) zero-knowledge

This thesis specifically focuses on zero-knowledge systems, essential tools in authentication applications. Zero-knowledge proofs (ZKPs) allow parties to establish trust without revealing confidential information. Typically, ZKPs involve one party proving to the other party that they possess the solution to a problem without revealing any additional information about the solution. Exploring ZKPs from a quantum perspective is intriguing for several reasons.

First, exploring the potential benefits of quantum cryptography for ZKPs is interesting, particularly how quantum encoding of information can enhance the security guarantees of

some protocols (e.g., from computational assumptions to information-theoretic security). Classically, ZKP protocols rely on commitment schemes, and it has been shown that any language in the class NP, i.e., the complexity class of problems that can be verified in polynomial-time, admits a zero-knowledge protocol *if* and *only if* the language has an *instance-dependent* commitment scheme [OV08]. Further, in classical cryptography, the existence of commitment schemes is *equivalent* to the existence of one-way functions [MY22] [Bra22] [HILL99]. Whether a similar equivalence between commitment schemes and one-way functions holds in the quantum context or if these can be constructed from weaker assumptions remains open, with recent research suggesting a contrary perspective. The presence of quantum-hard one-way functions, i.e., one-way functions that are assumed to be hard to compute for quantum computers, is known to imply the existence of primitives such as oblivious transfer [JB21]. However, [MY22] suggests that non-interactive quantum commitments can be based on pseudorandom states instead of quantum-hard one-way functions. As a result of this analysis, they conclude that primitives like quantum ZKPs for NP and quantum-secure oblivious transfer could also exist without quantum-secure one-way functions since quantum commitments imply their existence. Furthermore, a similar insight is presented by [Bra22], who demonstrated that protocols for quantum commitment schemes or quantum oblivious transfer could be constructed from EFI pairs (efficient quantum algorithms with statistically distant yet computationally indistinguishable outputs). These findings raise questions about the necessity of one-way functions in these contexts. Following up on these discussions, quantum cryptography may offer new forms of commitment, although with a non-zero cheating probability for one or both parties [AB16] [May97].

Second, it is necessary to reanalyze classical zero-knowledge protocols to assess their resilience against quantum adversaries with different computational power. Some classical zero-knowledge protocols are found to be insecure in the presence of quantum attacks, especially those relying on intractability assumptions related to factoring and computing discrete logarithms [AB20]. As a result, researchers are working to develop new quantum-resistant zero-knowledge protocols [AB20], [VZ09], [Wat09].

Proving the security of zero-knowledge protocols against quantum adversaries is a complex task. This entails establishing that a malicious quantum verifier cannot extract information about the problem witnesses, accounting for all potential attacks that could be executed on the given proof system.

1.3 Contribution of this thesis

In this thesis, we present a novel quantum zero-knowledge proofs (QZKPs) protocol for NP that aims to address the security challenges posed by quantum adversaries by leveraging the potential of quantum mechanics. Specifically, the protocol's commitment scheme is based on conjugate coding, which eliminates the need for one-way functions and relies solely on the principles of quantum mechanics.

The security of the commitment scheme against a malicious quantum verifier and the *soundness* of the proof system is demonstrated through semi-definite programming.

However, a comprehensive security analysis and the *proof of the zero-knowledge property* of the protocol still require examination within the traditional simulator framework. This aspect remains future work and represents the next step in establishing the protocol's sound security parameters.

Nevertheless, the security proof of the commitment scheme is a crucial initial step. Also, to our knowledge, using the semi-definite programming method is a new approach in the context of proving the security of ZKPs and can be integrated into the traditional framework of simulation-based security proofs.

2 Preliminaries

2.1 Computer Science Theory

This section will cover key concepts from computer science relevant to understanding the proof protocol construction and implementation. The chapter introduces common terminology relevant to the later thesis sections 2.1.1. It then introduces notions of complexity classes 2.1.2 and further outlines the general conept of ZKPs 2.1.3 It then focuses on security properties of cryptographic protocols 2.1.4 and on the core of the proof, which involves verifying an NP-complete problem, the satisfiability (SAT) problem 2.1.5. The theoretical basis of the proof construction relies on the well-known Probabilistically Checkable Proof (PCP) theorem 2.1.6. It continues to explain semi-definite programs 2.1.7, and the Chernoff bound theorem 2.1.8, enabling us to derive and analyze the security aspects of the ZKP protocol.

2.1.1 Terminology

This section provides an overview of the terminology used throughout the rest of the thesis, relevant for definitions and the protocol description.

Alphabet Σ

An alphabet is denoted as Σ. It is a non-empty set of letters/symbols. For example, we can denote a binary alphabet as $\Sigma = \{0, 1\}$ with the letters 0 and 1 [Wika].

Words over an alphabet Σ^*

A word over an alphabet can be any finite sequence, i.e., a string of letters. The set of all strings with a length of n over an alphabet Σ is denoted as Σ^n. The set of all finite strings (without specifying a length) is denoted as Σ^* [Wikd].

Polynomial-time algorithm $poly()$

An algorithm is solvable in polynomial-time if the number of steps required to complete the algorithm for a given input of size n is $O(n^k)$ for some integer $k > 0$, i.e., a polynomial function of n bounds the algorithm [Aca].

2.1.2 Complexity classes

Complexity classes distinguish computational problems by their computational hardness, i.e., problems within the same complexity class require similar time and memory resources for a specified computational model to find a solution. The most well-known classes are P and NP. P refers to polynomial-time and is the class of problems for which a deterministic Turing machine can find a solution in polynomial-time. Potential solutions can also be verified in polynomial-time. On the other hand, NP stands for non-deterministic polynomial-time. To be in NP, a problem requires a polynomial-time algorithm to check the correctness, i.e., verify a potential solution. Furthermore, a non-deterministic Turing machine can solve problems in this class in polynomial-time.

While traditional complexity classes are typically defined using a single Turing machine, such as NP, many classes have alternative formulations in the language of *interactive proof systems* [VZ09]. In an interactive proof system, two parties, a prover and a verifier, exchange information, and the system relies on bounds for *completeness* (C) - the minimum probability that a prover can convince a verifier of the correctness of a true statement when both parties are honest, and *soundness* (S) - the maximum probability that a dishonest prover can convince an honest verifier of the correctness of a wrong statement. Specific complexity classes emerge based on values for C and S and the number of messages exchanged (r) between the prover and verifier.

For instance, when the verifier is a polynomial-time Turing machine and $r = 1, C = 1, S = 0$, we obtain the class NP. When we set $r = 1, C = 2/3, S = 1/3$, the resulting class is MA (Merlin Arthur). If we allow the verifier to be a quantum machine and quantum communication between the prover and verifier, with $r = 1, C = 2/3, S = 1/3$, the complexity class becomes QMA (Quantum Merlin Arthur). Furthermore, by allowing r to be any polynomial in n, where n represents the size of the problem instance while maintaining the parameter setting from MA, we obtain the class IP (Interactive proof) [VZ09].

To analyze the computational complexity of problems, reductionist proofs play a crucial role. In reductionist proofs, we can lower bound a problem's computational complexity. If we can reduce problem A to another problem B in polynomial-time, we know that problem B has to be at least as hard as problem A. Thinking this further, if we know the computational complexity of problem A, we can conclude that problem B's complexity lies in either the same or a higher computational complexity class. An example of this is the class of NP-complete problems. This class is defined according to the observation that any problem in NP can be reduced to a problem in NP-complete, implying that problems in NP-complete are at least as hard as any problem in NP. Thus, solving an NP-complete problem would imply solving all problems in NP efficiently. Furthermore, it is important to note that all problems in the classes P, NP, and NP-complete are decision problems, i.e., it can be posed as a yes-or-no question about the input.

2.1.3 Classical ZKPs

Within the complexity classes of interactive proof systems, subclasses of ZKPs emerge. ZKPs are interactive proof systems between a prover (P) and a verifier (V) that reveal no information useful to a polynomial-time machine other than the validity of a statement and, in addition to completeness and soundness, also possess the *zero-knowledge property*. Goldwasser, Micali, and Rackoff introduced the concept of ZKPs in 1983 [GMR85]. Furthermore, Goldreich et al. (1991) [GMW91] could show that all languages in NP have ZKP systems.

The objective of ZKP protocols is to prove that a statement ϕ belongs to a certain language L, i.e., $\phi \in L$ while ensuring that no additional information, apart from the truth of the given statement, is revealed. A language L over an alphabet Σ is a set of words, i.e., a subset of Σ^* [Wikd]. If $\phi \in L$, then a proof of this statement should be accepted by a verifier with high probability. If $\phi \notin L$, any proof should lead to a rejection with high probability. We call a proof the set of interactions or evidence presented by the prover to convince the verifier of the correctness of the statement. Further, we call a witness x the confidential information the prover possesses and wants to prove their knowledge of without revealing it.

To give a more formal definition, when given a language $L \in NP$, an input instance $\phi \in L$, and a binary alphabet $\Sigma = \{0, 1\}$, then there exists a deterministic algorithm $V : \Sigma^*$ x $\Sigma^* \rightarrow \{0, 1\}$ and a $P \in \Sigma^*$ such that $V(\phi, P) = 1$ with $|P| < poly(|\phi|)$. This means that, by definition, for any language in NP, there exists a deterministic algorithm V that can verify the membership of an input ϕ to the language, given a proof P in polynomial-time. I.e., algorithm V takes two inputs: ϕ, the instance to be tested, and P, which represents the proof, and returns a binary output $\{0, 1\}$, where 1 signifies that the proof is valid for ϕ, i.e., $\phi \in L$ [Lyn].

Then a ZKP for $L \subseteq \Sigma^*$ is a pair (P, V) that must satisfy the following properties:

- *Completeness*: For all $\phi \in L$, V accepts the input after interacting with P with probability P_C (*completeness*). This property ensures that if the statement being proven is true, an honest verifier should accept the proof with a high probability P_C. In other words, a valid proof should convince an honest verifier.

- *Soundness*: For all $\phi \notin L$, and for all provers P^* (here the star denotes a dishonest party), a verifier should accept the proof after interacting with P^* with at most P_S (*soundness*) probability. This property ensures that if the prover acts dishonestly by providing a proof for a false statement, a verifier will reject the proof with high probability P_S. The proof should be robust against cheating attempts by the prover.

- *(Perfect) zero-knowledge*: For all verifiers V^*, there exists a simulator S, which is a randomized polynomial-time algorithm, such that for all $\phi \in L$, $\{\text{transcript}((P, V^*)(\phi))$ $= \{S(\phi)\}$ [Lyn]. A *transcript* refers to the sequence of messages the parties exchange during a protocol run. By comparing the probability distribution of the transcript generated during the interaction between the simulator S — which *mimics* the prover P engaging in the protocol, but without having access to the witness x

— and the verifier V, with the distribution of the transcript from the interaction between P and V, we can determine whether the proof protocol truly qualifies as zero-knowledge. This is the case when the distributions are identical, i.e., the above equality holds, implying that whatever V has learned when engaging in the protocol could have learned independently, i.e., without any knowledge about the proof [Vil]. This means that even if the verifier deviates from the ideal behavior or behaves dishonestly, the zero-knowledge property ensures that the protocol does not reveal any additional information about the statement beyond its truthfulness, which we call perfect zero-knowledge.

The zero-knowledge property is crucial because it guarantees the protocol maintains secrecy while achieving its intended purpose. It ensures that even though the verifier may learn the truth of the statement, no other knowledge or sensitive information is leaked. Indeed, the zero-knowledge property opens up different categories of ZKP properties that differentiate in the strength of the notion of zero-knowledge [Wat09]. Besides *perfect zero-knowledge*, there is also *statistical zero-knowledge*, and *computational zero-knowledge*. *Statistical zero-knowledge* refers to the case where $\{\text{transcript}((P, V^*)(\phi)) =_\epsilon \{S(\phi)\}$, where ϵ is a negligible statistical difference in the output distribution. *Computational zero-knowledge* means that $\{\text{transcript}((P, V^*)(\phi)) \sim_c \{S(\phi)\}$, i.e., no polynomial boolean circuit can distinguish between the output distributions. Computational zero-knowledge is the least strong notion, where zero-knowledge is only guaranteed if we require the adversary to be computationally bounded.

2.1.4 Computational vs. information-theoretical security

Classical ZKPs usually rely on the assumption that *one-way functions* exist [YMAD15], such as the original work of Goldwasser et al. (1983) that, based on the one-way function assumption, argued that there exists a ZKP for any language in NP. This statement was further extended to any language in PSPACE by Ben-Or et al.[BOGG$^+$90], based on the same assumption. One-way functions are functions that are easy to compute in one direction but hard in the other: A function $f : \{0,1\}^* \to \{0,1\}^*$ is one-way if a polynomial-time algorithm can compute f, but any polynomial-time randomized algorithm F that attempts to compute a pseudo-inverse for f succeeds with negligible probability. This is captured in the following equation for all sufficiently large $n = |x|$: $Pr[f(F(f(x))) = f(x)] < n^{-c}$, and is true for all randomized algorithms F, and all positive integers c. Here, the notion *hard to compute* refers to the average case, in contrast to complexity theory, where *hard* refers to the worst-case. Security based on hardness assumptions is termed as *computational security*. However, it is important to note that the *existence* of one-way functions is an open conjuncture [Wike] and, therefore, the security of protocols based on them is not proven to hold.

Information-theoretical security is the primal goal of protocols, as it implies that it is impossible to break such a scheme, even under the assumption of an adversary with unbounded computational power. One protocol that achieved such an implementation was done by Alkhani et al. (2021) [ABC$^+$21] using relativity. The concept revolves around

multiple provers responding to challenges from verifiers while adhering to space-time constraints dictated by the laws of relativity. By doing so, information exchange between the provers is rendered impossible, and verifiers can examine the provers' responses to obtain a convincing proof. Although information-theoretical security is achieved from the standpoint of how the protocol implements information exchanged between the parties, it relies heavily on devices that guarantee compliance with space-time constraints, introducing potential security drawbacks since those devices are automatically considered trustworthy in the scheme.

2.1.5 SAT Problems

The core problem around which the protocol of this thesis is constructed is a *SAT* problem or *satisfiability* problem. The SAT problem was the first problem for which it was proved to be in the NP-complete class by the Cook-Levin theorem. The theorem shows that any problem in NP can be reduced to an SAT problem.

A formal definition of the SAT problem can be given as follows: Given a boolean formula ϕ in conjunctive normal form (CNF), i.e., a conjunction of one or more clauses containing several variables, one must decide whether the formula is satisfactory. The boolean formula $\phi = C_1 \wedge C_2 \wedge ... \wedge C_y$ contains n boolean variables x_1, x_2, ..., x_n, where each of the C_i is a clause of the form $(l_{i1} \vee l_{i2} \vee ... \vee l_{il})$, with literals l_{ij} drawn from the set $\{x_1, x_2,...,x_n, \overline{x_1}, \overline{x_2},..., \overline{x_n}\}$. Finding a solution means then deciding whether or not there exists some setting of the boolean variables $x = (x_1,x_2,...,x_n)$ such that the formula ϕ takes on a boolean value of *true* [Cha].

Different kinds of satisfiability problems differ according to the number of literals within the clauses. For example, 3SAT is an SAT problem that follows the above definition, but where the clauses are of the form $C_i = (l_{i1} \vee l_{i2} \vee l_{i3})$, i.e., each clause contains precisely three literals. For our QZKP protocol, a 2-out-of-4 SAT problem will be used. 2-out-of-4 SAT problem consists of y clauses of the form $C_i = (l_{i1} \vee l_{i2} \vee l_{i3} \vee l_{i4})$, i.e., every clause has four literals. The clauses are satisfied if and only if exactly two variables are equal to 1, i.e., if $l_{i1} + l_{i2} + l_{i3} + l_{i4} = 2$. Per the definition of NP-complete, any problem in NP can be reduced 2-out-of-4 SAT in polynomial-time and verified [ADK18].

By engaging in the protocol, the prover wants to convince the verifier that some SAT instance ϕ is satisfiable, i.e., there exists some x such that ϕ results to true, which is equivalent to showing that it belongs to a language L - in this case, L is the language of NP-complete problems. In the context of ZKPs, we call a satisfying assignment x the *witness* of the proof. In this case, the problem instance ϕ would be a specific formula in conjunctive normal form. If ϕ is a *Yes-instance*, i.e., an instance where we can find an assignment to the literals, such that the instance results into true, we say $\phi \in L$. If ϕ is a *No-instance*, i.e., an instance where we cannot find an assignment to the literals, such that the instance results into true, we say $\phi \notin L$.

2.1.6 PCP theorem

A very important concept for the protocol construction is the Probabilistically Checkable Proof (PCP) theorem, which provides a theoretical framework for constructing proofs in ZKP settings. With the PCP theorem, it can be shown that it is possible to *rewrite every proof* for a statement of length n into a different proof of length poly(n) that can be *probabilistically checked by making only a constant number of queries* to the proof. It establishes that every decision problem in NP holds proofs that can be checked probabilistically by a randomized algorithm with logarithmic randomness complexity and constant query complexity: $NP = \text{PCP}[O(\log n), O(1)]$ [SA98].

In the context of ZKPs, this can be understood as follows: A proof (e.g. the encoded witness) is the information that a prover provides to convince a verifier of the truth of a statement. The size of the proof is typically determined by the complexity of the problem and the chosen encoding scheme, and it may vary depending on the problem instance. For checking, the verifier generates an $O(\log n)$ random bit string r (randomness complexity) that is used for choosing a number q of random bits to query, where q (query complexity) is a constant $O(1)$. Due to the hardness of approximating NP-complete problems, the PCP theorem binds the probability of accepting a proof to a wrong statement under the above-outlined conditions to a constant $\epsilon < 1$, called the soundness error [ALM+98]. The theorem has important implications: Suppose the input string ϕ of length n is in the language L. This means that there exists a proof that will be accepted by the verifier with a probability of one, therefore having perfect completeness. However, if the input is not in the language, no matter what proof is presented, the verifier will accept it with a probability of at most ϵ. In this sense, any NP language can be expressed in a witness format that can be verified with an error probability arbitrarily close to zero since by running the verification process independently for t copies of the verifier and requiring acceptance from all copies; the error probability can be reduced to ϵ^t [Din08].

The PCP theorem shows that it is possible to create NP proofs that allow for probabilistic checking, where a restricted verifier can determine if an input string satisfies a statement by reading out a constant number of bits. It states that we can write NP witnesses in a format where the verifier accepts false statements with a bounded probability, and this probability can be further reduced by running multiple independent verifications.

2.1.7 Semi-definite programming

We will now explain semi-definite programming, which was used to derive the protocol's security. Semi-definite programs are optimization programs [VB96] that optimize a linear objective function under linear constraints, such that solutions are positive semi-definite matrices. The set of feasible solutions forms a convex set or a convex cone. A cone in linear algebra is a subset of a vector space that is closed under scalar multiplication, i.e., C is a cone if $x \in C$ implies $sx \in C$ for all positive scalars s [Wikc]. A convex cone is a cone (additionally) closed under addition or, equivalently, a subset of a vector space that is closed under linear combinations with positive coefficients. We can define this as

follows: for two operators $X, Y \in C$, C is a convex cone if $\alpha X + \beta Y \in C$ for any $\alpha, \beta > 0$. Optimizing means finding the optimal positive semi-definite matrix within the convex set that optimizes the objective function, subject to the specified constraints. We can associate a dual problem with the optimization problem, which we now call the primal problem. The dual problem is obtained via the Lagrangian and Lagrange multipliers associated with each constraint of the primal objective function.

With this, we can write a semi-definite program: Let ϕ: $\mathrm{L}(\mathcal{H}_X) \to \mathrm{L}(\mathcal{H}_Y)$ be a Hermiticity-preserving linear map and A and B be two hermitian operators in $\mathcal{H}_X$ and $\mathcal{H}_Y$ respectively. Then we can write the primal and the dual optimization problem associated with the triple (ϕ, A, B) as

Primal problem
maximize $\langle A, X\rangle = \mathrm{Tr}(A^\dagger, X)$
subject to $\phi(X) = B$
and $X \geq 0$

where the optimal primal value is

$$\alpha = \sup\{\langle A, X\rangle : X \geq 0, \phi(X) = B\} \tag{2.1}$$

and

Dual problem
minimize $\langle B, Y\rangle = \mathrm{Tr}(B^\dagger, Y)$
subject to $\phi^*(Y) \geq A$
and $Y = Y^\dagger$

where the optimal dual value is

$$\beta = \inf\{\langle B, Y\rangle : Y = Y^\dagger, \phi^*(Y) = B\} \tag{2.2}$$

[AM12]. Using semi-definite programs to derive security, we must ensure that the optimal value of the objective function is global. For this, one needs to show that the optimal value α of the primal problem, giving the maximum of the primal objective function, equals β, the optimal solution of the dual problem, i.e.,

$$\alpha = \beta \tag{2.3}$$

This property is also known as strong duality. It will serve our purpose as a justification for the tight security bond we will derive for our zero-knowledge protocol, i.e., no better cheating attack probability is possible on the state for which we solve the semi-definite program.

2.1.8 Chernoff bounds

To bound the cheating probability of the respective parties engaging in the protocol, we use a Chernoff bound argument. This tool is widely used to derive bounds on the probability that a specific event within a finite sample closely aligns with its theoretical expectation value.

In our case, we obtain a value p_i for the probability that a dishonest party successfully cheats in the protocol. In the following, we denote the dishonest party as a binary variable X with two possible outcomes: successful cheating $X = 0$ with probability p_i and unsuccessful cheating $X = 1$ with probability $1 - p_i$. This gives a *theoretical expectation value* $\mu = \sum_{i=1}^{n} p_i = n \cdot p_i$ for the expected number of times the dishonest party can cheat successfully when the total number of trials is n (assuming the cheating probability p_i is the same for all n). However, to make statements about the security of our protocol, we need to bound the probability that the actual mean value $\overline{X} = \sum_{i=1}^{n} X_i$ for successful cheating is close, i.e., within some region $\epsilon \in [0, 1]$ to the expectation value μ. For this, we use the Chernoff bound theorem:

Theorem: Let $\overline{X} = \sum_{i=1}^{n} X_i$, where $X_i = 1$ with probability p_i and $X_i = 0$ with probability $1 - p_i$, and all X_i are independent. Let $\mu = n \cdot p_i$. Then,

(i) **Upper Tail**: $P(X \geq (1 + \epsilon) \cdot n \cdot p_i) \leq e^{-\frac{\epsilon^2}{2+\epsilon} \cdot n \cdot p_i}$ for all $\epsilon > 0$.

(ii) **Lower Tail**: $P(X \leq (1 - \epsilon) \cdot n \cdot p_i) \leq e^{-\frac{\epsilon^2}{2} \cdot n \cdot p_i}$ for all $0 < \epsilon < 1$.

For the security proof, we are interested in upper-bounding the cheating probability of a dishonest party and will, therefore, use the upper tail. See also 5.1

2.2 Quantum Theory Basics

This chapter will outline the fundamental quantum mechanical principles for the proof protocol. In addition to these basic concepts, a comprehensive understanding of quantum channels 2.2.5 and the Choi-Jamiolkowski isomorphism 2.2.6 is crucial. These concepts play an important role in formulating the semi-definite programs utilized for the security analysis in this thesis. Furthermore, a brief overview of fundamental quantum-cryptography protocols will be provided 2.3. This background will pave the way for a detailed exploration of the ZKP protocol's construction. Notably, the protocol is grounded in the same quantum cryptographic approach that underpins QKD and quantum money, namely, conjugate coding.

2.2.1 Quantum state space

Mathematically, quantum mechanics is formulated within Hilbert spaces, which are complex vector spaces equipped with an inner product. In this framework, quantum

states can be described as state vectors $\{|\psi\rangle\}$ in the vector space. The basis of a Hilbert space is orthonormal, satisfying the relation

$$\langle j|k\rangle = \delta_{\mathrm{j,k}} \tag{2.4}$$

and complete, given by

$$\sum_{i=0}^{n-1} |i\rangle \langle i| = \mathbb{1} \tag{2.5}$$

where the dimension can be *finite* or *infinite*. It is important to note that the choice of basis vectors is arbitrary and does not have a physical interpretation beyond its connection to measurements. Expanding a state vector $|\psi\rangle$ in a chosen basis $\{|i\rangle\}$ is expressed as:

$$|\psi\rangle = \sum_{i=0}^{n-1} c_{\mathrm{i}} |i\rangle \tag{2.6}$$

where $c_0, ..., c_{n-1}$ are complex coefficients linked to the probabilities of finding the system in the corresponding state upon measurement. A commonly used basis in Hilbert spaces is the set of eigenstates of a specific observable of interest. For instance, when describing a qubit, which is a two-level pure quantum state, the computational basis $\{|0\rangle, |1\rangle\}$ is typically chosen. In this case, the state can be written as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{2.7}$$

where $|\alpha|^2$ and $|\beta|^2$ correspond to the probabilities of measuring the qubit in the respective states $|0\rangle$ and $|1\rangle$ when the projective measurement observable $M_{\mathrm{z}} = |0\rangle \langle 0| + |1\rangle \langle 1|$ is measured.

Apart from the state vector representation in Hilbert spaces, a quantum state can also be defined as a square-integrable function over continuous variables in a Banach space. The mapping between these two formalisms is established by associating the wavefunction value $\psi(x)$ with the x-th component of the Hilbert space state vector $|\psi\rangle$ in the basis $\{|x\rangle\}$, which consists of the eigenvectors of the position operator $\hat{x}$ [Mar]. With that, we get

$$\psi(x) = \langle x|\psi\rangle \tag{2.8}$$

meaning the wavefunction is the projection of the state vector $|\psi\rangle$ onto the continuous position basis $\{|x\rangle\}$. The Hilbert space spanned by the basis $\{|x\rangle\}$ is an example of an infinite-dimensional Hilbert space, necessary when the quantum system is described using eigenvectors associated with observables possessing continuous eigenvalues. However, for further discussion, we will only consider finite-dimensional Hilbert spaces.

Bloch sphere:

Another frequently employed representation of quantum states is the Bloch sphere. This three-dimensional geometrical representation offers an intuitive depiction of quantum states, mainly when the wavefunction phases play a crucial role. Although the wavefunction phase is not directly measurable, the relative phase gives rise to interference effects when interacting with other wavefunctions. In the Bloch sphere representation of a qubit, the state is parametrized by two angles (θ, ϕ). The state vector of a qubit can then be expressed as:

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle \tag{2.9}$$

where the two angles θ and ϕ specify the rotation of the state vector on the Bloch sphere.

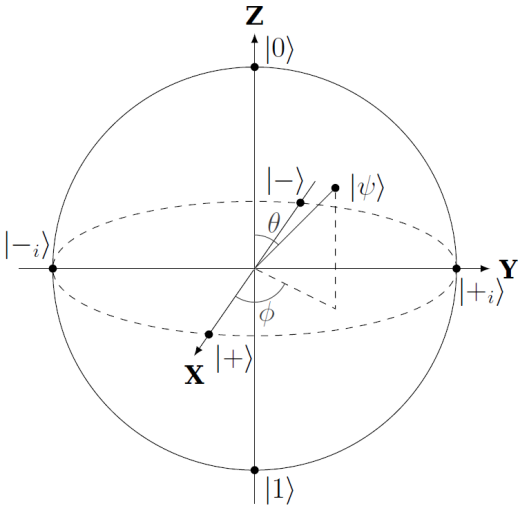

Figure 2.1: Bloch sphere representation

The vectors corresponding to the axes of the Bloch sphere are the eigenvectors of the three Pauli matrices:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\psi_{\text{z+}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle\,, \quad \psi_{\text{z-}} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\psi_{\text{x+}} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle\,, \quad \psi_{\text{x-}} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$$

$$\psi_{\text{y+}} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = |+_i\rangle\,, \quad \psi_{\text{y-}} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} = |-_i\rangle$$

In terms of the computational basis vectors $\{|0\rangle, |1\rangle\}$, we can express the following states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

and

$$|+_{\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \quad |-_{\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$

These basis states can also be obtained by introducing relative phase shifts ϕ:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\cdot 0}\,|1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}\,|1\rangle)$$

and

$$|+_{\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{2}}\,|1\rangle), \quad |-_{\mathrm{i}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{3\pi}{2}}\,|1\rangle)$$

The phase shift can be interpreted as a rotation of the state vector around the corresponding axis (in this case, the z-axis), with the angle representing the amount of phase shift. It is worth noting that $|0\rangle \perp |1\rangle$, $|+\rangle \perp |-\rangle$ are orthogonal, meaning that their wavefunctions have zero overlaps.

2.2.2 Quantum operators

Operators describe physical processes that induce changes in the state vector of a system or represent physical system properties that can be measured. When acting on a Hilbert space, operators map one state to another within the same or a different Hilbert space. Operators representing different transformations must possess certain properties to describe the physical reality accurately.

Observables pertain to measurable properties of a system, such as position, energy, or momentum, and are represented by *hermitian operators*. Hermiticity (and thus linearity) is required to ensure that these operators' eigenvalues and measurement outcomes are real, which is a fundamental postulates of quantum mechanics.

Similarly, the time evolution of quantum states, governed by a hermitian Hamiltonian, follows the requirement of being *unitary* for a closed system. Unitary operators represent reversible and deterministic evolutions of quantum states, preserving normalization and the inner product. Quantum operations involving non-unitary transformations include measurements and decoherence.

Mathematically, the distinct operator definitions possess the following properties:

Linear operators:

$$\hat{A}(c_1\,|\psi_1\rangle + c_2\,|\psi_2\rangle) = c_1\hat{A}\,|\psi_1\rangle + c_2\hat{A}\,|\psi_2\rangle \tag{2.10}$$

This property implies that an operator acting on the superposition state of two distinct states behaves as if it acts on each state individually.

Hermitian operators:

$$\hat{A}^\dagger = \hat{A} \tag{2.11}$$

$$\langle \hat{A}\psi|\phi\rangle = \langle\psi|\hat{A}\phi\rangle = \langle \hat{A}^\dagger\psi|\phi\rangle \tag{2.12}$$

$$\hat{A}\,|a\rangle = a\,|a\rangle\,, \quad a \in \mathbb{R} \tag{2.13}$$

$$\langle a_i|a_j\rangle = \delta_{i,j} \tag{2.14}$$

A Hermitian operator can be decomposed into its eigenvalues and eigenstates, known as spectral decomposition

$$\hat{A} = \sum_a \lambda_a\,|a\rangle\,\langle a| \tag{2.15}$$

Here, $|a\rangle\,\langle a|$ represents the projection onto the eigenspace of the operator.

Unitary operators:

$$\langle \hat{U}u|\hat{U}v\rangle = \langle u|v\rangle, \quad u, v \in V \tag{2.16}$$

This property indicates that unitary operators preserve inner products and, consequently, the norms of quantum states. Furthermore,

$$\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{1}. \tag{2.17}$$

This corresponds to the observation that unitary operations are reversible.

2.2.3 Mixed states

Mixed states generally describe quantum states, encompassing both quantum and classical aspects. They can be understood as statistical mixtures of different states $|\psi_i\rangle$, each with a corresponding probability p_i of being obtained in a measurement. When there are a total of N states, and the state $|\psi_i\rangle$ appears N_i times in the mixture, the probability of $|\psi_i\rangle$ is given by

$$p_i = \frac{N_i}{N}, \quad \text{where} \quad \sum_i p_i = 1. \tag{2.18}$$

These probabilities p_i are purely classical and do not represent quantum uncertainty. Mixed states are represented by *density matrices*, which are positive semi-definite operators acting on the Hilbert space. A density matrix possesses the following properties:

- $\rho^\dagger = \rho$ (hermiticity)

- $\mathrm{Tr}(\rho) = 1$ (normalization)
- $\rho \geq 0$ (positivity)

The density matrix can be expressed as the sum of its eigenstates $|\psi_i\rangle$ with corresponding probabilities p_i

$$\rho = \sum_{i=1}^{N} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| . \tag{2.19}$$

The unitary evolution of a density matrix can be written as

$$\rho \to \hat{U}\rho\hat{U}^\dagger = \sum_{i=1}^{N} p_i \hat{U} \left|\psi_i\right\rangle \left\langle\psi_i\right| \hat{U}^\dagger. \tag{2.20}$$

The expectation value of an observable $\hat{A}$ that measures the state ρ is computed as

$$\langle\hat{A}\rangle = \mathrm{Tr}(\rho\hat{A}). \tag{2.21}$$

2.2.4 Quantum measurement

Quantum measurements, unlike unitary evolutions governed by a Hamiltonian operator, involve interactions with an external system, resulting in a non-closed quantum system. While unitary transformations are reversible, quantum state measurements are inherently irreversible. In the previous section, hermitian observables were introduced as quantum mechanical operators associated with measurable properties of a quantum system. Measurements are often associated with hermitian observables, known as projective measurements onto the orthogonal eigenstates of the observable. In such measurements, the outcome corresponds to one of the eigenvalues, and the state collapses into the corresponding eigenstate. This is evident when expressing the observable in its spectral decomposition

$$\hat{M} = \sum_{m} m\hat{P}_m. \tag{2.22}$$

Here, $\hat{P}_m$ represents the projector onto the eigenspace of $\hat{M}$ associated with the eigenvalue m. Since eigenvectors of hermitian matrices are mutually orthogonal, requiring the measurement operator to be hermitian is equivalent to ensuring the orthogonality of the projection operators for the observable: $\hat{M}_m\hat{M}_{m'} = \delta_{m,m'}\hat{M}_m$.

However, there are cases where measurements are performed on properties that do not have corresponding observables, such as weak measurements, quantum state estimation, and information-based measurements. Thus, quantum measurements are defined more generally as a collection of measurement operators $\hat{M}_m$ that act on the state space of the measured system. This framework, known as positive operator-valued measurement (POVM), allows for a broader range of measurements. The operators in a POVM can be any positive operators satisfying the completeness relation

$$\sum_m \hat{M_m}^\dagger \hat{M_m} = \mathbb{1}. \tag{2.23}$$

Here, $\hat{M_m}$ represents the measurement operator associated with outcome m, and the probability of obtaining outcome m when the system is in state $|\psi\rangle$ is given by

$$p(m) = \langle\psi|\hat{M_m}^\dagger \hat{M_m}|\psi\rangle, \tag{2.24}$$

where we require $p(m) \geq 0$ for any vector $|\psi\rangle$. This equation is known as the Born rule. After the measurement, the system is left in this state

$$\frac{\hat{M_m}\,|\psi\rangle}{\sqrt{\langle\psi|\hat{M_m}^\dagger \hat{M_m}|\psi\rangle}}. \tag{2.25}$$

Unlike projective measurements, the measurement operators in a POVM are not necessarily orthogonal projectors onto the eigenstates of a specific observable. Thus, the POVM framework provides a more general measurement framework, allowing for outcomes that may not be associated with the eigenstates of a particular observable.

2.2.5 Quantum channels

A quantum channel is the most general operation that maps an input quantum state to an output quantum state. It encompasses various transformations: unitary transformations as reversible operations, noisy channels introducing noise or decoherence, and measurement channels that describe transformations occurring during quantum measurement. In essence, it formalizes the transmission and processing of quantum information. To be physically realizable, a quantum channel must satisfy certain properties. First, it should be a *linear* map. A linear map $\hat{N}$ acts linear on its input, meaning that

$$\hat{N}(\alpha\rho_1 + \beta\rho_2) = \alpha\hat{N}(\rho_1) + \beta\hat{N}(\rho_2) \tag{2.26}$$

Additionally, a quantum channel must be a *positive* map $\hat{N} \geq 0$ that maps positive operators $\rho \geq 0$ to positive operators, such that

$$\sigma = \hat{N}(\rho) \geq 0 \tag{2.27}$$

represents a valid positive operator again. Indeed, we require an even stronger property known as *complete positivity* (CP). A map is considered completely positive if and only if

$$(\hat{N} \otimes \mathrm{id})(\rho) \geq 0 \tag{2.28}$$

where $\hat{N} \otimes \mathrm{id}$ is a linear map acting on $\rho \in \mathcal{H} \otimes \mathcal{H}$ with $\mathcal{H} = \mathbb{C}^d$. This condition ensures that a positive input state is mapped onto a positive output state, even when the map N acts only on a subspace of a larger Hilbert space, i.e., transforms only a subsystem of the density matrix. Complete positivity is a more stringent requirement than positivity.

A quantum channel can also be trace-preserving (TP) or trace-decreasing to a quantum state ρ satisfying $Tr(\rho) = 1$. When talking about completely positive and trace-preserving (CPTP) maps we require the channel to be trace-preserving, which means that the channel needs to satisfy

$$Tr(\hat{N}(\rho)) = 1 \tag{2.29}$$

[Eis]. Furthermore, any CPTP map $\hat{N}$ can be decomposed as a sum of Kraus operators $\hat{A}_k$

$$\hat{N}(\rho) = \sum_{k=1}^{r} \hat{A}_k \rho \hat{A}_k{}^{\dagger} = \sum_{k=1}^{r} p_k \hat{A}_k \left|\psi_k\right\rangle \left\langle\psi_k\right| \hat{A}_k{}^{\dagger} \tag{2.30}$$

and the operators need to satisfy

$$\sum_{k=1}^{r} \hat{A}_k \hat{A}_k{}^{\dagger} = \mathbb{1}. \tag{2.31}$$

The smallest number r for which such a decomposition can be achieved is called *Klaus rank*. For unitary transformations, $r = 1$ since they can be expressed with only a single operator matrix.

2.2.6 Choi-Jamiolkowski isomorphism

There are various ways to represent quantum channels. One convenient approach is using the Choi-state and the corresponding Choi-Jamiolkowski isomorphism, also known as channel-state duality. This isomorphism establishes a one-to-one correspondence between *quantum channels* and *Choi-states*.

The intuition behind this is as follows: Consider a map T that takes $\mathcal{H}_A$ to $\mathcal{H}_{A'}$. We can introduce an auxiliary system $\mathcal{H}_R$. When T is a complete positive map, then by definition, it takes a maximally entangled state $|\Phi\rangle$ on $\mathcal{H}_{RA}$ to a nonnegative state in $\mathcal{H}_{RA'}$. Then we can associate the CP map T with a nonnegative state in $\mathcal{H}_R \otimes \mathcal{H}_{A'}$. Conversely, any nonnegative state in $\mathcal{H}_R \otimes \mathcal{H}_{A'}$ can be associated with a CP map T that takes $\mathcal{H}_A$ to $\mathcal{H}_{A'}$ [Pre].

If the mentioned correspondence is valid, indicating that the associated Choi-state can comprehensively capture the properties and characteristics of a quantum channel, and conversely, this relationship precisely defines the Choi-Jamiolkowski isomorphism.

In the following, we will show how the isomorphism works. This is based on the lecture notes of [Pre] on pages 20 - 21. To start, let's consider the maximally entangled state,

$$|\Phi\rangle_{RA} = \sum_{i=0}^{d-1} |i\rangle_R \otimes |i\rangle_A \tag{2.32}$$

where A denotes $\mathcal{H}_A$ and R to $\mathcal{H}_R$, and both A and R have the same dimension d. We normalize $|\Phi\rangle$ to $\sqrt{d}$ to avoid rewriting the normalization factor in the next lines. If we

take the map T to be completely positive, then $id \otimes T$ maps the input state $|\Phi\rangle\langle\Phi|$ to a nonnegative state, i.e., a density matrix $\sum_a(|\Psi_a\rangle\langle\Psi_a|)$ on $\mathcal{H}_{RA'}$

$$(id \otimes T)((|\Phi\rangle\langle\Phi|)_{RA}) = \sum_a (|\Psi_a\rangle\langle\Psi_a|)_{RA'}. \tag{2.33}$$

Expanding a vector $|\varphi\rangle$ in the basis of $\mathcal{H}_A$, we get

$$|\varphi\rangle_A = \sum_i \varphi_i |i\rangle_A = \sum_i \varphi_i ({}_R\langle i|\Phi\rangle_{RA}) = {}_R\langle\varphi^*|\Phi\rangle_{RA}. \tag{2.34}$$

Using the linearity condition of T and (2.33), we can express the map acting only on $\mathcal{H}_A$ as

$$T((|\varphi\rangle\langle\varphi|)_A) = T({}_R\langle\varphi^*|\Phi\rangle_{RA}{}_{RA}\langle\Phi|\varphi^*\rangle_R) = \sum_a (\langle\varphi^*|\Psi_a\rangle\langle\Psi_a|\varphi^*\rangle)_{A'} \tag{2.35}$$

We can now define an operator M_a: $\mathcal{H}_A \to \mathcal{H}_{A'}$ that, give a vector $|\Phi\rangle_{RA'}$ acts on $|\varphi\rangle_A$ in the following way

$$M_a |\varphi\rangle_A = {}_R\langle\varphi^*|\Psi_a\rangle_{RA'} \tag{2.36}$$

Thus (2.35) represents the map T as an operator sum that acts on the pure state $(|\varphi\rangle\langle\varphi|)_A$. This representation can be extended linearly to arbitrary density matrices:

$$T(\rho) = \sum_a M_a \rho M_a^\dagger \tag{2.37}$$

This equation demonstrates the relationship between a given state ρ and the associated channel, where the channel is represented by a sum of Kraus operators M_a.

(2.33) shows how to obtain a state on $\mathcal{H}_{RA'}$ from the channel $T : \mathcal{H}_A \to \mathcal{H}_{A'}$. Conversely, equations (2.36) and (2.37) show how the CP map T can be recovered from the state by transforming it with the corresponding Kraus operators. Together, these equations establish the isomorphism between the state and the channel, highlighting the mapping between them and the role of Kraus operators in the process.

The Choi-Jamiolkowski isomorphism plays a crucial role in semi-definite programming that concerns analyzing and solving optimization problems involving quantum channels. It transforms optimization problems containing quantum channels into equivalent problems over semi-definite matrices associated with those channels. To see this, we rewrite (2.33) into

$$(id \otimes T)((|\Phi\rangle\langle\Phi|)_{RA}) = \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes T(|i\rangle\langle j|) = J(T) \tag{2.38}$$

$J(T) : \mathcal{H}_{RA} \to \mathcal{H}_{RA'}$ is associated with the channel matrix that should be optimized for optimal values subject to some objective function while adhering to specified constraints. These constraints are well-defined, ensuring the preservation of the essential properties

of completely positive and trace-preserving maps. Specifically, we require $J(T)$ to be positive-semi-definite

$$J(T) \geq 0 \tag{2.39}$$

This ensures that the channel T is completely positive. Furthermore the constraint

$$Tr(J(T))_{\mathcal{H}_{A'}} = \mathbb{1}_{\mathcal{H}_A} \tag{2.40}$$

guarantees T to be a trace-preserving map. Another important and well-known relation is

$$\langle\phi| T\big(|\psi\rangle\langle\psi|\big)|\phi\rangle = \langle\phi| \otimes \langle\psi^*| J(T) |\phi\rangle \otimes |\psi^*\rangle \tag{2.41}$$

or equivalently

$$\mathrm{Tr}\big(|\phi\rangle\langle\phi| T\big(|\psi\rangle\langle\psi|\big)\big) = \mathrm{Tr}\big(|\phi\rangle \otimes |\psi\rangle\langle\phi| \otimes \langle\psi| J(T)\big) \tag{2.42}$$

2.2.7 Quantum Optics

The above-outlined quantum mechanical descriptions were very general, and we haven't specified the quantum system we are looking at yet. Indeed, qubits can be realized in different ways, such as via photons, electrons, nuclei, or Josephson junction, to name a few.

For this thesis, we consider photons as the information carrier units.

Second Quantization

Quantum optics is built on the formalism of the second quantization of the electromagnetic field, which treats photons as discrete energy packets or excitations. This framework views the field as a collection of independent harmonic oscillators. Each oscillator corresponds to a distinct mode i with a specific frequency ω_i, characterized by their wavevector $\vec{k}_i$ and polarization degree of freedom s_j, with $j \in \{1, 2\}$, and $\vec{k} \perp s_1, \perp s_2$. The oscillator of a mode represents the quantized excitations associated with that mode, i.e., the harmonic oscillators' discrete energy levels determined by the mode's frequency. Solving the wave equation for specified boundary conditions, one arrives at the specific mode functions as the eigenfunctions $\vec{u}_{\vec{k},s}(\vec{r})$

$$\nabla^2 \vec{u}_{\vec{k},s}(\vec{r}) = -k^2_{\vec{k},s} \vec{u}_{\vec{k},s}(\vec{r}). \tag{2.43}$$

As solution functions to the eigenvalue problem, they form an orthonormal basis

$$(\vec{u}_{\vec{k},s}, \vec{u}_{\vec{k'},s'}) = \int d\vec{r}^3 \vec{u}_{\vec{k},s}(\vec{r}), \vec{u}_{\vec{k'},s}(\vec{r}) = \delta_{s,s'}\delta(\vec{k} - \vec{k'}) \tag{2.44}$$

into which we can expand the electromagnetic field [Dak22]. Photons as excitations of the field are then populated into an independent mode i via the creation $\hat{a}_i^\dagger$ and the annihilation $\hat{a}_i$ operator, whose actions are expressed as

$$\hat{a}_i^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{2.45}$$

$$\hat{a}_i |n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{2.46}$$

Within this operator formalism, the harmonic oscillator of mode i is expressed by the following Hamiltonian

$$\hat{H} = \hbar\omega_i\Big(\hat{a}_i^\dagger \hat{a}_i + \frac{1}{2}\Big). \tag{2.47}$$

The states $|n\rangle$ with $n \in [0, \infty)$ are called *Fockstates* and are the energy eigenstates of the Hamiltonian

$$\hat{H}\,|n\rangle = \hbar\omega_i\Big(\hat{a}_i^\dagger \hat{a}_i + \frac{1}{2}\Big)\,|n\rangle\,. \tag{2.48}$$

With this, we have already motivated an important state space of quantum optics: the *Fock space* whose basis states are the number states $|n\rangle$. It is a direct sum of tensor product spaces, where each tensor product space corresponds to a specific mode of the quantized electromagnetic field and can be occupied by a different number of photons. Within the same mode or sub-Fockspaces, particles are indistinguishable. The Fockspace $\mathcal{F}$ can be written as

$$\mathcal{F} = F_0 \oplus F_1 \oplus ... \oplus F_N \tag{2.49}$$

In the direct sum, dimensions of vector spaces add up, i.e., for F_{d1} with dimension $d1$ and F_{d2} with dimension $d2$ the direct sum $F_{d1} \otimes F_{d2} = F_{d1+d2}$ has dimension $d1 + d2$. And for vectors, we get that if $|d1\rangle \in F_{d1}$ and $|d2\rangle \in F_{d2}$ then the direct sum space is spanned by all linear combinations of vectors from F_{d1} and F_{d2}, $|d1\rangle + |d2\rangle \in F_{d1} \otimes F_{d2}$. Therefore a basis for $F_{d1} \otimes F_{d2}$ is obtained by combining the basis of the individual particle number Fock spaces $\{F_i\}$. In this sense, the Fock space is spanned by the occupation number states for all possible numbers of particles, whereas

$$\langle d1|d2\rangle = \delta_{d1,d2}. \tag{2.50}$$

This means that basis vectors called *Fock states* with different numbers of particles are orthogonal. The number states are the eigenstates of the number operator $\hat{N}_i$, which counts the number of photons in the i-th mode

$$\hat{N}_i\,|n_1, ..., n_\mathrm{i}, ..., n_\mathrm{k}\rangle = n_i\,|n_1, ..., n_\mathrm{i}, ..., n_\mathrm{k}\rangle \tag{2.51}$$

and where

$$\hat{N}_i = \hat{a_i}^\dagger \hat{a}_i. \tag{2.52}$$

Linear optics

A qubit can be regarded as a superposition state across two *distinct degrees of freedom*. In the previous chapter, we explored how the electromagnetic field can be decomposed into the normal modes $\vec{u}_{\vec{k},s}(r)$, which are a complete and normalized set of solutions to Maxwell's equations. We assumed these solutions to be *monochromatic*, meaning they only have spatial variations and no time dependency. Such modes are referred to as *spatial modes*. However, as Titulaer and Glauber (1966) [TG66] pointed out, the concept of purely monochromatic electromagnetic field excitations (photons) isn't accurate in the real world [RW20]. In reality, we need to consider both spatial and temporal aspects, introducing a temporal degree of freedom in addition to the spatial ones. This interpretation allows normal modes to represent *spatial-temporal distributions*. Quantum superposition states can be composed over these spatial and temporal degrees of freedom, i.e., we can create spatial or temporal superposition states. However, for the subsequent sections of this thesis, our focus will be exclusively on spatial modes.

In a *beamsplitter* transformation, two spatial modes of light are combined, resulting in a superposition state encompassing the spatial modes involved. This superposition state can be expressed as a linear combination of the individual spatial modes in the beamsplitter transformation. These spatial modes can be considered as distinct basis states within the superposition. Specifically, the beamsplitter transformations of the incoming spatial modes $\hat{a}_0^\dagger$ and $\hat{a}_1^\dagger$ can be written as follows, with r and t being parameters for the reflectivity and transmittivity respectively

$$\hat{a}_0^\dagger \to \sqrt{r}\hat{a}_2^\dagger + \sqrt{t}\hat{a}_3^\dagger \tag{2.53}$$

$$\hat{a}_1^\dagger \to \sqrt{t}\hat{a}_2^\dagger - \sqrt{r}\hat{a}_3^\dagger. \tag{2.54}$$

The above transformation displayed for spatial modes can also be considered a transformation for a given polarization basis. For example, in the basis $\{|H\rangle, |V\rangle\}$, a polarization beamsplitter (PBS) would reflect and transmit incoming photons according to their polarization, therefore allowing to perform projective polarization measurements

$$\hat{a}_H^\dagger \to \sqrt{r}\hat{a}_H^\dagger + \sqrt{t}\hat{a}_V^\dagger \tag{2.55}$$

$$\hat{a}_V^\dagger \to \sqrt{t}\hat{a}_H^\dagger - \sqrt{r}\hat{a}_V^\dagger \tag{2.56}$$

Another fundamental optical transformation is that of a *phaseshifter* that introduces a phase shift ϕ in the spatial mode in which it is set

$$\hat{a}_0^\dagger \to e^{i\phi}\hat{a}_0^\dagger \tag{2.57}$$

We further require waveplates for the experimental implementation. The half-wave plate (HWP) introduces a phase shift of half a wavelength $\pm\pi$ between the two orthogonal polarization components $|H\rangle$ and $|V\rangle$ of the incident light. This causes a rotation of the polarization direction of the light wave. In terms of creation operators, the state transformation reads as follows

$$\hat{a}_H^\dagger \to \cos 2\theta \hat{a}_H^\dagger + \sin 2\theta \hat{a}_V^\dagger \tag{2.58}$$

$$\hat{a}_V^\dagger \to \sin 2\theta \hat{a}_H^\dagger - \cos 2\theta \hat{a}_V^\dagger \tag{2.59}$$

The quarter-wave plate (QWP) introduces a phase shift of a quarter of the wavelength $\pm\pi/2$ between the components. This state transformation then reads

$$\hat{a}_H^\dagger \to (\cos^2\theta - i\sin^2\theta)\hat{a}_H^\dagger + (1+i)\cos\theta\sin\theta\hat{a}_V^\dagger \tag{2.60}$$

$$\hat{a}_V^\dagger \to (1+i)\cos\theta\sin\theta\hat{a}_H^\dagger + (\sin^2\theta - i\cos^2\theta)\hat{a}_V^\dagger \tag{2.61}$$

2.3 Quantum Cryptography

There are several compelling reasons why quantum mechanics can be highly valuable in cryptography. One notable advantage is that, unlike classical bits, information encoded in quantum states cannot be fully deterministically accessed or measured. By encoding information into quantum states, cryptography can achieve the ultimate goal of information-theoretic security, where even the most powerful adversaries cannot break the security using computational means alone.

2.3.1 No-cloning principle

The no-cloning theorem states that creating a perfect copy of two non-orthogonal quantum states with the same unitary state transformation is impossible. Or stated differently: creating a perfect copy of a quantum state prepared in an unknown basis is impossible. Detailed proof of this theorem can be found in [Nie00] but will, due to its importance, also be outlined here: We start with two states $|\psi\rangle$ and $|s\rangle$, where $|\psi\rangle$ is the state of being copied into some pure state $|s\rangle$. The initial state is then

$$|\psi\rangle \otimes |s\rangle$$

The copying machine will be some unitary transformation U; therefore, we write

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

We apply the same transformation for another state $|\phi\rangle$

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Since U must be unitary, we require that it preserves inner products, thus taking the inner product between the first and second equation from both sides, respectively, results in

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$$

We see that the equation can only hold if either $|\psi\rangle = |\phi\rangle$ or $|\psi\rangle \perp |\phi\rangle$, implying that cloning is impossible for two non-orthogonal states, or, equivalently, for unknown states in general. This means a cloning machine U can clone $|\psi\rangle = |0\rangle$ and $|\phi\rangle = |1\rangle$ but cannot for instance clone $|\psi\rangle = |0\rangle$ and $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

The implication of this theorem is intuitive: if non-orthogonal quantum states could be cloned, it would be possible to distinguish between them by performing measurements on multiple copies, leading to a loss of uncertainty. Therefore, the inability to distinguish non-orthogonal quantum states directly stems from the no-cloning theorem. Additionally, [Ori18] pointed out that [Par70] already discussed in the 1970s that the no-cloning theorem implies the absence of a single, non-disturbing measurement between spins. This implies that it is impossible to measure any information that distinguishes between two non-orthogonal quantum states without altering them, which forms the foundation for quantum cryptographic protocols and gives them an inherent advantage over classical methods.

2.3.2 State discrimination

The no-cloning theorem establishes the impossibility of perfectly distinguishing non-orthogonal states. A key aspect here is the probabilistic rather than deterministic nature of information extraction from non-orthogonal quantum states upon measurement. For instance, consider the states $|0\rangle$ and $|-\rangle$, with an overlap calculated as the inner product of their respective Hilbert space states

$$\langle 0|-\rangle = \langle 0|\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle = \frac{1}{\sqrt{2}} \tag{2.62}$$

This non-zero overlap indicates that when measuring the $|-\rangle$ state in the computational basis, denoted as M_z, we obtain equal probabilities for the classical outcomes 0 and 1

$$M_z\,|-\rangle = (|0\rangle\langle 0| + |1\rangle\langle 1|)\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle \tag{2.63}$$

In contrast, distinguishing between orthogonal states, e.g., $|0\rangle$ and $|1\rangle$, is straightforward since they can be ideally identified by projecting them onto their corresponding basis.

$$M_z\,|0\rangle = (|0\rangle\langle 0| + |1\rangle\langle 1|)\,|0\rangle = |0\rangle \tag{2.64}$$

$$M_z\,|1\rangle = (|0\rangle\langle 0| + |1\rangle\langle 1|)\,|1\rangle = |1\rangle \tag{2.65}$$

However, it is possible to discriminate between non-orthogonal states more effectively. This can be illustrated by the following example, implementing an optimized measurement operation:

In the previous section, we outlined the criteria for a set of quantum measurement operators. Conversely, any set of operators that satisfy these properties corresponds to a valid measurement. Therefore, we can mathematically search for the optimal measurement by exploring sets of measurement operators that meet the requirements, with the understanding that such a measurement is physically realizable [SMB09].

As an example, to differentiate between $|0\rangle$, $|+\rangle$, and $|1\rangle$, $|-\rangle$ states, instead of using the measurement operators $M_z = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $M_x = |+\rangle\langle +| + |-\rangle\langle -|$, we can select the measurement basis as

$$\Pi_N = -|0\rangle\langle 0| - |+\rangle\langle +| = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \tag{2.66}$$

Here, we have implemented a valid positive operator-valued measurement (POVM), where the measurement operators are defined as follows

$$\Pi_z = |0\rangle\langle 0| \tag{2.67}$$

$$\Pi_+ = |+\rangle\langle +| \tag{2.68}$$

$$\Pi_N = \mathbb{1} - \Pi_z - \Pi_+ \tag{2.69}$$

The eigenvectors of Π_N are

$$v_0 = \frac{1}{1.0823}\begin{pmatrix} -\sqrt{2}+1 \\ 1 \end{pmatrix}$$

and

$$v_1 = \frac{1}{2.6131}\begin{pmatrix} \sqrt{2}+1 \\ 1 \end{pmatrix}$$

By projecting the basis states onto these eigenstates, we achieve a state discrimination probability of 85.35%. This enhancement of state discrimination probability by optimized measurements is important when considering security aspects in cryptographic protocols. As an example, if a protocol aims to hide the classical value 0 in the states $|0\rangle, |1\rangle$ and the classical value 1 in the states $|+\rangle, |-\rangle$, by implementing the POVM measurement from above, there is an 85.35% chance of retrieving these values upon such a measurement.

2.3.3 BB84 Quantum Key Distribution

The BB84 Quantum Key Distribution (QKD) [CHB84] protocol is a fundamental cryptographic protocol for securely creating a secret digital key shared between two trusted parties. Alice prepares a string of quantum states, in which she encodes each state randomly in one of two bases, either the H/V or +/- bases. The resulting states are sent to Bob via a quantum channel, which he measures randomly. After measurement, Alice and Bob communicate over a classical channel to compare the encoding and measuring bases. They discard the states where the bases do not match and retain the matching ones. To detect possible attacks by adversaries, they can now use some of the states that were measured in the correct basis to check for inconsistencies/errors. They can discard the key if incorrect values are detected, indicating a potential third-party attack. The remaining unleaked subset will form the final key if no attack is detected.

Compared to classical methods, the quantum advantage is that an eavesdropper attack would be detected due to the no-cloning theorem since this would render the quantum states. Suppose perfect quantum states are transmitted in a QKD protocol. In that case, the cheating probability can be quantified as follows: when a third party intercepts and measures the sent states, they can replace them with different ones based on the measurement outcome. In this case, the probability of correctly measuring the outcome is $\frac{3}{4}$, but this probability decreases exponentially as the number n of measured qubits increases. Specifically, the cheating probability p_d scales as $(\frac{3}{4})^n$.

However, if imperfect quantum states are sent, such as unintentional multiphoton states instead of single photon states, the protocol's security becomes vulnerable to a different type of attack. A third party can intercept and measure the additional states in this scenario. This obvious security drawback of the protocol has prompted extensive research efforts within the community to develop alternative protocols on the theoretical side and experimentally enhance the quality of photon sources.

2.3.4 Quantum Money

The concept of quantum money arose from the inability to clone a quantum state and was one of the pioneering protocols in quantum cryptography. The protocol presented by Wiesner in the 1970s predates the formulation of the no-cloning theorem in 1982, but it already utilizes the principles outlined in the last theorem.

The protocol aims to create banknotes signed with quantum states, ensuring they cannot be copied without introducing any error. When an attempt is made to copy the banknote, the quantum states are destroyed, rendering the counterfeit banknote unusable. The protocol operates as follows: a random classical secret bitstring k^s and a secret classical key b^s containing the basis for encoding the key is generated. If $b^s = 0$, k^s is encoded using the σ_x basis, while $b^s = 1$ corresponds to encoding using the σ_y basis. Consequently, the resulting state is a tensor product state represented as $|\Psi\rangle = \bigotimes_{i=0}^{n} |\psi_i^{k,b}\rangle$, where $|\psi_i^{k,b}\rangle \in \{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$. This state is stored in a quantum memory. When a transaction is requested, the banknote containing the n quantum states is sent to the bank for verification. The bank possesses the correct key string k^s and basis string b^s to check the validity of the banknote. The bank measures the states on the banknote according to b^s and compares the outcomes with k^s. If errors are found, the bank rejects the banknote. Due to the no-cloning principle, counterfeiters cannot create a perfect copy of the banknote, making the protocol information-theoretically secure [Wie83]. It has been shown that the upper bound probability for a cheating attack, where a malicious adversary tries to create two banknotes with the same serial number from one, scales with $p_d = (\frac{3}{4})^n$ [AM12].

There are two methods for verification: classical or quantum communication. The primary drawback of quantum verification, as proposed in Wiesner's original scheme, is that quantum states can be altered when transmitted to the bank due to channel losses or noise, compromising security. As an alternative, [Gav12] introduced a scheme that employs classical communication with the bank. In this scheme, the banknote holder

receives instructions from the bank on measuring the quantum states on the banknote and reports the results back to the bank via a classical channel for verification.

2.3.5 (Quantum) Bit Commitment

Commitment schemes are protocols designed to enable one party, called the *sender* to commit to a chosen value, ensuring that the value remains unchanged while being hidden from another party, the *receiver*. These protocols involve two distinct phases: the commit and the reveal phases. A value is selected, committed to, and transmitted to the other party in the commit phase. Subsequently, in the reveal phase, the sender discloses the committed value, allowing the receiver to verify its authenticity [Wikb]. Conceptually, commitment schemes can be associated with digital equivalents of safes, where the sender *hides* a message within a locked safe and transfers it to the receiver. Once the message is locked away, the sender cannot alter it (*binding property*), and the receiver cannot access its contents until provided with the key (*hiding property*).

Achieving perfect binding and hiding simultaneously is impossible, as demonstrated both classically and quantumly [May97]. In this context, *perfect* refers to the condition where even with unlimited computational resources, modifying the value after committing or retrieving the committed value before the reveal phase is impossible. To circumvent the so-called *no-go theorem* proved by Mayers, new protocols came up incorporating space-time arguments to ensure, in principle, perfect hiding and binding commitment schemes [Ken12]. However, these schemes introduce new security schemes as they require trusting external parties or devices.

As mentioned earlier in the section on ZKPs, classical commitment schemes mostly rely on computationally secure one-way functions. I would like to delve further into this topic, elucidating how quantum mechanical commitment schemes can be employed to commit to classical bits and can achieve, in principle, information-theoretical secure hiding *or* binding, without any computational complexity arguments.

We can conceptualize a commitment scheme using quantum states as follows. The sender party can hide a value by selecting an arbitrary basis for encoding (σ_z or σ_x), that is, choosing $|0\rangle$ or $|1\rangle$ for classical value 0 and $|+\rangle$ or $|-\rangle$ for classical value 1. Hiding is accomplished because the receiving party would need knowledge of the chosen encoding basis to extract the encoded classical values *deterministically*. If the incorrect basis is chosen, utilizing the measurement operators M_z or M_x, i.e., a projective measurement onto the two bases, would yield completely random measurement outcomes. Therefore retrieving the bit information is *probabilistic*, hence the hiding of the commitment scheme is information-theoretically secure as no computational assumptions are needed. The binding property is as follows: the receiver party can request the sender party to announce the classical values encoded in the transmitted states and the encoding basis. For all states measured correctly according to the sender's announcement, the measured and encoded values must perfectly match in an honest scenario. The binding is clearly imperfect, as in 75% of the cases (50% the wrong measurement basis will be chosen and the commitment cannot be checked, plus in 50% of the other half, the commitment state can be correctly *guessed*).

This simple commitment scheme was used in a similar form in [Sal98], giving an example of a commitment scheme that does not require computational assumptions and will also be the basis for the zero-knowledge protocol as explained in more detail in the next chapter.

3 State of the Art

The following chapter outlines important related work in quantum-proof systems, especially ZKP systems.

3.1 (Quantum) interactive proof systems

As pointed out in 2.1.2, interactive proof systems are models where computations are performed by letting two parties, a prover and a verifier, interact and exchange messages. All interactive proof systems are subject to completeness and soundness requirements. Different complexity classes emerge according to bounds on completeness, soundness, the number of messages exchanged, and the computational power of the interacting parties. The complexity class QMA is defined as the set of languages for which a polynomial-size quantum proof (a quantum state) exists for every string in the language that convinces a polynomial-time quantum verifier that the string is within the language with high probability. Moreover, the verifier will reject any proof with high probability when the string is not in the language [Wikf].

Studying interactive proof systems for the complexity class QMA, some previous work demonstrated a quantum advantage in verifying NP-complete problems regarding the witness size of the proof necessary to convince a polynomial-time verifier with high soundness of the statement's validity. The advantage was achieved via encoding the witness into quantum states and letting the prover and verifier interact quantumly. The initial work on this was done by [ABD$^+$09], who demonstrated an efficient proof protocol that can convince a verifier with constant soundness of the satisfiability of 3SAT, an NP-complete problem, given $O(\sqrt{n})$ witnesses, each encoded as $O(\log n)$ qubits, with n being the size of the input instance. The shown advantage is that while quantumly, the verification time for a witness of this size is linear in the input size, classically, it would still take exponential time, rendering a proof system of this form impossible. The protocol construction relies on the PCP theorem. Building on this, [ADK18] explored the theoretical aspects of transferring the idea to a quantum optical experimental setup. Both [ADK18] and [ABD$^+$09] employed witness encoding using spatial mode superposition states. However, the experimental feasibility becomes challenging as the witness size increases. [CKDK21] addressed this issue, resolved the experimental constraints by mapping the protocol to coherent states in a sequence of time modes, and gave a first experimental demonstration of the QMA proof system, showing that soundness and completeness hold in the practical implementation.

These earlier studies inspired our protocol design. We used similar reasoning to establish the properties of the *completeness* and *soundness* since our work also involves a PCP

SAT problem.

3.2 First work on ZKPs

ZKPs were first introduced in [GMR85] and have become a fundamental cryptographic resource. As described in [GMR85], the initial versions of zero-knowledge protocols relied on the quadratic residuosity and non-residuosity problems.

Furthermore, it was shown by [GMW91] that every language in NP has an interactive ZKP protocol (under reasonable hardness assumptions), which means that $NP \subseteq CZK$, where CZK stands for computational zero-knowledge. Another variant is SZK, which stands for statistical zero-knowledge. Generally, statistical zero-knowledge refers to an interactive proof system where an arbitrary malicious verifier cannot learn if an instance is a Yes-instance except for extracting negligible amounts of information. The computational variant provides the same guarantee for malicious polynomial-time verifiers, [VZ09, page 2]. The former is considered more secure than the latter.

3.3 Security analysis via simulator

To analyze the zero-knowledge property of a proof system, which determines the amount of information an arbitrary verifier can gain from the interaction with the prover, the simulator method is commonly employed [Mas21]. The simulation paradigm involves a *real/ideal* world approach, where the ideal world is the simulation itself. In the ideal world, the verifier does not need to check any witness statement for correctness, as they can trust a third party to report whether the witness is valid. In such a simulation protocol, a simulator acts as a prover without the witness as input, engaging in the proof protocol with an arbitrary verifier. The simulation can be rewound to a previous step if it fails, i.e., if the verifier gives an unwanted answer. An encryption scheme is deemed secure if its transcript output distribution is indistinguishable from the simulation transcript output distribution [Mas21]. For more details on simulators, refer to [Lin17].

Proving security for zero-knowledge protocols against quantum verifiers is not straightforward since the traditional rewinding technique, which allows a simulator to go backward steps in the protocol to handle unwanted answers or outputs from the verifier, cannot be directly applied in the quantum setting. This is due to the inherent nature of quantum states, where copying them is impossible, and measurements lead to alterations in the state. This means a simulator cannot make copies of the verifier's input or perform measurements to determine the success of a simulation, which is necessary if the zero-knowledge property of a protocol is argued with the rewinding argument [Wat09]. This fundamental difficulty was initially observed by [VDG98], and it has long been perceived as challenging to introduce QZKP protocols or provide security proofs against quantum verifiers.

However, the challenge was successfully addressed by [Wat09] by introducing a quantum rewinding technique. The quantum rewinding technique relies on an amplitude amplification lemma, which states that the probability of constructing a quantum circuit Q

that outputs a state that has high fidelity to a state of a successful simulation is almost independent of an auxiliary state $|\psi\rangle$ that is input to the circuit. This implies that the success probability of the simulator is nearly independent of the auxiliary input of a malicious verifier, enabling the simulator to produce the desired view of the simulation *independently*.

The significance of this technique lies in its ability to address the challenge posed by intermediate measurements, which can alter the quantum state and potentially compromise the success of future executions of the simulator algorithm [AB19]. When proving zero-knowledge, considering additional auxiliary input information incorporates the possibility that the verifier can access some outside information. This could be the case when the protocol is run as part of a larger subroutine. A proof protocol that is auxiliary input zero-knowledge shows that a protocol is closed under composition, i.e., an earlier execution of the proof system does not influence the security of the zero-knowledge protocol in later executions [GO94].

3.4 Post-quantum ZKP for NP

With Watrous' work enabling the implementation of the simulator technique for a wider range of zero-knowledge protocols in the quantum setting, considerable efforts have been dedicated to developing *post-quantum* ZKP protocols and reevaluating existing classical protocols to ensure their security against quantum verifiers. Although the computational difficulty of certain problems, like factoring and discrete logarithm computations, becomes compromised by quantum computers, rendering cryptographic schemes built upon these problems insecure, there are alternative candidates. For instance, the Learning with Error assumption (LWE) or Quantum Learning with Error assumption (QLWE) are considered potential contenders that could maintain post-quantum computational security [Mas21]. Building post-quantum ZKP protocols often involves adopting commitment schemes based on assumed quantum-secure functions.

For instance, in [Wat09] and [Adc02], quantum computationally concealing commitment schemes were defined under the assumption of quantum computationally concealing one-way functions.

Utilizing quantum rewinding, [Wat09] furthermore demonstrated statistical zero-knowledge of the *Goldreich-Micali-Wigderson Graph Isomorphism* and computational zero-knowledge of the *Goldreich–Micali–Wigderson 3-coloring* proof systems against arbitrary quantum verifiers, assuming post-quantum one-way functions. This result extends to all NP languages due to the NP-completeness of Graph 3-coloring.

Continuing this direction, [BS20] introduced a post-quantum ZKP *argument* protocol for NP with constant rounds. Their scheme relies on the existence of quantum fully-homomorphic encryption and employs non-black-box simulation to achieve computational soundness. Argument protocols offer weaker soundness guarantees, being secure only against computationally bounded provers.

An improvement was presented by [Chi21], who proposed a quantum-secure constant round interactive ϵ-*ZKP* for NP, incorporating black-box techniques and showed that it

is statistically sound under the assumption of collapsing hash functions. The construction of the protocol builds on the Golderich-Kahan protocol, a Σ - protocol in which the verifier is forced to commit to its challenges in advance. Their commitment scheme relies on the assumption of QLWE. *ϵ-zero-knowledge* only requires indistinguishability within an accuracy parameter ϵ [DNS98]. This is in contrast to perfect zero-knowledge, where a simulator can produce a perfectly indistinguishable view of the interaction between a malicious quantum verifier and a prover. Further, the notion of black-box zero-knowledge involves proving security with a universal simulator with access to *all* possible strategies a malicious verifier might employ [DNS98], i.e., there is one simulator for all verifiers. In contrast, non-black-box zero-knowledge only requires the construction of a simulator for all verifiers, which means there can be one simulator per verifier. In this sense, the notion of black-box zero-knowledge in the literature is stronger than non-black-box zero-knowledge.

In the same work, [Chi21] also presented a constant round interactive ϵ-zero-knowledge *argument* for NP that is both *black-box* and *computationally sound*. This scheme is based on Blum's Graph Hamiltonicity protocol, a Σ - protocol that utilizes a commitment scheme built upon the assumption of post-quantum one-way functions.

Notably, constant round black-box zero-knowledge for NP, secure against quantum attacks, is impossible unless $NP \subseteq BQP$ [CCLY22]. This implies that one of the security parameters must be relaxed, i.e., either using non-black-box schemes or the zero-knowledge property needs to be relaxed to ϵ-zero-knowledge instead of perfect zero-knowledge.

Finally, the work of [Mas21] offers a collection of classical protocols secure against malicious quantum adversaries based on QLWE, one-way functions, or other post-quantum assumptions.

The above approaches face a challenge in proving the security of schemes based on quantum computational one-way functions, as new quantum algorithms like Shor's could potentially compromise their security. Hence, there is a need for research into alternative commitment schemes.

3.5 ZKP for QMA

Besides work on post-quantum ZKPs for languages in the class NP, progress has also been made in studying ZKPs for languages in the quantum complexity class QMA, the quantum analog of NP. A significant contribution in this area was made by [AB20]. Their work demonstrated that, assuming the existence of a quantum computationally concealing and unconditionally binding commitment scheme, QMA is contained within the class $QCZK$ (quantum computational zero-knowledge). As a result, every problem in QMA now admits a quantum computational zero-knowledge interactive proof system. The quantum ZKP protocol in [AB20] is constructed around the QMA-complete *k-local Hamiltonian* problem. The *k-local Hamiltonian problem* aims to determine if the minimum eigenvalue of an n-qubit Hamiltonian $H = \sum_j H_j$, where each H_j acts nontrivially on only k out of the n qubits, is below a certain threshold. The solutions to this problem are quantum states, unlike the previous protocol problems, which had classical solutions. The protocol follows a Σ-structure, and the first message sent is the encoded witness

and a commitment to the information necessary to reverse the encoding and check the witness validity. Notably, the commitment to the quantum witness is purely classical and assumed to be perfectly binding and computationally concealing.

[VZ09] provided a zero-knowledge *argument* protocol for the QMA language, specifically the 2-local XZ Hamiltonian problem. The encoding scheme is similar to the one presented in [AB20], and a perfectly binding, quantum computationally concealing commitment protocol is assumed for committing to the quantum witness ρ of the 2-local Hamiltonian problem.

Additionally, [AB22] presented a protocol for QMA that serves as a computational ZKP system. The protocol follows a Σ - structure, with the key distinction to the above work that the commitment to the quantum solution state is done via a quantum one-time pad. The underlying problem is drawn from the complexity class k-SimQMA. Under the assumption that the commitment scheme is unconditionally binding and computationally hiding, the protocol is a computational *ZKP system* for QMA. The *completeness* and *soundness* properties follow trivially from the conditions on the commitment scheme, and zero-knowledge is shown via the rewinding technique [Wat09].

3.6 Integration into the existing body of literature

The contributions of this thesis can be contextualized within the existing body of research as follows: the developed protocol establishes a ZKP system, demonstrating both *completeness* and *soundness* properties in the experimentally ideal case, thereby proving its security against malicious quantum provers. Additionally, the security of the commitment scheme against a malicious verifier is founded on the notion that the quantum state received by the verifier resists transformation into a state that yields more information. These optimal state transformations, i.e., the most advantageous strategies for a malicious verifier and prover to cheat, are derived via semi-definite programming. This analysis establishes that the protocol's commitment scheme is perfectly binding, as the soundness can be approached arbitrarily close to zero. However, as we discuss later, achieving perfect binding comes at the cost of revealing additional information about the witness classically. Therefore, although the proof state remains securely hidden from an information-theoretical perspective employing the method of conjugate coding, the overall scheme can be considered quantum-computationally hiding.

In this sense, our commitment scheme deviates from prior schemes that rely on cryptographic assumptions, such as the Learning with Errors assumption or post-quantum fully homomorphic encryption, therefore establishing security by combining cryptographic constructions that rely on these primitives [AB22]. Our approach, however, is not based on one-way functions but rather ensures that information about the witness is information-theoretically concealed in the message state, even though in later steps of the commitment scheme some classical information leakage is necessary to guarantee perfect binding. The precise amount of information leakage will be explored in subsequent sections.

For the conclusive establishment of security, the next steps after this work involve delineating a simulator protocol, showing that our protocol indeed upholds the zero-

knowledge property, wherein a simulator's output remains indistinguishable from real protocol outputs.

An intriguing insight is that our protocol, through relaxing the zero-knowledge requirement, which means divulging minimal information that offers no meaningful computational advantage in solving the underlying NP problem, achieves a post-quantum protocol where when values of *completeness* and *soundness* are fixed, the required rounds are constant in the chosen problem size. As outlined in more detail in the next chapters, the number of rounds is equivalent to the amount of revealed information. Therefore, we get a protocol where the revealed information is also constant. Assuming the simulator construction supports this, zero-knowledge holds in the limit of the input instance size being much larger than the revealed information. This represents an enhancement compared to the leaked information regarding the quantum witness in the work of [ABD$^+$09], [ADK18] and [CKDK21] where the disclosed information increases proportionally with the input instance's size. It is important to point out that this statement is only true for the experimentally ideal case. The revealed information during the protocol might change when including parameters like losses and noise, as discussed later in section 6.2.2.

4 Quantum ZKP protocol

In this chapter, we will present one of the main findings of my thesis, which focuses on developing a quantum ZKP protocol. Chapter 5 outlines the security analysis of the protocol in the experimentally ideal case using semi-definite programs. We will begin by summarizing the protocol and formally describing the protocol steps. Later, we will describe the main points in more detail and specifically elaborate on the *completeness* property of the protocol.

The core problem for constructing the ZKP is a 2-out-of-4 SAT problem instance with n variables and y clauses shared between P and V. The fact that SAT problems belong to the complexity class of NP-complete is advantageous for two reasons. Firstly, it provides a security condition where the verifier can deduce that if they are convinced the prover possesses the solution to the shared problem, then the prover must know the solution, as brute-forcing a solution would require a worst-case computational effort of $O(k^n)$. Secondly, it renders the protocol applicable to a wide range of problems, as every problem in NP can be mapped (reduced) to an SAT problem with a polynomial-time overhead at most. The parameters of *completeness* $P_C \sim 1$ and *soundness* $P_S \sim 0$ are known and agreed upon by both parties in advance. An honest prover possesses a satisfying assignment, denoted as $x \in \{0,1\}^n$, which makes the shared instance evaluate to true. The goal of the protocol is for the verifier to be convinced by an honest prover, with high P_C, that the prover provides a satisfying assignment without gaining any additional information other than the truth of the statement. Conversely, if a dishonest prover provides an invalid solution, it should be accepted with, at most, P_S probability.

The prover encodes each classical solution bit into the basis information of a quantum state, as detailed in the *quantum encoding* section 4.1.2. After the encoding, the prover sends all n states to the verifier through a quantum channel. This thesis assumes ideal experimental conditions with a *perfect lossless channel*. Upon receiving the states, the verifier measures them in a random basis, following the explanation provided in the *quantum measurement* section 4.1.3. The verifier keeps track of which states were measured in which basis and records the measurement outcomes. Once all states are measured, the verifier sends a challenge to the prover, picking one or several clauses at random. This step is explained in the section *classical verification* 4.1.4. The number of how many clauses are allowed to be challenged is determined by the protocol parameters P_C and P_S. After checking the satisfiability of *at least* one clause, the verifier accepts or rejects the proof based on whether the clause was satisfiable or not.

We will now give a more formal description of the given intuition:

4.1 Protocol Overview

4.1.1 Quantum secure ZKP system for NP-complete problem

Let L be the language of 2-out-of-4 SAT problems for which a satisfying variable assignment exists, and let $\Sigma = \{0, 1\}$. Given a boolean formula ϕ, where ϕ has y clauses containing n variables. We require the promise that ϕ is a PCP instance. ϕ is given as a common input to the prover P and the verifier V. P wants to convince V that $\phi \in L$. It could do so by sending the witness, i.e., the variable assignment $x \in \Sigma^*$, such that $\phi(x) = \mathit{True}$, i.e., the assignment makes the formula evaluate to a logical *True*. But since we are in the zero-knowledge setting, P wants to convince V of the statement *without* revealing information about the witness x. The steps of the protocol to perform this task are the following:

1. $P \rightarrow V$: P encodes the witness x with $|x| = n$, according to the function commit(x_a, s_a) for a = 1,..., n and a secret random binary string $s \in \Sigma^*$ with $|s| = n$.
   The function is of the form

$$\text{commit}(x_a, s_a) = \begin{cases} |0\rangle & \text{if } x_a = 0 \text{ and } s_a = 0 \\ |1\rangle & \text{if } x_a = 0 \text{ and } s_a = 1 \\ |+\rangle & \text{if } x_a = 1 \text{ and } s_a = 0 \\ |-\rangle & \text{if } x_a = 1 \text{ and } s_a = 1 \end{cases} \tag{4.1}$$

   This results in the global state $|\Psi\rangle = \bigotimes_{a=0}^{n} |\psi_a\rangle$ where $|\psi_a\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. This is a tensor product of n quantum states. P sends the state $|\Psi\rangle$ to V and stores the random string s secretly.

2. $V \rightarrow P$: V measures each $|\psi_a\rangle$ in a random basis $\sigma \in \{\sigma_z, \sigma_x\}$. We denote the randomness of the chosen measurement basis as the string $m \in \Sigma^*$ with $|m| = n$ and $m_a = 0$ for measurement basis σ_z, as well as $m_a = 1$ for measurement basis σ_x. V secretly stores the measurement outcomes $u = (u_1, ..., u_n)$ for all the n states and the binary random string m.
   Then V chooses a clause c_r out of the $\{c_1, ..., c_y\}$ clauses for a random $r \in \{0, ..., y\}$ and sends the value r as a challenge to the prover.

3. $P \rightarrow V$: We denote the variables contained in the challenged clause c_r as $\{x_i, x_j, x_k, x_l\}$ for some indices $\{i, j, k, l\}$. P answers to the challenge by:

   (i) sending the values $\{s_i, s_j, s_k, s_l\}$, i.e., the values of the secret string s having the same indices as the variables in the challenged clause ($\{s_i, s_j, s_k, s_l\}$ are the commitment variables for the clause c_r, i.e. the measurement outcomes when the correct basis was chosen).

(ii) sending the values $\{x_i, x_j, x_k, x_l\}$, i.e., the four variable values of the witness that are contained in clause c_r (these correspond to the encoding bases).

4. After this step, the verifier checks the responses of the prover. For each of the four variables it received for the challenged clause c_r, there are two possible proceedings in the protocol. V starts the process with indices i for example and repeats the *same* process for the remaining indices $\{j, k, l\}$ of the challenged clause:
   - If $x_i = m_i$, i.e., the encoding basis matches the measurement basis, V continues to check whether $u_i = s_i$, i.e., if the measurement outcome matches the sent commitment. The verifier aborts the protocol if the last equality does not hold since this would imply a cheating prover. Otherwise, it stores the value x_i to later check if the challenged clause is satisfied.
   - If $x_i \neq m_i$, i.e., the encoding basis does not match the measurement basis, V cannot check the commitment for this value, since it must expect that the measurement gave a random outcome. But it can still use the value x_i to check whether the challenged clause is satisfied.
5. If V did not abort in step 4, it continues to check if the received variables $\{x_i, x_j, x_k, x_l\}$ do satisfy the clause c_r.
6. Repeat step 3 - step 5 t times until the desired values of P_C and P_S are reached.

We can summarize the inputs to P and V as follows:

Input to Prover

- Common shared input instance ϕ
- A quantum-computationally hiding and perfectly binding commitment scheme with non-zero cheating probability
- Variable assignment $x = (x_1, ..., x_n)$
- Random bit string $s = (s_1, ..., s_n)$, denoting the measurement outcomes of a correct measurement

Input to Verifier

- Common shared input instance ϕ
- A quantum-computationally hiding and perfectly binding commitment scheme with non-zero cheating probability
- Random bit string $m = (m_1, ..., m_n)$, denoting the chosen measurement basis
- Random value r denoting the challenged clause

Prover

Common input

2-out-of-4 SAT instance

Verifier

Encoding

Witness: **x** = (x_1,..., x_n)

Random bit string: **s** = (s_1,..., s_n)

x = (x_1,..., x_n)

s = (s_1,..., s_n)

commit $\Psi = (\Psi_1 \otimes, ..., \otimes \Psi_n)$

Measurement

Random bit string: **m** = (m_1,..., m_n)

Measures: $\Psi = (\Psi_1 \otimes, ..., \otimes \Psi_n)$

Stores outcomes: **u** = (u_1,..., u_n)

clause c_r

Challenge

Random clause c_r

Response

Send: c_r = {x_i, x_j, x_k, x_l}

Send: {m_i, m_j, m_k, m_l}

Response

Verification

for z in {i, j, k, l}:

If $m_z = x_z$

If $u_z = s_z$

→ *store* x_z

If $u_z = s_z$

→ *abort*

If $m_z = x_z$

store x_z

Commitment function hides the witness information theoretically

Commitment values can be checked when box is opened

The proof that prover knows the witness:
Bases announcement is the key and the proof simultaneously

We still have to answer how many rounds are required to reach the desired probabilities P_C and P_S. This directly corresponds to the number of clauses that a verifier is allowed to challenge. The rest of the chapter will continue to explain the protocol steps in more detail and elaborate on the *completeness* 4.2 property, which will also give a first constant t_c for the number of challenged clauses required such that the desired probability P_C is reached.

In the next chapter that concerns the security proof, we will quantify *soundness* 5.1 and *security of the commitment scheme* 5.3 with the help of semi-definite programs, which will then give the second constant t_s for the number of clauses required such that the desired probability P_S is reached. Together, t_c and t_s will give the total number of challenged clauses t required in the protocol. We will now elaborate in more detail on the following important protocol steps:

4.1.2 Quantum Encoding

The first step involves the prover, who possesses a bitstring $x \in \Sigma^*$ over an alphabet $\Sigma = \{0, 1\}$ with length $|x| = n$. In the honest case, x is a satisfying variable assignment to the instance ϕ such that $\phi(x) = \text{True}$.

The goal of the protocol is to convince V that $\phi(x) = \text{True}$, i.e., $\phi \in L$ which can be verified given an assignment x in polynomial-time since ϕ is in NP-complete. x is the secret information and the proof is done by letting V interact with P according to the protocol. When P is honest, V should accept with very high probability P_C. Conversely, if a dishonest prover P^* provides an invalid solution or deviates from the protocol, it should be accepted with, at most, probability P_S. An honest P encodes the bit values of the witness as follows: it generates a random bit string that we call s, having equal length as the witness. It then prepares a string of quantum states according to the *commit* function. *Commit* takes as input the variable pair (x_a, s_a) for the string indices $a = 1, ..., n$, i.e., we apply it on each of the n variables in x and s with the same indices individually. The scheme is as follows:

- if $x_a = 0$ and $s_a = 0$, P prepares the state $|0\rangle$ in the z-basis
- if $x_a = 0$ and $s_a = 1$, P prepares the state $|1\rangle$ in the z-basis
- if $x_a = 1$ and $s_a = 0$, P prepares the state $|+\rangle$ in the x-basis
- if $x_a = 1$ and $s_a = 1$, P prepares the state $|-\rangle$ in the x-basis

Note that each state is prepared individually, so the resulting global state is a n-qubit product state. As an example for $n = 5$, for a bitstring $x = (01001)$, and random string $s = (00110)$ the resulting global quantum state would be:

$$|\Psi\rangle = |0\rangle \otimes |+\rangle \otimes |1\rangle \otimes |1\rangle \otimes |+\rangle$$

P stores s secretly, since it will be later used for the verification. The resulting quantum state is then sent to the verifier through a quantum channel. The analysis in this thesis is done for the ideal case, so we assume a perfect, lossless channel.

4.1.3 Quantum Measurement

Upon receiving the states, the verifier individually measures each state $|\psi_a\rangle$. For this, it also generates a random bit string m, having equal length to the witness. Note that the instance ϕ is known by V, and the length of the witness is just the number of unique variables within the instance. It then measures the states according to the scheme:

For $a = 1, ..., n$:

- if $m_a = 0$, V measures the a-th state in the z-basis, i.e., applies the operator σ_z
- if $m_a = 1$, V measures the a-th state in the x-basis i.e., applies the operator σ_x

V secretly stores the bit string m, and the measurement outcomes $u = (u_1, ..., u_n)$. With this measurement strategy, the encoding basis will match the measurement basis in 50% of the time. Since $z-$ and x- bases are orthogonal to each other, a measurement in the *wrong* basis will yield totally random outcomes, whereas a measurement in the *correct* basis will yield deterministic outcomes, i.e., the measurement results match the states P has encoded. Formally, we can write this as follows:

- if $m_a = x_a$, V will get deterministic outcomes
- if $m_a \neq x_a$, V will get random outcomes

It is important to note that the measurement outcome, even when the state is measured in the correct basis, does not reveal any information about the solution bit value, as the prover randomly chooses the actual state. The state or the measurement outcome instead serves the protocol as a *binding* property, allowing the verifier to check whether the prover later announces indeed the values he or she has *committed to* in the first place.

The only way to obtain information about the solution values is through basis discrimination. The success of a basis discrimination attack will be analyzed in section 5.3. At this point, both, P and V are unaware of which states were measured correctly or incorrectly.

4.1.4 Classical Verification

Once all the states are measured, V picks a clause c_r at random. Let's denote the variables contained in c_r as $\{x_i, x_j, x_k, x_l\}$ with indices $\{i, j, k, l\}$. V then sends r as a challenge to P. P answers by sending back the solution values for the challenged clause, i.e. the values $\{x_i, x_j, x_k, x_l\}$ and the additional information about the initially encoded states, i.e., the values $\{s_i, s_j, s_k, s_l\}$, for the states contained in clause c_r. This is the *reveal phase*, where P opens the commitment. V can then do the verification for each $\{i, j, k, l\}$:

```
for z in {i, j, k, l} do
    if m_z = x_z then
        if u_z = s_z then
            store x_z Note: Here honest commitment could be checked
        else
            Break
        end
    else
        store x_z Note: Here honest commitment could not be checked
    end
end
```

We will explain the algorithm step-by-step:
V runs the process for all of the four received values of the challenged clause. *Line 2* describes the process of checking whether the encoding basis, which can be read from the solution value x_z for some $z \in \{i, j, k, l\}$, matches V's measurement basis m_z. If this is the case, V continues to check whether the commitment value s_z matches with its measurement result u_z (*line 3*). If this is the case, i.e., $u_z = s_z$ is satisfied, the solution value x_z is stored for later verifying the challenged clause c_r. If V detects inconsistencies at this step, it aborts, since in this case cheating behavior from the prover side has to be assumed. If, however, in *line 2*, V could see that encoding and measurement basis do not match, it cannot check the commitment but stores the value x_z for later checking the clause.

4.2 Completeness

We are now ready to analyze the *completeness* of the protocol. In order for V to assess whether the proof effectively meets the input instance, it must be capable of confirming *at least one clause*. Despite being in the perfectly honest scenario, we impose a verification condition on V, mandating it to verify at least one clause with variables for which the *honest commitment* in *line 3* of the algorithm could be checked. This condition implies that at least in one clause, all four variables must have been measured *in the same basis as they were encoded*. We know that the probability that $m_a = x_a$, i.e. measurement and encoding basis match, is $\frac{1}{2}$. Therefore, there is a $\frac{1}{16}$ chance that all four variables within one clause, were measured correctly. So the *completeness* P_C, if we would allow V to only challenge one clause, would be $\frac{1}{16}$. Since we want P_C, in general, to be as high as possible, i.e., the probability the protocol succeeds in a run is high, we can fix a desired value for P_C and then calculate from this the number of clauses t_c that must be revealed to V to achieve this probability. Thus, we have:

$$P_{\mathrm{C}}(t_c) = 1 - \left(\frac{15}{16}\right)^{t_c} \tag{4.2}$$

where we require $y > t_c$, i.e., the number of total clauses must be much higher than the number of revealed clauses. A very important point to outline here is the fact that

once P_C is fixed, the number of *revealed clauses* during the protocol is constant. Together with the second parameter t_s which is the number of clauses revealed to ensure the *soundness* of the protocol, we will see that the total number of *revealed clauses* is $O(1)$, i.e., is independent of the input size of the instance, without having to compromise on the protocol parameter. This is a very appealing property of the protocol, which we will work out in more detail in section 5.5.

5 Security analysis for the ideal protocol

In this section, we will examine potential cheating strategies that dishonest parties may employ to gain an advantage in the protocol. More generally, we will use semi-definite programs to quantify optimal attacks on the state of the commitment scheme and in terms of the *soundness* property of the protocol. We will heuristically derive possible cheating strategies for the prover and the verifier and will formalize and utilize semi-definite programs to calculate the probability of these attacks and to show that they are optimal.

The motivation behind employing semi-definite programs stems from the fact that semi-definite programs optimize over positive semi-definite matrices, as explained in section 2.1.7. When applying this method for security analysis, we seek the optimal quantum state maps that a party can prepare for a given state, considering the objective function as the cheating strategy. The Choi-Jamiolkowski isomorphism enables us to represent quantum maps as states (positive semi-definite matrices), hence to utilize SDPs for optimization. Additionally, the transformation must be completely positive and trace-preserving (CPTP) to ensure physical feasibility. This can be achieved by imposing the appropriate constraints on the problem, which directly follows from the Choi-Jamiolkowski isomorphism.

5.1 Soundness (P* , V)

The soundness of the protocol refers to the probability that, when the prover is dishonest (P^*) and deviates from the protocol, the verifier is unlikely to accept the proof.

To quantify the soundness, we need to consider the different strategies the prover could use to cheat. The first scenario, in which a wrong proof could get accepted is when V challenges clauses that are still satisfied by a solution assignment x, although the instance is a No-instance. Given the promise the instance is a PCP-instance, we know from the PCP theorem that there are at least a fraction of δ clauses that are unsatisfied, which means that a fraction of $(1-\delta)$ clauses are at most satisfied when such a wrong proof is sent. Therefore the probability that a wrong proof is accepted in this case is

$$p_{cheat1} = (1-\delta) \tag{5.1}$$

When the number t_s of clauses that are challenged grows, the probability will decrease to $(1-\delta)^{t_s}$.

Another possible cheating strategy is *decommiting*. Decommiting here means changing the solution value of the i-th variable corresponding to the encoding basis, denoted with x_i in the protocol description in the previous section. This can be done perfectly when the commitment values stored in s_i, i.e., the expected measurement results when a *correct*

measurement is performed cannot be checked by V. This is the case for $m_i \neq x_i$, i.e., when the measurement basis does not match the encoding basis.

A cheating strategy could, therefore, be that P^* announces the encoding basis x_i for some variable for that they wish to change the bit value, hoping that V measured the i-th state in the *opposite* basis. If this is the case, whatever value P^* announces as the commitment value s_i, V will not be able to check it, and therefore, this cheating attempt will not be detected. If V measured the i-th-state in the *same* bases as P^* announced, the probability that V's measurement outcome matches the randomly guessed announcement of P is still 50%. This means P^* can successfully cheat on 75% of the states they try this attack on. Recalling the PCP-theorem, we notice that in the worst case, P^* only needs to perform this attack on a fraction δ of all y clauses since this is the fraction of clauses that is at least unsatisfied by the sent solution assignment x. The other $(1-\delta)$ clauses would be still satisfied in this case and no cheating attempt has to be made. Recalling that in our 2-out-4 SAT problem each clause contains four variables, in the worst case a cheating P^* only has to manipulate one variable in a clause, such that it will be satisfied. Therefore this new cheating strategy would have a success probability of

$$p_{cheat2} = (1-\delta) + \delta \cdot 0.75 \tag{5.2}$$

In the above scenarios, we assumed that P^* was sending honest states, i.e. a $|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. If P sends honest states, the best they can do is guess the measurement outcomes, and the success probability of this strategy is p_{cheat2}. We consider the case for the last cheating strategy, where the prover sends an *optimized state*. To see how an optimal state for P^* could look, we need to consider how the optimal cheating attack could be done. The best way to change the bit values of the witness x is if P^* could know V's obtained measurement results u. In this case, it could respond to the challenge by announcing the commitment value to be the same as V's measurement outcomes and could arbitrarily change the values of x. We now want to evaluate, how the cheating probability increases, if we instead of the honest states, send some optimized state ρ. Since we cannot know which measurement basis V will choose, we want the enhance the probability of getting a certain measurement outcome for that optimized state, independent of the chosen measurement basis. The expectation value of projecting ρ onto the state $|0\rangle$ and therefore getting measurement outcome zero is written as $\mathrm{Tr}(\rho\pi_{0z})$, with $\pi_{0z} = |0\rangle\langle 0|$, and the expectation value of getting the same measurement outcome when ρ is measured in the orthogonal basis is $\mathrm{Tr}(\rho\pi_{0x})$ with $\pi_{0x} = \frac{1}{2}(|0\rangle + |1\rangle) \cdot (\langle 0| + \langle 1|)$. In this sense, we can write the problem of finding an optimal state ρ_0, such that the probability of getting measurement outcome 0 is maximal, independently of the chosen basis on which it is projected as

$$\max \mathrm{Tr}(\frac{1}{2}\rho_0(\pi_{0z} + \pi_{0x})) \tag{5.3}$$

And equivalently for a state ρ_1 that maximizes the probability of getting a measurement outcome 1 in both bases with $\pi_{1z} = |1\rangle\langle 1|$ and $\pi_{1x} = \frac{1}{2}(|0\rangle - |1\rangle) \cdot (\langle 0| - \langle 1|)$. To find the optimal ρ_0 and ρ_1, which gives the maximum probability of measurement outcome 0 and

1 respectively in both bases, we used the following semi-definite programs

Primal Problem a:
$$max \text{ Tr } (\tfrac{1}{2}\rho_0(\pi_{0z} + \pi_{0x}))$$
$$\text{s.t. } \rho_0 \geq 0$$
$$\text{Tr}(\rho_0) = 1$$

Primal Problem b:
$$max \text{ Tr } (\tfrac{1}{2}\rho_1(\pi_{1z} + \pi_{1x}))$$
$$\text{s.t. } \rho_1 \geq 0$$
$$\text{Tr}(\rho_1) = 1$$

The constraints $\rho \geq 0$ and $\text{Tr}(\rho) = 1$ ensure that the variables are indeed valid quantum states. The optimal primal value is found to be 85.36% for both states. The states ρ_0 and ρ_1 that maximize the cheating probability of the prover respectively are:

$$\rho_0 = \begin{pmatrix} 0.8536 & 0.3536 \\ 0.3536 & 0.1464 \end{pmatrix} \tag{5.4}$$

and

$$\rho_1 = \begin{pmatrix} 0.1464 & -0.3536 \\ -0.3536 & 0.8536 \end{pmatrix} \tag{5.5}$$

To demonstrate that this bound is tight, we need to show that the dual problem yields the same optimal success probability for the attack. The dual problem is as follows:

Dual Problem a:
$$min \text{ Tr } (Y_0)$$
$$\text{s.t. } Y_0 \otimes \mathbb{1}_{\mathcal{H}_2} \geq \tfrac{1}{2}(\pi_{0z} + \pi_{0x})$$

Dual Problem b:
$$min \text{ Tr } (Y_1)$$
$$\text{s.t. } Y_1 \otimes \mathbb{1}_{\mathcal{H}_2} \geq \tfrac{1}{2}(\pi_{1z} + \pi_{1x})$$

For the derivation of the dual problem we used the relation

$$Tr^*(Y) = Y\mathbb{1}$$

for all $Y \in \mathbb{C}$. By sending an optimized state ρ, P^* maximizes the probability that V obtains a particular measurement outcome, regardless of the basis used for measurement. This result implies, that out of all the states sent by P^*, 85.36% can be manipulated in a way that when the verifier asks for the bases and corresponding states (measurement outcomes), the prover can announce a random basis and avoid being caught by also

announcing the corresponding measurement outcome correctly. This is an enhancement to before, where the cheating success probability by sending honest states was 75%. When we again consider that the attack only has to be performed on a fraction δ of clauses and assume that in the worst case, P^* only needs to cheat on one variable in the clause, we obtain the new cheating probability as

$$p_{cheat3} = (1 - \delta) + \delta \cdot 0.8536 \tag{5.6}$$

We are concerned about the *optimal, worst case* cheating probability of a dishonest party, that is why in the following we will only use this last probability p_{cheat3}.

We will now derive the *soundness* property from p_{cheat3}. Recall that soundness is the probability that a wrong proof will be accepted. Since the protocol is aborted from the verifier's side, when inconsistencies in the announcement of the commitment values are detected, a wrong proof will be accepted only if *all* of the challenged states can be correctly announced by P^*. If a total of t_s clauses are challenged, on average $\mu = t_s \cdot p_{cheat3}$ can be successfully manipulated by P^*, but for the remaining ones, the cheating attempt would fail and be detected when V is checking the commitment values in step 4 of the protocol. μ is the theoretical expectation value. We can use the Chernoff bound (see also 2.1.8) to calculate the probability of deviating from this expected value μ. This will then give us the *soundness* of the protocol as the probability that a dishonest party can manipulate *more* than this expected number of states and will, therefore, succeed in making V accept a wrong proof.

The binary random variable X has the two possible outcomes: successful cheating ($p_{cheat3} = (1 - \delta) + \delta \cdot 0.8536$) or unsuccessful cheating (1 - p_{cheat3}). For binding the probability that the value of the random variable X is close to its expected value μ, we use the expression for the *upper bound*, introduced in 2.1.8:

$$P_S(X \geq (1 + \epsilon)t_s \cdot p_{cheat3}) \leq e^{-\frac{\epsilon^2}{2+\epsilon} t_s \cdot p_{cheat3}} \tag{5.7}$$

As the number of checked clauses t_s increases, the probability of X deviating more than ϵ from its expected value μ becomes small. In other words, by choosing a sufficiently large t_s, the probability that a dishonest prover successfully cheats on more than p_{cheat3} of the total t_s clauses decreases exponentially. We can use the same strategy as we did for the completeness condition of the protocol: to fix a certain soundness parameter P_s and determine a constant number of clauses that the verifier must check to be convinced of the validity of the proof.

5.2 Coherent Attacks

Another type of attack to consider is a coherent attack, where the attacker manipulates *all* the quantum states received by the verifier by combining and/or entangling them. While this attack is the most general one, I'll introduce it in this section of the chapter to justify the form of the state upon which the security proof of the commitment scheme is constructed (as discussed in 5.3). Essentially, it enables us to deduce the state that

a malicious verifier, who has no prior information about the state, perceives and can potentially employ in carrying out attacks.

For this, recall that the state received by the verifier is given by

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes ... \otimes |\psi_n\rangle \,. \tag{5.8}$$

This state is a tensor product state; thus, it is *permutation invariant*. This means that changing the sequence of the states will not alter the overall state $|\Psi\rangle$. The classical de Finetti theorem states that any sequence of exchangeable classical random variables can be approximated by a mixture of independent and identically distributed (i.i.d.) random variables. The quantum version of the theorem extends this concept to quantum states. We refer to quantum state $\rho \in \text{Dens}((\mathbb{C}^d)^{\otimes n})$ as n-exchangeable if it is invariant under the action of the permutation operator

$$P_d(\pi)\rho P_d(\pi) = \rho, \quad \forall \pi \in S_n \tag{5.9}$$

where $P_d(\pi)$ is the permutation operator defined as

$$P_d(\pi) = \sum_{i_1,...,i_n \in [d]} |i_{\pi(1)}, ..., i_{\pi(n)}\rangle \langle i_1, ..., i_n| \tag{5.10}$$

[Boh]. If ρ_n is *n-exchangeable*, it can be expressed as a convex combination or mixture of product states of the form $\sigma^{\otimes k}$ in most subsystems. The approximation holds because we can always find a *measure* μ for the subsystem such that:

$$||\text{Tr}_{n-k}[\rho] - \int \sigma^{\otimes k} d\mu(\sigma)||_1 \leq \frac{2k \cdot (k+d)}{n+d}, \quad \forall k \leq n \tag{5.11}$$

where $\rho = |\Psi\rangle \langle\Psi|$.

Concretely, the theorem implies that a permutation-invariant state from an adversary's point of view, or a party who does not know the state, can be expressed as a fully mixed state:

$$|\psi_1\rangle \otimes ... \otimes |\psi_n\rangle = \frac{1}{2^n} \sum_{k=1}^{2^n} |b_1...b_n\rangle \langle b_1...b_n| \tag{5.12}$$

Since a fully mixed state shows no coherence, meaning its off-diagonal elements are all zero, we can conclude that coherent state attacks are impossible for our protocol state given in equation (5.8) , i.e., we can limit our security analysis to examining attacks on *individual states* $|\psi_a\rangle$ with $a = 1, ..., n$.

5.3 Security of commitment scheme against a quantum malicious verifier (P , V*)

In this section, we consider possible attacks on the *hiding property* of the commitment scheme, i.e., we ask about the probability that a dishonest verifier can extract more

information out of the commitment state $|\Psi\rangle$ as the protocol intended. Heuristically, they could only do this by getting information about the encoding bases of states sent to them. In section 5.2, we argued that coherent attacks do not offer any potential advantage, following from the *de Finetti theorem*. Hence, a verifier V^* can only perform attacks on the mixed state

$$|\psi\rangle = \frac{1}{4}(\rho_0 + \rho_1 + \rho_+ + \rho_-) = \frac{1}{4}(|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|) = \mathbb{1} \tag{5.13}$$

$|\psi\rangle$ is the statistical mixture of possible states where each state has equal probability. The attempt of discriminating the basis corresponds to discriminating states ρ_0 and ρ_1 from the states ρ_+ and ρ_-.

One way to write the discrimination is by mapping the states onto distinct classical binary outcome states that we denote with $\Omega_0 = |0\rangle\langle 0|$ and $\Omega_1 = |1\rangle\langle 1|$ and that we will call *acceptance states* in the following. We could have taken any two mutually orthogonal states as representatives of the acceptance states.

We call the Hilbert space of the quantum states ρ as $\mathcal{H}_1$ and the Hilbert space of the acceptance states Ω as $\mathcal{H}_2$. We are now searching for the optimal map $\lambda : \mathcal{H}_1 \to \mathcal{H}_2$ that maps states ρ_0 and ρ_1 to some classical state Ω_0 and the states ρ_+ and ρ_- to some classical state Ω_1. As we have seen in section 2.2.6, one can represent a linear map λ as a state, the **Choi matrix** or **Choi state** $J(\lambda)$, which is defined on the tensor product space of the input and output states of the map: $\mathcal{H}_{J(\lambda)} = \mathcal{H}_2 \otimes \mathcal{H}_1$.

A dishonest verifier would now randomly get one of the states
$\rho \in \{|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|\}$ with equal probability and they would then apply a channel λ that takes a state ρ to the state $\lambda(\rho)$, such that the success probability of the basis discrimination attack, which can be written as

$$\frac{1}{4}\big(\langle\Omega_0|\,\lambda(|0\rangle\langle 0|)\,|\Omega_0\rangle + \langle\Omega_0|\,\lambda(|1\rangle\langle 1|)\,|\Omega_0\rangle + \langle\Omega_1|\,\lambda(|+\rangle\langle +|)\,|\Omega_1\rangle + \langle\Omega_1|\,\lambda(|-\rangle\langle -|)\,|\Omega_1\rangle\big) \tag{5.14}$$

is enhanced. From section 2.2.6 we know that we can rewrite the upper equation as

$$\begin{aligned}\frac{1}{4}\big(&\langle\Omega_0| \otimes \langle 0^*|\,J(\lambda)\,|\Omega_0\rangle \otimes |0^*\rangle + \langle\Omega_0| \otimes \langle 1^*|\,J(\lambda)\,|\Omega_0\rangle \otimes |1^*\rangle + \\ &\langle\Omega_1| \otimes \langle +^*|\,J(\lambda)\,|\Omega_1\rangle \otimes |+^*\rangle + \langle\Omega_1| \otimes \langle -^*|\,J(\lambda)\,|\Omega_1\rangle \otimes |-^*\rangle\big)\end{aligned} \tag{5.15}$$

or equivalently as

$$\mathrm{Tr}\frac{1}{4}\big(|\Omega_0\rangle\otimes|0\rangle\langle\Omega_0|\otimes\langle 0|+|\Omega_0\rangle\otimes|1\rangle\langle\Omega_0|\otimes\langle 1|+|\Omega_1\rangle\otimes|+\rangle\langle\Omega_1|\otimes\langle +|+|\Omega_1\rangle\otimes|-\rangle\langle\Omega_1|\otimes\langle -|, J(\lambda)\big) \tag{5.16}$$

This will be the objective function of our SDP, where we in principle overlap the Choi state

$$J(\lambda) = \sum_{i,j} \lambda(|i\rangle \langle j|) \otimes |i\rangle \langle j| \tag{5.17}$$

with the tensor product of the input state ρ and the acceptance state Ω. The Choi state is defined in the basis of a maximally entangled state, where the map is applied to only one subsystem but leaves the other one untouched. By optimizing expression (5.16), we can find the optimal matrix $J(\lambda)$ such that the success probability in equation (5.14) is maximized, i.e., we want to find the optimal map λ that maps the basis of the first subsystem of the maximally entangled state to some state $\lambda(|i\rangle \langle j|)$ that is maximally close to an acceptance state Ω.

This will give the upper bound on the cheating probability of a dishonest verifier in the protocol implementing the above-described attack. The final semi-definite program looks then as follows:

$$\begin{gathered} \textbf{Primal problem}: \\ max \quad \mathrm{Tr}\Big(\tfrac{1}{4}\big(\Omega_0 \otimes \rho_0 + \Omega_0 \otimes \rho_1 + \Omega_1 \otimes \rho_+ + \Omega_1 \otimes \rho_-\big), J(\lambda)\Big) \\ \text{s.t. } \mathrm{Tr(J}(\lambda))_{\mathcal{H}_2} = \mathbb{1}_{\mathcal{H}_1} \\ \mathrm{J}(\lambda) \geq 0 \end{gathered}$$

The constraint $\mathrm{Tr(J}(\lambda))_{\mathcal{H}_2} = \mathbb{1}_{\mathcal{H}_1}$ ensures that the resulting operation is trace-preserving (here $\mathcal{H}_1$ is the Hilbertspace of the input states ρ, and $\mathcal{H}_2$ is the Hilbertspace of the acceptance states Ω, i.e., we are tracing out the subsystem of the acceptance state), whereas $J(\lambda) \geq 0$ ensures that the map is completely positive, representing a physically realizable state transformation (CPTP map).

To prove the strong duality, we derive the dual problem:

$$\begin{gathered} \textbf{Dual problem}: \\ min \quad \mathrm{Tr(Y)} \\ \text{s.t. } \mathrm{Y} \otimes \mathbb{1}_{\mathcal{H}_2} \geq \tfrac{1}{4}\big(\Omega_0 \otimes \rho_0 + \Omega_0 \otimes \rho_1 + \Omega_1 \otimes \rho_+ + \Omega_1 \otimes \rho_-\big) \end{gathered}$$

We can show that strong duality holds by solving the primal and dual problems, yielding an optimal basis discrimination probability of 0.5. This result implies that a dishonest verifier has no cheating strategy that improves their probability of correctly determining the encoding basis beyond random guessing.

Note that this result is rather trivial since the state the verifier receives in the protocol is identity. However, the above SDP formulation will become important in deriving security when adding experimental imperfections to the state. This will be done in follow-up work to this thesis.

5.4 Outlook - simulator security proof

We must demonstrate that the view of an ideal-world verifier, one who only receives assurance from a trusted third party that the proof provided by a prover is valid without

direct access to the underlying witness, cannot be distinguished from the viewpoint of a real-world verifier engaged in the interactive protocol with the prover. To achieve this, we construct a simulator capable of generating message transcripts from interactions with a verifier. Determining whether the simulated message transcript is distinguishable from the transcript of an actual interaction serves as the criterion for the scheme's zero-knowledge property. In the case of security against malicious quantum verifiers, a quantum simulator is required, while security against classical verifiers necessitates a classical simulator [SH08].

As previously mentioned, the common technique used in simulator construction is known as *rewinding*. This allows the simulator to revert to a prior state if the verifier's output during the interaction is inconsistent with other parts of the randomly generated transcript [Wat09]. When dealing with quantum simulators, the limitations of this technique in the quantum context must be considered.

The quantum rewinding lemma, established by [Wat09], illuminates the feasibility of rewinding in the quantum domain. It establishes that rewinding is possible when the success probability, i.e., the probability of a successful simulation, is (almost) independent of any auxiliary input that a malicious verifier might employ. This scenario permits the quantum simulator to generate an output state that has high fidelity to a successful simulation state. The lemma further outlines that there exists a quantum circuit Q that can generate this high-fidelity state with a bounded error ϵ.

For our specific protocol, the task involves identifying the mapping that characterizes the interaction between the prover and verifier in the real-world protocol. This mapping is then compared against the mapping induced by the simulator. This comparison is facilitated through a distance metric called the *diamond norm*, which calculates the difference between two admissible superoperators.

The following definitions are taken from [Wat09], p.31.

Definition 1 *For any superoperator $\phi : L(X) \to L(Y)$ the value of this norm is defined as:*

$$||\phi||_\diamond = max\{||(\phi \otimes I_{L(W)})(X)||_{tr} : X \in L(X \otimes W), ||X||_{tr} \leq 1\}$$

where W is any space with a dimension equal to X. And further

Definition 2 *The diamond norm of the difference between two admissible superoperators $\phi_0 : L(X) \to L(Y)$ and $\phi_1 : L(X) \to L(Y)$ satisfies:*

$$||\phi_0 - \phi_1||_\diamond = max\{||(\phi_0 \otimes I_{L(W)})(\rho) - (\phi_1 \otimes I_{L(W)})(\rho)||_{tr} : \rho \in D(X \otimes W), ||X||_{tr} \leq 1\}$$

because the trace norm is convex and superoperators are linear, the maximum is always achieved for some pure state $\rho = |\psi\rangle \langle\psi|$.

The protocol achieves statistical zero-knowledge if the map ϕ_x resulting from the interaction between the verifier V^* and the simulator S_V, and the map ψ_x resulting from the interaction between verifier V^* and prover P, only differs by a negligible function δ.

This relationship is represented as $||\phi_x - \psi_x||\diamond \leq \delta(|x|)$ for all $x \in A_{yes}$, where x denotes the input for both circuits.

Given our protocol's Σ structure, which shares similarities with the protocol for which Watrous established zero-knowledge against a quantum verifier, and the already proven security of the commitment scheme, we have confidence that a thorough analysis within Watrous' framework is achievable. Nonetheless, due to the time constraints inherent in the scope of this thesis, the actual implementation of the mapping, the subsequent computation of the trace distance, and, consequently, the final assessment of the overall protocol's security are deferred to future endeavors.

5.5 Quantum Advantage

In summary, the number of revealed clauses required in the protocol is governed by two parameters: the first parameter, denoted as $P_C(t_c)$, represents the probability that when both parties are honest, the verifier can verify at least one clause with values for which the commitment check could be done and check its satisfiability, while the second parameter, denoted as $P_S(t_s)$, represents the probability that a dishonest prover convinces the honest verifier to accept the proof. Increasing the number of clauses allowed to be challenged during the protocol execution makes both probabilities arbitrarily close to one and zero, respectively.

When we fix the values of P_C and P_S as predetermined protocol parameters, we observe that both t_c and t_s remain constant, regardless of the number of variables n or clauses y in the instance. To determine the required number of total revealed clauses, we consider the value of t_s, which represents the number of clauses that the verifier needs to be able to check, i.e., t_s clauses need to be measured in the same bases as they were encoded in. Assuming a probability $P_{\mathrm{C}}(t_{\mathrm{c}}) = 1 - (\frac{15}{16})^{t_{\mathrm{C}}}$ for a clause to be measured in the correct basis (all four variables within it), the prover in total needs to reveal $t = t_{\mathrm{c}} \cdot t_{\mathrm{s}}$ clauses to the verifier.

Assuming that the analysis through the simulator does not uncover any security vulnerabilities in the other building blocks of the protocol, we argue that the zero-knowledge property of the protocol holds. Even though we intentionally disclose information about the witness, our claim is based on the fact that, based on the hardness of NP-complete problems for quantum computers, the information revealed in the protocol does not allow a verifier to find a solution to the problem more efficiently than before the interaction with a prover.

To elaborate, let's consider a scenario where each variable appears exactly *once* throughout the entire instance. In this context, let $4 \cdot t_c$ denote the count of *variables* disclosed for ensuring completeness, and $4 \cdot t_s$ represent the count of *variables* disclosed for ensuring soundness. Given that solving an NP-complete problem demands $O(k^n)$ time, where $k > 0$ and n signifies the total number of variables in the input instance, we can deduce that if the difference $|n - 16 \cdot t_c \cdot t_s| \geq \eta$ with a sufficiently substantial value of η, the computational complexity remains exponential, specifically $O(k^{n-16 \cdot t_c \cdot t_s})$, where $16 \cdot t_c \cdot t_s$ is constant. Thus, our protocol satisfies the zero-knowledge criterion against classical and

quantum-computational adversaries.

Based on the complexity argument presented, we can further conclude the *hiding* and *binding* aspects of the protocol.

In 5.3., we established that, under ideal experimental conditions, information about the witness is hidden with information-theoretic security within the commitment state. This means that the method relies solely on quantum principles and does not require computational hardness assumptions. It is important to note, however, that within the broader framework of the protocol, we are forced to disclose a constant amount of information to the verifier. This disclosure is necessary to uphold the soundness and completeness properties of the protocol. As a result, our overall commitment scheme cannot be classified as information-theoretically secure in its concealment; rather, it falls under the category of quantum-computationally secure concealment. This classification is because, despite the constant leakage of information in the form of clauses, solving the problem still demands exponential computational effort, as previously demonstrated. This assertion holds for both classical and quantum computers. Specifically, we assume that neither classical nor quantum computers possess efficient means to solve NP-complete problems, as is widely accepted. However, the disclosing of information allows to bring the soundness, i.e., the probability of a wrong proof being accepted, to zero. Hence, the binding property of our commitment scheme is perfect for a large enough amount of leaked information about the witness.

It's furthermore important to note that the same protocol would not be feasible in a classical setting. The verification process can be performed efficiently using quantum states to encode the solution with linear time complexity in n. In contrast, classically, the protocol would be infeasible since, for a large value of η, the correctness of the solution cannot be efficiently checked, i.e., in polynomial-time.

It is worth highlighting that although $t_\mathrm{c} \cdot t_\mathrm{s}$ is not directly dependent on n, for the implementation of the zero-knowledge protocol, the difference $|n - 16 \cdot t_c \cdot t_s|$ must be large. As we cannot make $t_\mathrm{c} \cdot t_\mathrm{s}$ arbitrarily small without compromising correctness and security, the practical implementation of the scheme is only feasible for instances with a large number of clauses/variables.

6 Discussion

In this thesis, we introduced a novel protocol employing a ZKP for an NP-complete problem. The prover and verifier must interact quantumly in the proof system to achieve information-theoretic security in the commitment scheme. The system admits a constant round of communication when the protocol parameters *soundness* and *completeness* in the commitment scheme are pre-determined to specific values. The number of rounds of communication in our protocol is equivalent to revealed clauses of the witness. Consequently, by adjusting the protocol's parameters, we can trade off information leakage about the solution for the closeness of these parameters to zero and one, respectively. Remarkably, our protocol's commitment scheme offers perfect binding and quantum-computational hiding within these established cheating bounds.

Moreover, the protocol's experimental setup is practical and feasible for implementation in a laboratory setting. It involves a straightforward encoding setup on the prover side and a measurement arrangement on the verifier side. While we have laid out the foundation and principles of the protocol in this thesis, its actual implementation remains for future work beyond the scope of this study.

6.1 Secure commitment scheme

By integrating quantum communication into our interactive proof system, we outline a protocol that does not rely on computational assumptions and is not constrained by space-time limitations.

Our commitment scheme is secure against quantum verifiers attempting to extract more information than the number of states they actively challenge and receive answers for during the proof process. We considered coherent attacks for the security analysis, where a malicious verifier targets the global state $|\Psi\rangle$. Utilizing the de Finetti theorem, we established that conducting a comprehensive attack on the overall state does not provide an advantage over attacking individual states $|\psi_i\rangle$. Furthermore, leveraging SDPs, we have shown that no superior quantum attack on the individual states is possible beyond random guesses of the bit values (encoding bases). This encompasses potential entanglement with auxiliary inputs, arbitrary transformations, and measurements. We, therefore, have demonstrated that our commitment scheme is quantum-computationally hiding in the experimental ideal case, i.e., for single-photon states.

On the prover's side, the most effective cheating strategy involves sending optimized quantum states to persuade the verifier to accept an invalid solution. This strategy achieves a success rate of 85.36%, and we have calculated an upper bound on the probability of manipulating more than this expected portion of states successfully within a constrained

sample size using Chernoff bound analysis. The security analysis of our commitment scheme against a malicious prover defines the protocol's security parameter soundness. Our protocol embodies a trade-off: it divulges a constant and instance-independent amount of information about the solution while ensuring a quantum-computationally hiding and perfectly binding proof system where soundness and completeness remain constant and instance-independent.

Given the assumed zero-knowledge property of our proof system, which still has to be shown formally within the simulator framework, our protocol demonstrates zero-knowledge characteristics concerning the amount of *leaked information*, wherein the importance of the disclosed information diminishes as the instance size grows. This attribute highlights the efficacy of our protocol as a ZKP system.

6.2 Next steps

6.2.1 Completing security proof

As mentioned, an important open question is how to prove that the protocol's overall *zero-knowledge* property holds against malicious quantum verifiers. To this point, the most widely used approach is constructing and analyzing the protocol with a simulator. An essential future step following this thesis will involve formulating the security proof within this framework.

In previous work, the simulator framework's implementation relied on the assumption of commitment scheme intractability, where the schemes primarily rested on post-quantum one-way functions, which lack total provable security [AB20], [VZ09]. A distinctive property of our commitment scheme is its independence from assumptions about one-way functions employed to encode the witness, as this is done in an information-secure manner in our case. However, it is crucial to acknowledge that the hiding property of the overall proof system relies on the assumption of the impractical solvability of NP-complete problems. Therefore, in our case, implementing the simulator framework will be grounded in this assumption rather than the intractability of one-way functions.

The critical task in constructing a simulator remains to show that further interactions and queries between the parties, i.e., on top of the commitment scheme, do not have security vulnerabilities. Our approach, therefore, takes a reverse trajectory, initially establishing security for the commitment scheme and subsequently subjecting the protocol to scrutiny and potential adjustments to ensure alignment with security constraints within the simulator framework.

6.2.2 Experimental implementation

Another crucial step involves progressing toward the laboratory implementation of the protocol. This entails considering experimental imperfections in the states exchanged during the protocol. Specifically, our focus will be on addressing imperfections in the first round of communication — the commitment state — given its quantum nature.

The experimental imperfections to consider are losses, noise, and detection errors. Integrating these factors is crucial, as their influence on the state exchange and protocol security parameters might necessitate an adaptation of the protocol for practical implementation.

For instance, within a lossy channel, the prover might need to transmit additional states to compensate for losses, unintentionally enlarging information leakage. In this setting, losses cannot be distinguished from a malicious verifier asking for more information. Conversely, a dishonest prover might cover a lack of witness knowledge by exploiting a lossy channel to replace states.

Additionally, introducing noise in the form of multi-photons introduces another layer of complexity that can enable enhanced cheating. Multi-photons amplify the amount of information transmitted — sending two photons instead of one increases the probability of a basis discrimination attack from $p = 0.5$ to $p = 0.75$. However, this concern is less significant than initially anticipated, as it only minimally affects the expected verification time. To elaborate, in the context of the NP-complete SAT problem, the solving time was previously upper-bounded by $O(k^n)$. Even after leaking some constant $t = 16 \cdot t_c \cdot t_s$ bits of information, it remains exponential, now represented as $O(k^{n-t})$. Furthermore, when we introduce multi-photons and factor in a constant probability p of information extraction per transmitted state by the verifier, the resulting upper limit for solving time becomes $O(k^{(n-pn-t)})$ or equivalently $O(k^{(n(1-p)-t)})$. We see that even with the inclusion of multi-photons, the solving time remains exponential. Hence, although the amount of leaked information is not constant anymore due to multi-photons, our argumentation for the proof system's zero-knowledge property, assuming the simulator framework supports our proof system construction, remains valid. This is because the interaction with the prover does not enhance the verifier's ability to solve the problem instance.

However, introducing multi-photons brings a security vulnerability on the verifier's side since they can lead to detector attacks, rendering the transmitted information meaningless. A malicious prover could exploit this vulnerability to cover a lack of knowledge, attempting to make a verifier accept an invalid proof.

The interplay of these factors highlights significant security trade-offs between the prover and verifier. A viable solution necessitates identifying a *sweet spot* wherein both parties engage in a protocol that offers no undue advantage to either side. This equilibrium results in a balanced cheating probability on both ends, preserving the integrity and security of the protocol.

6.3 Final remarks

This thesis is the initial phase of an ongoing project to realize a practically feasible ZKP system secure against quantum attacks. Given that the current setup involves standard optical components and procedures, the primary focus of advancing this project further lies primarily on the theory side. This entails finalizing the security proof within the framework of a simulator and incorporating potential experimental imperfections and non-ideal scenarios.

Bibliography

[AB16] Christian Schaffner Anne Broadbent. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, 2016.

[AB19] Alex B. Grilo Anne Broadbent. Zero-Knowledge for QMA from Locally Simulatable Proofs. *arXiv*, 2019.

[AB20] Fang Song John Watrous Anne Broadbent, Zhengfeng Ji. Zero-knowledge proof systems for QMA. *SIAM J. Comput.*, 49(2):245–283, 2020.

[AB22] Alex B. Grilo Anne Broadbent. QMA-hardness of consistency of local density matrices with applications to quantum zero-knowledge. *SIAM Journal on Computing*, 51(4):1400–1450, 2022.

[ABC+21] Pouriya Alikhani, Nicolas Brunner, Claude Crepeau, Sebastien Designolle, Raphael Houlmann, Weixu Shi, Weixu Yang, and Hugo Zbinden. Experimental relativistic zero-knowledge proofs. *Nature*, 599:47–50, 2021.

[ABD+09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009.

[Aca] Superwits Academy. Polynomial vs. exponential running time. `https://www.superwits.com/library/design-analysis-of-algorithm/course-content-daa/polynomialvsexponentialrunningtime`. Accessed: 2023-08-17.

[Adc02] Cleve R. Adcock, M. *A Quantum Goldreich-Levin Theorem with Cryptographic Applications.* In: Alt, H., Ferreira, A. (eds) STACS 2002. STACS 2002. Lecture Notes in Computer Science, vol 2285. Springer, Berlin, Heidelberg., 2002.

[ADK18] Juan M. Arrazola, Eleni Diamanti, and Iordanis Kerenidis. Quantum superiority for verifying np-complete problems with linear optics. *npj Quantum Information*, 56(4):1–8, 2018.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[AM12] John Watrous A Molina, T Vidick. *Optimal counterfeiting attacks and generalizations for Wiesner's quantum money.* (eds) Theory of Quantum Computation, Communication, and Cryptography. TQC 2012. Lecture Notes in Computer Science, vol 7582. Springer, Berlin, Heidelberg., 2012.

[BBR+18] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121(19):190502, 2018.

[BCKD20] Mathieu Bozzio, Ulysse Chabaud, Iordanis Kerenidis, and Eleni Diamanti. Quantum weak coin flipping with a single photon. *Phys. Rev. A*, 102(2):022414, Aug 2020.

[BDG19] Mathieu Bozzio, Eleni Diamanti, and Frédéric Grosshans. Semi-device-independent quantum money with coherent states. *Phys. Rev. A*, 99(2):022336, 2019.

[BOGG+90] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, and P. Rogaway. Everything provable is provable in zero-knowledge. In *Proceedings on Advances in Cryptology*, CRYPTO '88, page 37–56, Berlin, Heidelberg, 1990. Springer-Verlag.

[Boh] Thom Bohdanowicz. Lecture 13: Quantum de finetti theorems. `http://users.cms.caltech.edu/~vidick/teaching/286_qPCP/lecture13.pdf`. Accessed: 2023-08-01.

[Boz19] Mathieu Bozzio. *Security and implementation of advanced quantum cryptography: quantum money and quantum weak coin flipping.* PhD thesis, Universite Paris Saclay, 2019.

[Bra22] Zvika Brakerski. On the computational hardness needed for quantum cryptography. *arXiv*, 2022.

[BS20] Nir Bitansky and Omri Shmueli. Post-quantum zero knowledge in constant rounds. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, page 269–279, New York, NY, USA, 2020. Association for Computing Machinery.

[CCLY22] Nai-Hui Chia, Kai-Min Chung, Qipeng Liu, and Takashi Yamakawa. On the impossibility of post-quantum black-box zero-knowledge in constant round. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 59–67, 2022.

[Cha] Shuchi Chawla. Advanced algorithms lecture notes. `https://pages.cs.wisc.edu/~shuchi/courses/787-F16/index.html#lect`. Accessed: 2023-07-20.

[CHB84] Gilles Brassard Charles H. Bennett. Quantum Cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12*, 1984.

[Chi21] Chung KM. Yamakawa T. Chia, NH. *A Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Rounds.* In: Malkin, T., Peikert, C. (eds) Advances in Cryptology – CRYPTO 2021. CRYPTO 2021. Lecture Notes in Computer Science(), vol 12825. Springer, Cham., 2021.

[CKDK21] Federico Centrone, Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis. Experimental demonstration of quantum advantage for np verification with limited information. *Nat Commun*, 850(12), 2021.

[Dak22] Borivoje Dakic. Quantum Information Theory Lecture. 2022.

[Din08] Irit Dinur. Pcps with small soundness error. *SIGACT news*, 39(3):17, 2008.

[DLY16] Eleni Diamanti, Hoi-Kwong Lo, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2(16025), 2016.

[DNS98] Cynthia Dwork, Moni Naor, and Amit Sahai. Concurrent zero-knowledge. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 409–418, New York, NY, USA, 1998. Association for Computing Machinery.

[Eis] Jens Eisert. Quantum information theory. `https://www.physik.fu-berlin.de/en/einrichtungen/ag/ag-eisert/teaching/ws20-21/QuantumInformationTheoryChapter4.pdf`. Accessed: 2023-07-05.

[ELH+21] Sebastian Ecker, Bo Liu, Johannes Handsteiner, Matthias Fink, Dominik Rauch, Fabian Steinlechner, Thomas Scheidl, Anton Zeilinger, and Rupert Ursin. Strategies for achieving high key rates in satellite-based qkd. *npj Quantum Information*, 7(5), 2021.

[Gav12] Dmitry Gavinsky. Quantum money with classical verification. In *2012 IEEE 27th Conference on Computational Complexity*, pages 42–52, 2012.

[GMR85] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, page 291–304, New York, NY, USA, 1985. Association for Computing Machinery.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3):690–728, 1991.

[GO94] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, (7):1–32, 1994.

[HBD15] B. Hensen, H. Bernien, and A. et al. Dreau. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, (526):682–686, 2015.

[HILL99] Johan Hastad, Russell Impagliazzo, A. Leonid Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal of Computing*, 28(4):1364–1396, 1999.

[JB21] Dakshita Khurana Fermi Ma James Bartusek, Andrea Coladangelo. *One-way functions imply secure computation in a quantum world.* In: Malkin, T., Peikert, C. (eds) Advances in Cryptology – CRYPTO 2021. CRYPTO 2021. Lecture Notes in Computer Science(), vol 12825. Springer, Cham., 2021.

[Ken12] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109(13):130501, Sep 2012.

[Lin17] Y. Lindell. *How to Simulate it - A tutorial on the Simulation Proof Technique.* In: Lindell, Y. (eds) Tutorials on the Foundations of Cryptography. Information Security and Cryptography. Springer, Cham., 2017.

[LKB+15] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical relativistic bit commitment. *Phys. Rev. Lett.*, 115(3):030502, Jul 2015.

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, 2005.

[Lyn] Benn Lynn. Zero-knowledge proofs. `https://crypto.stanford.edu/pbc/notes/crypto/zk.html`. Accessed: 2023-08-17.

[Mar] Florian Marquardt. Lecture 13: From the wave function to the state vector. `https://mpl.mpg.de/fileadmin/user_upload/Marquardt_Division/Teaching/Lecture_13.pdf`. Accessed: 2023-07-15.

[Mas21] Rolando Massa. *Cryptographis Simulation Techniques with Applications to Quantum Zero-Knowledge and Copy-Protection.* PhD thesis, Massachusetts Institute of Technology, 2021.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, Apr 1997.

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I*, page 269–295, Berlin, Heidelberg, 2022. Springer-Verlag.

[Nie00] Chuang L. Isaac Nielsen, A. Michael. *Quantum Computation and quantum information.* Cambridge University Press, 2000.

[NYC+23] Simon Neves, Verena Yacoub, Ulysse Chabaud, Mathieu Bozzio, Iordanis Kerenidis, and Eleni Diamanti. Experimental cheat-sensitive quantum weak coin flipping. *Nature Communications*, 1855(14), 2023.

[Ori18] Juan Oritgoso. Twelve years before the quantum no-cloning theorem. *American Journal of Physics*, 86(3):201–205, 2018.

[OV08] J. Shien Ong and Salil Vadhan. *An Equivalence Between Zero Knowledge and Commitments.* In: Canetti, R. (eds) Theory of Cryptography. TCC 2008. Lecture Notes in Computer Science, vol 4948. Springer, Berlin, Heidelberg., 2008.

[Par70] L. James Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23–33, 1970.

[Pre] John Preskill. Lecture notes for ph219/cs219: Quantum information chapter 3. `http://theory.caltech.edu/~preskill/ph219/index.html`. Accessed: 2023-08-17.

[RKB+18] Marie-Christine Roehsner, A. Joshua Kettlewell, B. Tiago Batalhao, F. Joseph Fitzsimons, and Philip Walther. Quantum advantage for probabilistic one-time programs. *Nature Communications*, 9(5225):1–8, 2018.

[RW20] G. Michael Raymer and A. Ian Walmsley. Temporal modes in quantum optics: then and now. *Physica Scripta*, 95(6):1–17, 2020.

[SA98] Shmuel Safra Sanjeev Arora. Probabilistic Checking of Proofs: A new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.

[Sal98] Louis Salvail. Quantum bit commitment from a physical assumption. In *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '98, page 338–353, Berlin, Heidelberg, 1998. Springer-Verlag.

[SB12] Anne Broadbent Joseph F. Fitzsimons Anton Zeilinger Philip Walther Stefanie Barz, Elham Kashefi. Demonstration of Blind Quantum Computing. *Science*, 335(6066):303–308, 2012.

[SH08] Pranab Sen Shengyu Zhang Sean Hallgren, Alexandra Kolla. *Making Classical Honest Verifier Zero Knowledge Protocols Secure against Quantum Attacks.* In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds) Automata, Languages and Programming. ICALP 2008. Lecture Notes in Computer Science, vol 5126. Springer, Berlin, Heidelberg., 2008.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[SMB09] Sarah Croke Stephen M. Barnett. Quantum state discrimination. *Advances in Optics and Photonics*, 1(2):238–278, 2009.

[TG66] U. M. Titulaer and R. J. Glauber. Density operators for coherent fields. *Phys. Rev.*, 145(4):1041–1050, May 1966.

[VB96] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[VDG98] Jeroen Van De Graaf. *Towards a Formal Definition of Security for Quantum Protocols*. PhD thesis, CAN, 1998. AAINQ35648.

[Vil] Jorge L. Villar. Zero-knowledge proofs notes. `https://web.mat.upc.edu/jorge.villar/doc/notes/DataProt/zk.pdf`. Accessed: 2023-08-17.

[VZ09] Thomas Vidick and Tina Zhang. Classical zero-knowledge arguments for quantum computations. *Quantum*, 4(1):266–311, 2009.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[Wika] Wikipedia. Alphabeth (formal languages). `https://en.wikipedia.org/wiki/Alphabet_(formal_languages)`. Accessed: 2023-08-17.

[Wikb] Wikipedia. Commitment scheme. `https://en.wikipedia.org/wiki/Commitment_scheme`. Accessed: 2023-06-15.

[Wikc] Wikipedia. Convex cone. `https://en.wikipedia.org/wiki/Convex_cone#:~:text=A%20cone%20C%20is%20convex,more%20commonly)%20the%20real%20numbers.` Accessed: 2023-06-23.

[Wikd] Wikipedia. Formal language. `https://en.wikipedia.org/wiki/Formal_language`. Accessed: 2023-08-17.

[Wike] Wikipedia. One-way function. `https://en.wikipedia.org/wiki/One-way_function`. Accessed: 2023-07-01.

[Wikf] Wikipedia. Qma. `https://en.wikipedia.org/wiki/QMA`. Accessed: 2023-09-09.

[WTC21] Weilong Wang, Kiyoshi Tamaki, and Marcos Cury. Measurement-device-independent quantum key distribution with leaky sources. *Scientific Reports*, 1(11):1678, 2021.

[WYH22] Shuang Wang, Zhen-Qiang Yin, and De-Yong et al. He. Twin-field quantum key distribution over 830km fibre. *nature photonics*, 1(16):154–161, 2022.

[WZ82] William Wootters and H. Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[YFL22] Hua-Lei Yin, Yao Fu, and et al. Li, Chen-Long. Experimental quantum secure network with digital signatures and encryption. *National Science Review*, 10(4):1–11, 2022.

[YLL20] Juan Yin, Yu-Huai Li, and et al. Liao, Sheng-Kai. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(1):501–505, 2020.

[YMAD15] Ishai Yuval, Mahmoody Mohammad, Sahai Amit, and Xiao David. On zero-knowledge pcps: Limitations, simplifcations, and applications. *Available at: http://www.cs.virginia.edu/~mohammad/files/papers/ZKPCPs-Full.pdf.*, 2015.