On the Impossibility of Unconditionally Secure Quantum Bit Commitment

Bachelor's Thesis of

Frieder Haizmann

at the Department of Informatics
KASTEL – Institute of Information Security and Dependability

Reviewer:	Prof. Dr. Jörn Müller-Quade
Second reviewer:	Prof. Dr. Thorsten Strufe
Advisor:	M.Sc. Marcel Tiepelt

14. November 2020 – 15. March 2021

Karlsruher Institut für Technologie
Fakultät für Informatik
Postfach 6980
76128 Karlsruhe

I declare that I have developed and written the enclosed thesis completely by myself, and have not used sources or means without declaration in the text.

Karlsruhe, March 14, 2021

.....

(Frieder Haizmann)

Abstract

In 1997 Dominic Mayers, published a no-go theorem that stated, no unconditionally secure quantum bit commitment protocol is possible. However, the accompanying proof is not very accessible. In this thesis, first the necessary background to follow the proof is presented. Then the proof of the theorem is laid out step by step, illustrated with examples and put into perspective of later research. Furthermore, quantum bit commitment schemes, that do not fall under the no-go theorem are explored. The most common approaches for such quantum bit commitment schemes are compared, classified, and reviewed.

Zusammenfassung

Dominic Mayers veröffentlichte 1997 ein Unmöglichkeitstheorem, in welchem er zeigte, dass es keine quantenkryptographische bit-commitment Verfahren gibt, die uneingeschränkt sicher sind. Der begleitende Beweis lässt allerdings einige Details aus und ist somit schwer nachzuvollziehen. In dieser Bachelorarbeit werden also zunächst die Grundlagen vorgestellt, die notwendig sind um dem Beweis zu folgen. Dann wird der Beweis schrittweise in einer Form, der besser zu folgen ist, dargelegt und fehlende Details ergänzt. Des Weiteren wird der Beweis mit Beispielen illustriert, und der Beweis ins Verhältnis zu späteren Ergebnissen gesetzt. Darüber hinaus werden gängige Quanten-Bit-Commitment-Verfahren, die nicht unter das Unmöglichkeitstheorem fallen, erarbeitet. Diese Verfahren und Herangehensweisen, solche Verfahren zu konstruieren, werden miteinander verglichen, klassifiziert und begutachtet.

Contents

I. Introduction

Bit commitment is a powerful cryptographic primitive, that can be used to implement secure coin tossing[1], oblivious transfer[2], and secure two-party computation[3]. For this reason, an unconditionally secure bit commitment protocol, so a protocol that does not rely on computational assumptions, is highly desirable. It is well known that under classical assumptions unconditional bit commitment is impossible.

With the advent of quantum computation the cryptographic primitive of key distribution, that was previously only possible under some computational assumptions, was found to be possible in such a way that it relies only on the validity of quantum physics (Scarani et al. 2009; Shor and Preskill 2000). With bit commitment being a powerful primitive, cryptographers searched for such unconditional secure protocols for bit commitment, that rely only on quantum theory. However, in 1997 Dominic Mayers published a paper, proving that no such unconditionally secure quantum bit commitment (QBC) protocol exists. Mayers showed that if a quantum commitment protocol is unconditionally secure against the receiver, the sender can always successfully cheat.

Over the years, there have been some sceptics of the no-go theorem, whose protocols were later shown to still be vulnerable to the attack presented. However it is still possible to implement quantum bit commitment under certain conditions, or for some weaker security notions.

I.1. Problem Statement

In his proof Mayers does not give a high level of detail. Some theorems are cited and asserted to give rise to certain properties, without an explicit proof of these statements. For instance he mentions that there exists a transformation that lets the sender cheat, however it is not explained how exactly this transformation is constructed. While it is possible to verify that these statements are in fact true, it is not always straight forward to do so, and to follow along in the proof. In short, while Mayer's paper was ground-breaking, it is not very accessible.

While the no-go theorem is widely accepted, it does not take the role of special relativity or decoherence into account. With that a number of assumptions that can be made, under which unconditionally secure quantum bit commitment can still be achieved. In addition to this, (quantum) bit commitment protocols that may not be unconditionally secure but fulfil other security definitions, also have useful applications. Such protocols were explored by a number of authors. However it appears, that there exists no comprehensive overview of those different approaches.

[1] As shown by Blum (1983), who uses a form of bit commitment (though not named as such) to build his coin tossing protocol.

[2] Unconditionally secure quantum bit commitments are used by Bennett, Brassard, et al. (1992), Crépeau (1994), and Yao (1995) to implement secure oblivious transfer.

[3] Secure two-party computation can be based on oblivious transfer (Kilian 1988), or on "committed oblivious transfer" (Crépeau, van de Graaf, and Tapp 1995), a combination of oblivious transfer and bit commitment. As bit commitment enables oblivious transfer, secure two-party computation can also be attributed to bit commitment.

I.2. Related Work

The focus of this Thesis will be on Mayers (1997), which proves the impossibility of unconditionally secure quantum bit commitment. Mayers also mentions his anterior article (Mayers 1996) about the insecurity of a specific QBC scheme, which has more detail on some aspects of the 1997 paper. Independently of Mayers Lo and Chau (1998) also published an impossibility proof for quantum bit commitment, in which they use many of the same techniques as Mayers (1997), and elaborate on some parts while simplifying others. The BB84 quantum bit commitment scheme proposed by Bennett and Brassard (1984) will also be of interest, as it is the first quantum bit commitment scheme described, and whose existence lead to the general discussion of whether QBC is possible. In fact the "EPR-Attack" which was later generalized in the proofs of Lo and Chau (1998) and Mayers (1997), is presented by Bennet and Brassard alongside with the protocol.

As it has been noticed, that a secure QBC-protocol could be obtained by forcing the sender to perform measurements, attempts have been made, to do so using computationally secure classical bit commitments. However it was shown by Brassard, Crépeau, et al. (1998), that trying to force the sender to perform real measurements by using classical bit commitments fails at the classical bit commitments. They prove this by showing that classical bit commitment schemes are inherently vulnerable against quantum attacks.

An extended no-go theorem is provided by D'Ariano et al. (2007). They describe why some authors are not convinced by Mayers' proof, then introduce a model in which no fixed strategy has to be followed by the receiver of the commitment, so that it also includes protocols of sceptics like the one of Yuen (2005). Thereafter a no-go theorem of unconditional security on this most general model is formulated.

Nielsen and Chuang (2010) give a comprehensive introduction to quantum information and quantum computation. A well put together definition of quantum ensembles and a useful form of Schmidt's decomposition theorem are given by Hughston, Jozsa, and Wootters (1993), both of which are mentioned to be used by Lo and Chau (1998) and Mayers (1997), and whose usage will be made more explicit in the thesis. Aspects of entanglement are reviewed by Horodecki et al. (2009), and while quantum bit commitment is only briefly mentioned, it is very interesting to see how useful entanglement can be in other cryptographic applications, as opposed to quantum bit commitment where it is a weak point of most protocols that implement it.

A very interesting but impractical approach for a quantum bit commitment protocol that evades even the most general impossibility proof is one that takes general relativity into account. Such a protocol is presented by Kent (1999). The promising concept of *noisy storage* is proposed by Konig, Wehner, and Wullschleger (2012), where an unconditionally secure quantum bit commitment can be achieved trough forced storage which induces decoherence. Another protocol of interest is the one Crépeau, Légaré, and Salvail (2001) present, as it achieves either the unconditional hiding or the unconditional binding property without making strong assumptions.

I.3. Contribution and Outline

This thesis provides a wider look at Mayer's no-go theorem and a detailed explanation of its proof, including auxiliary theorems and how they are utilized. Mayers proved, the sender is able to perform an attack on the quantum bit commitment protocol. The thesis explicitly constructs this attack and provides examples, that illustrate the steps taken in the attack. For an interactive example, the attack on BB84 will be implemented in Q#, a functional programming language for quantum applications developed by Microsoft (Svore et al. 2018). To address the variety of proposed protocols, an overview is given over the most popular ways to achieve quantum bit commitment in some form or another. This

survey classifies those approaches by assumptions, sub-protocols used and level of security achieved, and puts their feasibility into perspective.

To start with, Chapter II will provide a preliminary overview of cryptographic, mathematical and quantum theoretical concepts needed for the following chapters. In Section II.1 some general cryptographic notions and the classical primitive of bit commitment are presented. Section II.2 gives mathematical definitions that will afterwards be used in Section II.3 as a foundation for quantum information theoretic definitions and theorems. In addition to that, Section II.3 provides an information theoretical and computational introduction to quantum theory. Core concepts that will be needed for the understanding of Mayer's proof and this thesis are presented here. Section II.4 then provides the quantum counterparts of cryptographic primitives, not only for bit commitment but also for primitives, that will later be explored in Chapter IV.

The in-depth proof of Mayers theorem, and context around it is then given in Chapter III. The first section of this chapter defines the environment in which the proof of the no-go theorem will be modeled. A generalized measurement to handle classical information in a quantum context is presented in Subsection III.1.1, which models classical information as special collapsed quantum states. With this generalized measurement, Subsection III.1.2 then shows how a generalized two-party system is modelled. Using this model in Section III.2, the quantum bit commitment protocol BB84 is presented alongside with an attack strategy on it. This attack is important as its generalization leads to Mayers' no-go theorem.

The generalized attack on quantum bit commitment protocols is then presented in Section III.3. With Alice being the participant which sends the commitment and Bob the participant which receives the commitment, Subsection III.3.1 explains, why one can assume the quantum bit commitment protocol to be secure against Bob, and what that means for the properties of the protocol. These properties are then addressed in Sections III.3.2–III.3.4, where initially it is shown which advantage Alice gains from the protocol being secure against Bob, and then in III.3.3 how she is able to cheat if the protocol is perfectly secure against Bob. Mayers proof uses Hughston, Jozsa, and Wootters (1993) to argue that there exists a unitary transformation on Alice side, that allows her to change her mind after the commitment. This transformation is explicitly constructed in this subsection. Then in III.3.4 it will be shown how Alice is still able to cheat, even if the protocol is only unconditionally secure against Bob. It will be shown that it is not possible for Bob to differentiate the cheating state after Alice changed her mind from the respective honest state.

The no-go theorem is then put into context in Sections III.4 and III.5. Section III.4 explains why Mayers' proof was criticised by some authors, and how D'Ariano et al. proved an even more general version of the no-go theorem that undoubtedly includes the sceptics attempts to circumvent the no-go theorem. Subsequently in Section III.5 a weaker form of quantum bit commitment, that does not fall under the framework of Mayers proof, is discussed. It is shown, that there already exist specific attack strategies against it, and that the more generalized proof, discussed in III.4, can also be applied to this form of quantum bit commitment.

Finally, Chapter IV presents ways in which quantum bit commitment still can still be achieved. Possibilities of protocols that do not fall under the setting of the no-go theorems, and can possibly achieve unconditional security under some specific assumptions, are explored in Section IV.1. Section IV.2 presents protocols that, while not achieving unconditional security, achieve either unconditional concealing, unconditional biding, or a different tradeoff of those properties.

A conclusion of this thesis is given in Chapter V. In Appendix A, an interactive example is presented, that implements the BB84 protocol and the attack on it in Q#.

II. Preliminaries

This chapter provides an introduction to cryptographic, mathematical and quantum theoretic concepts, that will be needed for the following chapters.

II.1. Cryptographic Primitives

In this section some cryptographic primitives and their security conditions will be presented.

Definition II.1 (Adjectives for security proprties). A property in (quantum) cryptography is defined to hold *unconditionally*, if it holds against a cheater with no limit on time, space or technology available to them.

A protocol is

- *perfectly* secure, if its security properties hold in any case against any attacker.
- It is *statistically* secure, if the probability of an unconditional attacker succeeding is negligible in its security parameter.
- It is *computationally* secure, if its security depends on the assumption that a certain (quantum) computation is hard to perform. ♣

II.1.1. Bit Commitment

Bit commitment is an asymmetric cryptographic primitive between two parties. One party wants to commit themselves to a bit and desires the other party not to be able to determine the contents of this commitment before they unveil it. Meanwhile, the other party is interested in the first party not being able to change their mind about the commitment. Throughout this thesis, the committing party will be called *Alice*, and the party receiving the commitment will be called *Bob*.

Often the analogy of a strong-box is used, where Alice writes her bit on a piece of paper and puts it in a box which she then gives to Bob and thus commits herself to this bit. Bob is not able to open this box without the key, which Alice provides when she decides to unveil the committed bit. A bit commitment protocol thus consists of two phases, the *commit* phase and the *unveil* phase.

During the *commit* phase, Alice decides on a bit to commit and encodes it in some way. The encoded bit is called a *commitment*. She then sends this commitment to Bob.

In the *unveil*, sometimes also called *decommitment* phase, Alice provides information to Bob that indicate the bit she committed herself to and that makes it possible for Bob to verify, whether she really did commit herself to that bit. Bob then either accepts that commitment or rejects it. If he accepted the bit he then announces what he thinks the committed bit was.

It is sometimes useful to model Alice's and Bob's actions these two phases through procedures commit(b) and unveil(c_b). Procedure commit(b) models the commit phase and takes the bit to commit as an input. It returns the commitment c_b. The unveil phase is modelled through unveil(c_b) which takes the commitment c_b as an input and either returns a bit b or $\perp$ on error, or if cheating has been detected.

During the commit and unveil phase additional communication and computation can occur. So as a more broad description, the *commit* phase is the phase from the start

of the protocol, including any setup procedures, until Bob has received and processed a commitment of some form, and the *unveil* phase is the phase at the end of the protocol where the contents of the commitment are unveiled to Bob and he verifies its correctness.

Sometimes the notion of a *holding* phase is useful. This phase describes processes in the time after the commit phase, but before the unveil phase. In most honest protocols nothing happens in this phase, therefore it is often omitted.

Definition II.2 (Correctness of a bit commitment). A bit commitment is *correct*, if in any case in which both parties are honest and Alice committed to $b \in \{0,1\}$, Bob accepts the commitment and is convinced that Alice committed to b. ♣

Definition II.3 (Perfectly and statistially binding for classical bit commitments). A bit commitment scheme is *perfectly binding*, if and only if every commitment that can be revealed to be $b \in \{0,1\}$ cannot be revealed to be $1-b$. A bit commitment scheme with a security parameter n is *statistically binding*, if and only if given any commitment c, the probability that Alice successfully reveals 0 in the unveil phase minus the probability that Alice successfully reveals 1 is negligible in the security parameter.

$$\forall \mathcal{A}(\cdot) \to c\colon \left|\Pr\left[\text{unveil}(c) \to 0\right] - \Pr\left[\text{unveil}(c) \to 1\right]\right| \leq \text{negl}(n)\,. \tag{II.1}$$

♣

Definition II.4 (Perfectly and statistically concealing for classical bit commitments). A bit commitment scheme is *perfectly concealing*, if and only if any commitment produced by commit$(\cdot)$ contains no information about the committed bit. A bit commitment scheme with security parameter n is *statistically concealing*, if and only if for any two commitments c_0 and c_1, that can honestly be revealed to 0 and 1 respectively, the probability that Bob is able to correctly differentiate between the two is negligible in the security parameter.

Note, a commonly used synonym for *concealing* is *hiding*. ♣

Definition II.5 (Perfect and unconditional security for classical bit commitments). A bit commitment scheme is *perfectly secure*, if and only if it is perfectly concealing and perfectly binding. It is *unconditionally secure*, if and only if it is perfectly or statistically concealing and perfectly or statistically binding against an unconditional adversary. ♣

It is known, that perfect and unconditionally secure bit commitment is impossible in the classical world (Kilian 1988, p. 24).

II.2. Linear Algebra

In quantum information and quantum computation, the fundamental unit of information is the quantum bit (*qubit*), analogous to the fundamental unit of information in classical information theory, which is the *bit*. In the same way that classical bits can have states that are described by the numbers 0 and 1, qubits can have states that are described by the vectors $|0\rangle$ and $|1\rangle$. Unlike classical bits, but like in Example II.1, states of qubits can be described as a superposition of multiple basis states.

II.1 Example The wave function of a photon can be described as $\alpha\,|\uparrow\rangle + \beta\,|\rightarrow\rangle$, whereas α and β are complex numbers, that encode the amplitude and phase of a wave function in the $\uparrow$ or $\rightarrow$ direction respectively. It is said that the photons state is in a *superposition* of the states $|\uparrow\rangle$ and $|\rightarrow\rangle$.

When measured, the photon will have either a vertical polarization with a probability of $|\alpha|^2$ or a horizontal polarization with a probability of $|\beta|^2$. ∗

This example shows some physical background of what is going to follow. To understand how to model the behaviour of a quantum mechanical system in a way that is useful for quantum information and quantum computation, first some mathematical foundations have to be laid out. The concepts laid out in this section will then be put in relation to quantum computing in Section II.3. The definitions in this section are based on Nielsen and Chuang (2010).

II.2.1. Hilbert Space

A vector space with an inner product is called an *inner product space*. Furthermore an inner product space that is a complete metric space is called a *Hilbert space*. All finite dimensional vector spaces are complete. In quantum computation and quantum information, finite complex vector spaces are used to describe quantum states as vectors. So in this context, inner product spaces are the same as Hilbert spaces.

The *dirac* notation is used to describe vectors of the n-dimensional Hilbert space $\mathcal{H} \coloneqq \mathbb{C}^n$ of vectors of complex numbers. It consists of the elements $|\cdot\rangle$ and $\langle\cdot|$, called *ket* and *bra* respectively. When writing $|\psi\rangle$, or $\langle\psi|$, ψ is the label assigned to the vector. Given

$$|\psi\rangle :\equiv \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix} , \tag{II.2}$$

it applies that

$$\langle\psi| \equiv \begin{pmatrix} \psi_1^* & \cdots & \psi_n^* \end{pmatrix} , \tag{II.3}$$

where ψ_i^* denotes the complex conjugate of ψ_i. This means that $\langle\psi| = (|\psi\rangle^*)^T$.

Dirac notation is useful for the *inner product* of two vectors in this complex vector space. The inner product of the vectors $|\psi\rangle$ and $|\phi\rangle$ is written as $\langle\psi|\phi\rangle$ and calculated as

$$\langle\psi|\phi\rangle \coloneqq \langle\psi|\,|\phi\rangle = \sum_i \psi_i^* \phi_i \,. \tag{II.4}$$

With the inner product defined, it is also possible to define the norm as

$$\| \,|\phi\rangle\, \| = \sqrt{\langle\phi|\phi\rangle} \,. \tag{II.5}$$

With respect to this norm, only vectors with unit length, so $\| \,|\psi\rangle\, \| = 1$, describe valid states of qubits.

As Hilbert spaces are vector spaces, different bases can be chosen so that linear combinations of those basis vectors span the Hilbert space. A basis $\{|b\rangle_1, \ldots, |b\rangle_k\}$ is *orthonormal*, if and only if its vectors are normalized and orthogonal to each other, so

$$\langle b_i|b_j\rangle = \delta_{ij} \coloneqq \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases} \tag{II.6}$$

for each two basis states $|b_i\rangle$,$|b_j\rangle$. Such a basis spans a complex Hilbert space of dimension k. Any orthonormal basis $\{|b\rangle_1, \ldots, |b\rangle_k\}$ for a vector space V fulfills the *completeness relation*

$$\sum_i |b\rangle_i = I \,. \tag{II.7}$$

The two-dimensional complex Hilbert space is used to describe the state of single qubits, and the basis usually chosen for this space is the so-called *computational*, or *rectilinear* basis. It consists of

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} . \tag{II.8}$$

Another base for the same Hilbert space is the *diagonal* basis $\{|+\rangle, |-\rangle\}$ with

$$|+\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) . \tag{II.9}$$

To differentiate in which basis a vector is referred to in, the notation $|\psi\rangle_\theta$ with $\theta \in +, \times$ is used.

$$|0\rangle_+ \coloneqq |0\rangle , \qquad |1\rangle_+ \coloneqq |1\rangle , \tag{II.10}$$

$$|0\rangle_\times \coloneqq |+\rangle , \qquad |1\rangle_\times \coloneqq |-\rangle . \tag{II.11}$$

If the index θ is not specified, $\theta = +$ is assumed. The naming and notation for the bases used here follows the naming and notations of Bennett and Brassard (1984).

II.2.2. Operators

A *linear operator* on a vector space V is a function $A\colon V \to V$ for which

$$A\left(\sum_i a_i |\psi_i\rangle\right) = \sum_i a_i A(|\psi_i\rangle), \forall |\psi_i\rangle \in V, a_i \in \mathbb{C} . \tag{II.12}$$

Matrices are linear operators and linear operators can have matrix representation (Nielsen and Chuang 2010, p. 64). So evaluating the matrix multiplication between the matrix representation of the operator A and vector $|\psi\rangle$ is equivalent to applying operator A to vector $|\psi\rangle$, $A(|\psi\rangle) = A|\psi\rangle$.

On a Hilbert space the *Hermitian conjugate* or *adjoint* of a matrix A is written as $A^\dagger$ and is the transpose of the complex conjugate A^* of A,

$$A^\dagger = (A^*)^T = ((a_{ij})^*)^T = (a^*_{ji}) . \tag{II.13}$$

This application of the adjoint on a matrix is derived from the definition of the adjoint for an operator. The adjoint of an operator on a Hilbert space is defined with the inner product of that hilbert space.

Definition II.6 (Adjoint). Let A be an operation on a Hilbert space $\mathcal{H}$, and for all $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ let $|\psi'\rangle \coloneqq A(|\psi\rangle)$ and $|\phi'\rangle \coloneqq A^\dagger(|\phi\rangle)$, then $A^\dagger$ is the only operation such that

$$\langle\phi|\psi'\rangle = \langle\phi'|\psi\rangle = \langle\phi|A|\psi\rangle . \tag{II.14}$$

♣

For every matrix representation of operator A, the adjoint of that matrix is a matrix representation of operator $A^\dagger$.

Definition II.7 (Hermitian, unitary and normal operators).

$$\text{An operator } A \text{ is } \begin{cases} \textit{Hermitian} \text{ or } \textit{self-adjoint}, \text{ iff} & A = A^\dagger \\ \textit{unitary}, \text{ iff} & AA^\dagger = I \\ \textit{normal}, \text{ iff} & AA^\dagger = A^\dagger A. \end{cases}$$

♣

Hermitian and unitary operators are normal.

Definition II.8 (Positive operators). A Hermitian operator A is *positive*, if and only if for all vectors $|v\rangle$ on the operators Hilbert space, $\langle v|A|v \geq 0\rangle$. It is *positive definite*, if and only if for all vectors $|v\rangle \neq 0$ on the operators Hilbert space, $\langle v|A|v > 0\rangle$. ♣

Definition II.9 (Projector). Given the n-dimensional vector space V and an m-dimensional subspace W of V, it is possible to construct an orthonormal basis $|v\rangle_1, \ldots, |v\rangle_n$ for V, such that $|v\rangle_1, \ldots, |v\rangle_m$ is a basis for W. The operator

$$P \equiv \sum_{i=1}^{m} |v_i\rangle \langle v_i| \tag{II.15}$$

is called the *projector* to subspace W. ♣

Projectors are Hermitian as $(|\psi\rangle \langle\psi|)^\dagger = |\psi\rangle \langle\psi|$ for any vector $|\psi\rangle$.

Let A be a linear operator, that acts on a vector space V. The *eigenvectors* and corresponding *eigenvalues* of A are the eigenvectors and corresponding eigenvalues of any of the matrix representations of that linear operator A. The eigenvectors and eigenvalues do not depend on a matrix representation, but the linear operator itself. Every eigenvalue λ has an *eigenspace*. It is the vector space that it is spanned by the eigenvectors to which the eigenvalue λ corresponds to, it also is a subspace of the operators vector space V.

Definition II.10 (Diagonal representation, diagonalizable). Let A be an operator on a vector space V and $\{|v_i\rangle\}$ an orthonormal set of eigenvectors of A with the eigenvalues λ_i. A *diagonal representation*, or *orthonormal decomposition*, of A is a representation of the form

$$A = \sum_i \lambda_i |v_i\rangle \langle v_i| \tag{II.16}$$

Not every operator has such a representation. Operators for which a diagonal representation exists are called *diagonalizable*. ♣

The following theorem is based on Nielsen and Chuang (2010, p. 72).

Theorem 1 (Spectral Decomposition):
Any diagonalizable operator is normal. Any normal operator M on a vector space V is diagonalizable. The orthonormal eigenvectors $\{|v_i\rangle\}$ that make up a decomposition of M are a basis for V. ♢

As $\{|v_i\rangle\}$ is an orthonormal basis for V, and $|v_i\rangle$ are eigenvectors of M with eigenvalues λ_i, $P_i \coloneqq |v_i\rangle \langle v_i|$ are projectors to the respective eigenspaces of M. So M can be decomposed into

$$M = \sum_i \lambda_i P_i \,. \tag{II.17}$$

Since $\{|v_i\rangle\}$ is an orthonormal basis for V, P_i fulfill the completeness relation

$$\sum_i P_i = I \,. \tag{II.18}$$

In addition to that, an orthonormality relation for P_i can be formulated as

$$P_i P_j = |v_i\rangle \overbrace{\langle v_i|v_j\rangle}^{=\delta_{ij}} \langle v_j| = \delta_{ij} P_i \,, \tag{II.19}$$

II.2.3. Tensor Product

To combine multiple Hilbert spaces the *tensor product* can be used.

Definition II.11 (Tensor product). Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be n and respectively m-dimensional Hilbert spaces. Then $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is a Hilbert space of dimension nm with the following properties. For its vectors:

$$\forall |\psi_1\rangle \in \mathcal{H}_1 |\psi_2\rangle \in \mathcal{H}_2 : \quad |\psi_1\rangle \otimes |\psi_2\rangle =: |\psi\rangle \in \mathcal{H} \tag{II.20}$$

$$\forall z \in \mathcal{C}, |\psi_1\rangle \in \mathcal{H}_1 |\psi_2\rangle \in \mathcal{H}_2 : \quad z(|\psi_1\rangle \otimes |\psi_2\rangle) = (z |\psi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes (z |\psi_2\rangle) \tag{II.21}$$

$$\forall |\psi_1\rangle, |\psi_1'\rangle \in \mathcal{H}_1 |\psi_2\rangle \in \mathcal{H}_2 : \quad (|\psi_1'\rangle + |\psi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1'\rangle \otimes |\psi_2\rangle \tag{II.22}$$

$$\forall |\psi_1\rangle \in \mathcal{H}_1 |\psi_2\rangle, |\psi_2'\rangle \in \mathcal{H}_2 : \quad |\psi_1\rangle \otimes (|\psi_2\rangle + |\psi_2'\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\psi_2'\rangle \ . \tag{II.23}$$

For any operator A on $\mathcal{H}_1$ and any operator B on $\mathcal{H}_2$, $C \coloneqq A \otimes B$ is an Operator on $\mathcal{H}$ and

$$\forall |\psi_1\rangle \in \mathcal{H}_1 |\psi_2\rangle \in \mathcal{H}_2 : \quad C(|\psi_1\rangle \otimes |\psi_2\rangle) \coloneqq A |\psi_1\rangle \otimes B |\psi_2\rangle \ . \tag{II.24}$$

♣

It is possible to generalize this definition to vector spaces and operators that map between different vector spaces, however this is not needed for the thesis and is therefore left out.

II.2 Example Let

$$|\psi\rangle \equiv \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix}, |\phi\rangle = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix} , \tag{II.25}$$

then the tensor product of those two vectors is

$$|\psi\rangle \otimes |\phi\rangle \equiv \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\phi\rangle \equiv \begin{pmatrix} \alpha_A |\phi\rangle \\ \beta_A |\phi\rangle \end{pmatrix} \equiv \begin{pmatrix} \alpha_A\alpha_B \\ \alpha_A\beta_B \\ \beta_A\alpha_B \\ \beta_A\beta_B \end{pmatrix} . \tag{II.26}$$

*

For brevity, the tensor symbol, $\otimes$, is sometimes omitted, and the dirac notation expanded, so

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle |\phi\rangle = |\psi, \phi\rangle \ . \tag{II.27}$$

For any number n of vectors of the form $|x_i\rangle_\theta$ with $x_i \in \{0, 1\}$ and $\theta \in \{+, \times\}$, a shorthand way to describe their tensor product is

$$|x\rangle_\theta = \bigotimes_{i=1}^{n} |x_i\rangle_\theta , x \in \{0, 1\}^n \tag{II.28}$$

II.3 Example

$$|01\rangle_+ = |0\rangle_+ \otimes |1\rangle_+ \tag{II.29}$$

*

With this, the computational basis for multi-qubit systems can be defined. An n-qubit system has 2^n computational basis states that span the 2^n-dimensional complex Hilbert space. The computational basis for this space is

$$\{|x_i\rangle : i \in \{0, \cdots, 2^n - 1\}\} , \tag{II.30}$$

where for each of the basis states $x_i \in \{0, 1\}^n$ is the binary representation of i.

II.4 Example Calculating the explicit vector $|x_i\rangle$ leads to the quite interesting observation, that the ith computational basis vector has a 1 in the ith place and zeroes everywhere else.

$$|x_i\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \text{index 0} \\ \\ \\ \text{index i} \\ \\ \\ \end{matrix}$$

*

The diagonal basis for n qubits can be defined analogously.

II.2.4. Operator functions

Functions on operators are defined by matrix functions acting on the spectral decomposition of an operator.

Definition II.12 (Operator function). Let A be a normal operator and $f\colon \mathbb{C} \to \mathbb{C}$ a function. With $A = \sum_i \lambda_i |v_i\rangle \langle v_i|$ being the spectral decomposition of A, the function

$$f'(A) \equiv \sum_i f(\lambda_i) |v_i\rangle \langle v_i| \ , \tag{II.31}$$

is the corresponding *operator function* to f. ♣

One such operator function is the *trace* function.

Definition II.13 (Trace). Given an operator A, the trace of A is

$$\mathrm{Tr}(A) \equiv \sum_i A_{ii} \tag{II.32}$$

The trace function is cyclic, linear, and invariant under similarity transformations. ♣

If an operator has the form $|\psi\rangle \langle\psi|$, the trace of that operator is

$$\mathrm{Tr}\left(|\psi\rangle \langle\psi|\right) = \langle\psi|\psi\rangle \ . \tag{II.33}$$

Related to the trace function is the *partial trace*.

Definition II.14 (Partial trace). Given two vector spaces, A and B, then $\forall\, |a_1\rangle, |a_2\rangle \in A$ and $\forall\, |b_1\rangle, |b_2\rangle \in B$, the *partial trace* over system B is the linear function

$$\mathrm{Tr}_B\left(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|\right) \equiv |a_1\rangle \langle a_2| \, \mathrm{Tr}\left(|b_1\rangle \langle b_2|\right). \tag{II.34}$$

♣

It is also possible to define the square root of an operator.

Definition II.15 (Square root of an operator). The square root of a positive operator B on a complex Hilbert space is the unique positive operator A, such that $A^2 = B$. ♣

II.3. Quantum Information and Quantum Computing

II.3.1. State Space

As described in Section II.2, quantum states can be represented as vectors on a complex Hilbert space. The state of a quantum system can be in a superposition of multiple states. In the vector representation this means, that the vector describing the state of the system in question is a linear combination of vectors describing other states, usually basis vectors.

II.5 Example A single qubit in superposition of the computational basis states can be written as

$$\alpha |0\rangle + \beta |1\rangle = |\psi\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2 \tag{II.35}$$

When measured in that basis, the result will be $|0\rangle$ with a probability of $|\alpha|^2$ and $|1\rangle$ with a probability of $|\beta|^2$. Like in Example II.1, the state describing the qubit *collapses* to one of the basis states. This means after measuring the qubit to be $|0\rangle$ (or $|1\rangle$ respectively) all future measurements will also show the qubit to be $|0\rangle$ (or $|1\rangle$ respectively). The details of measurement will be described in Section II.3.3. ∗

Given multiple systems, whose states can be described by the vectors $|\psi_i\rangle^{\mathcal{H}_i}$ acting on the Hilbert spaces $\mathcal{H}_i$ respectively, the state of the combined system can be described by the state vector

$$|\psi\rangle^{\mathcal{H}} = \bigotimes_i |\psi_i\rangle^{\mathcal{H}_i} \ , \tag{II.36}$$

acting on $\mathcal{H}$, the tensor product of the Hilbert spaces $\mathcal{H}_i$. This notation, to write the system a state belongs to as a superscript to the ket or bra describing that state, will be used throughout the thesis where applicable.

II.3.2. Evolution

The evolution of a closed quantum system is described by an operation that transforms the state of the system at time t_1 to the state of the system at time t_2. A closed system is a system that does not interact with its environment, while an open system is a system that is influenced in some way by its environment.

As quantum states can be represented as vectors on complex Hilbert spaces, linear operators that can be applied on quantum states have a matrix representation and act on the respective Hilbert spaces. An operation U applied to a quantum state $|\psi\rangle$ should also result in a valid quantum state $U|\psi\rangle = |\psi_{\text{new}}\rangle$. As the restriction to a vector to describe a valid quantum state is that it is of unit length, the restriction for a matrix to describe a valid operation on a state has to be that it is unitary.

II.6 Example One important operation is the Hadamard transformation,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{II.37}$$

It transforms the states $|0\rangle$ and $|1\rangle$ to a superposition of $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ respectively. H is also Hermitian, and since it is unitary $HH = I$. ∗

In addition to modelling operators as matrices, there exists the *quantum turing machine* and the *quantum circuit* model, which can help to structure quantum operations. The latter models operations as (reversible) *quantum logic gates* and will be explored in Subsection II.3.9.

II.3.3. Measurement

Measurement in Quantum mechanics can be described by a set of measurement operators $\{M_m\}$, acting on the Hilbert space of the system being measured. Each index m corresponds to a possible distinct measurement outcome that can occur. The probability for the measurement outcome m to occur is

$$\Pr[m] = \langle\psi| M_m^\dagger M_m |\psi\rangle \ , \tag{II.38}$$

with $|\psi\rangle$ being the state of the system before being measured. Has m occurred, the state of the system changes and the new state can be descried as

$$|\psi_{\text{new}}\rangle = \frac{M_m |\psi\rangle}{\sqrt{\Pr[m]}} \, . \tag{II.39}$$

All possible outcomes have to be described, and all probabilities have to sum up to one for any a priory system state, this is ensured with the *completeness equation*

$$\sum_m M_m^\dagger M_m = I \tag{II.40}$$

A special class of measurements are *projective measurements*. Instead of directly being described by a set of Measurement operators, they are described by an *observable* M, which is composed of a set of Hermitian, orthogonal projectors $\{P_m\}$. To be more precise, M has a spectral decomposition

$$M = \sum_m m P_m \, . \tag{II.41}$$

The projectors then act analogously to the Measurement operators in the general case, with the probability of receiving result m being

$$\Pr[m] = \langle\psi| P_m |\psi\rangle \ , \tag{II.42}$$

with the a priori system state $|\psi\rangle$. The a posteriori system state with the occurrence of m is

$$|\psi_{\text{new}}\rangle = \frac{P_m |\psi\rangle}{\sqrt{\Pr[m]}} \, . \tag{II.43}$$

Another name for projective measurements is *von Neumann measurements*. "Measuring a state in a basis" is a form of projective measurement, where the projectors correspond to the basis states,

$$P_m = |m\rangle \langle m| \ . \tag{II.44}$$

With Equation II.43, it can be verified that the new state after basis state $|m\rangle$ was measured, is in fact the same basis state $|m\rangle$,

$$|\psi_{\text{new}}\rangle = \frac{|m\rangle \langle m| |\psi\rangle}{\sqrt{\langle\psi| |m\rangle \langle m| |\psi\rangle}} = |m\rangle \ . \tag{II.45}$$

With Equation II.42, the probability to get the measurement result m can be calculated to be

$$\Pr[m] = \sqrt{\langle\psi| |m\rangle \langle m| |\psi\rangle} = \langle\psi|m\rangle \ . \tag{II.46}$$

II.7 Example Calculating the probabilities for the single qubit Example II.5:

$$\Pr[0] = \langle\psi|\,|0\rangle\,\langle 0|\,|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}^{\dagger}\begin{pmatrix}1\\ 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}^{\dagger}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = (1\alpha+0\beta)(1\alpha^*+0\beta^*) = |\alpha|^2 \tag{II.47}$$

$$\Pr[1] = \langle\psi|\,|0\rangle\,\langle 1|\,|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}^{\dagger}\begin{pmatrix}0\\ 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}^{\dagger}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = (0\alpha+1\beta)(0\alpha^*+1\beta^*) = |\beta|^2 \tag{II.48}$$

∗

A special case of the measurement formalism is the *POVM* formalism, it focuses on the measurement probability outcomes rather than the state after measurement. The initialism POVM stands for *"Positive Operator-Valued Measure"*, which classifies its elements. POVMs are defined to be a set $\{E_m\}$ of positive valued operators known as *POVM elements*, that satisfy the completeness relation $\sum_m E_m = I$. Given a POVM, a set $\{M_m\}$ of measurement operators can be derived by defining $M_m \coloneqq \sqrt{E_m}$. Similarly, given a set of measurement operators $\{M_m\}$, the POVM $\{E_m\}$ can be described with the elements $E_m = M_m^\dagger M_m$. Following the probability equation for measurement operators II.38, the probability for outcome m is given by $\Pr(m) = \langle\psi|E_m|\psi\rangle$. A completeness relation for POVMs can be derived, following the completeness relation II.40 for measurement operators.

II.3.4. Phase

Consider the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \alpha, \beta \in \mathbb{C}$ of a single qubit. As described in Example II.1 and Sections II.2.1 and II.3.1, the complex numbers α, β encode the amplitude and phase of a wave function in the chosen basis states. This can be explicitly shown by rewriting the state vector as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\right), \gamma, \varphi, \theta \in \mathbb{R}\,. \tag{II.49}$$

It is important to point out the relevance of the phase. The phases, or more precisely phase differences dictate how probability amplitudes of states interfere with each other.

II.8 Example Take the states $|\psi_1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$. With both of these states, measuring in the rectilinear basis, the probability of getting $|0\rangle$ or $|1\rangle$ respectively is $\frac{1}{2}$. But a system in equal superposition of those states is in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle) + \frac{1}{\sqrt{2}}(|\psi_2\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle) \tag{II.50}$$

$$= \frac{1}{2}(|0\rangle + |0\rangle) + \frac{1}{2}(|1\rangle - |1\rangle) \tag{II.51}$$

$$= |0\rangle\ . \tag{II.52}$$

Which, when measured in the rectilinear basis always results in $|0\rangle$. ∗

Since only the phase difference dictates how the probability amplitudes of states interact with each other, this also means that the global phase will have no effect on measurement outcomes and can safely be ignored. The state thus can be described by

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\,, \varphi, \theta \in \mathbb{R}\,. \tag{II.53}$$

It can be observed, that the state is dependent of two rational angles. The *boch sphere* (Figure II.3.1) visualizes this observation. A one qubit quantum state is illustrated as a point on the surface of the bloch sphere. Its position is defined by the angle φ off the x-Axis and the angle θ off the y-Axis. Observe that since $|0\rangle = \cos\frac{0}{2} + e^{i\varphi}\sin\frac{0}{2}\,|1\rangle$

and $|1\rangle = \cos\frac{\pi}{2}|0\rangle + e^{i\varphi}\sin\frac{\pi}{2}|1\rangle, \varphi \in \mathbb{R}$, the orthogonal basis states $|0\rangle$ and $|1\rangle$ lie on opposite sites of the same axis in the bloch-sphere-representation. So these states that are orthogonal in Hilbert space lie on the same axis in the bloch sphere. This also visualizes that θ represents the bias a state has towards one basis state or the other. In contrast to that, $|\varphi\rangle$ represents the phase difference between the basis states, which grows less important the closer states move to the poles. The states $\{|+\rangle, |-\rangle\}$ of the diagonal basis

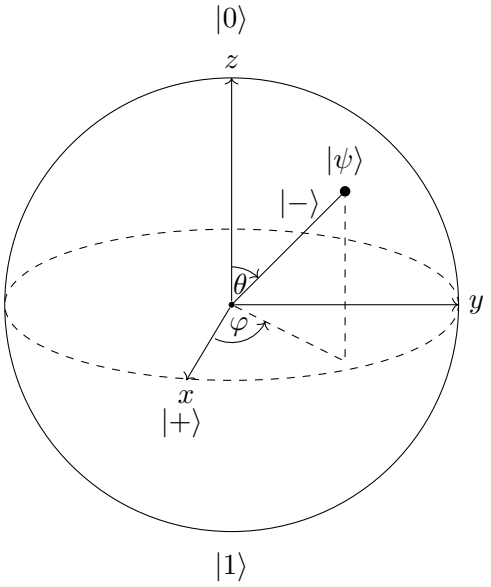


Figure II.3.1.: Bloch sphere

are at an $\theta = 90°$ angle to the computational basis states. As they are also orthogonal in Hilbert space, they also share an axis on the Bloch sphere.

II.3.5. Entangled States, Separable States

The state of a multi qubit system can be entangled. When a system is entangled, evolution or measurement on one part of the system instantaneously influences the measurement outcome another, spatially distant, part of the system.

II.9 Example An example for an entangled pair of qubits is the EPR-pair $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Here $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$ are the only possible results, so if one measures the left qubit to be $|0\rangle$ (respectively $|1\rangle$) it is known that a measurement of the right qubit will always return $|0\rangle$ (respectively $|1\rangle$) as well. ∗

There are degrees of entanglement a state can have. Genrally a state $|\psi\rangle^{A\otimes B}$ is *separable*, if and only if there exist states $|\psi\rangle^A$,$|\psi\rangle^B$ such that $|\psi\rangle^{A\otimes B} = |\psi\rangle^A \otimes |\psi\rangle^B$ and it is entangled if and only if it is not separable.

II.3.6. Density Operators

In a more general form than state vectors, states can also be descried by *density operators*.

Definition II.16 (Density operator). A positive operator ρ is a density operator, if and only if it has a trace equal to one,

$$\mathrm{Tr}(\rho) = 1\,. \tag{II.54}$$

♣

The state of a system that can be described by the vector $|\psi\rangle$ on a complex Hilbert space, can equivalently be described by the density operator $\rho = |\psi\rangle\langle\psi|$.

A system whose state can be described by a single density operator ρ may not necessarily be described by a single vector as well. A system can be in an *ensemble* of states, this means that for a set $\{|\psi_i\rangle\}$ of state vectors it is known to be in state $|\psi_i\rangle$ with probability p_i. Such a system is said to be in a *mixed state*, and this state can be described by a single density operator

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \,. \tag{II.55}$$

In terms of density operators, if a system is known to be in the state ρ_i with the probability $p_i \coloneqq \Pr(\rho_i)$, its density operator is

$$\rho = \sum_i p_i \rho_i \,. \tag{II.56}$$

A detailed definition of ensembles is given in Definition III.1. A quantum systems state is a *pure state*, if and only if it is known exactly. That is, when its state can be described by a single vector $|\psi\rangle$ or a density matrix ρ that can be written as $\rho = |\psi\rangle\langle\psi|$. For any pure state ρ, it applies that $\mathrm{Tr}(\rho^2) = 1$, and for any mixed state ρ', it applies that $\mathrm{Tr}(\rho') < 1$.

Let U be the unitary transformation that describes the evolution of a system from the state described by $|\psi\rangle$ to the state described by $U|\psi\rangle$. The same transformation can be applied to a system in a state described by the density operator ρ. The new state of the system is then described by $\rho_{\text{new}} = U\rho U^\dagger$.

Given a complete set $\{M_m\}$ of measurement operators and the a priori system state ρ, the probability for measurement outcome m to occur is given by

$$\Pr(m) = \mathrm{Tr}(M_m^\dagger M_m \rho) \tag{II.57}$$

and the state of the system after the measurement is

$$\rho_{\text{new}} = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m^\dagger)} \,. \tag{II.58}$$

Take multiple systems whose states can be described by the density operators $\rho_i^{\mathcal{H}_i}$, acting on their respective state spaces $\mathcal{H}_i$. Analogous to the state vector description, the composite system is described on the state space $\mathcal{H} = \bigotimes \mathcal{H}_i$, and its state is described by the operator

$$\rho^{\mathcal{H}} = \bigotimes_i \rho_i^{\mathcal{H}_i} \,. \tag{II.59}$$

Given a composite system in the state ρ, the states of the systems making up the composite system can be described using the partial trace over ρ. As with state vectors, when describing states of different or composite systems, a superscript is added to the density operator, indicating the respective system it acts on. Let $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ be the state space of the composite system of the systems $\mathcal{A}$ and $\mathcal{B}$ with the state spaces $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$ respectively. Denote $\rho^{\mathcal{H}}$ the state of the composite system, then the resulting *reduced density operator*of system $\mathcal{A}$ is

$$\rho^{\mathcal{H}_\mathcal{A}} = \mathrm{Tr}_\mathcal{B}(\rho^{\mathcal{H}}) \,, \tag{II.60}$$

and the reduced density operator for system $\mathcal{B}$ is

$$\rho^{\mathcal{H}_\mathcal{B}} = \mathrm{Tr}_\mathcal{A}(\rho^{\mathcal{H}}) \,. \tag{II.61}$$

With $\mathrm{Tr}_\mathcal{P}, \mathcal{P} \in \{\mathcal{A}, \mathcal{B}\}$ being the partial trace over system $\mathcal{P}$. Even when $\rho^{\mathcal{H}}$ is a pure state, in many cases $\rho^{\mathcal{H}_\mathcal{A}}$ or $\rho^{\mathcal{H}_\mathcal{B}}$ are mixed states.

Theorem 2 (Schmidt decomposition[1]):
Let $|\psi\rangle$ be a pure state of a system $\mathcal{H}_1 \otimes \mathcal{H}_2$, and let $k \coloneqq \min(\dim(\mathcal{H}_1), \dim(\mathcal{H}_2))$. Then there exist orthonormal bases $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ of systems $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, and coefficients $\{0 \leq \lambda_i \in \mathbb{R} \colon \sum_{i=1}^{k} \lambda_i = 1\}$, such that $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i=1}^{k} \lambda_i |e_i\rangle |f_i\rangle \ . \tag{II.62}$$

This is called the Schmidt decomposition *of $|\psi\rangle$.* ♢

To find such orthonormal states, the following corollary can be used.

Corollary 3 (Schmidt polar form[2]):
Let $|\psi\rangle$ be a pure state of a system $\mathcal{H}_1 \otimes \mathcal{H}_2$. Let $\rho_1 = \mathrm{Tr}_{\mathcal{H}_2}(|\psi\rangle\langle\psi|)$ and $\rho_2 = \mathrm{Tr}_{\mathcal{H}_1}(|\psi\rangle\langle\psi|)$ the reduced density operators of systems $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, and let $k \coloneqq \min(\dim(\mathcal{H}_1), \dim(\mathcal{H}_2))$. Then ρ_1 and ρ_2 have the same nonzero eigenvalues with the same multiplicities. Following that, if one space is larger than the other, the extra dimensions are made up with zero eigenvalues. Let $|e_i\rangle$ and $|f_i\rangle$ be orthonormal eigenvectors of ρ_1 and ρ_2 respectively. Then $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i=1}^{k} \sqrt{\lambda_i} |e_i\rangle |f_i\rangle \ . \tag{II.63}$$

This is sometimes also referred to as the Schmidt polar form. ♡

II.3.7. Distance Measures

Quantum distance measurements aim to describe how similar two states are, or how difficult it is to tell them apart. As it is not possible to read the exact amplitude and phase of a qubit, but only to measure it and receive some result with some probability, quantum distance measures are in some regards similar to measures differentiating probability distributions.

One such measure for difference in quantum states is the trace distance between those states.

Definition II.17 (Trace distance). The *trace distance* between two states ρ and σ is

$$D(\rho, \sigma) \coloneqq \frac{1}{2} \mathrm{Tr} |\rho - \sigma| \ , \tag{II.64}$$

with $|A| \coloneqq \sqrt{A^\dagger A}$ ♣

The trace distance between single qubit states can be visualized well on the bloch sphere, it is equal to $\frac{1}{2}$ the Euclidean distance between those states on it.

Another important measure is the fidelity.

Definition II.18 (Fidelity). The *fidelity* between two states ρ and σ is

$$F(\rho, \sigma) \coloneqq \mathrm{Tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}} \, . \tag{II.65}$$

For all

$$\rho, \sigma, 0 \leq F(\rho, \sigma) \leq 1 \, , \tag{II.66}$$

where equality in II.66 is achieved on the left side if and only if ρ and σ are orthogonal, and on the right side if and only if $\rho = \sigma$. ♣

[1] This theorem is based on the phrasing Nielsen and Chuang (2010, p. 109) give of Schmidt (1907, §15).
[2] This corollary is based on the application Hughston, Jozsa, and Wootters (1993, p. 5) give of Schmidt (1907, §15).

So a higher fidelity between states means that they are harder to tell apart, while a higher trace distance implies that the states are less similar to each other. Both fidelity and trace distance are invariant under unitary transformations that are applied to both states.

Given an unknown state $|\psi_i\rangle$ from a set of known orthonormal states $\{|\psi_i\rangle\}$, it is possible to determine which state of the set was given by performing an appropriate measurement. However, if given a state $|\phi_i\rangle$ from a set of known non-orthogonal states $\{|\phi_i\rangle\}$, it is not possible to determine which state was given with absolute certainty . The amount of information that is possible to gain about $|\phi_i\rangle$ is dependent of how close $\{|\phi_i\rangle\}$ are to each other. The closer they are, the harder they are to differentiate. This observation is related to the no-cloning theorem.

Theorem 4 (No-cloning):
Non-orthogonal quantum states cannot be copied. That is, for any given quantum device that performs a valid operation modelled by a unitary operation U: If U is able to copy $|\psi\rangle$ and $|\phi\rangle$ as follows

$$|\psi\rangle\,|\xi_{target}\rangle\,U = |\psi\rangle\,|\psi\rangle \tag{II.67}$$
$$|\phi\rangle\,|\xi_{target}\rangle\,U = |\phi\rangle\,|\phi\rangle\ , \tag{II.68}$$

then $|\psi\rangle$ and $|\phi\rangle$ are either the same state, or orthogonal to each other. ◇

See also the no-cloning theorem as given by Nielsen and Chuang (2010, p. 532).

II.3.8. Decoherence

While in quantum information usually closed systems are considered, in reality most systems are influenced by their environment. Consider a system in a pure a state represented by the matrix ρ, the diagonal elements are called *populations* while the off-diagonal elements are called *coherences*. When interacting with the environment the populations stay unaffected, while the coherences get multiplied with a factor of modulus of less than one and thus get suppressed with more interactions over time (Hornberger 2009, p. 224). After the interaction, the system is not in a pure state anymore. The populations measure the probabilities that the system is in either state of the basis states. The coherences measure the amount of quantum interference between the states (Brandt 2003, p. 309) and characterize the ability of the system to display a superposition between basis states (Hornberger 2009, p. 224). This loss of coherence occurs in a special basis, determined by the type of environmental interaction.

II.10 Example Let the state of a system be the pure state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. The corresponding density operator is

$$\rho = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\ . \tag{II.69}$$

Through interaction with the environment, ρ eventually loses its coherences. The system is now in the mixed state

$$\rho' = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\ . \tag{II.70}$$

Thus it is not in superposition, but in an ensemble of the states $|0\rangle$ and $|1\rangle$, each with probability $\frac{1}{2}$, analogous to a system that has been measured but whose result has been forgotten. ∗

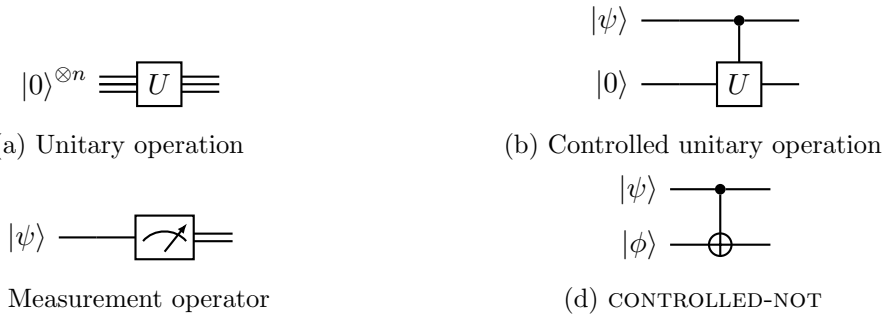
Decoherence is also the reason why large scale systems do not seem to show quantum behaviour.

II.3.9. Quantum Circuits

Computing is fundamentally reversible. However, in classical computing some information is not kept track of, so that it is not reversible anymore. This is not the case for quantum computing, as operations are carried out on individual particles or a set of individual particles. This is also modeled in the algebraic sense: operations are unitary matrices and thus invertible. In fact, the inverse of a unitary matrix is its complex conjugate.

The quantum circuit model models operations as quantum logic gates, similar to classical circuits that use classical logic gates. There are some differences between quantum and classical circuits, as per the no-cloning theorem, fanout operations are not permitted. As quantum operations have to be reversible, and the classical OR operation is not, fan-in is not permitted either. Time in a quantum circuit diagram is modeled to go in one direction. In this thesis, it is always modeled going from left to right.

In a quantum circuit diagram single qubits are presented on quantum "wires", classical wires for classical bits are drawn as double stroked wires. A quantum circuit usually consists of quantum and classical wires, quantum logic gates and measurement operators. On the left side of a quantum circuit, for each quantum wire, the state that wire starts in can be denoted. Quantum logic gates can be unitary operations, CONTROLLED-NOT-gates, or controlled unitary operations. A controlled operation means that the operation is only applied to the target qubit, if the control qubit is one. Gates that have multiple control or target qubits are also valid quantum logic gates. Those parts of quantum circuit diagrams are illustrated in Figure II.3.2.



(a) Unitary operation

(b) Controlled unitary operation

(c) Measurement operator

(d) CONTROLLED-NOT

Figure II.3.2.: Components of a quantum circuit

All quantum circuits can be rewritten to use only a discrete subset of quantum logic gates, so called *universal gates*. The number of those universal gates in a circuit can be a good metric of how complex the operation being modelled, is.

Theorem 5 (Deferred measurement):
The usage of a measuring apparatus at any point of the quantum circuit can be moved to the end of said circuit, without changing its behavior ♢

Theorem 6 (Implicit measurement):
Any unterminated quantum wire is assumed to be measured. This does not change the circuits' behaviour. ♢

Compare to principles of deferred and implicit measurement as given by Nielsen and Chuang (2010, p. 186 et seq.).

II.4. Quantum Cryptography

II.4.1. Quantum bit commitment

Quantum bit commitment (QBC) works analogous to classical bit commitment, however instead of a classical commitment c_b, the bit b is encoded in a quantum state $|\psi_b\rangle$. A difference is that an encoding $|\psi_b\rangle$ can be chosen so that the probability of $unveil(|\psi_b\rangle) \to b$ is an arbitrary probability p. This is reflected in the modified security definitions.

Definition II.19 (Perfectly binding for quantum bit commitments). A quantum bit commitment scheme is *perfectly binding*, if and only if for any commitment $|\psi\rangle$ and for any procedures $\text{unveil}'_1, \text{unveil}'_2$, modified by a dishonest Alice,

$$|\Pr\left[\text{unveil}'_1(|\psi\rangle) \to b\right] - \Pr\left[\text{unveil}'_2(|\psi\rangle) \to (1-b)\right]| = 0\,. \tag{II.71}$$

♣

Definition II.20 (Perfectly concealing for quantum bit commitments). A quantum bit commitment scheme is *perfectly concealing*, if and only if every commitment $|\psi_{b,\eta}\rangle$ produced by a honest Alice is perfectly concealing. The random string η denotes all the classical information available to Bob after the commit-phase. The encoding is perfectly concealing, if and only if the following two conditions are met: No information about b is provided by η. The reduced density operators, $\rho^B(|\psi_{0,\eta}\rangle)$ and $\rho^B(|\psi_{1,\eta}\rangle)$, of the collapsed states in Bob's systems B for $b = 0$ and $b = 1$ respectively given η are identical, so

$$F(\rho^B(|\psi_{0,\eta}\rangle), \rho^B(|\psi_{1,\eta}\rangle)) = 1\,. \tag{II.72}$$

♣

It is known that there exists no *perfectly secure*, that means perfectly binding and perfectly concealing, quantum bit commitment scheme. Therefore, it is reasonable to define weaker properties.

Definition II.21 (Statistically binding for qbc). A quantum bit commitment scheme with security parameter n is *statistically binding*, if and only if it can be made arbitrarily close to perfectly binding by an increase of n. So if and only if for every commitment $|\psi\rangle$ and for procedures $\text{unveil}'_1, \text{unveil}'_1$, modified by a dishonest Alice,

$$|\Pr\left[\text{unveil}'_1(|\psi\rangle) \to b\right] - \Pr\left[\text{unveil}'_2(|\psi\rangle) \to (1-b)\right]| \leq \text{negl}(n)\,. \tag{II.73}$$

♣

Definition II.22 (Statistically concealing for qbc). A quantum bit commitment scheme with security parameter n is *statistically concealing*, if and only if it can be made arbitrarily close to perfectly concealing by an increase of n. So with the same notation as in Definition II.20, an increasingly small amount of information about b is contained in η, and

$$F(\rho^B(|\psi_{0,\eta}\rangle), \rho^B(|\psi_{1,\eta}\rangle)) = 1 - \delta, \quad \delta \geq 0\,, \tag{II.74}$$

♣

with $\delta \leq \text{negl}(n)$.

Definition II.23 (Statistical security for qbc). Finally, a QBC-protocol (with security parameter n) is *statistically secure*, if and only if it is statistically binding and statistically concealing. ♣

As with the classical definitions, the statistical definitions can be extended to *unconditional* binding, concealing or secure, if they hold against an unconditional adversary.

II.4.2. Controllable Algorithms

As described in Subsection II.3.9, quantum circuits are reversible which means for every quantum circuit, given all outputs, all inputs can be determined. However, only some of the output is relevant for the algorithm the quantum circuit is trying to implement.

II.11 Example Consider the CONTROLLED-NOT gate (Figure II.4.1a), take both inputs, but only regard the second output, then it acts just like a classical XOR-gate. Given only the output 0 of an XOR gate, one cannot determine, whether both inputs were 1, or if both inputs were 0. With the extra (upper) output of a CONTROLLED-NOT gate, which does not change its value, one can determine both inputs and thus reverse the operation. Is one to implement an XOR function using (reversible) quantum gates, the upper output however is of no relevance. ∗

Those outputs not relevant for the algorithm are labeled as *trash* and are not regarded as part of the actual output. In general, trash bits have an undefined value. Not all input bits are of special relevance either, inputs that have predefined values are called *presets* and not regarded as part of the actual input.

II.12 Example To implement an AND gate, one can take a CONTROLLED-CONTROLLED-NOT-gate (Figure II.4.1b), set the c wire to the preset 0, and leave the a, b wires as inputs. The c wire, on which the target bit is carried, then carries the output and the a and b wires, which carried the control bits, are trash. ∗

(a) CONTROLLED-NOT (b) CONTROLLED-CONTROLLED-NOT

Figure II.4.1.: Controlled operations with labeled inputs

A controllable algorithm is then defined to be an efficient reversible algorithm, where the total number of garbage bit configurations is polynomial in the size of the input (Chau and Lo 1997).

II.4.3. Quantum One-Way Functions and Permutations

In this subsection, the definitions for quantum one-way functions and quantum one-way permutations are following Crépeau, Légaré, and Salvail (2001). There are functions that can be evaluated by quantum computers more efficiently than by classical computers, such as integer factoring (Shor 1994, 1999). So it makes sense to phrase the definitions of quantum one-way functions and permutations in such a way as to include those functions which a quantum computer could, but a classical computer could not, compute in the forward direction (Dumais, Mayers, and Salvail 2000).

Definition II.24 (Quantum one-way function). A classical function $f : \{0,1\}^n \to \{0,1\}^{l(n)}$, with $l(n)$ being a function in the security parameter n, is called a quantum one-way function (QOWF), if and only if $f(x)$ can be efficiently computed by a quantum computer given any $x \in \{0,1\}^n$ but for any polynomial-time quantum adversary $\mathcal{A}$

$$\Pr[\mathcal{A}(1^n, y) \in f^{-1}(y) \colon y := f(x), x \in_R \{0,1\}^n] \leq \mathrm{negl}(n)\,. \tag{II.75}$$

Such an adversary is often called an *inverter*. ♣

Definition II.25 (Quantum one-way permutation). A classical permutation $f : \{0,1\}^n \to \{0,1\}^n$ is called a quantum one-way permutation (QOWP), if and only if $p(x)$ can be efficiently computed by a quantum computer given any $x \in \{0,1\}^n$ but for any polynomial-time quantum adversary $\mathcal{A}$

$$\Pr[\mathcal{A}(1^n, y) \in p^{-1}(y) \colon y := p(x), x \in_R \{0,1\}^n] \leq \mathrm{negl}(n)\,. \tag{II.76}$$

♣

One might wonder whether the existence of reversible computing is opposed to the concept of one-way functions, as one could, with knowledge of the quantum circuit that produces $y = f(x)$, run said quantum circuit in reverse to produce $x = f^{-1}(y)$. However, as described in Section II.4.2, a quantum algorithm usually also produces trash bits, which are disregarded and not part of the considered output, but would be necessary, to execute the circuit in reverse. So Chau and Lo (1997) give and prove a precision for the definition of quantum one-way functions (respectively permutations). They show a one-to-one function[3] that can be computed efficiently, is one-way exactly when it cannot be computed by any controllable algorithm.

II.4.4. Quantum Hard-Predicate

To concentrate the one-wayness of a quantum one-way permutation to a single bit, Adcock and Cleve (2002) give a definition of a hard-predicate.

Definition II.26 (Hard-Predicate). Given a quantum one-way permutation $f \colon \{0,1\}^n \to \{0,1\}^n$, $h \colon \{0,1\}^n \to \{0,1\}$ is a *hard-predicate* of f, if and only if for any random $a \in \{0,1\}^n$ $h(a)$ is easy to predict, but for any quantum adversary $\mathcal{A}$,

$$\Pr\left[\mathcal{A}(f(a)) = h(a)\right] \leq \frac{1}{2} + \mathrm{negl}(n)\,. \tag{II.77}$$

♣

II.4.5. Quantum Oblivious Transfer

There are several types of oblivious transfer, the one relevant for this thesis is quantum one-out-of-two oblivious transfer, abbreviated with QOT. The definitions in this subsection are based on Crépeau (1994).

In QOT, Alice prepares two messages, b_0 and b_1, for Bob and Bob chooses a $c \in \{0,1\}$, that specifies which one of those messages he wishes to receive. Alice should not be able to discover which message Bob chose to receive, and Bob should only able to retrieve information about the message he chose, without being able to gain any information about the other. So a one-out-of-two quantum oblivious transfer has to fulfill the following criteria

Definition II.27 (Correctness). A QOT-protocol is *correct*, if and only if whenever Alice and Bob both follow the protocol honestly, Alice starts with input bits b_0 and b_1, and Bob makes the choice c, the protocol ends with Bob receiving b_c ♣

Definition II.28 (Privacy). A QOT-protocol is *private*, if and only if

1. for all b_0 and b_1, Alice chooses, for all a priori information H[4] she has access to, and whatever program she runs, she is not able to gain any information about c.
2. for all a priori information H Bob has access to, for all b_0 and b_1 Alice chooses and for all c he chooses, and whatever program he runs, he is not able to gain information about more than one of b_0 and b_1. ♣

[3] When regarding presets as part of the inputs and trash as part of the outputs, all quantum circuits always have the same number of inputs as outputs, and thus implement one-to-one functions.

[4] H identifies information the participant has before the protocol starts.

The statistical definitions of these properties are for some constraint $0 < \varepsilon < 1$ and the security parameter n. The protocol is *statistically correct*, if and only if it is correct except with a probability of at most ε^n. Furthermore it is *statistically private*, if and only if it is private except with a probability of at most ε^n.

Also of note is that Crépeau (1994) introduces a QOT-protocol which they claim to be secure, however they base its privacy on the security of the BCJL-protocol (Brassard, Crepeau, et al. 1993) which was later shown to be insecure by the very proof that is explored in this thesis (Mayers 1997). However, its privacy could be based upon another secure bit commitment. This is explored in Subsection IV.2.3.

III. The Impossible

In this chapter the no-go theorem of Mayers (1997) will be explored. First the generalized environment, in which the proof of the no-go theorem will take place, is presented. Then the explicit BB84 scheme will be put into this environment. A cheating strategy and an example for it will be subsequently shown. Later in this chapter it will be discussed, how the cheat for Alice, as described by Mayers, works in a general scenario.

III.1. Environment

The environment in which the no-go theorem will be presented assumes that neither party or means of communication are affected by decoherence. In addition to that, relativistic effects will not be taken into account. It is also assumed, that parties not following the honest protocols are not bounded by space, time or computational power. It follows, that they are able to perform any valid quantum mechanical measurement or evolution. Let Alice be the party sending the commitment and Bob the party receiving it. The entire system is described by a set of subsystems

$$\underbrace{\underbrace{\mathcal{H}_{S,\mathcal{A}} \otimes \mathcal{H}_{S,\mathcal{B}}}_{\mathcal{H}_S} \otimes \mathcal{H}_{E,\mathcal{A}} \otimes \mathcal{H}_{E,\mathcal{B}}}_{\mathcal{H}_E} \otimes \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \tag{III.1}$$

$\mathcal{H}_{\mathcal{A}}, \mathcal{H}_{\mathcal{B}}$ are two-dimensional quantum registers, belonging to Alice and Bob respectively. However, Alice and Bob are able to introduce new registers, initialized in the $|0\rangle$ state.

- $\mathcal{H}_E = \mathcal{H}_S \otimes \mathcal{H}_{E,\mathcal{A}} \otimes \mathcal{H}_{E,\mathcal{B}}$ is the environment.
- $\mathcal{H}_S = \mathcal{H}_{S,\mathcal{A}} \otimes \mathcal{H}_{S,\mathcal{B}}$ stores *transmitted classical* Bits.
- $\mathcal{H}_{S,\mathcal{A}}$ bits Alice transmitted or received and $\mathcal{H}_{S,\mathcal{B}}$ bits Bob transmitted or received.
- $\mathcal{H}_{E,\mathcal{A}}$ and $\mathcal{H}_{E,\mathcal{B}}$ store *untransmitted classical* Bits of Alice and Bob respectively.
- $|\psi_b\rangle$ of $\mathcal{H}_E \otimes \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ is an encoded commitment.

III.1.1. Measuring a State

Let the measured system be in an initial state $|\phi\rangle = \alpha |\phi_0\rangle + \beta |\phi_1\rangle$. To execute a binary measurement outcome, participant $\mathcal{P} \in \{\mathcal{A}\text{lice}, \mathcal{B}\text{ob}\}$ introduces a new quantum register which initially is in the state $|0\rangle$. $\mathcal{P}$ entangles it with the measured system, the new state of the entire system is of the form $\alpha |0\rangle |\phi_0\rangle + \beta |1\rangle |\phi_1\rangle$. After that, they send the new register to a measurement apparatus $\mathcal{H}_{E,\mathcal{P}}$. This process of entangling $|\phi\rangle$ with a new register and sending this register to a measuring apparatus is later referred to as *sending $|\phi\rangle$ to the environment.*

As an external viewer, which is not aware of this measurement outcome, this can be seen as if the measuring apparatus amplifies and stores each component $|x\rangle$ as a state $|x\rangle^{\mathcal{H}_{E,\mathcal{P}}}$. The resulting state is

$$\alpha |0\rangle^{\mathcal{H}_{E,\mathcal{P}}} |\phi_0\rangle^{\mathcal{H}_{\mathcal{P}}} + \beta |1\rangle^{\mathcal{H}_{E,\mathcal{P}}} |\phi_1\rangle^{\mathcal{H}_{\mathcal{P}}} . \tag{III.2}$$

This is illustrated as a quantum circuit in Figure III.1.1. However, as the state actually has collapsed into the state $|\xi\rangle$, this collapse has to be taken into account when modelling transformations on the new state of the system.

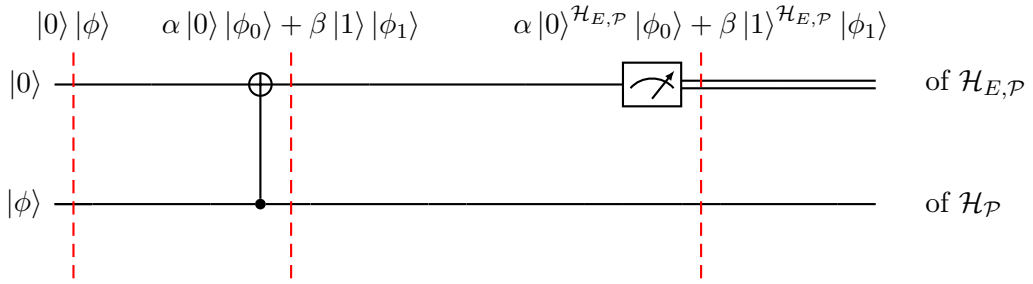


Figure III.1.1.: Quantum Circuit demonstrating how Participant $\mathcal{P}$ measures a system

In this simple case, the amplitudes are dependent on whether $\mathcal{P}$s measurement outcome was 0 or 1, thus they are dependent on the occurrence of the bit $\xi_{\mathcal{P}}$, and III.2 can be written as

$$\sum_{\xi_{\mathcal{P}}=0}^{1} \alpha(\xi_{\mathcal{P}})\,|\xi_{\mathcal{P}}\rangle^{\mathcal{H}_{E,\mathcal{P}}}\,|\phi_{\xi_{\mathcal{P}}}\rangle^{\mathcal{H}_{\mathcal{P}}}\ . \tag{III.3}$$

As multiple measurements accumulate, and as multi qubit-measurements can be modelled likewise, $\xi_{\mathcal{P}}$ can also represent a bit-string.

III.1.2. State of the Entire System

The state of the system $\mathcal{H}_{E,\mathcal{P}} \otimes \mathcal{H}_{\mathcal{P}}$ can always be represented as

$$\sum_{\xi_{\mathcal{P}}} \alpha(\xi_{\mathcal{P}})\,|\xi_{\mathcal{P}}\rangle^{\mathcal{H}_{E,\mathcal{P}}}\,|\phi_{\xi_{\mathcal{P}}}\rangle\ . \tag{III.4}$$

To represent the transmission of classical bits from Alice to Bob, a transformation is used that maps $|x\rangle^{(E,\mathcal{A})}\,|0\rangle^{(E,\mathcal{B})}$ into $|x\rangle^{(S,\mathcal{A})}\,|x\rangle^{(S,\mathcal{B})}$. This is not in conflict with the no-cloning theorem, as the underlying information in this process is classical and states representing classical information are orthogonal to each other. Analogously to represent the transmission of classical bits from Bob to Alice, a transformation is used that maps $|0\rangle^{(E,\mathcal{A})}\,|x\rangle^{(E,\mathcal{B})}$ into $|x\rangle^{(S,\mathcal{A})}\,|x\rangle^{(S,\mathcal{B})}$. This means Alice keeps a record of the transmitted bits and Bob likewise. So the contents of $\mathcal{H}_{S,\mathcal{A}}$ and $\mathcal{H}_{S,\mathcal{B}}$ are always the same and the string ξ_S can be used to label bits that have been transmitted between the parties.

As a result, the total system is always in a state

$$\sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}} \alpha_{(\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}})}\,|\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}\rangle^{\mathcal{H}_S\otimes\mathcal{H}_{E,\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{B}}}\,|\psi(\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}})\rangle^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\ . \tag{III.5}$$

- $|\psi(\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}})\rangle$ is the state of $\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}$ associated with the occurrence of $\xi_S,\xi_{\mathcal{A}}$ and $\xi_{\mathcal{B}}$.
- $\eta = (\xi_{\mathcal{B}},\xi_S)$ random classical information available to Bob after encoding, stored in $\mathcal{H}_S\otimes\mathcal{H}_{E,\mathcal{B}}$.
- $|\psi_{b,\eta}\rangle$ is the corresponding state of system $\mathcal{H}_{E_{\mathcal{A}}}\otimes\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}$ after the encoding.
- $\rho_{\mathcal{B}}(|\psi_{b,\eta}\rangle) = \mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}(|\psi_{b,\eta}\rangle\,\langle\psi_{b,\eta}|)$ the reduced density operator on $\mathcal{H}_{\mathcal{B}}$ given η.

III.2. BB84

BB84 is the name given to a QBC-protocol first presented on in the conference paper *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* by Bennett and Brassard (1984). The conference paper was later published in "Quantum Cryptography" (Bennett and Brassard 2014).

The idea of BB84 is to create a commitment by encoding random bits in either the rectilinear or the diagonal basis, and to unveil it by unveiling the random bits used to create the commitment. To *encode a classical bit b in the rectilinear or diagonal basis*, means to create a state $|b\rangle_+$ or $|b\rangle_\times$ respectively. These bases are used because for $b = 0, 1$, measuring $|b\rangle_+$ in the diagonal basis yields $|0\rangle_\times$ and $|1\rangle_\times$ with equal probabilities, and measuring $|b\rangle_\times$ in the rectilinear basis yields $|0\rangle_+$ and $|1\rangle_+$ with equal probabilities. The security parameter n dictates how many random bits will be encoded in this way.

In the commit-phase, Alice chooses whether to commit to $b = 0$ or $b = 1$ and chooses the diagonal or rectilinear basis respectively. She then generates n perfectly random bits w_i, which she encodes in the chosen basis. Bob receives the encoded bits $|r_i\rangle$ from Alice and measures each of those qubits in a basis that was chosen perfectly random between the rectilinear and the diagonal basis. An algorithmic description of the commit phase is given by Algorithm 1

Algorithm 1: commit

1 **Alice**
2 $b \leftarrow \{0, 1\}$
3 $\theta = b \; ? \quad \times \quad : \quad +$
4 **for** $i \in \{1 \dots n\}$ **do**
5 $w_i \xleftarrow{\$} \{0, 1\}$
6 $|r_i\rangle \coloneqq |w_i\rangle_\theta$
7 **Alice** $\xrightarrow{|r_i\rangle}$ **Bob**
8 $\mathbf{w} \coloneqq \begin{pmatrix} w_1 & \cdots & w_n \end{pmatrix}^T$
9 **Bob**
10 $\hat{\theta}_1 \dots \hat{\theta}_n = \hat{\theta} \xleftarrow{\$} \{+, \times\}^n$
11 **foreach** r_i **do**
12 $\hat{w}_i = M_{\hat{\theta}_i} |r_i\rangle$

In Lines 5–7 of Algorithm 1 the state

$$|\psi_{b,\mathbf{w}}\rangle \coloneqq \frac{1}{\sqrt{2}} \left(|0\rangle_\theta^{\mathcal{H}_{E,\mathcal{A}}} |0\rangle_\theta^{\mathcal{H}_\mathcal{B}} + |1\rangle_\theta^{\mathcal{H}_{E,\mathcal{A}}} |1\rangle_\theta^{\mathcal{H}_\mathcal{B}} \right) , \tag{III.6}$$

is created. This is because from an outsider perspective, Line 5 can be seen as creating the state $|0\rangle_\theta + |1\rangle_\theta$ and measuring it, as described in Section III.1. Abstracted further and with the principle of deferred measurement applied, the Lines 5 to 7 can be seen as first creating a random state, transforming its basis if necessary, and then measuring it in the respective basis. This is expressed as a quantum circuit in Figure III.2.1.

In the unveil-phase, Alice sends Bob the bits w_i she used to create the encodings in commit. Bob knows that for all w_j that Alice has sent, which do not match his own corresponding measurement results, $\hat{w}_j$, the basis $\hat{\theta}_j$ he used for his measurement must not have been the one that Alice used to create $|r_j\rangle$. Since Alice used the same basis for all w_i-encodings, all those $\hat{\theta}_j$ on Bob's side, where $\hat{w}_j$ mismatched w_j, have to correspond to the same basis. So Bob understands the complement of one such $\hat{\theta}_j$ as the basis Alice chose, and then tests whether the other $\hat{\theta}_j$ would have resulted in the same basis. If not all of those $\hat{\theta}_j$ correspond to the same basis, Alice must have not followed the honest protocol.

A failure case that can occur is when all of Bob's measurements $\hat{w}_i$ also match Alice's bits w_i, where Bob chose a different Basis than θ. In this case he can derive no information about the basis Alice chose or whether she cheated, and thus the protocol fails. However,

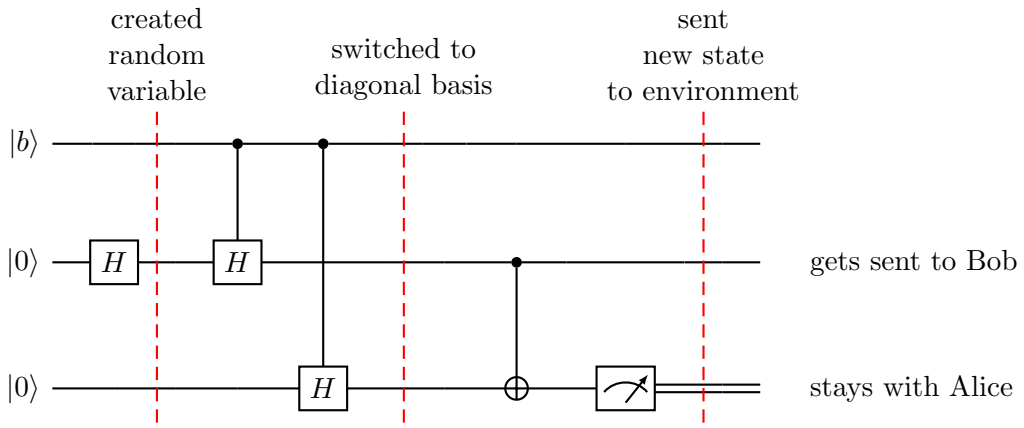


Figure III.2.1.: Quantum circuit describing Lines 5–7 of Algorithm 1

Algorithm 2: unveil

1 **Alice** $\overset{\mathbf{w}}{\to}$ **Bob**
2 **Bob**
3 $j' \leftarrow \{j \ : \ w_j \neq \hat{w}_j\}$
4 $\tilde{\theta} := \begin{cases} +, & \hat{\theta}_{j'} = \times \\ \times, & \hat{\theta}_{j'} = + \end{cases}$
5 **foreach** $j \ : \ w_j \neq \hat{w}_j$ **do**
6 **if** $\hat{\theta}_{j'} \neq \hat{\theta}_j$ **then**
7 **return** $\perp$
8 **return** $\tilde{\theta} \overset{?}{=} \times$

the probability of this happening decreases exponentially with an increase of the security parameter.

III.2.1. Defeating BB84

A dishonest Alice executes honest commit for $b = 0$ but never sends anything to the environment. Thus, the underlying systems of the State III.6 changes

$$|\psi'_{0,\mathbf{w}}\rangle = 1/\sqrt{2}\left(|0\rangle_+^{\mathcal{H}_\mathcal{A}}|0\rangle_+^{\mathcal{H}_\mathcal{B}} + |1\rangle_+^{\mathcal{H}_\mathcal{A}}|1\rangle_+^{\mathcal{H}_\mathcal{B}}\right). \tag{III.7}$$

While this is formally the same state as the one generated in an honest commit, due to the change of the underlying systems there now exists a unitary transformation on Alice's side to transform III.7 into

$$|\psi'_{1,\mathbf{w}}\rangle = 1/\sqrt{2}\left(|0\rangle_\times^{\mathcal{H}_\mathcal{A}}|0\rangle_\times^{\mathcal{H}_\mathcal{B}} + |1\rangle_\times^{\mathcal{H}_\mathcal{A}}|1\rangle_\times^{\mathcal{H}_\mathcal{B}}\right). \tag{III.8}$$

In the BB84 case this transformation is the identity transformation:

$$\begin{aligned}
|\psi'_{0,\mathbf{w}}\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_+^{\mathcal{H}_\mathcal{A}}|0\rangle_+^{\mathcal{H}_\mathcal{B}} + |1\rangle_+^{\mathcal{H}_\mathcal{A}}|1\rangle_+^{\mathcal{H}_\mathcal{B}}\right) && \text{(III.9)}\\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{2}\left(|0\rangle_+^{\mathcal{H}_\mathcal{A}}|0\rangle_+^{\mathcal{H}_\mathcal{B}} + |0\rangle_+^{\mathcal{H}_\mathcal{A}}|1\rangle_+^{\mathcal{H}_\mathcal{B}} + |1\rangle_+^{\mathcal{H}_\mathcal{A}}|0\rangle_+^{\mathcal{H}_\mathcal{B}} + |1\rangle_+^{\mathcal{H}_\mathcal{A}}|1\rangle_+^{\mathcal{H}_\mathcal{B}}\right)\right. && \text{(III.10)}\\
&\quad \left. + \frac{1}{2}\left(|0\rangle_+^{\mathcal{H}_\mathcal{A}}|0\rangle_+^{\mathcal{H}_\mathcal{B}} - |0\rangle_+^{\mathcal{H}_\mathcal{A}}|1\rangle_+^{\mathcal{H}_\mathcal{B}} - |1\rangle_+^{\mathcal{H}_\mathcal{A}}|0\rangle_+^{\mathcal{H}_\mathcal{B}} + |1\rangle_+^{\mathcal{H}_\mathcal{A}}|1\rangle_+^{\mathcal{H}_\mathcal{B}}\right)\right) && \text{(III.11)}\\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|0\rangle_+^{\mathcal{H}_\mathcal{A}} + |1\rangle_+^{\mathcal{H}_\mathcal{A}}\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_+^{\mathcal{H}_\mathcal{B}} + |1\rangle_+^{\mathcal{H}_\mathcal{B}}\right)\right. && \text{(III.12)}\\
&\quad \left. + \frac{1}{\sqrt{2}}\left(|0\rangle_+^{\mathcal{H}_\mathcal{A}} - |1\rangle_+^{\mathcal{H}_\mathcal{A}}\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_+^{\mathcal{H}_\mathcal{B}} - |1\rangle_+^{\mathcal{H}_\mathcal{B}}\right)\right) && \text{(III.13)}\\
&= \frac{1}{\sqrt{2}}\left(|0\rangle_\times^{\mathcal{H}_\mathcal{A}}|0\rangle_\times^{\mathcal{H}_\mathcal{B}} + |1\rangle_\times^{\mathcal{H}_\mathcal{A}}|1\rangle_\times^{\mathcal{H}_\mathcal{B}}\right) = |\psi'_{1,\mathbf{w}}\rangle\,. && \text{(III.14)}
\end{aligned}$$

How this allows Alice to cheat is demonstrated in the following example.

III.1 Example (Attack on BB84, four qubit case) Let $n = 4$. Alice chooses $b = 0$. Instead of choosing random $w_1 \dots w_4 \leftarrow \{0,1\}^4$ and creating $|r_i\rangle = |w_i\rangle_+$, Alice creates the EPR pairs

$$|h_i\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_+ + |11\rangle_+\right), i = 1, \dots, 4\,. \tag{III.15}$$

For each pair she labels one bit $|r_i\rangle$ and sends those $|r_i\rangle$ to Bob, keeping the other registers. Let Bob choose the Bases

$$\hat{\theta} = \begin{pmatrix} + \\ + \\ \times \\ \times \end{pmatrix}, \tag{III.16}$$

and let him measure

$$\hat{\mathbf{w}} = 0101\,. \tag{III.17}$$

This is the end of the commit procedure.

$|00\rangle_\theta$ and $|11\rangle_\theta$ are the only possible measurement outcomes, when measuring $|00\rangle_\theta \pm |11\rangle_\theta$ in the θ basis. This means, the EPR pairs have collapsed to

$$\left(|00\rangle_+, |11\rangle_+, |00\rangle_\times, |11\rangle_\times\right). \tag{III.18}$$

If Alice does not want to change her commitment, she does nothing to her state and measures it in the rectilinear basis. For $i = 1, 2$ this is the same basis Bob has measured his

qubits in, and since the first two EPR pairs have collapsed to $|00\rangle_+$ (for $i = 1$) and $|11\rangle_+$ (for $i = 2$) respectively, she measures $|0\rangle_+$ and $|1\rangle_+$ respectively on her bits and receives the same bits Bob has measured:

$$w_{1,2} = \hat{w}_{1,2} = 01\,. \tag{III.19}$$

For $i = 3$ Bob measured $|0\rangle_\times$, so the total state of this pair has collapsed to $|00\rangle_\times = \frac{1}{2}(|00\rangle_+ + |01\rangle_+ + |10\rangle_+ + |11\rangle_+)$. Since Alice measures in the rectilinear base, she receives 0 or 1 with equal probabilities, so a random bit w_3.

Similarly for $i = 4$, Bob measured $|r_4\rangle$ in the diagonal basis and since $|11\rangle_\times = \frac{1}{2}(|00\rangle_+ + |01\rangle_+ - |10\rangle_+ - |11\rangle_+)$, Alice receives a random bit again. This means, there are four possibilities for $\mathbf{w}$

$$\mathbf{w} = \begin{cases} 0100 =: \mathbf{w}^{(1)} \\ 0101 =: \mathbf{w}^{(2)} \\ 0110 =: \mathbf{w}^{(3)} \\ 0111 =: \mathbf{w}^{(4)}\,. \end{cases}$$

She sends her $\mathbf{w}$ to Bob and Bob looks at the i where $w_i \neq \hat{w}_i$

$$w_4^{(1)} \neq \hat{w}_4 \quad \Rightarrow \quad \theta = +, b = 0 \tag{III.20}$$

$$\mathbf{w}^{(2)} = \hat{\mathbf{w}} \quad \Rightarrow \quad \perp \tag{III.21}$$

$$w_{3,4}^{(3)} \neq \hat{w}_{3,4} \wedge \hat{\theta}_3 = \hat{\theta}_4 \quad \Rightarrow \quad \theta = +, b = 0 \tag{III.22}$$

$$w_3^{(4)} \neq \hat{w}_3 \quad \Rightarrow \quad \theta = +, b = 0\,. \tag{III.23}$$

Where the inconclusive result is the same that would have occurred in an honest scenario where Bob would have measured by chance the same string that Alice has chosen. So Alice succeeds in convincing Bob she was always committed to $b = 0$.

If Alice wants to change her commitment to $b = 1$, she "transforms" $|\psi'_{0,\hat{\mathbf{w}}}\rangle$ into $|\psi'_{1,\hat{\mathbf{w}}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_\times + |11\rangle_\times)$ by measuring it in the diagonal basis instead of the rectilinear one. Analogous to above, for $i = 3, 4$ this is the same basis as the one Bob has measured his qubit in, and since $|00\rangle_\times$ and $|11\rangle_\times$ are the only possible outcomes, she receives the same bits as Bob has measured

$$w_{3,4} = \hat{w}_{3,4} = 01\,. \tag{III.24}$$

For $i = 1, 2$ Bob measured in the rectilinear basis, and since Alice measures in the diagonal basis, she receives random bits $w_{3,4}$.

As above, the bits she measured in the same basis as Bob (diagonal) are the same as Bob's and thus are not looked at. All bits that can differ from bits Bob measured, belong to Bob's rectilinear basis measurements and thus Bob is convinced that Alice really committed $b = 1$. Effectively she cheated by delaying her measurement until after the commit phase and indirectly transforming the commitment state. ∗

III.3. Attack on Generalized QBC

It is assumed that initially all quantum registers are set to $|\mathbf{0}\rangle$, as QBC with pre-shared entangled states are practically of no use, as trust in such a state would have to be assumed which defeats the purpose of a QBC or BC[1].

[1] For the no-go theorem that is presented here and was presented by Lo and Chau (1997) and Mayers (1996), it is sufficient to assume that no pre-existing shared entanglement exists. The assumption, that all quantum registers are set to $|\mathbf{0}\rangle$ at the beginning of the protocol follows Mayers (1996), while Lo and

Let $\text{commit}^{\mathcal{A}}, \text{unveil}^{\mathcal{A}}, |\psi^{\mathcal{A}}\rangle$ modified by dishonest Alice, $\text{commit}^{\mathcal{B}}, |\psi^{\mathcal{B}}\rangle$ modified by dishonest Bob. While looking at one cheating party, it is assumed that the other party is bund to a fixed honest strategy.

As many notations presented throughout this thesis will be combined in this section, a summary of these notations is given here. Everything inside a ket is part of the label for that state vector. A different label usually means a different state. Every sub- and superscript outside the ket describes attributes that state has.

$$|\psi\rangle_{\theta}^{\mathcal{H}} \tag{III.25}$$

$$|\psi_{b,\xi}^{\mathcal{P}}\rangle \tag{III.26}$$

State III.25 is a state with label ψ, encoded in the basis θ, that acts on the Hilbert space $\mathcal{H}$. State III.26 is a commitment, encoding b, created by dishonest party $\mathcal{P}$, which has stored ξ in their classical registers.

III.3.1. Scheme is Secure Against Bob

A cheating Bob follows a modified commit procedure, $\text{commit}^{\mathcal{B}}$, in which he never sends a register away to the environment. Denote $\eta = \xi_B, \xi_S$ the classical information stored on Bob's side and γ the string of transmitted bits, stored in $\mathcal{H}_S$ after $\text{commit}^{\mathcal{B}}$. Since Bob does not send anything to the environment, ξ_B is the empty string and $\eta = \gamma$. For the same reason, the state $|\psi_{b,\eta}^{\mathcal{B}}\rangle$ that is produced in $\text{commit}^{\mathcal{B}}$ is the state of the system $\mathcal{H}_{E,\mathcal{A}} \otimes \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. Bob succeeds in cheating if he is able to gain some information about b before the unveil-phase. To be more precise, he succeeds if he is able to break the *concealing*-property of the scheme. Following Definition II.22, for the scheme to be secure against Bob, the fidelity of the reduced density operators on Bob's side has to be

$$F''(\eta) \coloneqq F\left(\rho_{\mathcal{B}}\left(|\psi_{0,\eta}^{\mathcal{B}}\rangle\right), \rho_{\mathcal{B}}\left(|\psi_{1,\eta}^{\mathcal{B}}\rangle\right)\right) = 1 - \delta, \quad \delta \geq 0\,, \tag{III.27}$$

with δ close to zero.

For this insecurity proof it is assumed that the scheme is secure against Bob because otherwise the scheme would already be insecure.

III.3.2. Security Against Bob Implies Insecurity Against Alice

As in the attack on BB84, without loss of generality, cheating Alice in $\text{commit}^{\mathcal{A}}$ chooses $b = 0$ and does not send any registers to the environment, with the exception of classical bits she is required to transfer to Bob (using a non quantum channel).

γ is the classical, random string stored in $\mathcal{H}_S$ after $\text{commit}^{\mathcal{A}}$ and is in fact the same string as the one stored in $\mathcal{H}_S$ after $\text{commit}^{\mathcal{B}}$. $|\psi_{b,\gamma}^{\mathcal{A}}\rangle$ is the collapsed state of the commitment. This is the state of the remaining system $\mathcal{H}_{E,\mathcal{B}} \otimes \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, as $\mathcal{H}_{E,\mathcal{A}}$ is not used in $\text{commit}^{\mathcal{A}}$. Thus, the reduced density matrix on Bob's side $\rho_{\mathcal{B}}\left(|\psi_{b,\gamma}^{\mathcal{A}}\rangle\right)$ is the state of system $\mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{E,\mathcal{B}}$.

Lemma 1:
If the scheme is perfectly or unconditionally secure against Bob the expected value of the fidelity

$$F'(\gamma) \coloneqq F\left(\rho_{\mathcal{B}}\left(|\psi_{0,\gamma}^{\mathcal{A}}\rangle\right), \rho_{\mathcal{B}}\left(|\psi_{1,\gamma}^{\mathcal{A}}\rangle\right)\right) \tag{III.28}$$

is equal to, or respectively arbitrarily close to, 1. ♠

Chau (1997) assumes that no entanglement is pre-shared, and the system starts in a pure state. Both of these assumptions can be lifted to also include non-static QBC-protocols, so protocols where the state of Bob's system at the start of the protocol is not known to Alice. This is shown by Li et al. (2011) without changing actual the proof. However for the sake of readability Mayer's assumption is kept in this thesis.

Proof: $|\psi^{\mathcal{A}}_{b,\gamma}\rangle$ and $|\psi^{\mathcal{B}}_{b,\gamma}\rangle$ are formally identical. They can be expressed as follows:

$$|\psi^{\mathcal{A}}_{b,\gamma}\rangle = \sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}} \alpha_{(\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}})}|\xi_S\rangle^{\mathcal{H}_S}|\xi_{\mathcal{A}}\rangle^{\mathcal{H}'_{\mathcal{A}}}|\xi_{\mathcal{B}}\rangle^{\mathcal{H}_{E,\mathcal{B}}}|\psi\rangle^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}} \tag{III.29}$$

$$|\psi^{\mathcal{B}}_{b,\gamma}\rangle = \sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}} \alpha_{(\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}})}|\xi_S\rangle^{\mathcal{H}_S}|\xi_{\mathcal{A}}\rangle^{\mathcal{H}_{E,\mathcal{A}}}|\xi_{\mathcal{B}}\rangle^{\mathcal{H}''_{\mathcal{B}}}|\psi\rangle^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\,, \tag{III.30}$$

where $\mathcal{H}'_{\mathcal{A}}$ is the subsystem of $\mathcal{H}_A$, that replaces $\mathcal{H}_{E,\mathcal{A}}$ in cheating Alice's $|\psi^{\mathcal{A}}_{b,\gamma}\rangle$ and $\mathcal{H}''_{\mathcal{B}}$ is the subsystem of $\mathcal{H}_{\mathcal{B}}$, that replaces $\mathcal{H}_{E,\mathcal{B}}$ in cheating Bob's $|\psi^{\mathcal{B}}_{b,\gamma}\rangle$. $\rho_{\mathcal{B}}(|\cdot\rangle)$ is the reduced density operator of Bob's systems. This means all of Alice's systems are traced out.

It will now be shown that the reduced density operators on Bob's side after commit$^{\mathcal{A}}$ and after commit$^{\mathcal{B}}$ are also formally identical.

$$\begin{aligned}
&\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{b,\gamma}\rangle\right) && \text{(III.31)}\\
&= \mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(|\psi^{\mathcal{A}}_{b,\gamma}\rangle\langle\psi^{\mathcal{A}}_{b,\gamma}|\right)\\
&= \mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(\left(\sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha|\xi_S\rangle^{\mathcal{H}_S}|\xi_{\mathcal{A}}\rangle^{\mathcal{H}'_{\mathcal{A}}}|\xi_{\mathcal{B}}\rangle^{\mathcal{H}_{E,\mathcal{B}}}|\psi\rangle^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\right.\\
&\qquad\left.\left(\sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha^*\langle\xi_S|^{\mathcal{H}_S}\langle\xi_{\mathcal{A}}|^{\mathcal{H}'_{\mathcal{A}}}\langle\xi_{\mathcal{B}}|^{\mathcal{H}_{E,\mathcal{B}}}\langle\psi|^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\right)\\
&= \sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha\alpha^*\\
&\quad\left(\mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(|\xi_S\rangle\langle\xi_S|^{\mathcal{H}_S}\otimes|\xi_{\mathcal{A}}\rangle\langle\xi_{\mathcal{A}}|^{\mathcal{H}'_{\mathcal{A}}}\otimes|\xi_{\mathcal{B}}\rangle\langle\xi_{\mathcal{B}}|^{\mathcal{H}_{E,\mathcal{B}}}\otimes|\psi\rangle\langle\psi|^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\right)\\
&= \sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha\alpha^*\left(|\xi_S\rangle\langle\xi_S|^{\mathcal{H}_S}\otimes|\xi_{\mathcal{B}}\rangle\langle\xi_{\mathcal{B}}|^{\mathcal{H}_{E,\mathcal{B}}}\otimes\mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}}\left(|\psi\rangle\langle\psi|^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\langle\xi_{\mathcal{A}}|\xi_{\mathcal{A}}\rangle\right)\,, && \text{(III.32)}
\end{aligned}$$

and

$$\begin{aligned}
&\rho_{\mathcal{B}}\left(|\psi^{\mathcal{B}}_{b,\gamma}\rangle\right) && \text{(III.33)}\\
&= \mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(|\psi^{\mathcal{B}}_{b,\gamma}\rangle\langle\psi^{\mathcal{B}}_{b,\gamma}|\right)\\
&= \mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(\left(\sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha|\xi_S\rangle^{\mathcal{H}_S}|\xi_{\mathcal{A}}\rangle^{\mathcal{H}_{E,\mathcal{A}}}|\xi_{\mathcal{B}}\rangle^{\mathcal{H}''_{\mathcal{B}}}|\psi\rangle^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\right.\\
&\qquad\left.\left(\sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha^*\langle\xi_S|^{\mathcal{H}_S}\langle\xi_{\mathcal{A}}|^{\mathcal{H}_{E,\mathcal{A}}}\langle\xi_{\mathcal{B}}|^{\mathcal{H}''_{\mathcal{B}}}\langle\psi|^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\right)\\
&= \sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha\alpha^*\\
&\quad\left(\mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(|\xi_S\rangle\langle\xi_S|^{\mathcal{H}_S}\otimes|\xi_{\mathcal{A}}\rangle\langle\xi_{\mathcal{A}}|^{\mathcal{H}_{E,\mathcal{A}}}\otimes|\xi_{\mathcal{B}}\rangle\langle\xi_{\mathcal{B}}|^{\mathcal{H}''_{\mathcal{B}}}\otimes|\psi\rangle\langle\psi|^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\right)\\
&= \sum_{\xi_S,\xi_{\mathcal{A}},\xi_{\mathcal{B}}}\alpha\alpha^*\left(|\xi_S\rangle\langle\xi_S|^{\mathcal{H}_S}\otimes|\xi_{\mathcal{B}}\rangle\langle\xi_{\mathcal{B}}|^{\mathcal{H}''_{\mathcal{B}}}\otimes\mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}}\left(|\psi\rangle\langle\psi|^{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{\mathcal{B}}}\right)\langle\xi_{\mathcal{A}}|\xi_{\mathcal{A}}\rangle\right)\,. && \text{(III.34)}
\end{aligned}$$

When comparing III.32 and III.34, it can be observed that the density operators of the cheating states on Bob's side are in fact formally identical.

$$\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{b,\gamma}\rangle\right) = \rho_{\mathcal{B}}\left(|\psi^{\mathcal{B}}_{b,\gamma}\rangle\right)\,. \tag{III.35}$$

As Bob does not send registers away to the environment, $\xi_{\mathcal{B}}$ is the empty string in commit$^{\mathcal{B}}$ and $\eta = (\xi_{\mathcal{B}}, \xi_S) = \xi_S = \gamma$, and thus

$$F''(\eta) = F''(\gamma) = F\left(\rho_{\mathcal{B}}\left(\psi^{\mathcal{B}}_{0,\gamma}\right), \psi^{\mathcal{B}}_{1,\gamma}\right) \overset{\text{III.35}}{=} F\left(\rho_{\mathcal{B}}\left(\psi^{\mathcal{A}}_{0,\gamma}\right), \psi^{\mathcal{A}}_{1,\gamma}\right) = F'(\gamma)\,. \tag{III.36}$$

Since the scheme is asserted to be perfectly or respectively unconditionally secure against Bob, the value of $F''(\eta)$ has to be equal or respectively arbitrarily close to one and so $F'(\gamma)$ has to be as well. ∎

III.3.3. Transforming Zero to One

Suppose the commitment protocol is perfectly secure against Bob. This means, following Lemma 1, that $F'(\gamma) = 1$. So $\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{0,\gamma}\rangle\right) = \rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{1,\gamma}\rangle\right) \coloneqq \rho_{\mathcal{B}}$. It is shown that Alice is then able to cheat, by changing her commitment during the holding phase. Later this will be extended to commitment protocols that are not perfectly, but unconditionally, secure against Bob.

Definition III.1 (ensembles[2]). An *ensemble* of quantum states is a collection of normalized states $|\hat{\psi}_1, \cdots, \hat{\psi}_n\rangle$ with fixed a priori probabilities $p_1, \cdots, p_n$. To any such ensemble a density matrix is associated with.

$$\rho = \sum_{i=1}^{n} p_i \, |\hat{\psi}_i\rangle \, \langle\hat{\psi}_i| \; . \tag{III.37}$$

For convenience, the ensemble is represented as $\{|\psi_i\rangle, \cdots, |\psi_n\rangle\}$ where $|\psi_i\rangle = \sqrt{p_i}\,|\hat{\psi}_i\rangle$, so that $p_i = \langle\psi_i|\psi_i\rangle$ and

$$\rho = \sum_{i=1}^{n} |\psi_i\rangle \, \langle\psi_i| \tag{III.38}$$

An *eigen-ensemble* of a given state ρ on an n-dimensional Hilbert space with an orthonormal basis of eigenvectors $\hat{e}_1, \ldots, \hat{e}_n$ that have the eigenvalues $\lambda_1, \ldots, \lambda_n$, is an ensemble of the form $\{|e_1\rangle, \ldots, |e_k\rangle\}$ where $\langle e_i|e_i\rangle = \lambda_i$ for each i. States $|e_1\rangle$ where the eigenvalues $\lambda_i = 0$ are not included in the ensemble, thus $k = \mathrm{rank}(\rho) \leq n$. ♣

Theorem 7 (Ensembles of a density matrix[3]):
For a given density matrix ρ on an n-dimensional Hilbert space, let $|\phi_1\rangle, \ldots, |\phi_n\rangle$ be any ensemble of pure states with associated density matrix ρ. Then there exists a matrix $N \in \mathbb{C}^{s\times k}$ whose columns are k orthonormal vectors in $\mathbb{C}^r$, so $r \geq k \coloneqq rank(\rho)$, such that

$$|\phi_i\rangle = \sum_{j=1}^{k} N_{ij} \, |e_j\rangle \, , i = 1, \ldots, s \, . \tag{III.39}$$

♢

Theorem 8 (Zero to One):
$|\psi^{\mathcal{A}}_{b,\gamma}\rangle$ is the corresponding collapsed state of the remaining system $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{E,\mathcal{B}}$. $\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{0,\gamma}\rangle\right) = \rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{1,\gamma}\rangle\right)$ implies that there exists a unitary transformation on Alice's side which maps $|\psi^{\mathcal{A}}_{0,\gamma}\rangle$ into $|\psi^{\mathcal{A}}_{1,\gamma}\rangle$. ♢

Proof: $\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{0,\gamma}\rangle\right) = \rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{1,\gamma}\rangle\right) =: \rho_{\mathcal{B}} = \mathrm{Tr}_{\mathcal{H}_{\mathcal{A}}\otimes\mathcal{H}_{E,\mathcal{A}}}\left(|\psi^{\mathcal{A}}_{b,\gamma}\rangle \, \langle\psi^{\mathcal{A}}_{b,\gamma}|\right)$ is the reduced density matrix of Bob's systems $\mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{E,\mathcal{B}}$. According to Schmidt's decomposition theorem, $|\psi^{\mathcal{A}}_{0,\gamma}\rangle$ can be written as

$$|\psi^{\mathcal{A}}_{0,\gamma}\rangle = \sum_{i=1}^{s} \sqrt{\lambda_{0,i}} \, |\hat{a}^{(0)}_i\rangle^{\mathcal{H}_{\mathcal{A}}} \otimes |\hat{b}^{(0)}_i\rangle^{\mathcal{H}_{\mathcal{B}}\otimes\mathcal{H}_{E,\mathcal{B}}} \; , \tag{III.40}$$

[2]Following Hughston, Jozsa, and Wootters (1993, section 1).
[3]Following Hughston, Jozsa, and Wootters (1993, section 2).

where $|\hat{a}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{A}}$ are eigenstates of $\rho_A\left(|\psi_{0,\gamma}^\mathcal{A}\rangle\right)$ forming an orthonormal basis of $\mathcal{H}_\mathcal{A}$ and $|\hat{b}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}$ are eigenstates of ρ_B forming an orthonormal basis for system $\mathcal{H}_{E,\mathcal{B}}$. $\lambda_{0,i}$ are the eigenvalues of $\mathrm{Tr}_{\mathcal{H}_\mathcal{A}\otimes\mathcal{H}_{E,\mathcal{A}}}(|\psi_{0,\gamma}^\mathcal{A}\rangle\langle\psi_{0,\gamma}^\mathcal{A}|)$ and of $Tr_{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}(|\psi_{0,\gamma}^\mathcal{A}\rangle\langle\psi_{0,\gamma}^\mathcal{A}|)$ with the same multiplicity where any extra dimensions are made up with zero eigenvalues (Hughston, Jozsa, and Wootters 1993). This means that

$$\rho_\mathcal{B} = \sum_{i=1}^{s} \lambda_{0,i}\, |\hat{b}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}\, \langle\hat{b}_i^{(0)}|^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}\ , \tag{III.41}$$

and thus

$$\left\{\sqrt{\lambda_{0,i}}\, |\hat{b}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}\right\} \tag{III.42}$$

is a $\rho_\mathcal{B}$ eigen-ensemble, as

$$\langle\hat{b}^{(0)}\sqrt{\lambda_{0,i}}|\sqrt{\lambda_{0,i}}\hat{b}^{(0)}\rangle^{|\hat{b}_i^{(0)}\rangle \text{ is normal}} = \sqrt{\lambda_{0,i}}\sqrt{\lambda_{0,i}} = \lambda_{0,i}\,. \tag{III.43}$$

Similarly, since $|\psi_{1,\gamma}^\mathcal{A}\rangle$ is a pure state it can be written as a decomposition of eigenstates and eigenvalues.

$$|\psi_{1,\gamma}^\mathcal{A}\rangle = \sum_{i=1}^{s} \sqrt{\lambda_{1,i}}\, |\hat{a}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{A}} \otimes |\hat{b}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}\ , \tag{III.44}$$

so $\left\{\sqrt{\lambda_{1,i}}\, |\hat{b}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}}\right\}$ is an eigen-ensemble of $\rho_\mathcal{B}$. As eigen-ensembles are unique, it follows that $\lambda_{0,i} = \lambda_{1,i} =: \lambda_i$ are the same eigenvalues and

$$|\hat{b}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}} = |\hat{b}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}} =: |\hat{b}_i\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}} \tag{III.45}$$

are the same eigenstates.

There exists a unitary matrix that transforms one orthonormal basis of $\mathcal{H}_\mathcal{A}$ into another orthonormal basis of $\mathcal{H}_\mathcal{A}$. Let S be the matrix that transforms $|\hat{a}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{A}}$ into $|\hat{a}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{A}}$, so

$$S\, |\hat{a}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{A}} = |\hat{a}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{A}}\ . \tag{III.46}$$

The same matrix can be used to transform $|\psi_{0,\gamma}^\mathcal{A}\rangle$ into $|\psi_{1,\gamma}^\mathcal{A}\rangle$, as is shown below.

$$|\psi_{1,\gamma}^\mathcal{A}\rangle = \sum_{i=1}^{s} \lambda_i\, |\hat{a}_i^{(1)}\rangle^{\mathcal{H}_\mathcal{A}} \otimes |\hat{b}_i\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}} \tag{III.47}$$

$$= \sum_{i=1}^{s} \lambda_i S\, |\hat{a}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{A}}\, |\hat{b}_i\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}} \tag{III.48}$$

$$= S \sum_{i=1}^{s} \lambda_i\, |\hat{a}_i^{(0)}\rangle^{\mathcal{H}_\mathcal{A}} \otimes |\hat{b}_i\rangle^{\mathcal{H}_\mathcal{B}\otimes\mathcal{H}_{E,\mathcal{B}}} \tag{III.49}$$

$$= S\, |\psi_{0,\gamma}^\mathcal{A}\rangle\ . \tag{III.50}$$

■

Theorem 9 (Perfect security against Bob implies insecurity against Alice):
Any QBC*-protocol that is perfectly concealing is not unconditionally binding.* ♢

Proof: Following Lemma 1, $F'(\gamma) = 1$, thus $\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{0,\gamma}\rangle\right) = \rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{1,\gamma}\rangle\right)$. Then Theorem 8 asserts that there exists a unitary transformation on Alice's side which maps $|\psi^{\mathcal{A}}_{0,\gamma}\rangle$ into $|\psi^{\mathcal{A}}_{1,\gamma}\rangle$. This means without loss of generality, Alice can cheat by choosing $b = 0$, executing commit$^{\mathcal{A}}$, and applying the transformation S in unveil$^{\mathcal{A}}$[4] if she wishes to change her mind. Further in unveil$^{\mathcal{A}}$ she sends the states to the environment, that she was supposed to send to the environment in commit and continues with honest unveil after that. ∎

III.2 Example (Modified BB84) In Subsection III.2.1 it was shown that in BB84, $|\psi^{\mathcal{A}}_{0,\gamma}\rangle = |\psi^{\mathcal{A}}_{1,\gamma}\rangle$. This example modifies BB84 to demonstrate application of theorem zero to one. Consider the new basis that arises when rotating the states of the rectilinear basis on the bloch sphere by 45° around the y-axis and then 135° around the z-axis. Its states are

$$|0\rangle_{\wr} := |\nwarrow\rangle := \cos\left(\frac{\pi}{8}\right)|0\rangle + e^{i\frac{\pi}{4}}\ \sin\left(\frac{\pi}{8}\right)|1\rangle \tag{III.51}$$

$$|1\rangle_{\wr} := |\nearrow\rangle := \sin\left(\frac{\pi}{8}\right)|0\rangle + e^{i\frac{5\pi}{4}}\cos\left(\frac{\pi}{8}\right)|1\rangle\ . \tag{III.52}$$

BB84 is now modified as follows: wherever the original protocol uses the diagonal basis, the new protocol uses the new basis. This means the cheating states of the new protocol are

$$|\psi^{\mathcal{A}}_{0,\gamma}\rangle = \frac{1}{\sqrt{2}}|00\rangle_{+} + \frac{1}{\sqrt{2}}|11\rangle_{+} \tag{III.53}$$

$$|\psi^{\mathcal{A}}_{1,\gamma}\rangle = \frac{1}{\sqrt{2}}|00\rangle_{\wr} + \frac{1}{\sqrt{2}}\ |11\rangle_{\wr}\ . \tag{III.54}$$

$|\psi^{\mathcal{A}}_{1,\gamma}\rangle$ can be simplified as follows:

$$|\psi^{\mathcal{A}}_{1,\gamma}\rangle = \frac{1}{\sqrt{2}}|00\rangle_{\wr} + \frac{1}{\sqrt{2}}|11\rangle_{\wr} \tag{III.55}$$

$$\equiv \frac{1}{\sqrt{2}}\begin{pmatrix}\cos(\frac{\pi}{8})\\ \sqrt{i}\sin(\frac{\pi}{8})\end{pmatrix}\otimes\begin{pmatrix}\cos(\frac{\pi}{8})\\ \sqrt{i}\sin(\frac{\pi}{8})\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}\sin(\frac{\pi}{8})\\ -\sqrt{i}\cos(\frac{\pi}{8})\end{pmatrix}\otimes\begin{pmatrix}\sin(\frac{\pi}{8})\\ -\sqrt{i}\cos(\frac{\pi}{8})\end{pmatrix} \tag{III.56}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}\cos^2(\frac{\pi}{8})\\ \sqrt{i}\cos(\frac{\pi}{8})\sin(\frac{\pi}{8})\\ \sqrt{i}\cos(\frac{\pi}{8})\sin(\frac{\pi}{8})\\ i\sin^2(\frac{\pi}{8})\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}\sin^2(\frac{\pi}{8})\\ -\sqrt{i}\cos(\frac{\pi}{8})\sin(\frac{\pi}{8})\\ -\sqrt{i}\cos(\frac{\pi}{8})\sin(\frac{\pi}{8})\\ i\cos^2(\frac{\pi}{8})\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\i\end{pmatrix} \tag{III.57}$$

$$\equiv \frac{1}{\sqrt{2}}|00\rangle_{+} + \frac{1}{\sqrt{2}}i\,|11\rangle_{+}\ . \tag{III.58}$$

[4] Or at any point in the holding phase.

The reduced density operators on Bob's side are

$$\begin{aligned}
&\rho_{\mathcal{B}}\left(\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle\right) = \mathrm{Tr}_{\mathcal{A}}\left(\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle\left\langle\psi_{1,\gamma}^{\mathcal{A}}\right|\right) && \text{(III.59)}\\
&= \mathrm{Tr}_{\mathcal{A}}\left(\left(\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{i}{\sqrt{2}}\left|11\right\rangle\right)\left(\frac{1}{\sqrt{2}}\left\langle 00\right| + \frac{-i}{\sqrt{2}}\left\langle 11\right|\right)\right)\\
&= \mathrm{Tr}_{A}\Bigg(\quad\left(\frac{1}{\sqrt{2}}\left|0\right\rangle^{\mathcal{H}_{\mathcal{A}}}\otimes\left|0\right\rangle^{\mathcal{H}_{\mathcal{B}}}\right)\left(\frac{1}{\sqrt{2}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&\qquad + \left(\frac{1}{\sqrt{2}}\left|0\right\rangle^{\mathcal{H}_{\mathcal{A}}}\otimes\left|0\right\rangle^{\mathcal{H}_{\mathcal{B}}}\right)\left(\frac{-i}{\sqrt{2}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&\qquad + \left(\frac{i}{\sqrt{2}}\left|1\right\rangle^{\mathcal{H}_{\mathcal{A}}}\otimes\left|1\right\rangle^{\mathcal{H}_{\mathcal{B}}}\right)\left(\frac{1}{\sqrt{2}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&\qquad + \left(\frac{1}{\sqrt{2}}\left|1\right\rangle^{\mathcal{H}_{\mathcal{A}}}\otimes\left|1\right\rangle^{\mathcal{H}_{\mathcal{B}}}\right)\left(\frac{1}{\sqrt{2}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\right)\Bigg)\\
&= \frac{1}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|0\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|0\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}}\right) + \frac{-i}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|0\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|0\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&\quad + \frac{i}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|1\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|1\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}}\right) + \frac{1}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|1\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|1\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&= \frac{1}{2}\left\langle 0|0\right\rangle\left|0\right\rangle\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{-i}{2}\overbrace{\left\langle 0|1\right\rangle}^{=0}\left|0\right\rangle\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{i}{2}\overbrace{\left\langle 1|0\right\rangle}^{=0}\left|1\right\rangle\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{1}{2}\left\langle 1|1\right\rangle\left|1\right\rangle\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\\
&= \frac{1}{2}\left|0\right\rangle\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\\
&= \frac{1}{2}\left\langle 0|0\right\rangle\left|0\right\rangle\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{1}{2}\overbrace{\left\langle 0|1\right\rangle}^{=0}\left|0\right\rangle\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{1}{2}\overbrace{\left\langle 1|0\right\rangle}^{=0}\left|1\right\rangle\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}} + \frac{1}{2}\left\langle 1|1\right\rangle\left|1\right\rangle\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\\
&= \frac{1}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|0\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|0\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}}\right) + \frac{1}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|0\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|0\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&\quad + \frac{1}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|1\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|1\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 0\right|^{\mathcal{H}_{\mathcal{B}}}\right) + \frac{1}{2}\mathrm{Tr}_{\mathcal{A}}\left(\left|1\right\rangle^{\mathcal{H}_{\mathcal{A}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}}\otimes\left|1\right\rangle^{\mathcal{H}_{\mathcal{B}}}\left\langle 1\right|^{\mathcal{H}_{\mathcal{B}}}\right)\\
&= \mathrm{Tr}_{\mathcal{A}}\left(\left(\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle\right)\left(\frac{1}{\sqrt{2}}\left\langle 00\right| + \frac{1}{\sqrt{2}}\left\langle 11\right|\right)\right)\\
&= \mathrm{Tr}_{\mathcal{A}}\left(\left|\psi_{0,\gamma}^{\mathcal{A}}\right\rangle\left\langle\psi_{0,\gamma}^{\mathcal{A}}\right|\right) = \rho_{\mathcal{B}}\left(\left|\psi_{0,\gamma}^{\mathcal{A}}\right\rangle\right). && \text{(III.60)}
\end{aligned}$$

Thus, the conditions of theorem zero to one are met.

Define $\rho_{\mathcal{B}} \coloneqq \rho_{\mathcal{B}}\left(\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle\right)$. Analogous to Equations III.59–III.60,

$$\rho_{\mathcal{A}}\left(\left|\psi_{0,\gamma}^{\mathcal{A}}\right\rangle\right) = \rho_{\mathcal{A}}\left(\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle\right) = \frac{1}{2}\left|0\right\rangle\left\langle 0\right|^{\mathcal{H}_{\mathcal{A}}} + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|^{\mathcal{H}_{\mathcal{A}}} = \frac{1}{2}\begin{pmatrix}1 & \\ & 1\end{pmatrix}. \tag{III.61}$$

So $\rho_{\mathcal{B}}, \rho_{\mathcal{A}}\left(\left|\psi_{0,\gamma}^{\mathcal{A}}\right\rangle\right)$ and $\rho_{\mathcal{A}}\left(\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle\right)$ have the eigenvalues $\lambda_1 = \lambda_2 = \frac{1}{2}$.

$$\left|f_1\right\rangle \coloneqq \left|0\right\rangle, \left|f_2\right\rangle \coloneqq \left|1\right\rangle \tag{III.62}$$

are eigenvectors of ρ_B,

$$\left|e_1^{(0)}\right\rangle \coloneqq \left|0\right\rangle, \left|e_2^{(0)}\right\rangle \coloneqq \left|1\right\rangle \tag{III.63}$$

eigenvectors of $\rho_{\mathcal{A}}\left(\left|\psi_{0,\gamma}^{\mathcal{A}}\right\rangle\right)$ and

$$\left|e_1^{(1)}\right\rangle \coloneqq \left|0\right\rangle, \left|e_2^{(1)}\right\rangle \coloneqq i\left|1\right\rangle \tag{III.64}$$

eigenvectors of $\rho_{\mathcal{A}}\left(\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle\right)$. With that, Schmidt decompositions of $\left|\psi_{0,\gamma}^{\mathcal{A}}\right\rangle$ and $\left|\psi_{1,\gamma}^{\mathcal{A}}\right\rangle$ are

$$\left|\psi_{b,\gamma}^{\mathcal{A}}\right\rangle = \sum_{i=1}^{2}\sqrt{\lambda_i}\left|e_i^{(b)}\right\rangle\left|f_i\right\rangle, \quad b \in \{0,1\}. \tag{III.65}$$

To find S the following equations are solved.

$$S\,|0\rangle = |0\rangle \Rightarrow S \quad = \begin{pmatrix} 1 & \\ & * \end{pmatrix} \tag{III.66}$$

$$S\,|1\rangle = i\,|1\rangle \Rightarrow S = \begin{pmatrix} * & \\ & i \end{pmatrix}. \tag{III.67}$$

It follows, that

$$S = \begin{pmatrix} 1 & \\ & i \end{pmatrix} \tag{III.68}$$

is the operation Alice has to apply only on her side to convert $|\psi^{\mathcal{A}}_{0,\gamma}\rangle$ to $|\psi^{\mathcal{A}}_{1,\gamma}\rangle$. ∗

III.3.4. Non-Perfect QBC

It will now be shown, that such a transformation not only exists if the QBC-protocol is perfectly concealing, but also if it is unconditionally concealing. Thus, it will be shown a cheating transformation on Alice's side exists if $F'(\gamma)$ is not equal, but arbitrarily close to one.

Definition III.2 (Purification[5]). Let ρ be any mixed state on Hilbert space $\mathcal{H}_1$. A *purification* of ρ is any pure state $|\phi\rangle$ in any extended hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ with the property that $\rho = \mathrm{Tr}_{\mathcal{H}_2}(|\phi\rangle\langle\phi|)$. ♣

Theorem 10 (Uhlmann's theorem[6]):
Let ρ_1, ρ_2 be states of the same quantum system $\mathcal{H}_1$ and $|\phi_1\rangle, |\phi_2\rangle$ purifications of ρ_1 and ρ_2 respectively into $\mathcal{H}_1 \otimes \mathcal{H}_2$. Then the fidelity between ρ_1, ρ_2 is the maximization over the inner product of all such purifications.

$$F(\rho_1, \rho_2) = \max_{|\phi_1\rangle, |\phi_2\rangle} |\langle\phi_1|\phi_2\rangle| \tag{III.69}$$

♢

For readability the following short labels for states and density operators will be used:

$$\rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{0,\gamma}\rangle\right) =: \rho_0, \quad \rho_{\mathcal{B}}\left(|\psi^{\mathcal{A}}_{1,\gamma}\rangle\right) =: \rho_1, \quad |\psi_{0,\gamma}\rangle =: |\psi_0\rangle, \quad |\psi^{\mathcal{A}}_{1,\gamma}\rangle =: |\psi_1\rangle\,. \tag{III.70}$$

Theorem 11 (Unconditional security against Bob implies insecurity against Alice):
Any QBC-protocol that is unconditionally concealing is not unconditionally binding. ♢

Proof: Following Lemma 1, $0 < F'(\gamma) = F(\rho_0, \rho_1) = 1 - \delta$, with $\delta > 0$, for a very small delta. Per Definition III.2, $|\psi_1\rangle$ is a purification of ρ_1. As Uhlmann's theorem applied to ρ_0 and ρ_1 describes a maximization over all purifications of those states, there exists a purification $|\psi_{01}\rangle$ of ρ_0, such that

$$\langle\psi_{01}|\psi_1\rangle \geq F'(\gamma)\,. \tag{III.71}$$

Since $|\psi_0\rangle$ and $|\psi_{01}\rangle$ are purifications of the same reduced density operator ρ_0, there exists an operation on $\mathcal{H}_{\mathcal{A}}$ that transforms $|\psi_0\rangle$ into $|\psi_{01}\rangle$. Equation III.71 implies, that the probability of Bob being able to differentiate $|\psi_1\rangle$ from $|\psi_{01}\rangle$ and thus detect Alice's cheat, goes to zero as δ goes to zero and $F'(\gamma)$ nears one. This is underlined in the following equation.

$$F(|\psi_{01}\rangle\langle\psi_{01}|, |\psi_1\rangle\langle\psi_1|) \geq 1 - \delta\,. \tag{III.72}$$

■

[5] Following Jozsa (1994, Definition 1).
[6] Following Jozsa (1994, Theorem 2).

Theorem 12 (Unconditionally secure qbc is impossible):
No quantum bit commitment that falls under the framework presented in this chapter is unconditionally secure. ♢

Proof: A QBC-protocol that is not unconditionally hiding is not unconditionally secure. Assume the protocol is unconditionally hiding. Then following Theorems 9 and 11 it is not unconditionally binding. ■

III.3.5. Complexity of Alice's Cheat

A malicious Alice has been modeled as an unconditional attacker. In this section it will be shown how much computational power Alice would actually need to perform the attack, by showing the computational complexity of the attack to be in $\mathcal{O}(2^{n\omega}), \quad 2 < \omega < 2.37369$.

III.3.5.1. Complexity of the Transformation

As seen in Subsection III.3.3, to find the cheating transformation that maps a state committing to zero to a state committing to one, an eigen-decomposition of the reduced density operator on Bobs side has to be calculated and an appropriate basis transformation has to be found. Transforming one basis into another in high dimensions is a costly procedure. This is shown in an example and then generalized.

III.3 Example The Hilbert Space for a two qubit system is of dimension $2^2 = 4$, thus a basis consists of four, four-dimensional state vectors. Two bases of this Hilbert Space are considered:

$$b = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\} \tag{III.73}$$

and

$$b' = \{\mathbf{b}'_1, \mathbf{b}'_2, \mathbf{b}'_3, \mathbf{b}'_4\} \ , \tag{III.74}$$

where for $i = 1, 2, 3, 4$

$$\mathbf{b}_i = \begin{pmatrix} \alpha_i \\ \beta_i \\ \gamma_i \\ \delta_i \end{pmatrix} \tag{III.75}$$

and

$$\mathbf{b}'_i = \begin{pmatrix} \alpha'_i \\ \beta'_i \\ \gamma'_i \\ \delta'_i \end{pmatrix} \tag{III.76}$$

respectively. An operation S is searched, such that it transforms states of b to states of b'. Thus, such an operator has to fulfill the following system of equations

$$S \begin{pmatrix} \alpha_i \\ \beta_i \\ \gamma_i \\ \delta_i \end{pmatrix} = \begin{pmatrix} \alpha'_i \\ \beta'_i \\ \gamma'_i \\ \delta'_i \end{pmatrix}, \quad i = 1, 2, 3, 4 \, . \tag{III.77}$$

Written differently

$$S\overbrace{\begin{pmatrix}\alpha_1 & \beta_1 & \gamma_1 & \delta_1\\ \alpha_2 & \beta_2 & \gamma_2 & \delta_2\\ \alpha_3 & \beta_3 & \gamma_3 & \delta_3\\ \alpha_4 & \beta_4 & \gamma_4 & \delta_4\end{pmatrix}}^{=(\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4)} = \overbrace{\begin{pmatrix}\alpha'_1 & \beta'_1 & \gamma'_1 & \delta'_1\\ \alpha'_2 & \beta'_2 & \gamma'_2 & \delta'_2\\ \alpha'_3 & \beta'_3 & \gamma'_3 & \delta'_3\\ \alpha'_4 & \beta'_4 & \gamma'_4 & \delta'_4\end{pmatrix}}^{=(\mathbf{b}'_1,\mathbf{b}'_2,\mathbf{b}'_3,\mathbf{b}'_4)}, \tag{III.78}$$

and since $(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4)$ is orthonormal,

$$S = (\mathbf{b}'_1, \mathbf{b}'_2, \mathbf{b}'_3, \mathbf{b}'_4)(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4)^T . \tag{III.79}$$

*

Alice has created the states that make up the density operator on her side, so she is aware of that concrete operator. However, she still has to find the eigenstates, needed to calculate the cheating operation. Decomposing the density operator into eigenstates has the same complexity as matrix multiplication (Demmel, Dumitriu, and Holtz 2007). To calculate the basis conversion S, which is also the cheating transformation operation, a matrix multiplication has to be performed, which for a system of dimension k has a complexity of $\mathcal{O}(k^\omega)$, $2 < \omega < 2.37369$ (Davie and Stothers 2013).

In the general case, if the honest protocol requires n-bit (classical) string to be transferred ($\mathbf{w}$ in the BB84 scheme), the Hilbert Space on dishonest Alice's side is of dimension $k = 2^n$. Thus, the complexity of transforming $|\psi^{\mathcal{A}}_{0,\gamma}\rangle$ into $|\psi^{\mathcal{A}}_{1,\gamma}\rangle$ is $\mathcal{O}(2^{n^\omega} + 2^{n^\omega}) = \mathcal{O}(2^{n^\omega}) = \mathcal{O}(2^{n\omega})$, $\quad 2 < \omega < 2.37369$.

III.3.5.2. Finding the Cheating State

To find the purification $|\psi_{01}\rangle$ described in Equation III.71, no maximization problem has to be solved. Instead, the proof by Jozsa (1994, section 4) describes how to construct this state. First Schmidt polar forms of $|\psi_0\rangle$ and $|\psi_{01}\rangle$ are computed:

$$|\psi_0\rangle = \sum_{i=1}^{k} \sqrt{\lambda_i}\, |e_i\rangle\, |f_i\rangle \tag{III.80}$$

and

$$|\psi_{01}\rangle = \sum_{i=1}^{k} \sqrt{\mu_i}\, |\tilde{e}_i\rangle\, |g_i\rangle\ . \tag{III.81}$$

This is possible, even though $|\psi_{01}\rangle$ is not yet known, since the Schmidt polar form is given by the eigenvalues λ_i, μ_i and the orthonormal eigenvectors $|e_i\rangle, |\tilde{e}_i\rangle$ of ρ_0 and ρ_1 respectively. Then matrices are calculated that transform the different orthonormal bases into each other,

$$|\tilde{e}_i\rangle = V\, |e_i\rangle\,, \quad |g_i\rangle = U_1\, |\tilde{e}_i\rangle\ . \tag{III.82}$$

And since $|e_i\rangle, |\tilde{e}_i\rangle$ are eigenvectors of ρ_0 and ρ_1 respectively

$$\sqrt{\lambda_i}\, |e_i\rangle = \sqrt{\rho_0}\, |e_i\rangle\,, \quad \sqrt{\mu_i}\, |e_i\rangle = \sqrt{\rho_1}\, |\tilde{e}_i\rangle\ . \tag{III.83}$$

Using Jozsa (1994, Lemma 7), it then can be shown analogous to Jozsa (1994, Section 4), that $|\psi_{01}\rangle$ can be constructed as follows

$$|\psi_{01}\rangle = \sum_{i=1}^{k} \sqrt{\rho_1} U_1^T V V^T\, |e_i\rangle \otimes |e_i\rangle\ . \tag{III.84}$$

The eigen-decomposition and basis transforming operator can be reused to find the operator S, that maps $|\psi_0\rangle$ into $|\psi_{01}\rangle$, following Subsection III.3.3.

Thus $|\psi_{01}\rangle$ and S can be found by calculating eigen-decompositions and basis transformations. The complexity to do these operations, where the honest protocol requires the transfer of n bits, was already shown to be $O(2^{n\omega}), \quad 2 < \omega < 2.37369$ in III.3.5.1.

III.4. Different Strategies for Bob

The proof of Mayers and Lo and Chau, assumes a fixed honest strategy followed by Bob. This has been criticized by some who assert, that this assumption of Bob's behavior would lose the generality of the proof.

One such skeptic is Yuen (2005), who presents a protocol using so called *anonymous states*, which they claim to be unconditionally secure. Such skeptics argue, that Mayers' and Lo-Chau's proof is merely a demonstration of the impossibility for Kerckhoffian protocols, so protocols that follow the principle that security of cryptographic protocols should not rely on keeping parts of the algorithm secret.

However, an extended version of Mayers' no-go theorem is still applicable. This was shown by D'Ariano et al. (2007). The Authors extend the no-go theorem to general strategies for both Alice and Bob.

D'Ariano et al. make a distinction between protocols and strategies. Protocols are the framework that regulates the exchange of messages. Strategies are the particular plans Alice and Bob have for operating their local laboratories. When Bob follows a specified honest strategy $b_\star$, which is publicly known in accordance with Kerckhoff's principle, their proof coincides with the analysis in Mayers, Lo and Chau's proof.

Mayers, Lo and Chau treat classical information quantum mechanically and send it over noiseless quantum channels. In contrast to that, the model of D'Ariano et al. explicitly allows information transfer over classical channels. As a formalism to explicitly handle classical information in protocols, D'Ariano et al. identify quantum systems by their observable algebras. In this formalism, a quantum system with Hilbert space $\mathcal{H}$ represented by the algebra $\mathcal{B}(\mathcal{H})$ of operators on $\mathcal{H}$.

Another formalism used is the *communication tree* to represent different stages of the protocol and their relation to each other. Every node represents the classical information shared up to that point. The nodes also indicate whose turn it is by associating the first node to Bob's turn and then alternating between parties' turns. Branches represent possible signals to be sent. It is also noted for every classical signal, which kind of quantum system accompanies it. However, the observable algebras of Alice and Bob's laboratories do not only depend on the node in the communication tree but also on their chosen strategies.

Cheating becomes harder for Alice if the protocol requires some exchange of classical information as she no longer has full control over the two commitment states. Unitaries which introduce superpositions of states which belong to different classical values already sent to Bob are forbidden. Thus, Alice has to find a cheating unitary for every classical communication history.

With those formalisms, D'Ariano et al. give a general framework for two-party cryptographic protocols, in which they then show that secure quantum bit commitment is impossible. A protocol that falls out of this setting is also presented. It relies on decoherence in Bob's lab and explores the distinction between local erasure of information and destruction of quantum correlations. It will be revisited in IV.1.1.2.

The soundness and security conditions in the impossibility proof are quantified. Alice's honest strategies for committing 0 or 1, i.e. a_0 or a_1, can be distinguished with high probability on Bob's side. If Alice honestly followed a_k, and Bob's measurement results in

k with a probability $\geq (1-\eta)$ for a very small $\eta \geq 0$, then the protocol is η-verifiable or η-sound.

The protocol is ε-concealing, if Alice's honest strategies cannot be distinguished (up to an error of ε) by Bob before the opening phase. Probabilities he measures differ by at most ε, no matter which strategy he follows. When this condition holds with $\varepsilon = 0$, the protocol is perfectly concealing.

A pair of cheating strategies $a_0^\#, a_1^\#$ for Alice, such that Bob cannot distinguish a_0 from $a_0^\#$ and a_1 from $a_1^\#$ better than with probability difference δ, is called a δ-cheating strategy. $a_0^\#$ must be the same as $a_1^\#$ throughout the commitment phase. Such a δ-cheating strategy necessarily has to work against all of Bob's strategies.

If no δ-cheating strategies exist, the protocol is δ-binding. If this is the case and the protocol has a public opening rule — this means in the opening phase the participants meet and Alice allows Bob to perform arbitrary measurements in her system — not even Alice herself could help Bob to tell the difference between her strategies in the opening phase. It is shown, that any protocol that is ε-concealing allows δ-cheating protocol for Alice with $\delta \leq 2\sqrt{\varepsilon}$.

In an anonymous state protocol as described by Yuen (2005), Bob sends a system to Alice whose state is only known to him, and which an honest Alice has to use in some way for the creation her commitment. Such an anonymous state protocol would lead Alice to lack some information such that Uhlmann's theorem still implies existence of a cheating transformation, but the transformation might be unknown to her. In an anonymous state protocol, Alice effectively chooses not a state, but a channel to encode her commitment. Thus, Uhlmann's theorem no longer applies and a Stinespring representation is used in place.

The Stinespring representation generalizes Uhlmann's theorem from quantum states to quantum channels. States can also be expressed as channels with the one-dimensional input space $\mathbb{C}$. This generalization is the basis for the result of D'Ariano et al.

To not restrict generality of their proof by simplifying assumptions, a large class of strategies are to be considered. The framework presented poses no restriction to finite dimensional systems or number of rounds. The only restriction is, that the *expected* number of rounds should be finite. Arbitrarily many rounds of communication of varying lengths, infinite dimensional local laboratory Hilbert spaces etc., all fit into the framework. The idea followed for simplifications is that "obviously inferior methods of analysis for Bob" or "inferior methods to cheat for Alice" need not be considered. What an "obviously inferior strategy" is, is then explicitly defined in their proof.

The discussion presented in the article is restricted to QBC-protocols in which concealment is guaranteed for all branches of the communication tree. Such types of commitment protocols are sometimes referred to as *strong bit commitments*. In a *weak bit commitment*, Bob may learn the value of the bit as long as Alice receives a message stating the bit value has been disclosed. Weak bit commitment is argued to also be impossible.

III.5. Cheat-Sensitive Bit Commitment

Bit commitment as presented in II.4.1 and as used by Lo and Chau (1997) and Mayers (1997) is *strong bit commitment*. Weak bit commitment is defined to be secure, not only if the probability of a successful attack is arbitrarily close to zero, but also if there is a non-zero chance of a cheating party being detected doing so. For this reason this form of bit commitment is also called *cheat-sensitive* bit commitment.

Hardy and Kent (2004) describes two such supposedly cheat-sensitive QBC schemes, a non-relativistic and a relativistic one. The only additional assumption that they use is,

that the commitment will eventually be revealed. The protocol provides challenges for Alice and Bob each, that reveal cheating with some probability when challenged. It works by defining a game that decides which party is challenged and what that means for the continuation of the protocol. A key point to mention, is that they have at one point in the protocol a quantum coin-flip operation to decide the party to be challenged.

Independently Aharonov et al. (2000) presented a so called *quantum escrow* protocol, which is either cheat-sensitive-binding, or cheat-sensitive-concealing. It also features a challenge, that is given to either party. They also provide a biased quantum coin-flipping protocol.

In a later issue (the one cited here), Aharonov et al. (2000) acknowledge Hardy and Kent (2004) and explain how their quantum escrow protocol could also be combined with their coin-flipping protocol to possibly achieve a cheat-sensitive QBC-protocol. However, they note that the security of such a protocol is still an open question, as the independence between the protocols is hard to prove or disprove, and thus leave the security of their third protocol as an open question. They also criticize Hardy and Kent (2004) for not regarding the security against a cheater that tries to correlate the two parts of the protocol to their advantage.

Indeed, cheating methods for the above mentioned type of supposed cheat-sensitive protocols are provided by S. Ishizaka (2007) using this kind of exploit. The authors show how a cheating Bob is able to recover the state he collapsed whenever he looses the coin-flip, and that modifications of the protocol that obstruct this cheating method for Bob open up cheating methods for Alice. They conclude that this dilemma (that either Bob or Alice is able to cheat in a QBC-like protocol) cannot be solved but only postponed by introducing a coin-flipping subroutine. This conclusion is further explored by Satoshi Ishizaka (2008).

In addition to that, as mentioned in IV.1.1.2, D'Ariano et al. (2007, p. 24) argue, a modified version of their no-go theorem can also be applied to cheat-sensitive QBC.

IV. The Possible

While quantum bit commitment in the framework of Lo and Chau (1997) and Mayers (1997) has shown to be impossible, one might consider different assumptions (such as physical assumptions or technological constraints), or even different security definitions under which quantum bit commitment can be securely implemented. Figure IV.2.1 gives an overview of the different assumptions, primitives, and forms of QBC, discussed in this chapter.

IV.1. Unconditional Security

After the protocol and attack of Bennett and Brassard (1984) was first published, protocols were proposed, falsely claiming to achieve unconditional secure QBC-protocols. Notable is a protocol by Brassard, Crepeau, et al. (1993), which was later called BCJL, as its disproval lead to Mayers' generalized no-go theorem and proof. However, there has still been a large number of papers that tried to circumvent Mayers' and Lo and Chau's proof without changing the assumptions, for example by combining quantum protocols with classical protocols or by using anonymous states (Yuen 2005). Those protocols were then disproven by D'Ariano et al. (2007) who published a more general no-go theorem.

This does not mean that unconditionally secure QBC is impossible under all assumptions. By introducing new assumptions like the existence of noise in certain places or by taking special relativity into account, unconditionally secure QBC schemes can be constructed. Modifying the goal for security has also been considered.

IV.1.1. Noise and Decoherence

Decoherence usually describes the phase-dampening process that causes a particle to lose its quantum properties by interacting with many environmental particles and *quantum-noise* is usually used more broadly to describe the loss of coherence. However, the two terms have historically been used interchangeably by some authors (Nielsen and Chuang 2010, p. 398).

Noise is usually an unwanted property in quantum computation as loss of quantum properties is counterproductive when trying to use them in calculations. As a consequence, quantum error-correction is a field of great interest (Nielsen and Chuang 2010, p. 453). However, in *quantum cryptography* there have been investigations on whether noise or decoherence can be used to actually make protocols *more* secure, as many attacks, including the Mayers-Lo-Chau attack, rely on cohering quantum properties to be carried out successfully.

IV.1.1.1. Noisy Storage

Konig, Wehner, and Wullschleger (2012) introduce the concept of a *noisy-storage* channel to formally relate the security of a QBC-protocol to sending information through such a channel. They assume that no large scale reliable quantum storage is available, therefore they introduce a model in which storage is limited and stored qubits are subjected to a specified level of noise over time. In that they also assume Markovian noise, as they assume that noise only ever increases and thus information stored only ever decreases.

They force participants of a protocol to use the storage device by introducing time delays and then argue that realistic levels of noise rule out even the most general attack. This model also includes the *bounded quantum-storage* model as initiated by Damgard et al. (2005) as a special case.

The decoding probability is defined to be the probability that a randomly chosen bit string sent through a storage device can be successfully retrieved. It is shown that arbitrary channels, that have the property that the decoding probability decays exponentially above a certain threshold, can be used to achieve security. The authors also show that the number of classical bits, that can be sent through the noisy-storage channel, being limited is a sufficient condition for security.

For their QBC-protocol they introduce a novel cryptographic primitive, called *weak string erasure*, on which they base the protocol on. The authors prove their protocol to be secure in the model they presented and explain that their new primitive could be of independent interest.

As the noisy-channel assumption is the only restriction to the adversary, and they claim the noisy-channel assumption to be particular realistic itself, the assumptions needed for this approach appear rather reasonable.

IV.1.1.2. Trusted Decoherence

In addition to generalizing Mayers' proof, D'Ariano et al. (2007) also use decoherence cleverly to define a decoherence-based QBC scheme, not affected by their own proof.

They present three ways to use decoherence for a more secure protocol. Trusted decoherence in Alice's laboratory is implemented by a notary overseeing Alice's actions during the commitment phase, who is able to take some part of Alice's system and destroy it if cheating is suspected. The notary is able to leave after the commit phase and thus the authors argue, this protocol is cheaper than one where a notary oversees Alice for the whole protocol. The constructed protocol is proven to be perfectly concealing and statistically binding.

A notary overseeing Alice actions is quite a strong assumption, even it is only for the commit phase, so they also present a protocol based on a weaker assumption. In this protocol, coherence in Bob's Laboratory is destroyed by a process that Bob has no control over, such that only classical records remain for him. While this would at first glance weaken the already weaker partner, it is argued if one is able to convince Alice this decoherence is really occurring, she will have lower demands on concealment. So a protocol, that is both statistically concealing and statistically binding, can be constructed under these assumptions. In their paper, such a construction is shown and proven to be secure.

A third place where trusted decoherence can be used to implement secure bit commitment is the transmission-line between Alice's and Bob's laboratories. The authors do not show a protocol of their own for this, but rather refer to other implementations that have been shown at the time.

IV.1.1.3. Sender Unable to Perform Large Coherent Measurements

Salvail (1998) assumes Alice is not able to perform generalized measurements involving more than n-qubits.

To be more precise Salvail first explains, that coherent measurements can be seen as a unitary transformation acting on the observed system and an ancilla, followed by von Neumann measurements in the computational basis, not dissimilar from how measurements are described in Subsection II.3.3. He then argues performing such a n-coherent measurement for a large n is difficult, given that a large, coherent, unitary transformation has to be carried out. A scheme is then presented, for which it is subsequently shown that such large coherent measurements need be performed in order to apply Mayers' attack on it. So it is proven that the scheme is both statistically binding and statistically concealing under the aforementioned assumption of difficulty, performing large n-coherent measurements.

The assumption of the impossibility to perform n-coherent generalized measurements is difficult to assess. This is because, while at the time of writing such measurements are not

possible yet, they could become possible in the future. Blumoff et al. (2016) demonstrate a highly coherent quantum computing architecture based on superconducting qubits, and use it to establish specific multi-qubit measurements, and Kjaergaard et al. (2020) review this superconducting mode of operation to be promising for larger scale, error-corrected quantum computers. So, it cannot be ruled out, that with future development, the generalized n-coherent measurements as described by Salvail will in fact be possible.

IV.1.2. Special Relativity

Special relativity and relativistic quantum theory is interesting for cryptography, as its principles allow new models in which tasks are possible that are impossible in purely quantum theoretic models and vice versa. Those principles include the no-signaling principle which prohibits superluminal signaling (that is sending signals faster than the speed of light) and the principle of information causality which forbids two spacelike separated events to have influence on each other. The principles of relativistic quantum theory are given by Kent (2012), and a great introduction to spacetime and what it means for events to be spacelike separated is given by John D. Norton (2020). An example for a task that is impossible in relativistic quantum theory but not in non-relativistic is *summoning*, as given by the no-summoning theorem (Kent 2012).

A cryptographic protocol that makes use of special relativity is called a *relativistic* protocol. The impossibility of sending signals faster than the speed of light can be used in such a way as to guarantee that communication from one cooperating partner to the other is not possible in less than a fixed amount of time, which in turn can be used instead of the very strong assumption that (one of) the partners is situated in a faraday cage.

Kent (1999) introduces an unconditionally secure BC protocol based on special relativity. This is a classical protocol, the enforcement of classicality is suggested to be implemented by use of trusted decohering channels as described in IV.1.1.2. It works by splitting Alice and Bob each in two cooperating parties and makes it possible for Bob to verify that indeed they cannot communicate with each other. This is achieved by using a sequence of communications which to maintain security have to be kept up, even after the revelation of the commitment.

In the implementation, the locations $\underline{x}_1, \underline{x}_2$ are defined and the Laboratories A_i, B_i of Alice and Bob have to be within distance δ of these locations $\underline{x}_i$ for $i = 1, 2$, where $\triangle x = |\underline{x}_1 - \underline{x}_2| \gg \delta$. The test Bob can perform to confirm Alice's locations works as follows: with the speed of light set to $c = 1$, let B_i send test signals to A_i and to pass the test, A_i has to reply to these messages within 2δ time.

A_i need to share a random string between them before the protocol starts. In the protocol, classical bit commitments are carried out in regular intervals, alternating between commitments from A_1 to B_1 and commitments from A_2 to B_2 where each commitment consumes an increasingly long segment of the random string shared by the Alices. The time in which each of those commitments has to be completed is limited to a fixed interval $\triangle t \gg \triangle x$. This is continued until an Alice chooses to unveil the commitment. To verify the unveiled bit, Bob has to gather data of both B_1 and B_2 in one place. It is proven that this need to wait for information, both for unveiler and unveilee, implies that the protocol presented is not vulnerable to Mayers' or Lo and Chau's attack. It also is not vulnerable against the attack of D'Ariano et al. (2007).

A quantum version of the protocol where Alice is able to keep a qubit in superposition is also discussed, but it is argued that this gives her no advantage over randomly choosing a classical bit. However, it is mentioned that while this is true for a standalone QBC-protocol, caution has to be held when using it as a sub-protocol of another protocol.

It is also noted that an implementation of this protocol would need an exponential increase in channel capacity for an increasing commitment time, as an ever-increasing

amount of information has to be sent in a fixed time interval.

Channel capacity describes how much information can be transmitted over a classical channel such as a copper wire, or over a respective quantum channel. It is clear that the requirement for an exponential increasing channel capacity makes the protocol not actually practically usable. The protocol thus is a *theoretical* solution to the problem of unconditionally secure bit commitments over arbitrary long time intervals. It is argued however, that the time delay enforcement, on which the protocol is based around, could also be implemented using other physical assumptions.

IV.2. Concealing and Binding Security Tradeoffs

While in most if not all realistic settings unconditionally secure, non-relativistic quantum bit commitment is impossible, protocols fulfilling weaker security conditions are possible, considering some assumptions. Of particular interest are those protocols that are either unconditionally binding or unconditionally concealing and computationally concealing or computationally binding respectively, as other cryptographic protocols can be based upon QBC-protocols with these properties. For example zero knowledge arguments can be based on unconditionally concealing bit commitment (Brassard, Chaum, and Crépeau 1988).

Most of the protocols presented in this section are based on the assumption of the existence of either quantum one-way functions, or quantum one-way permutations.

IV.2.1. Unconditionally Concealing

IV.2.1.1. From Quantum One-Way Permutations

Dumais, Mayers, and Salvail (2000) introduce and prove the security of a perfectly concealing and computationally binding QBC scheme based on quantum one-way permutations. For the perfectly concealing property, it is shown that the commitment states on Bobs side are in fact always identical. The authors parametrize their binding definition with a performance success ratio, $R(n) \geq T(n)/S(n)$ where $T(n)$ is the number of universal gates, needed to implement an adversary, $S(n)$ the probability they are successfully able to cheat and n the security parameter. To be more precise, they define a QBC to be $R(n)$-binding if no adversary with $R(n) \geq T(n)/S(n)$ exists. An analogous definition of a $R(n)$-secure family of quantum one-way functions is also given. In their analysis they then show, that for any $R(n)$-secure family of quantum one-way permutations their QBC-protocol, that takes such a family as an input, is $R'(n)$-binding with $R'(n) \in \Omega\left(\sqrt{R(n)}\right)$. They also argue, alongside with Salvail (1998), that the limitation keeping a conditional attacker from breaking the scheme is not their computational power, but the size of the entanglement that their quantum computer can deal with.

IV.2.1.2. From Quantum One-Way Functions

Crépeau, Légaré, and Salvail (2001) improve this by proving that it is possible to convert a statistically binding (and computationally concealing) QBC scheme to a statistically concealing (and computationally binding) one. This means that a statistically concealing and computationally binding QBC scheme can be based upon any quantum one-way function.

Their proof works as follows: a statistically concealing and computationally binding QBC is constructed from a quantum oblivious transfer protocol and a statistically binding QBC. For quantum oblivious transfer it is shown that it can be based on a statistically binding bit commitment scheme. It is proven that the classical statistically binding commitment scheme given by Naor (1991), which is based upon a pseudo-random bit generator, is secure against an adversary with access to a quantum computer if this pseudo-random bit generator is also secure against a quantum adversary. This can be achieved using a

quantum one-way function. The one-way function is used to construct a pseudo-random bit generator which is resistant to quantum distinguishers.

Thus, both statistically binding and computationally concealing QBC and computationally binding and statistically concealing QBC can be constructed from a quantum one-way function. This stands in contrast to the classical case, where a statistically binding and computationally concealing BC can be based upon a one-way function, but computationally binding and statistically concealing BC schemes can be based on one-way permutations, but not on one-way functions. This means in this instance, the assumptions in the quantum case can be weakened compared to the classical case.

IV.2.2. Unconditionally Binding

IV.2.2.1. From Quantum One-Way Permutations

Adcock and Cleve (2002) show a perfectly binding and computational concealing QBC-protocol from any quantum one-way permutation, as a complement to Dumais et al. computationally binding protocol.

The classical Goldreich-Levin-Theorem reduces inverting a one-way function to predicting a hard-predicate of this function. Adcock and Cleve present a quantum version of this theorem. They then use it to construct a perfectly binding, computationally concealing QBC.

IV.2.2.2. From Approximate-Preimage-Size Quantum One-Way Functions

Koshiba and Odaira (2009) define the *almost onto* property for quantum one-way functions. The existence of such quantum one-way functions is an assumption that is stronger than that of quantum one-way functions in general, but weaker than the assumption of quantum one-way permutations. Such a quantum one-way function is called an *approximate-preimage-size quantum one-way function*. Based on such approximate-preimage-size quantum one-way function, they define a QBC-protocol that is statistically concealing and computationally binding. Their QBC-protocol is a generalization of the protocol described in IV.2.1.1, in which they replace the quantum one-way permutations of Dumais, Mayers, and Salvail (2000) with quantum one-way functions.

In their proof, they base the computational binding property on the quantum one-way property of the function used by the protocol and the statistically concealing property on its almost-onto property.

IV.2.2.3. From Quantum One-Way Functions

As mentioned in IV.2.1.2, Crépeau, Légaré, and Salvail (2001) also show a statistically binding and computationally secure QBC based on Naors classical BC. While the protocol of Crépeau, Légaré, and Salvail (2001) only assumes quantum one way functions and Koshiba and Odaira (2009) thus hold stronger assumptions, the advantage of the latter over the former protocol is that it is non-interactive and thus easier to analyze for potential flaws. Koshiba and Odaira (2009) also argue, if there exists a general construction of an almost-onto quantum one-way function, then a statistically concealing quantum bit commitment scheme can be constructed from any quantum one-way function which would, for the reason mentioned above, be an advantage over Crépeau, Légaré, and Salvail (2001).

IV.2.3. Partially Binding, Partially Concealing

As various protocols with varying degrees of concealment and bindingness have been introduced, the question arises what the best possible tradeoff between those two properties looks like. Spekkens and Rudolph (2001) explore exactly that. They define measures

for bindingness, Alice's control $0 \leq C \leq \frac{1}{2}$, and concealment, Bob's gain $0 \leq G \leq \frac{1}{2}$. They then explore the bounds of those measures on their own and by fixing the one while maximizing the other. Their result for $G^{\max}$, the maximum amount of information Bob can gather is given by the trace distance: $G^{\max} \geq \frac{1}{2}D(\rho_0, \rho_1)$. In contrast to that, the maximum amount of control Alice has to change her mind, $C^{\max}$, is restricted by the fidelity: $C^{\max} \geq \frac{1}{2}F(\rho_0, \rho_1)^2$. The states ρ_0 and ρ_1 are the states in Bob's possession after the commit-phase. They also define the class of so-called *purification bit commitment protocols*, of which BB84 is part of. It is shown that protocols of that class saturate the bounds $G^{\max} = \frac{1}{2}D(\rho_0, \rho_1)$ and $C^{\max} \geq \frac{1}{2}F(\rho_0, \rho_1)$.

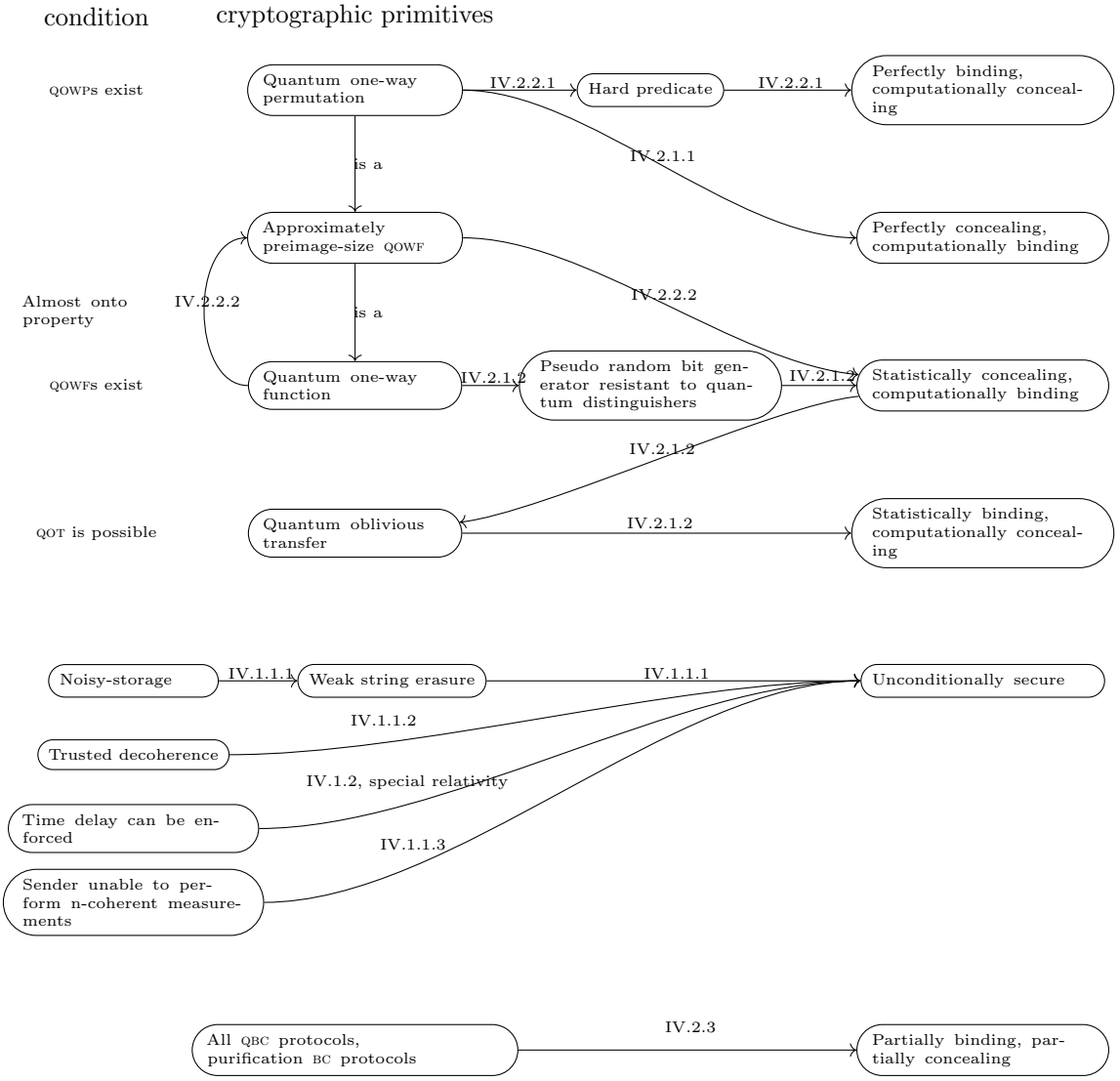


Figure IV.2.1.: Relation between assumptions, other primitives and different levels of security for QBC

V. Conclusion

It has been shown that in a very general setting, unconditional quantum bit commitment is impossible. However, it also has been shown that there are some promising non-standard settings, that could potentially be implemented, in which unconditional quantum bit commitment would be possible. Weaker forms of quantum bit commitment also have been presented.

There still are some open questions that this thesis could not answer which need further analysis. One such question is, that D'Ariano et al. 2007 claim that Alice and Bob may also draw on an unlimited supply of certified classical or quantum correlations, in the form of an arbitrary shared initial state ρ_0, and yet their no-go theorem still applies and secure QBC remains impossible. This conflicts with Mayers (1997) and Lo and Chau 1997, who claim that QBC with pre-shared entangled states can be trivially realized.

Another question left unanswered is the one of quantum string commitment, where instead of bits, bit strings are being committed. Of course it is possible to implement string commitment given bit commitment, but there is some research, that presents quantum string commitment as a weaker form of qbc, even weaker than weak qbc. Possibilities, applications and limitations of quantum string commitments are being discussed by amongst others Buhrman et al. (2008), Jain (2005), and Unruh (2016).

Lastly whether or not generalized measurements as described in IV.1.1.3 actually can be applied remains to be seen.

A. Interactive Example

In Listing A.1 an interactive version of the attack on BB84 is given in Q#. For a guide to install the Q# development kit (QDK) see `https://docs.microsoft.com/en-us/azure/quantum/install-command-line-qdk`. After QDK has been installed, to compile and execute the program A.1 and A.2 have to be in the same folder. Then execute for example `dotnet run -alice-change-mind true -n 10`. The first flag determines whether Alice will change her mind from committing to $b = 0$ to $b = 1$ and the second flag is the security parameter n, so how many qubits will be transferred from Alice to Bob.

The source code can also be found in `https://git.scc.kit.edu/urpyg/Ausarbeitung`.

```
namespace BB84Attack {
    open Microsoft.Quantum.Canon;
    open Microsoft.Quantum.Intrinsic;
    open Microsoft.Quantum.Measurement;
    open Microsoft.Quantum.Convert;
    open Microsoft.Quantum.Diagnostics;

    // Supervisor is a neutral party to work around Q# limitations, that only
    // allows qubits to be used within a block.
    // Starts Alice and Bob as functions,
    // aliceChangeMind controls whether Alice will change her mind after
    // commit.
    @EntryPoint()
    operation Supervisor(aliceChangeMind: Bool, n: Int) : Result {
        // failed indicates whether the protocol failed.
        mutable failed = false;
        // resB stores the result Bob determines the commitment to be
        mutable resB = One;
        // aliceUnveil controls which bit Alice will unveil
        mutable aliceUnveil = Zero;

        // This block acquires qubits to use for the commitment and attack,
        // envBits are qubits, kept in Alice's environment for the attack,
        // sendBits are qubits, that will be sent to Bob for the commitment.
        use (envBits, sendBits) = (Qubit[n],Qubit[n]) {
            Message("Commit Phase");
            // Alice's part of the commit procedure
            commitAlice(envBits, sendBits);
            Message($"Alices qubits={envBits}; Bobs={sendBits}");
            // Bob's part of the commit procedure.
            // Supervisor gives Bob the qubits that Alice "sends" him.
            // thetaHat, θ̂, are the bases Bob chose to measure the qubits in,
            // wHat, ŵ, is the measurement results of Bob.
            let (thetaHat, wHat) = commitBob(sendBits);
            Message("Holding Phase");
            holdAlice(aliceChangeMind, envBits);
            if (aliceChangeMind) {
                set aliceUnveil= One;
            }
            Message("Unveil phase");
            let w = unveilAlice(aliceUnveil, envBits);
            set (resB, failed) = unveilBob(thetaHat, wHat, w);
            // cleanup, not important for attack
            ResetAll(envBits);
            ResetAll(sendBits);
        }
```

```
47          if (failed){
48              Message("Commitment failed");
49          } else {
50              Message("Bob determined commitment to be");
51          }
52          return resB;
53      }
54
55      // commitAlice is the part of the commit procedure
56      // that is executed by dishonest Alice.
57      // She always commits to Zero and does not send anything to the
58      // environment.
59      // envBits are the qubits, that Alice will keep.
60      // bitsToSend are the qubits, that Alice will send to Bob
61      operation commitAlice(envBits: Qubit[], bitsToSend: Qubit[]) : Unit {
62          Message("Alices commit Procedure");
63          // Create random states, but do not send them to the environment,
64          // entangles those states with the bits to send.
65          for i in 0.. Length(envBits) -1{
66              H(envBits[i]);
67              CNOT(envBits[i],bitsToSend[i]);
68          }
69      }
70
71      // commitBob is the part of the commit procedure, executed by Bob.
72      // receivedBits are the qubits, Bob received from Alice.
73      operation commitBob(receivedBits: Qubit[]) : (Result[], Result[]) {
74          Message("Bobs commit procedure");
75          // bases stores the bases θ̂, Bob uses to measure the qubits in
76          mutable bases = new Result[0];
77          // wHat, ŵ, stores the measurement results
78          mutable wHat = new Result[0];
79          use rand = Qubit(){
80              // The random bases are generated by putting qubits into equal
81              // superposition and sending them to the environment
82              // (measuring them).
83              for i in 0.. Length(receivedBits) -1{
84                  H(rand);
85                  set bases += [MResetZ(rand)];
86              }
87          }
88          // Measures the qubits, Alice sent in the bases determined above.
89          Message("Bob measures his qubits");
90          for i in 0.. Length(receivedBits) -1{
91              set wHat += [measureRectOrDiag(bases[i], receivedBits[i])];
92          }
93          return (bases, wHat);
94      }
95
96      // holdAlice is where a cheating Alice would apply her cheating
97      // transformation to her qubits.
98      // However as it has been shown in BB84 this transformation is the
99      // identity, so nothing happens here.
100     operation holdAlice(changeMind: Bool, envBits: Qubit[]) : Unit {
101         Message("Alices hold procedure");
102         if (not changeMind) {
103             // Do nothing
104             return ();
105         }
106         // Apply Transformation
107     }
108
109     // unveilAlice is Alice's part of the unveil procedure,
110     // bitToUnveil determines which bit she will unveil to Bob.
```

```
111     operation unveilAlice(bitToUnveil: Result, envBits: Qubit[]) : Result[] {
112         Message("Alices unveil procedure");
113         Message("Alice unveiling One? "+ BoolAsString(ResultAsBool(
    bitToUnveil)));
114         // Only now, she measures her qubits
115         Message("Alice measures her qubits");
116         mutable w = new Result[0];
117         for i in 0.. Length(envBits) -1{
118             // The bit to unveil determines the basis she measures the qubits
119             // in
120             set w += [measureRectOrDiag(bitToUnveil, envBits[i])];
121         }
122         return w;
123     }
124 
125     // unveilBob  is Bob's part of the unveil procedure.
126     // thetaHat are the same Bases, Bob used in commitBob.
127     // wHat are his measurement results from commitBob,
128     // w is the bit-string sent by Alice to unveil the commitment.
129     // returns committed bit and whether the protocol failed.
130     operation unveilBob(thetaHat: Result[], wHat: Result[], w: Result[]) : (
    Result, Bool) {
131         Message("Bobs unveil procedure");
132         Message($"thetaHat={thetaHat}) , wHat={wHat}");
133         mutable mismatches = new Int[0];
134         for i in 0.. Length(wHat) -1{
135             if (wHat[i] != w[i]) {
136                 set mismatches += [i];
137             }
138         }
139         Message($"Mismatches={mismatches}");
140         if (Length(mismatches) == 0) {
141             // Cannot determine commitment, as all w and ŵ are equal
142             Message("All w and wHat equal");
143             return (Zero, true);
144         }
145         let thetaTilde = flipResult(thetaHat[mismatches[0]]);
146         for i in 0.. Length(mismatches) - 1{
147             if (thetaTilde == thetaHat[mismatches[i]]){
148                 // Alice must have cheated
149                 Message("Alice must have cheated");
150                 return (Zero, true);
151             }
152         }
153         return (thetaTilde, false);
154     }
155 
156     // measureRectOrDiag measures a qubit in rectilinear or diagonal basis.
157     // basis is  Zero for rectilinear, One for diagonal
158     // bitToMeasure qubit to measure,
159     // returns measurement result.
160     operation measureRectOrDiag(basis: Result, bitToMeasure: Qubit) : Result
    {
161         if (basis == Zero) {
162             //Used for rectilinear basis
163             let r = M(bitToMeasure);
164             Message($"Measured {bitToMeasure} in Rect, got " + ResultAsString
    (r));
165             return r;
166         } else {
167             let r =  Measure([PauliX], [bitToMeasure]);
168             Message($"Measured {bitToMeasure} in Diag, got " + ResultAsString
    (r));
169             return r;
```

```
170         }
171     }
172
173     // flipResult fips a measurement result, Zero to One and One to Zero.
174     operation flipResult(b: Result) : Result {
175         return BoolAsResult(not ResultAsBool(b));
176     }
177
178     operation ResultAsString(r: Result) : String {
179         if (ResultAsBool(r)){
180             return "One";
181         } else {
182             return "Zero";
183         }
184     }
185 }
```

Listing A.1: BB84Attack/Program.qs

```
1 <Project Sdk="Microsoft.Quantum.Sdk/0.15.2102129448">
2
3
4   <PropertyGroup>
5     <OutputType>Exe</OutputType>
6     <TargetFramework>netcoreapp3.1</TargetFramework>
7   </PropertyGroup>
8
9 </Project>
```

Listing A.2: BB84Attack/BB84Attack.csproj

Bibliography

Adcock, Mark and Richard Cleve (2002). "A Quantum Goldreich-Levin Theorem with Cryptographic Applications". In: *STACS 2002*. Ed. by Helmut Alt and Afonso Ferreira. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 323–334. ISBN: 978-3-540-45841-8. DOI: 10/d5zwq7.

Aharonov, Dorit et al. (May 1, 2000). "Quantum Bit Escrow". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. STOC '00. New York, NY, USA: Association for Computing Machinery, pp. 705–714. ISBN: 978-1-58113-184-0. DOI: 10/ctck7d. URL: https://doi.org/10.1145/335305.335404 (visited on 02/16/2021).

Bennett, Charles H. and Gilles Brassard (Dec. 1984). *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India, pp. 175–179.

— (Dec. 4, 2014). "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Theoretical Computer Science*. Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84 560, pp. 7–11. ISSN: 0304-3975. DOI: 10/3d6. arXiv: 2003.06557. URL: http://www.sciencedirect.com/science/article/pii/S0304397514004241 (visited on 12/11/2020).

Bennett, Charles H., Gilles Brassard, et al. (1992). "Practical Quantum Oblivious Transfer". In: *Advances in Cryptology — CRYPTO '91*. Ed. by Joan Feigenbaum. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 351–366. ISBN: 978-3-540-46766-3. DOI: 10/c9wr7f.

Blum, Manuel (Jan. 1, 1983). "Coin Flipping by Telephone a Protocol for Solving Impossible Problems". In: *ACM SIGACT News* 15.1, pp. 23–27. ISSN: 0163-5700. DOI: 10/b44nfn. URL: https://doi.org/10.1145/1008908.1008911 (visited on 03/10/2021).

Blumoff, J. Z. et al. (Sept. 14, 2016). "Implementing and Characterizing Precise Multiqubit Measurements". In: *Physical Review X* 6.3, p. 031041. DOI: 10/f83ztz. URL: https://link.aps.org/doi/10.1103/PhysRevX.6.031041 (visited on 01/04/2021).

Brandt, Howard E. (May 8, 2003). "Quantum Decoherence and Qubit Devices". In: *Noise and Information in Nanoelectronics, Sensors, and Standards*. Noise and Information in Nanoelectronics, Sensors, and Standards. Vol. 5115. International Society for Optics and Photonics, pp. 308–344. DOI: 10/crfdg8. URL: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5115/0000/Quantum-decoherence-and-qubit-devices/10.1117/12.488482.short (visited on 01/05/2021).

Brassard, Gilles, David Chaum, and Claude Crépeau (Oct. 1, 1988). "Minimum Disclosure Proofs of Knowledge". In: *Journal of Computer and System Sciences* 37.2, pp. 156–189. ISSN: 0022-0000. DOI: 10/bfj632. URL: https://www.sciencedirect.com/science/article/pii/0022000088900050 (visited on 03/05/2021).

Brassard, Gilles, Claude Crepeau, et al. (Nov. 1993). "A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties". In: *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, pp. 362–371. DOI: 10/dts6zf.

Brassard, Gilles, Claude Crépeau, et al. (June 9, 1998). *Defeating Classical Bit Commitments with a Quantum Computer*. arXiv: quant-ph/9806031. URL: http://arxiv.org/abs/quant-ph/9806031 (visited on 11/20/2020).

Buhrman, Harry et al. (Aug. 11, 2008). "Possibility, Impossibility and Cheat-Sensitivity of Quantum Bit String Commitment". In: *Physical Review A* 78.2, p. 022316. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.78.022316. arXiv: quant-ph/0504078. URL: http://arxiv.org/abs/quant-ph/0504078 (visited on 12/04/2020).

Chau, Hoi Fung and Hoi-Kwong Lo (Apr. 1, 1997). "One-Way Functions in Reversible Computations". In: *Cryptologia* 21.2, pp. 139–148. ISSN: 0161-1194. DOI: 10/cbjwmj. URL: https://www.tandfonline.com/doi/abs/10.1080/0161-119791885869 (visited on 12/13/2020).

Crépeau, Claude (Dec. 1, 1994). "Quantum Oblivious Transfer". In: *Journal of Modern Optics* 41.12, pp. 2445–2454. ISSN: 0950-0340. DOI: 10/bxbq7r. URL: https://doi.org/10.1080/09500349414552291 (visited on 01/09/2021).

Crépeau, Claude, Frédéric Légaré, and Louis Salvail (2001). "How to Convert the Flavor of a Quantum Bit Commitment". In: *Advances in Cryptology — EUROCRYPT 2001*. Ed. by Birgit Pfitzmann. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 60–77. ISBN: 978-3-540-44987-4. DOI: 10/fvfvd4.

Crépeau, Claude, Jeroen van de Graaf, and Alain Tapp (1995). "Committed Oblivious Transfer and Private Multi-Party Computation". In: *Advances in Cryptology — CRYPT0' 95*. Ed. by Don Coppersmith. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 110–123. ISBN: 978-3-540-44750-4. DOI: 10/bhmkc2.

D'Ariano, Giacomo Mauro et al. (Sept. 26, 2007). "Reexamination of Quantum Bit Commitment: The Possible and the Impossible". In: *Physical Review A* 76.3, p. 032328. DOI: 10/dj7tfv. URL: https://link.aps.org/doi/10.1103/PhysRevA.76.032328 (visited on 11/11/2020).

Damgard, I. B. et al. (Oct. 2005). "Cryptography in the Bounded Quantum-Storage Model". In: *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.* IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005. Pp. 24–27. DOI: 10/bwwz37.

Davie, A. M. and A. J. Stothers (Apr. 2013). "Improved Bound for Complexity of Matrix Multiplication". In: *Proceedings of the Royal Society of Edinburgh Section A: Mathematics* 143.2, pp. 351–369. ISSN: 0308-2105, 1473-7124. DOI: 10/ggcmbf. URL: https://www.cambridge.org/core/journals/proceedings-of-the-royal-society-of-edinburgh-section-a-mathematics/article/improved-bound-for-complexity-of-matrix-multiplication/998F772AF916572803EBA9C1AD7B4FC1 (visited on 12/02/2020).

Demmel, James, Ioana Dumitriu, and Olga Holtz (Nov. 1, 2007). "Fast Linear Algebra Is Stable". In: *Numerische Mathematik* 108.1, pp. 59–91. ISSN: 0945-3245. DOI: 10/c46kqt. URL: https://doi.org/10.1007/s00211-007-0114-x (visited on 12/02/2020).

Dumais, Paul, Dominic Mayers, and Louis Salvail (2000). "Perfectly Concealing Quantum Bit Commitment from Any Quantum One-Way Permutation". In: *Advances in Cryptology — EUROCRYPT 2000*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 300–315. ISBN: 978-3-540-45539-4. DOI: 10/fvbq7z.

Hardy, Lucien and Adrian Kent (Apr. 16, 2004). "Cheat Sensitive Quantum Bit Commitment". In: *Physical Review Letters* 92.15, p. 157901. DOI: 10/ccqfjd. URL: https://link.aps.org/doi/10.1103/PhysRevLett.92.157901 (visited on 12/06/2020).

Hornberger, K. (2009). "Introduction to Decoherence Theory". In: *Entanglement and Decoherence: Foundations and Modern Trends*. Ed. by Andreas Buchleitner, Carlos Viviescas, and Markus Tiersch. Lecture Notes in Physics. Berlin, Heidelberg: Springer, pp. 221–276. ISBN: 978-3-540-88169-8. DOI: 10.1007/978-3-540-88169-8_5. URL: https://doi.org/10.1007/978-3-540-88169-8_5 (visited on 01/11/2021).

Horodecki, Ryszard et al. (June 17, 2009). "Quantum Entanglement". In: *Reviews of Modern Physics* 81.2, pp. 865–942. DOI: 10/d2vqp8. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.865 (visited on 12/04/2020).

Hughston, Lane P., Richard Jozsa, and William K. Wootters (1993). "A Complete Classification of Quantum Ensembles Having a given Density Matrix". In: *Physics Letters A* 183.1, pp. 14–18. ISSN: 0375-9601. DOI: 10.1016/0375-9601(93)90880-9. URL: http://www.sciencedirect.com/science/article/pii/0375960193908809.

Ishizaka, S. (Mar. 13, 2007). *Is Cheat Sensitive Quantum Bit Commitment Really Possible?* CERN Document Server. URL: https://cds.cern.ch/record/1024125 (visited on 02/16/2021).

Ishizaka, Satoshi (Feb. 19, 2008). "Dilemma That Cannot Be Resolved by Biased Quantum Coin Flipping". In: *Physical Review Letters* 100.7, p. 070501. DOI: 10/d36zxf. URL: https://link.aps.org/doi/10.1103/PhysRevLett.100.070501 (visited on 02/16/2021).

Jain, R. (May 31, 2005). *On the Impossibility of Quantum String Commitment*. quant-ph/0506001. URL: https://cds.cern.ch/record/839053 (visited on 12/04/2020).

John D. Norton (July 18, 2020). *Einstein for Everyone*. URL: https://www.pitt.edu/~jdnorton/teaching/HPS_0410/chapters_July_18_2020/index.html (visited on 03/10/2021).

Jozsa, Richard (Dec. 1, 1994). "Fidelity for Mixed Quantum States". In: *Journal of Modern Optics* 41.12, pp. 2315–2323. ISSN: 0950-0340. DOI: 10/c7v8h3. URL: https://doi.org/10.1080/09500349414552171 (visited on 12/04/2020).

Kent, Adrian (Aug. 16, 1999). "Unconditionally Secure Bit Commitment". In: *Physical Review Letters* 83.7, pp. 1447–1450. ISSN: 0031-9007, 1079-7114. DOI: 10/bpp2jx. arXiv: quant-ph/9810068. URL: http://arxiv.org/abs/quant-ph/9810068 (visited on 11/27/2020).

— (Oct. 2012). "Quantum Tasks in Minkowski Space". In: *Classical and Quantum Gravity* 29.22, p. 224013. ISSN: 0264-9381. DOI: 10/gh6tn9. URL: https://doi.org/10.1088/0264-9381/29/22/224013 (visited on 03/03/2021).

Kilian, Joe (Jan. 1, 1988). "Founding Crytpography on Oblivious Transfer". In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. New York, NY, USA: Association for Computing Machinery, pp. 20–31. ISBN: 978-0-89791-264-8. DOI: 10/cr4hh9. URL: https://doi.org/10.1145/62212.62215 (visited on 03/10/2021).

Kjaergaard, Morten et al. (2020). "Superconducting Qubits: Current State of Play". In: *Annual Review of Condensed Matter Physics* 11.1, pp. 369–395. DOI: 10/ggwcbd. URL: https://doi.org/10.1146/annurev-conmatphys-031119-050605 (visited on 01/11/2021).

Konig, R., S. Wehner, and J. Wullschleger (Mar. 2012). "Unconditional Security From Noisy Quantum Storage". In: *IEEE Transactions on Information Theory* 58.3, pp. 1962–1984. ISSN: 1557-9654. DOI: 10/ghmhwt.

Koshiba, Takeshi and Takanori Odaira (2009). "Statistically-Hiding Quantum Bit Commitment from Approximable-Preimage-Size Quantum One-Way Function". In: *Theory of Quantum Computation, Communication, and Cryptography*. Ed. by Andrew Childs and Michele Mosca. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 33–46. ISBN: 978-3-642-10698-9. DOI: 10/b6wbtn.

Li, Qin et al. (July 2011). "On the Impossibility of Non-Static Quantum Bit Commitment between Two Parties". In: *Quantum Information Processing* 11.2, pp. 519–527. DOI: 10.1007/s11128-011-0259-5.

Lo, Hoi-Kwong and Hoi Fung Chau (Apr. 28, 1997). "Is Quantum Bit Commitment Really Possible?" In: *Physical Review Letters* 78.17, pp. 3410–3413. ISSN: 0031-9007, 1079-7114. DOI: 10/fhb8k8. arXiv: quant-ph/9603004. URL: https://link.aps.org/doi/10.1103/PhysRevLett.78.3410 (visited on 11/11/2020).

— (Sept. 1, 1998). "Why Quantum Bit Commitment and Ideal Quantum Coin Tossing Are Impossible". In: *Physica D: Nonlinear Phenomena*. Proceedings of the Fourth Workshop

on Physics and Consumption 120.1, pp. 177–187. ISSN: 0167-2789. DOI: 10/bvtcmw. URL: http://www.sciencedirect.com/science/article/pii/S0167278998000530 (visited on 11/11/2020).

Mayers, Dominic (Aug. 4, 1996). *The Trouble with Quantum Bit Commitment*. arXiv: quant-ph/9603015. URL: http://arxiv.org/abs/quant-ph/9603015 (visited on 11/10/2020).

— (Apr. 28, 1997). "Unconditionally Secure Quantum Bit Commitment Is Impossible". In: *Physical Review Letters* 78.17, pp. 3414–3417. DOI: 10.1103/PhysRevLett.78.3414. URL: https://link.aps.org/doi/10.1103/PhysRevLett.78.3414 (visited on 11/09/2020).

Naor, Moni (Jan. 1, 1991). "Bit Commitment Using Pseudorandomness". In: *Journal of Cryptology* 4.2, pp. 151–158. ISSN: 1432-1378. DOI: 10/bbpnj4. URL: https://doi.org/10.1007/BF00196774 (visited on 03/06/2021).

Nielsen, Michael A. and Isaac L. Chuang (Dec. 9, 2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press. 709 pp. ISBN: 978-1-139-49548-6.

Salvail, Louis (1998). "Quantum Bit Commitment from a Physical Assumption". In: *Advances in Cryptology — CRYPTO '98*. Ed. by Hugo Krawczyk. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 338–353. ISBN: 978-3-540-68462-6. DOI: 10/ck4wpd.

Scarani, Valerio et al. (Sept. 29, 2009). "The Security of Practical Quantum Key Distribution". In: *Reviews of Modern Physics* 81.3, pp. 1301–1350. DOI: 10/dshjwp. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.1301 (visited on 03/10/2021).

Schmidt, Erhard (Dec. 1, 1907). "Zur Theorie der linearen und nichtlinearen Integralgleichungen". In: *Mathematische Annalen* 63.4, pp. 433–476. ISSN: 1432-1807. DOI: 10/cv6g28. URL: https://doi.org/10.1007/BF01449770 (visited on 02/02/2021).

Shor, Peter W. (Nov. 1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. DOI: 10/czq562.

— (Jan. 1, 1999). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Review* 41.2, pp. 303–332. ISSN: 0036-1445. DOI: 10/dx85sg. URL: https://epubs.siam.org/doi/10.1137/S0036144598347011 (visited on 01/06/2021).

Shor, Peter W. and John Preskill (July 10, 2000). "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: *Physical Review Letters* 85.2, pp. 441–444. DOI: 10/fc7dvn. URL: https://link.aps.org/doi/10.1103/PhysRevLett.85.441 (visited on 03/10/2021).

Spekkens, R. W. and T. Rudolph (Dec. 11, 2001). "Degrees of Concealment and Bindingness in Quantum Bit Commitment Protocols". In: *Physical Review A* 65.1, p. 012310. DOI: 10/cwk7j7. URL: https://link.aps.org/doi/10.1103/PhysRevA.65.012310 (visited on 12/06/2020).

Svore, Krysta et al. (Feb. 24, 2018). "Q#: Enabling Scalable Quantum Computing and Development with a High-Level DSL". In: *Proceedings of the Real World Domain Specific Languages Workshop 2018*. RWDSL2018. New York, NY, USA: Association for Computing Machinery, pp. 1–10. ISBN: 978-1-4503-6355-6. DOI: 10/gdcc72. URL: https://doi.org/10.1145/3183895.3183901 (visited on 03/11/2021).

Unruh, Dominique (2016). "Collapse-Binding Quantum Commitments Without Random Oracles". In: *Advances in Cryptology – ASIACRYPT 2016*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, pp. 166–195. ISBN: 978-3-662-53890-6. DOI: 10/ghrm32.

Yao, Andrew Chi-Chih (May 29, 1995). "Security of Quantum Protocols against Coherent Measurements". In: *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*. STOC '95. New York, NY, USA: Association for Computing Machinery, pp. 67–75. ISBN: 978-0-89791-718-6. DOI: 10/cxc9xz. URL: https://doi.org/10.1145/225058.225085 (visited on 03/10/2021).

Yuen, Horace P. (May 17, 2005). *Unconditionally Secure Quantum Bit Commitment*. arXiv: quant-ph/0505132. URL: http://arxiv.org/abs/quant-ph/0505132 (visited on 11/11/2020).