Composable Security of Quantum Bit Commitment Protocol

Miloš Prokop

4th Year Project Report
Artificial Intelligence and Mathematics
School of Informatics
University of Edinburgh

2020

Abstract

Bit Commitment is a basic cryptographic primitive that has an important use in construction of more sophisticated cryptographic protocols. To allow for such constructions, composable security needs to be proven in order to guarantee that its security is preserved if it is arbitrarily composed with copies of itself or any other cryptographic protocols. By a recent impossibility result by V.Vilasini et al., composable bit commitment is impossible without any further assumption. This project presents a historical development of important possibility and impossibility theorems concerned with construction of bit commitment protocols up to this novel no-go theorem. It then analyzes the proof of the result and identifies necessary assumptions for evading it. We find that a trusted shared resource that does not take any input from any involved party and that acts before the protocol starts, is many times sufficient assumption to evade the no-go theorem. We define several general definitions describing properties of shared resources and argue about their necessity and sufficiency for evading the impossibility theorems and motivate further research by analyzing possibilities for their relaxations. On top of the determined results, a specific composable bit commitment protocol is proposed assuming a trusted third party and its composable information-theoretic security is proven even against quantum adversaries. The Casual Boxes Framework, which is an extension of Abstract Cryptographic Framework, is used for the proofs in this project as it extends its scope to relativistic settings.

Acknowledgements

Let me express my deep thank to my family who supported me throughout all my studies and without who all this work would not be possible.

I am especially grateful to my project supervisor Dr. Petros Wallden who introduced me to fascinating world of quantum computing and with his careful explanations shaped me in six months from a person with zero knowledge in quantum computing and cryptography to somebody starting to make some tiny contributions to the area. I particularly appreciate his useful comments and suggestions that pushed me every time I got stuck and which many times revealed connections of our findings to a considerably broader scope and provided me with much more complex understanding of our results.

... and I should not forget about:

- Karma Coffee, local Slovak micro roastery whose supplies have been converted to almost every page of this project with a desperate hope that quality could be still somehow preserved.
- My flatmates Matúš Macko and Samuel Kollár for trying to persuade me that beer brewing evenings are as important as spending them by evading impossibility results in cryptography. Thanks to their hard effort I have loads of interesting batches to try once I submit this report.
- Two sneaky guys Alice and Bob, the main characters of this crypto-drama.

Table of Contents

Chapter 1

Introduction

1.1 Motivation

The rise of quantum computing poses new challenges in standardizing cryptographic protocols as new classes of possible attacks become available by exploiting capabilities of quantum hardware. Security of modern classical cryptographic protocols often relies on computational guarantees which might no longer hold in quantum world, for instance, by making use of Shor's algorithm, the polynomial-time quantum algorithm for integer factorization. Moreover, many abilities of classical or quantum computers still remain greatly undiscovered and consequently even the protocols that rely on computational assumptions believed to be practically unbreakable may become vulnerable in the future. Therefore, there has been a trend in development of information-theoretic secure cryptographic protocols based on postulates of quantum mechanics and physical properties of the world. These protocols are unbreakable by arbitrarily powerful classical or quantum computers as long as the underlying physics is correct. Cryptography can be thought as of a resource theory that construct complex protocols from more basic primitive ones. One of them is bit commitment which allows construction of many protocols of a great importance, for example, coin flipping [2], zero-knowledge proofs of statements in NP complexity class [18, 15], contract signing [12] or multiparty computation [30]. However, such constructions require composability property. By novel result by V.Vilasini, C.Portmann and L.Del Rio [31], construction of secure composable bit commitment protocol is impossible unless extra assumptions are introduced. Concerning the wide range of applications of composable secure bit commitment, our aim is to tackle the problem by determination of such extra assumptions.

1.2 Aims

In this project we intend to give a brief historical overview on development of bit commitment protocols and on breakthrough impossibility results that have shaped the research directions. We believe that a brief understanding of the results is especially important for further development as it provides much better intuition about feasible implementations and is also essential to understand our motivation in proposing spe-

cific extra assumptions and particular bit commitment implementations. In addition, we aim to provide a specific example of such assumption and prove composable security of the corresponding protocol.

1.3 Contributions

The project fully satisfies the proposed aims. In particular,

- Chapters 2 - 5 provide a historical perspective on bit commitment protocol and discuss breakthrough possibility/impossibility results that had significant impact on research in the area.
- Chapter 7 proposes an Assymetric Quantum Beamer resource and a bit commitment protocol that makes use of it. It also proves its security and composability and argues how it avoids security impossibility result by Lo and Chau [21] and the composability impossibility result by Vilasini et al. [31].

Furthermore, we carried on with our research achieving results beyond the objectives.

- We expanded the Vilasini's et al. proof in Chapter 5 by presenting more detailed arguments with a particular focus on steps which do not necessary longer apply when new assumptions presented in Chapter 6 are introduced. Moreover, we state and prove Theorem 5.0.1 which is implicitly assumed by Vilasini's et al. impossibility proof, although the justification in their work is missing.
- In Chapter 6 we motivate an assumption of a trusted third party, define its properties useful for thorough analysis and derive a relation of its security parameters that needs to be satisfied in order to evade Vilasini's et al. impossibility result.
- We show an example of a practical application of our theorems developed in Chapter 6 in showing that our bit commitment protocol using Assymetric Quantum Beamer avoids Vilasini's et al. result.
- Based on facts and observations from all the chapters, we devote Chapter 8 to general discussion about sufficiency, necessity and practicality of various extra assumptions that are considered throughout the work and motivate further research.

In fact, part of Chapter 5 and all of Chapters 6 - 8 constitute entirely our contribution. In addition to finding a specific assumption allowing composable bit commitment, we pushed the research further by identifying some necessary assumptions and identifying where some assumptions can get relaxed and consequently allow a more practical real-world implementation of composable bit commitment protocol.

Chapter 2

Overview of Bit Commitment protocol

Bit commitment is a basic cryptographic primitive. It involves two parties, typically called Alice and Bob and consists of two phases, the *commitment phase* followed by the *reveal phase*. In the *commitment phase*, Alice chooses a bit $b \in \{0,1\}$ to which she commits. After the commitment, Bob has no information about the bit b. This property is called **concealing**. At the same time, it is desired that Alice is no longer able to change her decision about the bit b without Bob noticing it. We shall call this property **binding**. In the *reveal phase* initiated by Alice, Bob learns the bit b.

2.1 Applications of the protocol

Despite appearing to be very trivial and "boring", bit commitment has many important applications in construction of more sophisticated cryptographic protocols in post-quantum era. It allows construction of half-biased coin flipping by famous Blum's protocol [2] provided the parties have a power to abort the protocol. If we assume they lack such capability, an unbiased coin-flipping protocol can by constructed by the same technique instead. Blum's protocol will be of a particular use later in this project. Details of the construction are explained in proof of Theorem 5.0.3 in Chapter 5. It has also its use in constructing zero-knowledge proofs, where the aim of Alice is to prove to Bob that she knows some information without revealing the content of the information to Bob. As for a widely used example, Alice might want to prove to Bob that she knows the proof of Riemann hypothesis without revealing the proof to him. It is shown [18, 15] that bit commitment can provide zero-knowledge proofs of statements in NP complexity class. Another important application is multi-party computation [30] in which both parties want to extract relation between their informations that are kept secret from each other. For example, two companies might want to compare their income without revealing it to each other. The multi-party computation is in this case an abstract protocol that takes income information from both companies and outputs to both of them which one is greater without revealing the actual values of the incomes.

2.2 Security of classical Bit Commitment

Several ideas are being used to construct bit commitment protocols without use of quantum resources. They are usually based on collision-free hashing functions [14] or pseudo-random generators [25]. The former assumes computationally bounded sender and hardness of finding collisions in collision-free hash functions [22] and the latter assumes *cryptographically secure pseudorandom number generator* (CPSRNG). Assuming capabilities of current classical hardwares the schemes are still being considered secure.

2.2.1 Vulnerability to quantum adversaries

There exist quantum database search algorithms, such as *Grover's algorithm*, that offer an exponential speedup in searching over an unsorted database. Specifically, given a one-way function $f(\cdot)$ it might be practically feasible to search for x over countable domain $\mathcal{D}$ of f such that given y, $f(x) = y$. This suggests that computational hardness assumptions that are valid today are likely to be vulnerable against sufficiently powerful quantum hardware that is expected to become available in near future. For instance, in [7] an algorithm offering quantum time speedup for finding collisions in collision-free hash functions is proposed or [13] describes a polynomial-time quantum attacks on Blum–Micali or Blum-Blum-Shub pseudorandom generators that are proven to be secure against classical attacks. However, there exist classes of CPSRNG, whose security relies on lattice-based problems [1], that are conjectured to be hard to break even for quantum computers, although this still remains as an open problem. However, to the best of our knowledge, there exists no classical bit commitment protocol with assumptions that are proven to remain secure even against quantum adversaries.

2.3 Motivation of Composability Requirement

Bit commitment is a trivial functionality which is rarely interesting for practical applications when used just on its own. It is usually used as part of a more complex protocol. This implies need to retain its security when used in a combination with any other protocol or when an arbitrary number of copies of themselves are run in parallel or series. To illustrate the problem we consider a much simpler example discussed in [31]. Consider an adversary playing two online chess sessions with different colors against stronger players who simultaneously reproduces the opponents' moves to make them ultimately play against each other. This way the player either loses in one game and wins in the other one or ties in both of them. However, the widely-used Elo rating system awards the lower-ranked player with a high number of points whereas the penalization for the loss is comparably lower. Hence the adversary improves his score disregarding the outcome of the matches. This instance of a man-in-the middle attack is one of the ways the security under composition of protocols can fail. The possibility/impossibility results in our work follow from security definitions in *The Casual Boxes Framework* (Appendix B) where Casual Boxes that emulate protocols are allowed to be composed in series, in parallel and/or through feedback loops. Such composition results in another Casual Box which can be checked if it can be securely

constructed (according to Definition A.0.6) from given initial Casual Boxes,.e. from simpler protocols.

2.3.1 Canetti's and Fischlin's no-go theorem

In 2001, R.Canetti and M.Fischlin proved that no composable classical secure bit commitment protocol can exist [6] without any further assumption. In the same paper they also specified an assumption called *common reference string (crs)* which can be thought as of a third party that distributes the same random string to both Alice and Bob from some specific random distribution prior to running the protocol. However, it is complicated to argue that this scheme holds if we assume quantum capabilities of the involved parties as composability in this case relies on security of claw-free pairs of trapdoor permutations which is a computational assumption. There has been no proof existence of trapdoor claw-free permutations secure against quantum adversaries, however in [3] a scheme based on Learning with Errors (LWE) is proposed which is conjectured to be hard to break even for quantum devices. This motivates to determine a simpler assumption with quantum capabilities that could be introduced instead of *crs* in the post-quantum era.

Chapter 3

Impossibility of Quantum Bit Commitment in the plain model

We present the famous Lo & Chau [21] attack in a simplified way showing no secure bit commitment scheme is possible unless further assumptions are introduced. It shows that disregards the protocol implementation, Alice is able to apply a specific unitary in the opening phase to change her commitment. Hence no bit commitment protocol in plain model can be binding. This breakthrough result from 1996 has since been motivating researchers to come up with minimal possible assumptions that would evade it and the question still remains open today. We prove the result for the case when Bob has no information about the commited bit before the reveal phase. The case when Bob can guess the commited bit with some small non-zero probability, which is more realistic scenario in the real-world implementations, is discussed by D.Mayers in [24]. It follows the same idea presented here, but provides a solid argument considering fidelity of the two commitment states that correspond to commiting zero or one after we perform a partial trace over the system $\mathcal{A}$. Note, that even though the proof assumes quantum capabilities of Alice, it applies to classical setting as well since it is just a special case of the quantum ones. The proof starts by observation that any bit commitment in the plain model can be described by a quantum composite system $\mathcal{A} \otimes \mathcal{B}$, where $\mathcal{A}$ and $\mathcal{B}$ are Alice's and Bob's systems respectively, and follows the following procedure:

1. Commitment phase:

   (a) Alice, who wants to commit to a bit b, prepares
   if $b = 0$:
   $$|0\rangle = \sum_{i \in \alpha} c_i |\mu_i\rangle_{\mathcal{A}} \otimes |\phi_i\rangle_{\mathcal{B}}$$
   if $b = 1$:
   $$|1\rangle = \sum_{i \in \alpha} c'_i |\mu_i\rangle_{\mathcal{A}} \otimes |\phi'_i\rangle_{\mathcal{B}}$$
   for some scalars c_i, c'_i, orthonormal basis $\{|\mu_1\rangle, |\mu_2\rangle, ...\}$ and some states $\{|\phi_1\rangle, |\phi_2\rangle, ...\}$, $\{|\phi'_1\rangle, |\phi'_2\rangle, ...\}$ such that
   $$\mathrm{Tr}_A |0\rangle\langle 0| = \mathrm{Tr}_A |1\rangle\langle 1| \tag{3.1}$$

Equation 3.1 is required for concealing property against dishonest Bob who is not supposed to learn the value of the commitment before the reval phase.

(b) **Honest** Alice then measures first register in the $|\mu_i\rangle$ basis, remembers the measurement outcomes m. Note, that if her system is classical, there is a measurement which lefts it intact and hence this step is not explicitly present in all the existing protocols.

(c) Alice sends the second register, i.e. $|\phi_i\rangle$ (or $|\phi_i'\rangle$) to Bob as an evidence for her commitment.

2. Reveal phase:

(a) Alice sends the commitment bit b to Bob with the measurement outcome m from 1b) as an evidence

(b) Bob measures $|\phi_i\rangle$ (or $|\phi_i'\rangle$ and checks if the outcome is consistent with b and m

It is argued in [21] that any bit commitment protocol follows the above general procedure. We now proceed to show that Alice can change her commitment anytime between commit and reveal phase. In the rest of this chapter we summarize relevant ideas from Nielsen and Chuang book [26] and John Watrous's lecture notes [32] about application of Schmidt decomposition and purification in the impossibility proof.

Consider an ideal case, where Bob has no information about the committed bit b. Suppose Alice prepares two states as in 1a). Then $\mathrm{Tr}_A|0\rangle\langle 0| = \mathrm{Tr}_A|1\rangle\langle 1|$. Let $m := \dim(\mathcal{A})$ and $n := \dim(\mathcal{B})$. Then any pure state $|\psi\rangle \in \mathcal{A}\otimes\mathcal{B}$ can be rewritten as

$$|\psi\rangle = \sum_{1\le i\le m, 1\le j\le n} a_{ij}|i\rangle|j\rangle \tag{3.2}$$

for any choice of orthonormal bases $\{|i\rangle\}_i$ and $\{|j\rangle\}_j$ that correspond to $\mathcal{A}$ and $\mathcal{B}$ respectively and some corresponding $m\times n$ matrix $A \approx a_{ij}$ determined by the choice of bases. Suppose for simplicity that $m \ge n$. The case $n < m$ follows by the same reasoning. By singular value decomposition

$$A = UD'V$$

for some unitary $m\times m$ matrix U, unitary $n\times n$ matrix V and diagonal matrix D' of the form $D' := \begin{bmatrix} D \\ \mathbf{0} \end{bmatrix}$ where $\mathbf{0}$ is $n\times(m-n)$ zero matrix and D is diagonal $n\times n$ matrix. Write U in the form $U = [U_1\ U_2]$ where U_1 is $m\times n$ matrix. Then

$$A = U_1 DV$$

Then we can rewrite $|\psi\rangle$ as

$$|\psi\rangle = \sum_{1\le i\le m, 1\le j,k\le n} u_{ik}d_{kk}v_{kj}|i\rangle|j\rangle$$

where $U_1 = (u_{ik})_{1\le i\le m, 1\le k\le n}$, $D = (d_{kk})_{1\le k\le n}$, $V = (v_{kj})_{1\le j,k\le n}$. Defining $|k_A\rangle := \sum_i u_{ik}$, $|k_B\rangle := \sum_j v_{kj}$ and $\lambda_k := d_k k$ we get that

$$|\psi\rangle = \sum_k \lambda_k |k_A\rangle|k_B\rangle$$

Moreover,

$$\begin{aligned}\mathrm{Tr}_A|\psi\rangle\langle\psi| &= \mathrm{Tr}_A\left(\sum_{k,k'}\lambda_k\lambda_{k'}|k_A\rangle\langle k'_A|\otimes|k_B\rangle\langle k'_B|\right)\\ &= \sum_{k,k'}\lambda_k\lambda_{k'}|k_B\rangle\langle k'_B|\,\mathrm{Tr}(|k_A\rangle\langle k'_A|)\\ &= \sum_{k,k'}\lambda_k\lambda_{k'}|k_B\rangle\langle k'_B|\langle k'_A|k_A\rangle\\ &= \sum_k\lambda_k^2|k_B\rangle\langle k_B|\end{aligned}$$

The result is known as Schmidt decomposition. The reason we provide a proof rather than referencing it is to stress out a point that in Equation 3.2 we are allowed to choose arbitrary orthonormal basis $\{|j\rangle\}$ for Hilbert space of the system $\mathcal{B}$. This fact will be of a particular usefulness in Chapter 7. Once this has been done, observe that there is a unique orthonormal basis $\{|i\rangle\}$ given $|\psi\rangle$.

Let $\rho := \mathrm{Tr}_A|0\rangle\langle 0| = \mathrm{Tr}_A|1\rangle\langle 1|$. Then the density operator ρ has a spectral decomposition

$$\rho = \sum_i \lambda_i|\phi_i\rangle\langle\phi_i|$$

where $\{|\phi_k\rangle\}_k$ is some orthonormal basis of $\mathcal{B}$. Following the above procedure, Alice can find two distinct orthonormal bases $\{|\mu_i\rangle\}_i$ and $\{|\mu'_i\rangle\}_i$ such that

$$\begin{aligned}|0\rangle &= \sum_i \sqrt{\lambda_i}|\mu_i\rangle|\phi_i\rangle\\ |1\rangle &= \sum_i \sqrt{\lambda_i}|\mu'_i\rangle|\phi_i\rangle\end{aligned}$$

and $\rho = \sum_i \lambda_i|\phi_i\rangle\langle\phi_i|$. This technique is called a *purification*. Since there clearly exists a "change of basis" unitary operator U that maps $\{|\mu_i\rangle\}_i$ to $\{|\mu'_i\rangle\}_i$, Alice can always cheat in a way that she follows a bit commitment protocol as if she wanted to commit towards $b = 0$ with the difference that she skips the measurement step 1b) but sends an evidence of commitment as in 1c). If she decides to change her commitment before the reveal phase, she applies U on her register, essentially changing $|0\rangle \to |1\rangle$. She then proceeds to run the 1b) and follows the rest of the protocol for the reveal phase as normal.

Chapter 4

Possibility of non-composable Quantum Bit Commitment in relativistic model

Following the impossibility result presented in Chapter 3 much research has been done on finding possible weak assumptions that would allow bit commitment protocol with binding and concealing properties. One of interesting observations that has been done is that the physical world is relativistic, i.e. the events can be modeled in Minkowski space-time with limited signalling speed. This assumption has demonstrated to be of a significant importance as it allowed to construct several secure bit commitment schemes. The core ideas of implementation of these protocols have been proposed by Kent [16, 9, 17]. However, these protocols involve some implementation difficulties that include limited maximal secure commitment time and requirement of trusted Alice's and Bob's agents to be light-like separated from Alice's location at the beginning of her commitment phase. There have been a few improvements of the Kent's protocol that relax, but not completely avoid these limitations, for example [20, 8]. In this chapter we present the Kent's protocol [17] that inspired the development in the area and discuss how it evades the Lo and Chau no-go theorem.

4.1 Minkowski space-time

Following the Kent's works, we assume a Minkowski space-time description of the world. It is a four dimensional manifold $\mathcal{M}$ resulting from a combination of Euclidean three-dimensional space and time. Given two points $P,Q \in \mathcal{M}$ we write $P \prec Q$ if Q is reachable by light from P. We will use notion of **future light-cone** of a point P which is informally a set of points in Minkowski space-time reachable by light from P, i.e.

$$\text{future light-cone}_P = \{Q \in \mathcal{M} | P \prec Q\}$$

Given two locations l_1 and l_2 we say that l_1 and l_2 are **light-like** separated from P if $P \prec l_1, P \prec l_2$ and there is no point $Q \in \mathcal{M}, P \prec Q, Q \neq P$ such that $Q \prec l_1$ and $Q \prec l_2$.

4.2 Unconditional Secure Bit Commitment by Transmitting Measurement outcomes

We give an intuition about the famous Kent's protocol [17]. Alice and Bob agree on a space-time location P. The protocol begins by Bob sending a sequence of independently randomly chosen BB84 states $\{|0\rangle, |1\rangle, |-\rangle, |+\rangle\}$ at $P' \prec P$ to Alice at P. Assuming Alice wants to commit to a bit b, she either measures the quantum states in $\{|0\rangle, |1\rangle\}$ basis if $b = 0$ or measures them in $\{|-\rangle, |+\rangle\}$ basis if $b = 1$. She then sends the measurement outcomes and b to her light-like separated agents located at Q_0 and Q_1. In the reveal phase, Alice's agents at Q_0 and Q_1 reveal the measurement outcomes and the bit b to Bob's agents located at Q'_0 and Q'_1 as illustrated in Figure 4.1. For the simplicity of argument, suppose that the distance between Q_0 and Q'_0 (and for Q_1 and Q'_1) is negligible. The Bob's agents later meet in the intersection of their light cones to check if they both received the same unveilings and if they correspond to the states prepared at P'. If so, they accept the commitment and reject otherwise.

The protocol is obviously secure against dishonest Bob who learns nothing about Alice's commitment until her agents unveil the commitment at Q'_0 and Q'_1. To see that it is secure against dishonest Alice, observe that since Q_0 and Q_1 are light-like separated, Alice has no chance of consistently changing her commitment for both space-time locations Q_0 and Q_1. Hence Bob would discover cheating behaviour of Alice by observing inconsistent outcomes received at Q'_0 and Q'_1 up to some small probability ε that could be forced to be arbitrarily small by sending a sufficiently long sequence of BB84 states at P'. See [9] for formal proof of the security.

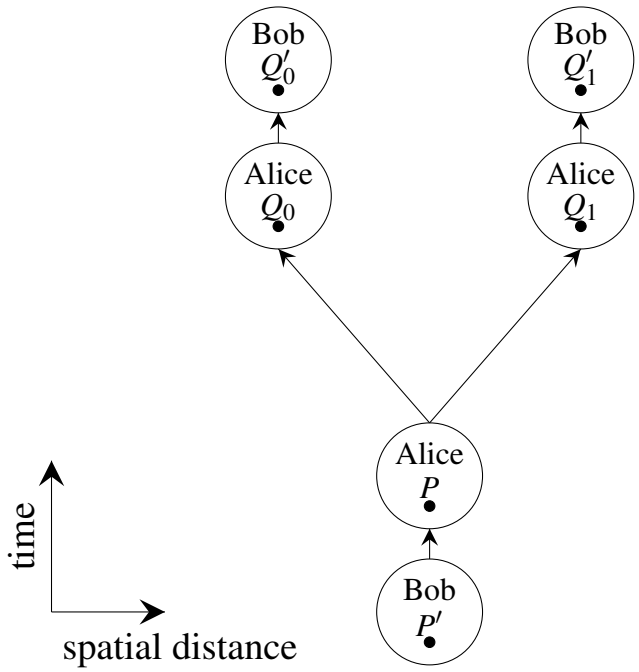


Figure 4.1: Kent's relativistic bit commitment by transmitting measurement outcomes

Chapter 5

Impossibility of Composable Quantum Bit Commitment

The class of bit commitment protocols discussed in Chapter 4 not only possess practical implementation issues, e.g. limited commitment time or light-like separation of agents, but has been shown by recent result by Vilasini [31] to be non-composable unless further assumptions are introduced. In this chapter we expand the Vilasini's proof by providing more detailed justifications with focus on the step we discovered that can be evaded.

The following chapters assume familiarity with Casual Boxes framework (Appendix B) which is an extension of Abstract Cryptography framework (Appendix A). We proceed to provide informal introduction the concepts, but for the solid understanding it is essential that reader gets familiar with the concepts in Appendices. The Casual Boxes framework views protocols as a constructive resource theory in a sense that by combination of protocols (resources) we can construct new ones and gives a method for evaluation of security of such constructions not only when both parties are honest, but considers also dishonest Bob and dishonest Alice cases. The dishonest Alice and dishonest Bob case is omitted from proofs as it is impossible to argue about such cases since Alice and Bob can take whatever actions possible and it does not intuitively make sense to consider security of protocols where both parties are trying to behave dishonestly. The security of the construction is defined as a probabibility of distinguishing between the constructed resource and the ideal "black box" resource maximized over all the three cases. The security measure is called a *distinguishing advantage* and is maximized over all possible *distinguishers* interacting with the resources. We denote $R \approx_\varepsilon S$ if the optimal distinguisher for R, S has distinguishing advantage less than ε. In the below proofs we shall consider two resources, a half-biased coin flipping $CF^{\frac{1}{2}}$ and a bit commitment resource BC. BC is defined similarly as in Chapter 2 and $CF^{\frac{1}{2}}$ is a resource that outputs to both parties the same random bits. However, if either party is dishonest, it has a probability $\frac{1}{2}$ to change the coin-flip outcome. See Appendices B.1, B.2 for detailed specifications of the functionalities.

The proof of impossibility to construct a composable bit commitment protocol follows as a contrapositive statement to a possibility to construct $CF^{\frac{1}{2}}$ within a distance 0 (see

Definition A.0.6) from a *BC* protocol [2, 10] given a proof that secure construction of $CF^{\frac{1}{2}}$ is impossible (Theorem 5.0.2). In order to provide a rigid proof of the result we shall be in need of the following theorem:

Theorem 5.0.1. *Let $\mathbb{S}$ be a set of available resources. Then $\forall R, S, \alpha \in \mathbb{S}$ the following two statements hold:*

$$R \approx_\varepsilon S \Rightarrow \alpha R \approx_\varepsilon \alpha S$$
$$R \approx_\varepsilon S \Rightarrow R\alpha \approx_\varepsilon S\alpha$$

Proof. Suppose $R \approx_\varepsilon S$, let $\alpha \in \mathbb{S}$ and let $\mathcal{D} \in \mathbb{D}$ be the set of all considered distinguishers. Then $\mathcal{D}\alpha \in \mathbb{D}$ and hence

$$\begin{aligned} d^{\mathbb{D}}(\alpha R, \alpha S) &= \sup_{\mathcal{D}\in\mathbb{D}} |P(\mathcal{D}(\alpha R) = 0) - P(\mathcal{D}(\alpha S) = 0)| \\ &= \sup_{\mathcal{D}\in\mathbb{D}} |P(\mathcal{D}\alpha(R) = 0) - P(\mathcal{D}\alpha(S) = 0)| \\ &= d^{\mathcal{D}\alpha}(R, S) \\ &\leq \sup_{\mathcal{D}\in\mathbb{D}} d^{\mathcal{D}}(R, S) \\ &\leq \varepsilon \end{aligned}$$

The similar reasoning shows $d^{\mathbb{D}}(R\alpha, S\alpha) \leq \varepsilon$. □

The proof of the impossibility result follows in the rest of this chapter. See Definition A.0.6 in Appendix A for explanation of graphical illustrations used in the proofs.

Theorem 5.0.2. *It is impossible to construct with $\varepsilon < \frac{1}{12}$ a $CF^{\frac{1}{2}}$ protocol in all classical, quantum, relativistic and non-relativistic settings without any further assumptions.*

Proof. (Extended from [31] with focus on important details) Suppose it is possible to construct a $CF^{\frac{1}{2}}$ protocol within a distance ε. Let $\mathbb{D}$ be a set of all possible distinguishers including quantum, relativistic and non-relativistic ones, $\mathbb{S}$ be a set of all relevant simulators and suppose $\Pi = (\Pi_A, \Pi_B)$ is a protocol followed by the two parties. Then by Definition A.0.6, all the conditions below must be true:

$$d^{\mathbb{D}}(\Pi_A\Pi_B, CF^{\frac{1}{2}}) \leq \varepsilon \tag{5.1}$$
$$\exists \sigma_A \in \mathbb{S} : d^{\mathbb{D}}(\Pi_B, \sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon \tag{5.2}$$
$$\exists \sigma_B \in \mathbb{S} : d^{\mathbb{D}}(\Pi_A, CF_B^{\frac{1}{2}}\sigma_B) \leq \varepsilon \tag{5.3}$$

By triangle inequality and Theorem 5.0.1 the equations can be combined in the following way

$$d^{\mathbb{D}}(\Pi_A\Pi_B, \Pi_A\sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon \qquad (\star : 5.2 + \text{Thm } 5.0.1)$$
$$d^{\mathbb{D}}(\Pi_A\sigma_A CF_A^{\frac{1}{2}}, CF_B^{\frac{1}{2}}\sigma_B\sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon \qquad (\blacklozenge : 5.3 + \text{Thm } 5.0.1)$$
$$d^{\mathbb{D}}(\Pi_A\sigma_A CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \leq 2\varepsilon \qquad (\lozenge : \star + 5.1)$$
$$d^{\mathbb{D}}(CF_B^{\frac{1}{2}}\sigma_B\sigma_A CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \leq 3\varepsilon \qquad (5.4: \blacklozenge + \lozenge)$$

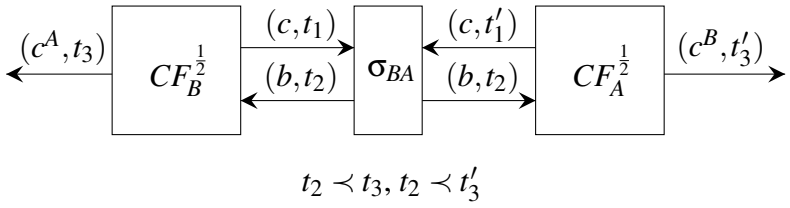


Figure 5.1: Biased Coin Flipping Casual Box for dishonest Alice and honest Bob.

Collapsing $\sigma_B\sigma_A$ into a single simulator σ_{BA} and realizing that a distinguisher, which guesses a constructed non-ideal resource every time $c_0^A \neq c_0^B$ has at least $P(c_0^A \neq c_0^B)$ probability of making a right guess, we have that

$$3\varepsilon \geq d^{\mathbb{D}}(CF_B^{\frac{1}{2}}\sigma_{BA}CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \geq P(c_0^A \neq c_0^B) \tag{5.5}$$

where

$$\begin{aligned}
P(c_0^A \neq c_0^B) &= 1 - P(c_0^A = c_0^B) \\
&= 1 - P(c_0^A = c_0^B | c = c')P(c = c') - P(c_0^A = c_0^B | c \neq c')P(c \neq c') \\
&= 1 - 1 \times \frac{1}{2} - \frac{1}{2}(P(c_0^A = c_0^B | c \neq c)) \\
&= \frac{1}{2} - \frac{1}{2}(P(c_0^A = c_0^B | c \neq c', \text{both biased})P(\text{both biased}) \\
&\qquad P(c_0^A = c_0^B, \text{A biased})P(\text{A biased}) \\
&\qquad P(c_0^A = c_0^B, \text{B biased})P(\text{B biased}) \\
&\qquad P(c_0^A = c_0^B, \text{none biased})P(\text{none biased})) \\
&= \frac{1}{2} - \frac{1}{2}\left[1 \times \left(\frac{1}{2}\right)^2 - 0 \times \left(\frac{1}{2}\right)^2 - 1 \times \left(\frac{1}{2}\right)^2 - 0 \times \left(\frac{1}{2}\right)^2\right] \\
&= \frac{1}{4}
\end{aligned}$$

Substituting back into Equation 5.5 we find a lower bound $\varepsilon \geq \frac{1}{12}$. □

Theorem 5.0.3. *It is impossible to construct a composable bit commitment protocol in any of classical, quantum and relativistic settings without any further assumptions.*

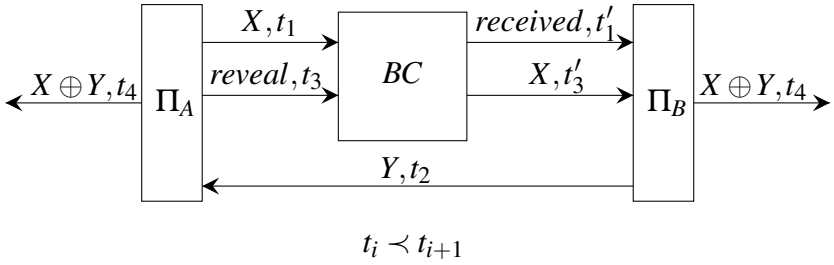


Figure 5.2: Blum's protocol

Proof. Let $\Pi = (\Pi_A, \Pi_B)$ be a protocol where Alice starts by generating a random bit X and committing to it towards Bob. She then postpones the reveal phase until she receives a random bit Y from Bob. Both parties now consider the random variable $X \oplus Y$ as the coin flip outcome. If any party aborts protocol, the other one uniformly generates a random output bit. It is proved in [10] that the protocol (depicted in Figure 5.2) perfectly constructs $CF^{\frac{1}{2}}$ in the Casual Box framework which assumes a general class of distinguishers including quantum and relativistic ones. Hence the result directly follows as a contrapositive since by Theorem 5.0.2 the secure construction of $CF^{\frac{1}{2}}$ is not possible. See Figure 5.2 for a graphical depiction of this construction. □

Chapter 6

Evading proof of Composability No-Go Theorem

The use of initial shared resource is suggested in [31] although not justified. It can be modeled as a Casual Box (see Figure 6.1). In this chapter we show that given the

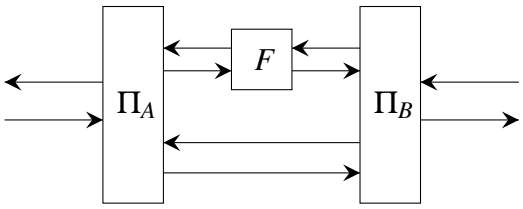


Figure 6.1: Connecting a shared resource F in Casual Box Framework to Alice and Bob. The resulting resource in the figure is denoted by $\Pi_A F \Pi_B$.

assumption of a shared resource, the Inequality 5.5 in Chapter 5 is no longer necessarily true and we can evade the lower bound on ε imposed by Vilasini's et al. proof. This is, however, not the case for any considered shared resource and hence we begin the chapter by assuming some general properties of it that turn out to be useful in the later proofs. A specific example of such shared resource is then presented in Chapter 6 and discussion about necessity of the assumptions for shared resources can be found in Chapter 8.

6.1 General properties of shared resources

Definition 6.1.1. A **setup stage** t_0 is a space-time region in which neither Alice nor Bob executes any action other than storing messages in their memory that appear on their input interfaces.

Definition 6.1.2. We call a shared resource F

- *Non-interactive* if F lacks input interface. Such resource cannot take any input from any party involved in the protocol. F is *interactive* if its actions can be conditioned on some input.

- *Symmetric* if its interfaces commute in the sense that $d^{\mathbb{D}}(\Pi_A F \Pi_B, \Pi_B F \Pi_A) = 0$ for any $\Pi = (\Pi_A, \Pi_B)$. A shared resource whose interfaces do not commute is called *asymmetric*.
- *Inactive* if F never produces a message on its output interface at time t_i where $t_i \succ t_0$.
- *Active* if $d^{\mathbb{D}}(\Pi_A F \Pi_B, \Pi_B \phi F \phi \Pi_A) > 0$ where ϕ is a "filter" resource acting as identity in the setup stage t_0 and acting as a blank resource outside t_0.
- $(\varepsilon, \lambda, \rho)$-*effective with respect to protocol* $\Pi = (\Pi_A, \Pi_B)$ *and resource* R if F uniformly samples with probability ρ its output from its image

$$\begin{aligned} \mathrm{img}(F) = \{(\alpha_F, \beta_F) | \forall \alpha_F : &\exists! \beta_F \text{ s.t. } (\alpha_F, \beta_F) \in \mathrm{img}(F) \\ &\wedge \\ \forall \beta_F : &\exists! \alpha_F \text{ s.t. } (\alpha_F, \beta_F) \in \mathrm{img}(F)\} \end{aligned}$$

  i.e. $\rho = \frac{1}{|\mathrm{img}(F)|}$ if $\mathrm{img}(G)$ is finite($p = 0$ otherwise), and the following two inequalities hold

$$d^{\mathbb{D}}(\Pi_A F \Pi_B, R) \leq \varepsilon \tag{6.1}$$

$$\inf_{\eta \in \Delta} d^{\mathbb{D}}(\Pi_A \eta \Pi_B, R) = \lambda \tag{6.2}$$

  where Δ is a set of shared resources whose image is complement to image of F in a set of all possible images of a shared resource. Let α_Γ be a message(or set of messages) produced on the left interface of a shared resource Γ in t_0 and similarly β_Γ be a message(or set of messages) produced on the right interface in t_0. We will use notation

$$\begin{aligned} \alpha_\Gamma \parallel_F \beta_\Gamma &\iff (\alpha_\Gamma, \beta_\Gamma) \in \mathrm{img}(F) \\ \alpha_\Gamma \nparallel_F \beta_\Gamma &\iff (\alpha_\Gamma, \beta_\Gamma) \notin \mathrm{img}(F) \end{aligned}$$

  If the corresponding protocol $\Pi = (\Pi_A, \Pi_B)$ or the corresponding resource R is obvious from the context, it does not need to be explicitly mentioned.

6.2 Evading the composability no-go theorem

The result of this section determines a relation of security parameters of a trusted shared resource that needs to hold in order to achieve secure construction of composable bit commitment. We state the main result and then proceed to prove various useful lemmas before restating it and providing a proof.

Theorem 6.2.1. *Let* $\varepsilon > 0$ *and* $\Pi = (\Pi_A, \Pi_B)$ *a protocol followed by Alice and Bob. Suppose further that both parties share a non-interactive and* $(\lambda, \varepsilon, \rho)$-*effective resource* F *such that protocol* Π ε-*constructs bit commitment resource BC. I.e.,*

$$\begin{aligned} d^{\mathbb{D}}(\Pi_A F \Pi_B, BC) &\leq \varepsilon \\ \exists \sigma_A \in \mathbb{S} : d^{\mathbb{D}}(F \Pi_B, \sigma_A BC) &\leq \varepsilon \\ \exists \sigma_B \in \mathbb{S} : d^{\mathbb{D}}(\Pi_A F, BC \sigma_B) &\leq \varepsilon \end{aligned}$$

Then if

$$\frac{1}{4} \leq \lambda(1-\rho)$$

then $\Pi_A F \Pi_B$ ε*-constructs bit commitment resource BC which evades Vilasini's et al. impossibility Theorem 5.0.3.*

Proof. Proof to be found at the end of the chapter. □

This result is very surprising for us as it shows that very weak assumptions are sufficient to evade Vilasini's et al. impossibility Theorem 5.0.3. Informally, if one constructs a secure bit commitment protocol that assumes a non-interactive trusted third party F with uniformly distributed output, then it is almost guaranteed that the constructed bit commitment protocol evades the composability no-go theorem. Indeed, any reasonable shared party has image of size greater than 2 since otherwise it is useless as it can me omitted from the protocol without influencing its functionality. Hence $\rho \leq \frac{1}{2}$. Similarly, if a shared resource η with image that does not intersect image of F is used instead of F then there should be a distinguisher that has at least $\frac{1}{2}$ probability of spotting this substitution unless the constructed resource F plays no important role in the protocol. Hence $\lambda \geq \frac{1}{2}$ and by Theorem 6.2.1 it evades the famous Vilasini's impossibility Theorem 5.0.3.

6.2.1 Proof of sufficiency result in evading no-go composability theorem

Suppose there is a resource F used as a trusted third party by a protocol $\Pi = (\Pi_A, \Pi_B)$ and that there is a construction of $CF^{\frac{1}{2}}$ within some distance ε that can be made arbitrarily small by adjusting security parameters, similarly as in the proof of Theorem 5.0.2. Then

$$d^{\mathbb{D}}(\Pi_A F \Pi_B, CF^{\frac{1}{2}}) \leq \varepsilon \tag{6.3}$$

$$\exists \sigma_A \in \mathbb{S} : d^{\mathbb{D}}(F\Pi_B, \sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon \tag{6.4}$$

$$\exists \sigma_B \in \mathbb{S} : d^{\mathbb{D}}(\Pi_A F, CF_B^{\frac{1}{2}} \sigma_B) \leq \varepsilon \tag{6.5}$$

By triangle inequality and Theorem 5.0.1 the equations can be combined in the following way

$$d^{\mathbb{D}}(\Pi_A F \Pi_B, \Pi_A \sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon \qquad (\star : 6.4 + \text{Thm } 5.0.1)$$

$$d^{\mathbb{D}}(\Pi_A F \sigma_A CF_A^{\frac{1}{2}}, CF_B^{\frac{1}{2}} \sigma_B \sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon \qquad (\blacklozenge : 6.5 + \text{Thm } 5.0.1)$$

$$d^{\mathbb{D}}(\Pi_A \sigma_A CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \leq 2\varepsilon \qquad (\lozenge : \star + 6.3)$$

By triangle inequality

$$\begin{aligned} d^{\mathbb{D}}(CF_B^{\frac{1}{2}}\sigma_{BA}CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \leq & d^{\mathbb{D}}(\Pi_A\sigma_A CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \\ & + \\ & d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, \Pi_A\sigma_A CF_A^{\frac{1}{2}}) \\ & + \\ & d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, CF_B^{\frac{1}{2}}\sigma_B\sigma_A CF_A^{\frac{1}{2}}) \\ & = 3\varepsilon + d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, \Pi_A\sigma_A CF_A^{\frac{1}{2}}) \\ & = 3\varepsilon + \kappa \end{aligned} \tag{6.6}$$

where $\kappa := d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, \Pi_A\sigma_A CF_A^{\frac{1}{2}}))$. In the proof of the impossibility Theorem 5.0.2, F can be considered to be the identity resource (forwarding the messages both ways). Hence $\kappa = 0$, determining a lower bound for ε by Equation 5.5. If F is not an identity resource, we are no longer guaranteed that $\kappa = 0$. In the rest of this chapter we will explore what are sufficient assumptions for F such that for any $\varepsilon > 0$ Inequality 6.6 is satisfied. We assume that F is non-interactive and $(\lambda, \varepsilon, \rho)$-effective with respect to some protocol $\Pi = (\Pi_A, \Pi_B)$ and protocol $CF^{\frac{1}{2}}$ for some $\lambda, \varepsilon, \rho$. Chapter 8 is dedicated to discussion about necessary assumptions of F to satisfy the Inequality 6.6 and it will indeed argue that non-interactivity is an essential property to assume. We start by proving lemmas that will find their use in proof of Theorem 5.0.3.

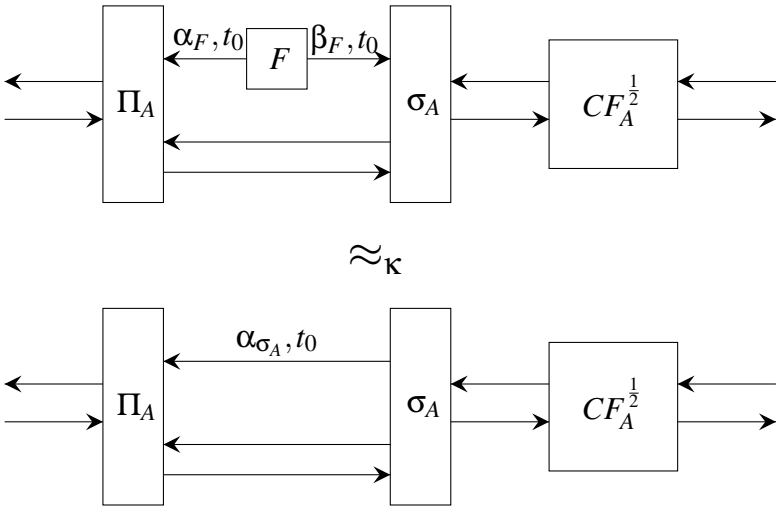


Figure 6.2: Definition of κ depicted in Casual Box Framework

Lemma 6.2.2. *Suppose F is non-interactive and $(\lambda, \varepsilon, \rho)$-effective shared resource and that FF is a shared resource constructed by connecting two identical copies of F in series. Let α_{FF} be output of FF on its left interface and β_{FF} on its right interface. Then*

$$P(\alpha_{FF} \|_F \beta_{FF}) = \rho$$

, i.e. probability that $(\alpha_{FF}, \beta_{FF}) \in img(F)$ is ρ.

Proof. By definition of image of F there exists a unique $\tilde{\beta}_F$ such that $\alpha_{FF} \parallel_F \tilde{\beta}_F$. Since F is non-interactive, the right output β_{FF} is independent of its left output α_{FF}. Hence

$$P(\alpha_{FF} \parallel_F \beta_{FF}) = P(\beta_{FF} = \tilde{\beta}_F | \alpha_{FF}) = P(\beta_{FF} = \tilde{\beta}_F) = \rho$$

□

There is likely a confusion that reader can experience in proof of the next lemma. Note that $\mathcal{CF}^{\frac{1}{2}} = (CF^{\frac{1}{2}}, CF_A^{\frac{1}{2}}, CF_B^{\frac{1}{2}})$ is a triple of half-biased coin flipping protocols for three cases: when both parties are honest, when Alice is dishonest and when Bob is dishonest respectively. Hence when refering to $CF^{\frac{1}{2}}$ we assume the coin flip protocol that does not allow any party to change the coin outcome. Such assumption is reasonable but odd since the ability to cheat would never be used by honest parties. We are aware that this is confusing, but there is no other way to model half-biased coin flipping as a Casual Box since the dishonest party needs to receive the coin flip outcome before the other party in order to be able to bias it and therefore this Casual Box cannot provide both parties with power to bias the outcome. However, this problem is obviously not present in the real world implementation of the half-biased coin flipping as a dishonest behaviour is defined as any action that does not follow the protocol $\Pi = (\Pi_A, \Pi_B)$. This approach has been followed in Vilasini's et al. impossibility proof [31] as well and took us a considerable time to understand it and approve the approach. Hence we suggest for a reader that reads this chapter for the first time just to accept the fact that output$(CF^{\frac{1}{2}}) \in \{(0,0),(1,1)\}$, which means that both involved parties will always receive the same bits from $CF^{\frac{1}{2}}$, and to proceed on.

Lemma 6.2.3. *Suppose FF is the shared resource as in Lemma 6.2.2 used by protocol $\Pi = (\Pi_A, \Pi_B)$ that ε-constructs $\mathcal{CF}^{\frac{1}{2}} = (CF^{\frac{1}{2}}, CF_A^{\frac{1}{2}}, CF_B^{\frac{1}{2}})$ and that FF outputs α_{FF} on its left interface and β_{FF} on its right interface. Then the probability that either Alice or Bob successfully change the coin flip outcome given that output of FF is in image of F is upper bounded by ε. I.e.,*

$$P(\Pi_A FF \Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \parallel_F \beta_{FF}) \leq \varepsilon$$

Proof. Suppose $\alpha_{FF} \parallel_F \beta_{FF}$. FF is identical to F because $(\alpha_{FF}, \beta_{FF}) \in \text{img}(F)$. Define a distinguisher $\mathcal{D} \in \mathbb{D}$ as

$$\mathcal{D}(\mathcal{R}) = \begin{cases} \Pi_A F \Pi_B & \text{if output}(\mathcal{R}) \in \{(0,1),(1,0)\} \\ CF^{\frac{1}{2}} & \text{if output}(\mathcal{R}) \in \{(0,0),(1,1)\} \end{cases}$$

By Inequality 6.1 and since output$(CF^{\frac{1}{2}}) \in \{(0,0),(1,1)\}$,

$$\begin{aligned} \varepsilon \geq d^{\mathbb{D}}(\Pi_A F \Pi_B, CF^{\frac{1}{2}}) &\geq d^{\mathcal{D}}(\Pi_A F \Pi_B, CF^{\frac{1}{2}}) \\ &= |P(\mathcal{D}(\Pi_A F \Pi_B) = \Pi_A F \Pi_B) - P(\mathcal{D}(CF^{\frac{1}{2}}) = \Pi_A F \Pi_B)| \\ &= |P(\mathcal{D}(\Pi_A F \Pi_B) = \Pi_A F \Pi_B) - 0| \\ &= P(\Pi_A F \Pi_B \in \{(0,1),(1,0)\}) \\ &= P(\Pi_A FF \Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \parallel_F \beta_{FF}) \end{aligned}$$

□

Lemma 6.2.4. *Let F be $(\varepsilon,\lambda,\rho)$-effective. Then*

$$d^{\mathbb{D}}(\Pi_A F F \Pi_B, CF^{\frac{1}{2}}) = P(\Pi_A F F \Pi_B \in \{(0,1),(1,0)\})$$

and moreover, $D \in \mathbb{D}$ defined as

$$D(R) = \begin{cases} \Pi_A F F \Pi_B & \text{if output}(\mathcal{R}) \in \{(0,1),(1,0)\} \\ CF^{\frac{1}{2}} & \text{if output}(\mathcal{R}) \in \{(0,0),(1,1)\} \end{cases}$$

is a maximal distinguisher in a sense that

$$d^{\mathcal{D}}(\Pi_A F F \Pi_B, CF^{\frac{1}{2}}) = d^{\mathbb{D}}(\Pi_A F F \Pi_B, CF^{\frac{1}{2}})$$

Proof. Let $\mathcal{D} \in \mathbb{D}$ be a maximal distinguisher of $\Pi_A F F \Pi_B$ and $CF^{\frac{1}{2}}$. Since output$(CF^{\frac{1}{2}}) \in \{(0,0),(1,1)\}$, $\mathcal{D}(R) = \Pi_A F F \Pi_B$ whenever output$(R) \in \{(0,1),(1,0)\}$. Hence $\mathcal{D}$ is of the form

$$\mathcal{D}(\mathcal{R}) = \begin{cases} \Pi_A F F \Pi_B & \text{if output(R)} \in \{(0,1),(,10)\} \\ \begin{cases} \Pi_A F F \Pi_B \text{ with probability } p \\ CF^{\frac{1}{2}} \text{ with probability } 1-p \end{cases} & \text{if output(R)} \in \{(0,0),(1,1)\} \end{cases}$$

for some probability p. Then

$$d^{\mathbb{D}}(\Pi_A F F \Pi_B, CF^{\frac{1}{2}}) = |P(\mathcal{D}(\Pi_A F F \Pi_B) = \Pi_A F F \Pi_B) - P(\mathcal{D}(CF^{\frac{1}{2}}) = \Pi_A F F \Pi_B)| \tag{6.7}$$

where

$$\begin{aligned} P(\mathcal{D}(\Pi_A F F \Pi_B) = \Pi_A F F \Pi_B) &= P(\mathcal{D}(\Pi_A F F \Pi_B) = \Pi_A F F \Pi_B | \Pi_A F F \Pi_B \in \{(0,0),(1,1)\}) \\ &\quad \times P(\Pi_A F F \Pi_B \in \{(0,0),(1,1)\}) \\ &\quad + \\ &\quad P(\mathcal{D}(\Pi_A F F \Pi_B) = \Pi_A F F \Pi_B | \Pi_A F F \Pi_B \in \{(0,1),(1,0)\}) \\ &\quad \times P(\Pi_A F F \Pi_B \in \{(0,1),(1,0)\}) \\ &= p \times P(\Pi_A F F \Pi_B \in \{(0,0),(1,1)\}) \\ &\quad + \\ &\quad 1 \times P(\Pi_A F F \Pi_B \in \{(0,1),(1,0)\}) \\ P(\mathcal{D}(CF^{\frac{1}{2}}) = \Pi_A F F \Pi_B) &= P(\mathcal{D}(CF^{\frac{1}{2}}) = \Pi_A F F \Pi_B | CF^{\frac{1}{2}} \in \{(0,0),(1,1)\}) \\ &\quad \times P(CF^{\frac{1}{2}} \in \{(0,0),(1,1)\}) \\ &\quad + \\ &\quad P(\mathcal{D}(CF^{\frac{1}{2}}) = \Pi_A F F \Pi_B | CF^{\frac{1}{2}} \in \{(0,1),(1,0)\}) \\ &\quad \times P(CF^{\frac{1}{2}} \in \{(0,1),(1,0)\}) \\ &= p \times 1 + 0 \times 0 \end{aligned}$$

By substituting into Equation 6.7, p maximizes the following quantity

$$\begin{aligned}
d^{\mathbb{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) &= |pP(\Pi_A FF\Pi_B \in \{(0,0),(1,1)\}) + P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\}) - p| \\
&= |p[(P(\Pi_A FF\Pi_B \in \{(0,0),(1,1)\}) + P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\})] \\
&\quad + \\
&\quad (1-p)P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\}) - p| \\
&= |p + (1-p)P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\}) - p| \\
&= |(1-p)P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\})|
\end{aligned}$$

Hence $p = 0$ as $\mathcal{D}$ is a maximal distinguisher and thus

$$d^{\mathbb{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) = P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\}) \tag{6.8}$$

□

Lemma 6.2.5. *Let F be non-interactive and $(\varepsilon,\lambda,\rho)$-effective. Then*

$$d^{\mathbb{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) \geq \lambda(1-\rho)$$

Proof. Let $\mathcal{D}$ be the maximal distinguisher as in Lemma 6.2.4. Suppose FF outputs α_{FF} on its left interface and β_{FF}. If $\alpha_{FF} \not\parallel_F \beta_{FF}$, we can find an upper bound for λ with the help of Inequality 6.2:

$$\begin{aligned}
\lambda \leq d^{\mathbb{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) &= d^{\mathcal{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) \\
&= |P(\mathcal{D}(\Pi_A FF\Pi_B) = \Pi_A FF\Pi_B | \alpha_{FF} \not\parallel_F \beta_{FF}) \\
&\quad - \\
&\quad P(\mathcal{D}(CF^{\frac{1}{2}}) = \Pi_A FF\Pi_B | \alpha_{FF} \not\parallel_F \beta_{FF})| \\
&= |P(\mathcal{D}(\Pi_A FF\Pi_B) = \Pi_A FF\Pi_B | \alpha_{FF} \not\parallel_F \beta_{FF}) - 0| \\
&= P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \not\parallel_F \beta_{FF})
\end{aligned}$$

By Lemmas 6.2.2,6.2.3 and 6.2.4:

$$\begin{aligned}
d^{\mathbb{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) &= P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\}) \text{ by Lemma 6.2.4} \\
&= P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \parallel_F \beta_{FF}) P(\alpha_{FF} \parallel_F \beta_{FF}) \\
&\quad + \\
&\quad P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \not\parallel_F \beta_{FF}) P(\alpha_{FF} \not\parallel_F \beta_{FF}) \\
&= P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \parallel_F \beta_{FF}) \rho \\
&\quad + \\
&\quad P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\} | \alpha_{FF} \not\parallel_F \beta_{FF}) (1-\rho) \\
&= \varepsilon'\rho + \lambda'(1-\rho) \quad \text{for some } 0 \leq \varepsilon' \leq \varepsilon,\ \lambda \leq \lambda' \leq 1 \\
&\geq \lambda'(1-\rho) \\
&\geq \lambda(1-\rho)
\end{aligned}$$

where

$$P(\alpha_{FF} \|_F \beta_{FF}) = \rho \text{ by Lemma 6.2.2,}$$
$$P(\Pi_A FF\Pi_B \in \{(0,1),(1,0)\} || \alpha_{FF} \|_F \beta_{FF}) \leq \varepsilon \text{ by Lemma 6.2.3,}$$

□

We now have enough results to prove the following theorem that has a key importance in evading Vilasini's et al. impossibility proof.

Theorem 6.2.6. *Let F be non-interactive and $(\lambda,\varepsilon,\rho)$-effective. Then*

$$\kappa := d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, \Pi_A \sigma_A CF_A^{\frac{1}{2}}) \geq \lambda(1-\rho) - 3\varepsilon$$

Proof. See Figure 6.3 for a geometric illustration of this proof. The proof just summarizes previous results and uses properties of the distinguishing advantage metric space to prove the theorem.

- $d^{\mathbb{D}}(\Pi_A \sigma_A CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \leq 2\varepsilon$ by Inequality $\Diamond$
- $d^{\mathbb{D}}(\Pi_A FF\Pi_B, \Pi_A F\sigma_A CF_A^{\frac{1}{2}}) \leq \varepsilon$ by Inequality 6.4 and Theorem 5.0.1
- $d^{\mathbb{D}}(\Pi_A FF\Pi_B, CF^{\frac{1}{2}}) \geq \lambda(1-\rho)$ by Lemma 6.2.5
- $d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \geq \lambda(1-\rho) - \varepsilon$ by triangle inequality
- $d^{\mathbb{D}}(\Pi_A F\sigma_A CF_A^{\frac{1}{2}}, \Pi_A \sigma_A CF_A^{\frac{1}{2}}) \geq \chi - 2\varepsilon \geq \lambda(1-\rho) - 3\varepsilon$ by triangle inequality

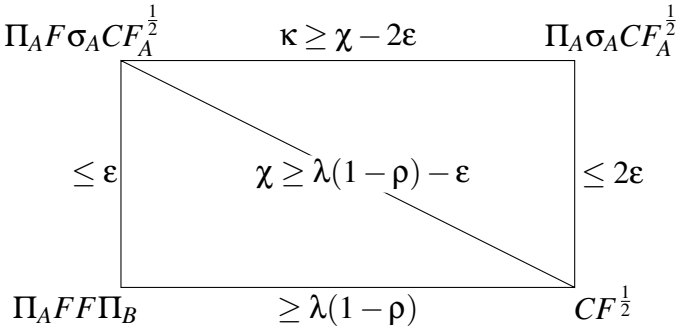


Figure 6.3: Depiction of proof of Lemma 6.2.6. A line label denotes a metric in distinguishing advantage space over $\mathbb{D}$.

□

Assuming a $(\lambda,\varepsilon,\rho)$-effective shared resource F between Alice and Bob, the next theorem is of a great importance in finding an implementation of F as it gives us a sufficient condition for the three parameters $(\lambda,\varepsilon,\rho)$ such that the Vilasini's impossibility proof of composable bit commitment [31] is evaded.

Theorem 6.2.1. *Let* $\varepsilon > 0$ *and* $\Pi = (\Pi_A, \Pi_B)$ *a protocol followed by Alice and Bob. Suppose further that both parties share a non-interactive and* $(\lambda, \varepsilon, \rho)$*-effective resource* F *such that protocol* Π ε*-constructs bit commitment resource BC. I.e.,*

$$\begin{aligned} d^{\mathbb{D}}(\Pi_A F \Pi_B, BC) &\leq \varepsilon \\ \exists \sigma_A \in \mathbb{S} : d^{\mathbb{D}}(F\Pi_B, \sigma_A BC) &\leq \varepsilon \\ \exists \sigma_B \in \mathbb{S} : d^{\mathbb{D}}(\Pi_A F, BC\sigma_B) &\leq \varepsilon \end{aligned}$$

Then if

$$\frac{1}{4} \leq \lambda(1-\rho)$$

then $\Pi_A F \Pi_B$ ε*-constructs bit commitment resource BC which evades Vilasini's et al. impossibility Theorem 5.0.3.*

Proof. The impossibility Theorem 5.0.3 of bit commitment follows as a consequence of impossibility Theorem 5.0.2 of half-biased coin flipping. We have seen that evading the Theorem 5.0.2 can be achieved by finding a shared resource F with certain properties that would satisfy the Inequality 6.6 for the given ε. By Figure 6.4 it is obvious that F is a shared resource between Alice and Bob in bit commitment protocol $\Pi = (\Pi_A, \Pi_B)$ if and only if F is a shared resource in the corresponding Blum's construction discussed in Theorem 5.0.2. Hence the properties of F in half-biased coin flipping protocol that allow to construct $CF^{\frac{1}{2}}$ also evade the Vilasini's impossibility result. Suppose F is non-interactive and $(\lambda, \varepsilon, \rho)$-effective. By Equation 5.5, Inequality

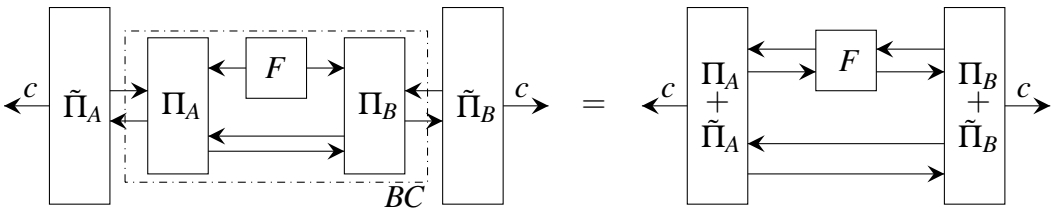


Figure 6.4: Blum's protocol with shared resource

6.6 and Theorem 6.2.6 it follows that

$$\frac{1}{4} = P(c_0^A \neq c_0^B) \leq d^{\mathbb{D}}(CF_B^{\frac{1}{2}} \sigma_{BA} CF_A^{\frac{1}{2}}, CF^{\frac{1}{2}}) \leq 3\varepsilon + \kappa$$

Therefore

$$\frac{1}{4} - (\lambda(1-\rho) - 3\varepsilon) \leq \frac{1}{4} - \kappa \leq 3\varepsilon$$

After algebraic manipulation we find that the Inequality 6.6 is satisfied if λ and ρ are such that

$$\frac{1}{4} \leq \lambda(1-\rho)$$

□

Chapter 7

Quantum Beamer Bit Commitment Algorithm

In the previous chapter we motivated an assumption of a trusted non-interactive third party acting only in the setup phase prior Alice and Bob take any actions. In this chapter we develop an example of such party which we call an Asymmetric Quantum Beamer, prove its security in Casual Boxes framework and use the results of the previous chapter to show it does not conflict with the novel Vilasini's et al. impossibility proof [31].

7.1 Asymmetric quantum beamer assumption

We introduce a non-interactive, inactive and assymetric trusted third party Assymetric Quantum Beamer F_{QB}. See Algorithm 1 for the definition of F_{QB} and see Algorithm 2 for the proposed protocol $\Pi = (\Pi_A, \Pi_B)$ that uses F_{QB}. To the best of our knowledge, the idea emerged just recently in literature in [19]. The shared party used in [19] however relies on existence of appropriate perfectly non-linear bijections which they claim are difficult to determine. Our proposed Assymetric Quantum Beamer does not require any such assumption making it easier for practical implementation purposes. Classically, a similar assumption has been made in [5] showing that *common reference string(crs)* model, in which both parties have access to a randomly generated string from some probability distribution, is a sufficient assumption to achieve computationally-secure composability of bit commitment. It is unclear whether such scheme is secure against quantum adversaries, see Section 2.3.1 for details. However, note that *crs* model achieves composability when applied to an already existing secure non-composable bit commitment protocol whereas our proposed Assymetric Quantum Beamer is an essential assumption to construct even a single instance bit commitment protocol given the protocol $\Pi = (\Pi_A, \Pi_B)$. Hence Assymetric Quantum Beamer is a much stronger assumption that *crs*. Possibilities of weaker assumptions are discussed in Chapter 8.

Algorithm 1: Non-interactive asymmetric quantum beamer resource F_{QB}

Input:

- Security parameter l

Output:

- To Alice:
  - bit b
  - a bit string s of length l
- To Bob:
  - set of BB84 states $\{|\psi_i\rangle\}_{i\in 1,\ldots,l}$

F_{QB}**:**

sample $b \sim \{0,1\}$ uniformly

randomly generate $s \sim \{0,1\}^l$

if $b = 0$ **then**

  prepare $\{|\psi_i\rangle\}_{i\in 1,\ldots,l}$ such that $|\psi_i\rangle = \begin{cases} |0\rangle \text{ if } s_i = 0 \\ |1\rangle \text{ if } s_i = 1 \end{cases}$

end

if $b = 1$ **then**

  prepare $\{|\psi_i\rangle\}_{i\in 1,\ldots,l}$ such that $|\psi_i\rangle = \begin{cases} |-\rangle \text{ if } s_i = 0 \\ |+\rangle \text{ if } s_i = 1 \end{cases}$

end

7.2 Security analysis of the proposed protocol

We first prove the standalone security against dishonest Alice (binding) and against dishonest Bob (conceailing). We then discuss why the proposed protocol evades both Lo & Chau [21] attack and Vilasini's et al. impossibility theorem [31]. The rest of the section is devoted to proof of composability in the UC framework.

7.2.1 Binding + Concealing

If Alice acts dishonestly in the reveal phase, i.e. she flips a bit m, Bob measures the states $\{|\Psi_i\rangle\}$ in wrong basis, obtaining measurement outcomes $\{\tilde{a}_i\}$ inconsistent with s up to a negligible probability λ. Assuming Bob measures in the wrong basis, for every i there is $\frac{1}{2}$ probability that $\tilde{a}_i = s_i$. Hence Bob accepts the dishonest commitment with probability $\lambda = 2^{-l}$.

The protocol is perfectly concealing against dishonest Bob since prior the reveal phase Bob learns nothing about Alice's commitment as the received bit $c = m \oplus b$ does not provide any information about m given that b is unknown to Bob.

7.2.2 Security against Lo and Chau Attack

The protocol evades the Lo & Chau and Mayers [21, 24] impossibility proof as once Alice creates the state $|m\rangle$ corresponding to commitment of bit m, up to a negligible

Algorithm 2: Bit commitment protocol $\Pi = (\Pi_A, \Pi_B)$ using F_{QB}

Π_A**:**
  Input:
    - (b, s) from F_{QB}
    - commitment bit m
  COMMIT PHASE:
    send $c = m \oplus b$ to Bob
  REVEAL/ABORT PHASE:
    if *Alice wants to reveal* **then**
      send (m, s) to Bob
    end
    else if *Alice wants to abort* **then**
      send **abort** to Bob
    end

Π_B**:**
  Input:
    - $\{|\psi_i\rangle\}_{i\in 1,\ldots,l}$ from F_{QB}
  COMMIT PHASE:
    After receiving c from Alice output **received** notification
  REVEAL/ABORT PHASE:
    if *"***abort***" received* **then**
      output **abort**
    end
    else
      After receiving (m, s) from Alice**:**
        $\tilde{b} := c \oplus m$
        $\forall i = 1, \ldots, l$: $\tilde{a}_i :=$ Measurement$(|\Psi_i\rangle,$ basis $= \tilde{b})$
        if $\forall i : s_i = \tilde{a}_i$ **then**
          output m
        end
        else
          output **abort**
        end
    end

probability she cannot guess the state $|m \oplus 1\rangle$ as it requires predicting Bob's measurement outcomes in $b \oplus 1$ basis. We provide a more formal argument of the statement. After Alice commits to a bit m, the phase of the joint system of Alice and Bob $\mathcal{A} \otimes \mathcal{B}$ can be expressed as follows.

if $m = 0$:

$$|0\rangle = \sum_{i \in \alpha} c_i |\mu_i\rangle_{\mathcal{A}} \otimes |\phi_i\rangle_{\mathcal{B}} \otimes |\xi_i\rangle_{\mathcal{B}}$$

if $m = 1$:

$$|1\rangle = \sum_{i \in \alpha} c'_i |\mu_i\rangle_{\mathcal{A}} \otimes |\phi'_i\rangle_{\mathcal{B}} \otimes |\xi_i\rangle_{\mathcal{B}}$$

for some scalars c_i, c'_i, orthonormal basis $\{|\mu_1\rangle_{\mathcal{A}}, |\mu_2\rangle_{\mathcal{A}}, ...\}$ and some states $\{|\phi_1\rangle_{\mathcal{B}}, |\phi_2\rangle_{\mathcal{B}}, ...\}$, $\{|\phi'_1\rangle_{\mathcal{B}}, |\phi'_2\rangle_{\mathcal{B}}, ...\}$, $\{|\xi_1\rangle_{\mathcal{B}}, |\xi_2\rangle_{\mathcal{B}}, ...\}$. The states $\{|\phi_1\rangle_{\mathcal{B}}, |\phi_2\rangle_{\mathcal{B}}, ...\}$, $\{|\phi'_1\rangle_{\mathcal{B}}, |\phi'_2\rangle_{\mathcal{B}}, ...\}$ are prepared by Alice and sent to Bob as in step 1c) in Chapter 3 whereas $\{|\xi_1\rangle_{\mathcal{B}}, |\xi_2\rangle_{\mathcal{B}}, ...\}$ are prepared and sent to Bob by the Asymmetric Quantum Beamer and hence these states are unknown to Alice. Note, that in the original impossibility proof the states $\{|\xi_1\rangle_{\mathcal{B}}, |\xi_2\rangle_{\mathcal{B}}, ...\}$ are not present as a shared resource is not assumed in their work. Suppose Alice wants to cheat by changing $|0\rangle \rightarrow |1\rangle$ (the same argument works vice-versa) between commitment and reveal phases. Let Ξ be a collection of all possible measurement outcomes of $\{|\xi_1\rangle_{\mathcal{B}}, |\xi_2\rangle_{\mathcal{B}}, ...\}$ in basis $b = 1$. In the commitment phase, she has prepared a state

$$|0\rangle = \sum_{i \in \alpha} c_i |\mu_i\rangle_{\mathcal{A}} \otimes |\phi_i\rangle_{\mathcal{B}} \otimes |\xi_i\rangle_{\mathcal{B}}$$

Let $\tau \in \Xi$ be a string of measurement outcomes that Bob will obtain when he measures $\{|\xi_1\rangle_{\mathcal{B}}, |\xi_2\rangle_{\mathcal{B}}, ...\}$ in basis $b = 1$. Since the states are prepared in basis $b = 0$ according to Algorithm 1, τ is a string of uniformly random bits. Let

$$|1^{\tau}\rangle = \sum_{i \in \alpha} c_i^{\tau} |\mu_i\rangle_{\mathcal{A}} \otimes |\phi_i\rangle_{\mathcal{B}} \otimes |\xi_i\rangle_{\mathcal{B}}$$

be a state that corresponds to commitment of $m = 1$ where $(s, b) = (\tau, 1)$. By the concealing property proven in Section 7.2.1, there is a density operator $\rho = \mathrm{Tr}_A |0\rangle\langle 0| = \mathrm{Tr}_A |1^{\tau}\rangle\langle 1^{\tau}|$ with spectral decomposition

$$\rho = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i|$$

where $\{|\varphi_i\rangle\}_i$ is a unique orthogonal basis of $\mathcal{B}$ given $|0\rangle$. The uniqueness property is an essential observation and is stressed in proof of Schmidt decomposition in Chapter 3. If Alice wants to apply the technique from Lo and Chau attack, she must find purifications of ρ

$$|0\rangle = \sum_i \sqrt{\lambda_i} |\mu\rangle_{\mathcal{A}} |\varphi\rangle_{\mathcal{B}}$$
$$|1^{\tau}\rangle = \sum_i \sqrt{\lambda_i} |\mu'^{\tau}_i\rangle_{\mathcal{A}} |\varphi\rangle_{\mathcal{B}}$$

However, since τ is an outcome of a random variable independent from Alice's actions, she does not know $|1^{\tau}\rangle$ and hence cannot determine $|\mu'^{\tau}_i\rangle_{\mathcal{A}}$. This is the key difference to the original impossibility result where Alice has an ultimate power over state of Bob's system. In such settings Alice would create the states $\{|\xi_1\rangle_{\mathcal{B}}, |\xi_2\rangle_{\mathcal{B}}, ...\}$ by herself in basis $b = 1$ and hence would know the value of τ. Hence the only thing that Alice can try is to make guess about τ. The size of Ξ is in our algorithm the number of possible strings τ, i.e. $|\Xi| = 2^l$. Denote the Alice's guess as τ_A. Hence there is $p = 2^{-l}$ probability $\tau_A = \tau$. She follows the procedure in Chapter 3 and prepares purifications

$$|0\rangle = \sum_i \sqrt{\lambda_i} |\mu_i\rangle_{\mathcal{A}} |\varphi_i\rangle_{\mathcal{B}}$$
$$|1^{\tau_{\mathcal{A}}}\rangle = \sum_i \sqrt{\lambda_i} |\mu'^{\tau_{\mathcal{A}}}_i\rangle_{\mathcal{A}} |\varphi_i\rangle_{\mathcal{B}}$$

Let $U_{\tau_{\mathcal{A}}}$ be the change of basis unitary that rotates $|0\rangle \to |1^{\tau_\alpha}\rangle$. She applies $U_{\tau_{\mathcal{A}}}$ on the state $|0\rangle$ with a hope that $\tau_A = \tau$. Hence with negligible probability $p = 2^{-l}$ the state of the system becomes $|1^{\tau}\rangle$ and Bob accepts the cheating behaviour of Alice when she proceeds to reveal phase. Otherwise, the state of $\mathcal{A} \otimes \mathcal{B}$ is transformed to $|1^{\tau_{\mathcal{A}}}\rangle$. By uniqueness of $\{|\varphi_i\rangle\}_i$ justified earlier, $|1^{\tau}\rangle$ is the only state that will result in Bob accepting the dishonest commitment and hence he rejects the Alice's commitment as his measurement outcomes τ do not correspond to the evidence string $s = \tau_A$ received from Alice.

7.2.3 Avoiding Vilasini's impossibility proof

Once we check that $\Pi_A F \Pi_B$ ε-constructs BC in UC framework(see Section 7.2.4) for any $\varepsilon > 0$ we are done with the proof of composability. In this subsection we show F_{QB} is not ruled-out by Theorem 6.2.1 and hence it is as a reasonable assumption for the shared resource. Otherwise we would not need to develop lengthy argument in Section 7.2.4 and would rethink the implementation of the shared resource. The claim is simple and gives an example of how our result from Chapter 6 might be used as a "quick check" when developing new bit commitment protocols that assume a trusted third party.

Let η be a shared resource between Alice and Bob such that $\alpha_\eta \not\parallel_{F_{QB}} \beta_\eta$ for all $(\alpha_\eta, \beta_\eta) \in \text{img}(F_{QB})$. Observe that if η provides output in invalid form, i.e. if it doesn't send a message to any of the party at t_0 or the length and structure of the message is different that the one of F_{QB} than either party aborts the protocol and $d^{\mathbb{D}}(\Pi_A \eta \Pi_B, BC) = 1$. Let us now restrict our attention to η such that it provides output of the valid form but such that $\alpha_\eta \not\parallel_F \beta_\eta$. Define a distinguisher $\mathcal{D} \in \mathbb{D}$ as

$$\mathcal{D}(\mathcal{R}) = \begin{cases} \Pi_A \eta \Pi_B & \text{if output}(\mathcal{R}) \approx \textbf{abort} \\ BC & \text{otherwise} \end{cases}$$

and let $\mathcal{D}$ be such that it never aborts the protocol and commits to a random bit c. Then

$$\begin{aligned} d^{\mathbb{D}}(\Pi_A \eta \Pi_B, BC) &\geq d^{\mathcal{D}}(\Pi_A \eta \Pi_B, BC) \\ &= |P(\mathcal{D}(\Pi_A \eta \Pi_B) = \Pi_A \eta \Pi_B) - P(\mathcal{D}(BC) = \Pi_A \eta \Pi_B)| \\ &= |P(\mathcal{D}(\Pi_A \eta \Pi_B) = \Pi_A \eta \Pi_B) - 0| \\ &= P(\text{output}(\Pi_A \eta \Pi_B) = \textbf{abort}) \\ &\geq 1 - 2^{-l} \end{aligned}$$

because if η is used as a shared resource, then Bob either measures $\{|\psi_i\rangle\}$ in the wrong basis b or it compares the measurements to a wrong measurement outcomes string s. Hence there is at most 2^{-l} probability that he accepts the commitment.

Since there are 2×2^l possibilities for (b,s) and $\{|\psi_i\rangle\}$ are completely determined by (b,s) (see Algorithm 1), the size of image of F is 2^{l+1}. By construction of F_{QB}, the Assymetric Quantum Beamer uniformly samples from its image and hence F_{QB} is $(\geq 1 - 2^{-l}, \varepsilon, 2^{-(l+1)})$-effective resource (see Definition 6.1.2). Identifying $\lambda \geq 1 - 2^{-l}$,

$\rho = 2^{-(l+1)}$ we find that

$$\lambda(1-\rho) \geq (1-2^{-l})(1-2^{-(l+1)}) \geq \frac{1}{4} \text{ for } l \geq 1$$

and hence the Assymetric Quantum Beamer bit commitment algorithm evades the the Vilasini's et al. proof by Theorem 6.2.1 and hence it is reasonable to check if F_{QB} satisfies the ε-construction in UC framework.

7.2.4 Composability proof in UC framework

Since F_{QB} has been shown not to be ruled-out by result of Theorem 6.2.1, we proceed to a careful check whether the protocol Π ε-constructs *BC*. See B.1 for definition of ideal Bit Commitment resource BC. We strongly suggest to follow the graphical depictions of the arguments.
Honest case. Bob is guaranteed to measure $\{|\Psi_i\rangle\}$ in correct basis and hence outputs the committed bit m. Hence no distinguisher is capable of distinguishing the constructed and ideal resources (Figure 7.1).

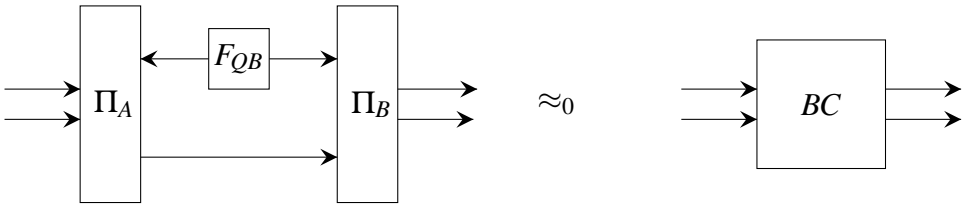
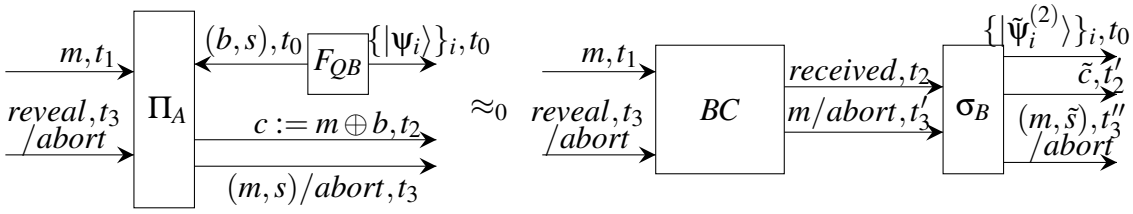


Figure 7.1: $d^{\mathbb{D}}(\Pi_A F_{QB} \Pi_B, BC) = 0$

Honest Alice and dishonest Bob (Figure 7.2).



$$t_i \prec t_{i+1}, t_i \prec t_{i'}, t_i' \prec t_{i+1}$$

Figure 7.2: $\exists \sigma_B : d^{\mathbb{D}}(\Pi_A F_{QB}, BC_B \sigma_B) = 0$

The role of simulator σ_B is to minimize distinguishing advantage of the constructed and the ideal resources. Let σ_B simulate F_{QB} by generating l EPR pairs $\{(|\tilde{\psi}_i^{(1)}\rangle, |\tilde{\psi}_i^{(2)}\rangle)\}_{i=1,\ldots,l}$ and the corresponding $(b, \tilde{s})$ as in Algorithm 1 and sending $\{|\tilde{\psi}_i^{(2)}\rangle\}_i$ to the outer interface. Upon receiving **received** message from *BC*, it randomly generates and outputs

$\tilde{c}$ to the outer interface. If Alice aborts the protocol, σ_B sends an **abort** message at t_3 and hence both resources produce identical output. Assuming Alice does not abort the protocol, after receiving commitment m from BC, σ_B calculates $\tilde{b} := \tilde{c} \oplus m$ and checks if $\tilde{b} = b$. If the equality holds, it outputs (m,s) to the outer interface. Otherwise it measures $\{|\tilde{\psi}_i^{(1)}\rangle\}_i$ in basis $\tilde{b}$ and outputs (m,s') where s' is the string of measurement outcomes.

Since σ_B follows procedure of Algorithm 1 for F_{QB} we have that density matrices ρ_A and ρ_B, corresponding to quantum systems $A := \bigotimes_i |\psi_i\rangle$ and $B := \bigotimes_i |\tilde{\psi}_i^{(2)}\rangle$ respectively, satisfy $\rho_A = \rho_B$ and hence are not distinguishable by any distinguisher. Moreover, as $b, \tilde{c}$ are independently drawn from the same probability distribution and equivalently for $s, \tilde{s}$, no distinguisher can gain any distinguishing advantage by comparing the inputs from outer interface of the resources. If a distinguisher checks for consistency of the inputs, i.e. when measuring $\{|\tilde{\psi}_i^{(2)}\rangle\}_i$ in $\tilde{c} \oplus m$ basis (or equivalently $\{|\psi_i\rangle\}_i$ in $c \oplus m$ basis) it always finds out the measurement is consistent with $\tilde{s}$ (or s). This property is guaranteed by constructing $\tilde{s}$ in a way it corresponds to measurement outcomes of measurement of $\{|\tilde{\psi}_i^{(1)}\rangle\}_i$ in $\tilde{c} \oplus m$ basis. Hence there is zero distinguishing advantage for any possible distinguisher.

Dishonest Alice and honest Bob (Figure 7.3).

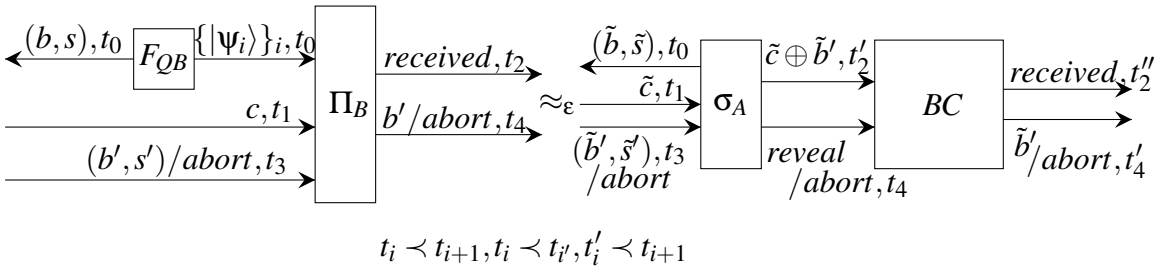


Figure 7.3: $\exists \sigma_A : d^{\mathbb{D}}(F_{QB}\Pi_B, \sigma_A BC_A) \leq \varepsilon$

The optimal strategy for σ_A involves simulating F_{QB} by generating a pair $(\tilde{b},\tilde{s})$ and sending it to Alice. After receiving the commitment information $\tilde{c}$, let σ_A emulate Π_A by extracting the commitment $m := \tilde{c} \oplus \tilde{b}$ and commiting the value m to BC. Hence if Alice acts consistently with Algorithm 2, the two resources $F_{QB}\Pi_B$ and $\sigma_A BC$ have identical outputs, disregards if she aborts the protocol. Hence we only consider distiguishers that emulate cheating Alice sending $(b',s') \neq (b,s)$ (or $(\tilde{b}',\tilde{s}') \neq (\tilde{b},\tilde{s})$) at t_3.

If cheating Alice does not flip the 'basis bit' b (or b') she sends (b,s') (or $(\tilde{b},\tilde{s}')$) to Bob where $s \neq s'$ (or $\tilde{s} \neq \tilde{s}'$). Then since Bob measures $\{|\psi_i\rangle\}_i$ in the correct basis, he always discovers the cheating behavior of Alice by comparing the measurement outcomes to s' (or $\tilde{s}'$). Hence Π_B outputs the **abort** message. Similarly, σ_A can check for the malicious behavior by discovering $\tilde{s} \neq \tilde{s}'$ and hence we define it to abort the protocol in this case as well. Hence in this case the resources $F_{QB}\Pi_B$ and $\sigma_A BC$ are

indistinguishable.

If she flips the 'basis bit' b (or b'), i.e. if she sends $b' := b \oplus 1$ (or $\tilde{b}' := b' \oplus 1$) to Bob at t_3 then σ_A can detect the malicious behavior by observing $\tilde{b} \neq \tilde{b}'$. We define σ_A to abort the protocol in this scenario. Considering the case for F_{QB}, since Bob has no information about b, he is unable to detect the malicious behavior as easily as σ_A. He proceeds to measure $\{|\psi_i\rangle\}_i$ in b' basis and compares the outcomes with s'. Since $\{|\psi_i\rangle\}_i$ was prepared in b basis, the result of the measurement is a random bit string where each bit is uniformly sampled from a Bernoulli distribution with $p = \frac{1}{2}$. Since Alice does not posses a clone of $\{|\psi_i\rangle\}_i$, she has probability $\lambda := 2^{-l}$ of producing a string s' such that Bob accepts the malicious commitment.

Algorithm 3: Definition of distinguisher $\mathcal{D}$

$\mathcal{D}$**:**
- Receive (b,s) from F_{QB} or σ_A
- Randomly generate m with uniform probability
- **COMMIT PHASE:**
  - send $c := m \oplus b$ to F_{QB} or σ_A
- **REVEAL PHASE:**
  - send $((b \oplus 1), s)$ to F_{QB} or σ_A
- **DISTINGUISHING PHASE:**
  - $o \leftarrow$ output of the outer interface of the resource connected to $\mathcal{D}$
  - **if** $o = (m \oplus 1)$ **then**
    - with probability $\frac{1}{\varepsilon+1}$ guess *ideal*
    - with probability $\frac{\varepsilon}{\varepsilon+1}$ guess *constructed*
  - **end**
  - **else if** o=***error*** **then**
    - guess *constructed*
  - **end**

Let $\mathcal{D} \in \mathbb{D}$ be a distinguisher that upon receiving (b,s) at t_0 sends $(b \oplus 1, s')$ where $s \in \{0,1\}^l$ is randomly generated, see Algorithm 3. By the above argument, $\mathcal{D}$ has the greatest distinguishing advantage over the set $\mathbb{D}$ of all possible distinguishers. Therefore

$$\begin{aligned} d^{\mathbb{D}}(F_{QB}\Pi_B, \sigma_A BC_A) &= \sup_{\tau \in \mathbb{D}} d^{\tau}(F_{QB}\Pi_B, \sigma_A BC_A) \\ &= d^{\mathcal{D}}(F_{QB}\Pi_B, \sigma_A BC_A) \\ &= |P(\mathcal{D}(F_{QB}\Pi_B) = ideal) - P(\mathcal{D}(\sigma_A BC_A) = ideal)| \end{aligned} \tag{7.1}$$

where

$$\begin{aligned}
P(\mathcal{D}(F_{QB}\Pi_B) = ideal) &= P(\mathcal{D}(F_{QB}\Pi_B) = ideal | F_{QB}\Pi_B = (m \oplus 1))P(F_{QB}\Pi_B = (m \oplus 1)) \\
&\quad + \\
&\quad P(\mathcal{D}(F_{QB}\Pi_B) = ideal | F_{QB}\Pi_B = \textbf{error})P(F_{QB}\Pi_B = \textbf{error}) \\
&= 0 \times \lambda + \frac{1}{1+(1-\lambda)} \times (1-\lambda) \\
&= \frac{1-\lambda}{2-\lambda} \\
P(\mathcal{D}(\sigma_A BC) = ideal) &= P(\mathcal{D}(\sigma_A BC) = ideal | \sigma_A BC = (m \oplus 1))P(\sigma_A BC = (m \oplus 1)) \\
&\quad + \\
&\quad P(\mathcal{D}(\sigma_A BC) = ideal | \sigma_A BC = \textbf{error})P(\sigma_A BC = \textbf{error}) \\
&= 0 \times 0 + \frac{1}{1+(1-\lambda)} \times 1 \\
&= \frac{1}{2-\lambda}
\end{aligned}$$

It then follows by substitution into Equation 7.1 that

$$\begin{aligned}
d_A^{\mathbb{D}}(F_{QB}\Pi_B, \sigma_A BC) &= |P(\mathcal{D}(F_{QB}\Pi_B) = ideal) - P(\mathcal{D}(\sigma_A BC) = ideal)| \\
&= \frac{\lambda}{2-\lambda}
\end{aligned}$$

Theorem 7.2.1. *Let* $\varepsilon > 0$. *Then there exists security parameter* l *(see Algorithm 2) such that BC is constructed within distance* ε *from* F_{QB} *via protocol* $\Pi = (\Pi_A, \Pi_B)$ *with respect to a set of all possible distinguishers* $\mathbb{D}$.

Proof. If $\varepsilon > 1$ the statement is trivial since 1 is an upper bound for any distinguishing advantage metric. Suppose $\varepsilon \in (0,1]$. Let $l := \lceil -\log(\varepsilon) \rceil$ where logarithm is in base 2. Then

$$\begin{aligned}
\lambda = 2^{-l} &= 2^{-\lceil -\log(\varepsilon) \rceil} \\
&= \begin{cases} 2^{\lceil \log(\varepsilon) \rceil} & \text{if } \log(\varepsilon) \in \mathbb{Z} \\ 2^{-(1-\lceil \log(\varepsilon) \rceil)} & \text{if } \log(\varepsilon) \notin \mathbb{Z} \end{cases} \\
&= \begin{cases} 2^{\lfloor \log(\varepsilon) \rfloor} & \text{if } \log(\varepsilon) \in \mathbb{Z} \\ 2^{-(1-(\lfloor \log(\varepsilon) \rfloor + 1))} & \text{if } \log(\varepsilon) \notin \mathbb{Z} \end{cases} \\
&= 2^{\lfloor \log(\varepsilon) \rfloor} \\
&\leq \varepsilon
\end{aligned}$$

Hence since $1 \leq 2 - \lambda \leq 2$,

$$\frac{\lambda}{2-\lambda} \leq \lambda \leq \varepsilon$$

and by above results in this section it follows that

$$\begin{aligned} d^{\mathbb{D}}(\Pi_A F_{QB} \Pi_B, BC) &= 0 && \leq \varepsilon \\ \exists \sigma_A : d^{\mathbb{D}}(F_{QB} \Pi_B, \sigma_A BC_A) &= \frac{\lambda}{2-\lambda} && \leq \varepsilon \\ \exists \sigma_B : d^{\mathbb{D}}(\Pi_A F_{QB}, BC_B \sigma_B) &= 0 && \leq \varepsilon \end{aligned}$$

□

The Theorem 7.2.1 concludes the composability proof of Assymetric Quantum Beamer bit commitment algorithm in terms of Casual Boxes Framework (Appendix B) since it shows that $BC = (\Pi_A F_{QB} \Pi_B, F_{QB} \Pi_B, \Pi_A F_{QB})$ can be modeled as a Casual Box that is ε-constructed for arbitrary $\varepsilon > 0$.

Chapter 8

On Minimal Assumptions for Composable Bit Commitment

In Chapter 7 we have demonstrated that non-interactive, inactive, assymetric and $(\lambda, \varepsilon, \rho)$-effective shared resource with respect to $CF^{\frac{1}{2}}$ is a sufficient assumption to construct composable secure bit commitment. It is indeed a strong assumption since neither Alice nor Bob can detect malicious behavior of the shared resource. In this chapter we discuss what properties are required in order to evade Vilasini's et al. proof and what properties could possibly get relaxed after further explorations in order to obtain practically most feasible implementation.

8.1 Sufficiency and necessity of shared resource properties

Note, that since the protocol $\Pi = (\Pi_A, \Pi_B)$ considered in proof of impossibility Theorem 5.0.2 was arbitrary, the only way to break the proof is to consider a resource that cannot be merged with Π_A or Π_B. Hence a trusted third party acting in the protocol is essential to achieve composability. Let F be a shared resource between Alice and Bob for the rest of this chapter. Recall that we follow Definition 6.1.2 to describe properties of F which are in particular:

- $(\varepsilon, \lambda, \rho)$-effectiveness
- activity / inactivity
- interactivity / non-interactivity
- symmetry / asymmetry.

By our result in Theorem 6.2.1, if λ and ρ satisfy relation

$$\frac{1}{4} \leq \lambda(1-\rho)$$

then Vilasini's et al. impossibility proof of composability is evaded. However, note that our proof in Chapter 6 did not consider converse at all and it hence might be possible

to relax this sufficiency result even more, although the practicality of such approach is very unlikely as the relation is satisfied by (almost) all reasonable shared resources that have a significant role in the protocol as discussed in the beginning of Section 6.2.

The next sections discusses necessity and/or sufficiency of the other remaining properties.

8.1.1 Inactivity and non-interactivity properties

If F is *active* and *interactive*, i.e. if it can take input from Alice and Bob after the setup stage, then the assumption is no weaker than a trusted party emulating bit commitment protocol which receives Alice's commitment bit at the commit phase and reveals it to Bob when Alice triggers reveal phase. Such protocol is obviously silly from point of cryptography and hence we need either of *non-interactivity* or *inactivity* as a necessary assumption.

If F is *interactive* and *inactive*, then by Definition 6.1.2 it provides output only in the *setup-stage* space-time region. However, by Definition 6.1.1 of the setup-stage, neither Alice nor Bob outputs any message to the shared resource outside the *setup-stage* region and hence it is perfectly indistinguishable from the shared resource $\phi F \phi$, where ϕ is a "filter" resource which forwards output from F to its output interface unchanged but blocks any input. $\phi F \phi$ is clearly *non-interactive*. In other words, *inactivity* cancels out any effect of *interactivity* and hence we don't reduce size of the set of possible candidates for shared resources that apply in Theorem 5.0.2 by requiring *non-interactivity*.

On the other hand, if F is *active* and *non-interactive*, then informally, F keeps sending messages to Alice and Bob during runtime of the protocol and the protocol is conditioned on output from F. Although we haven't devoted our time in finding whether such F that allows composable security exits, in Chapter 7 we presented a shared resource that has weaker assumptions by being *inactive* and *non-interactive*. We indeed consider the case to be weaker since if F is *active*, then it requires a big level of trust that it behaves honestly towards both parties while the protocol is active. If it is inactive, there could be implementations of F that would allow both parties to check that it is "shut down", e.g. in simplest case by unplugging power from a corresponding quantum device that realizes the shared resource and hence to ensure it does not behave dishonestly towards any party after the set-up stage. Therefore we are of the opinion that this direction is not worth exploring as the resulting resource would not require less level of trust than the Assymetric Quantum Beamer (AQB) defined in Chapter 7.

To conclude, *non-interactivity* is an essential property of F, whereas it remains as an open, but likely not very interesting question, whether *inactivity* is required as well. As argued, *active* asymmetric shared resource would be a stronger assumption compared to AQB and hence it has no interesting use unless it allows to relax any other assumption introduced by AQB with asymmetry as the only candidate that remains.

8.1.2 Symmetry / Asymmetry

The security of AQB bit commitment protocol (Chapter 6) is based on asymmetry of the shared resource F_{QB}. To see why, observe that before the reveal phase, Bob is in possession of qubits $\{|\psi_i\rangle\}_i$ prepared in an unknown basis b to him and Alice knows the basis b and string $\{s_i\}_i$ of corresponding measurement outcomes. This allows Alice to send Bob evidence of her commitment $m \oplus b$ which is unique given the commitment bit m and concealing property holds since Bob does not know b. The binding property holds since if Alice decides to open commitment to $m \oplus 1$ then she must lie to Bob about the basis, announcing to him that $\{|\psi_i\rangle\}_i$ are prepared in $b \oplus 1$ basis. (Note that $b = 0$ means basis is $\{|0\rangle, |1\rangle\}$ and $\{|-\rangle, |+\rangle\}$ otherwise). Then up to some negligible probability, Alice is unable to generate and announce to Bob string of measurement outcomes $\tilde{s}$ that would be consistent with his measurement. See Chapter 7 for more detailed description of the protocol. Furthermore, we have shown in Section 7.2.2 that assymetry property was also useful in proving security against Lo & Chau attack. The asymmetric construction of F_{QB} is in AQB protocol essential to construct a secure (not necessary composable) bit commitment protocol and the composability proof that follows does not explicitly require this property.

Indeed, we didn't use the symmetry/asymmetry assumption in the proof of Theorem 6.2.1. The symmetric shared resource is just a special case of the $(\varepsilon, \lambda, \rho)$-efficient shared resource with a restricted image. Hence the Theorem 6.2.1 holds for the symmetric case as well. An interesting question to ask is whether there exists a secure bit commitment protocol with a symmetric shared resource. Such resource would be more interesting than AQB as it might not require such high level of trust by both parties in practical implementation. E.g. it could be open-source implemented on a server accessible worldwide and it would not allow any interaction by the necessity for non-interactive property argued in Section 8.1.1. It would not therefore be able to favor any of the involved parties. In contrast, because of the asymmetric property of AQB, neither Alice nor Bob can check honesty of AQB. For example, a dishonest AQB could send EPR pairs of $\{|\psi_i\rangle\}_i$ to Alice and hence she would be able to produce a string of measurement outcomes $\tilde{s}$ that would correspond to Bob's outcomes when measuring in the wrong basis. Hence he would never detect Alice changing the commitment value. Similarly, if AQB announces basis b to Bob he would be able to extract the commitment bit m before the reveal phase by applying XOR of b and the evidence $b \oplus m$ sent by Alice.

We motivated a question of existence of a *symmetric* shared resource that would allow secure and composable bit commitment. We provided an intuition with specific examples where asymmetric property finds its important use and we conclude it would be challenging to find a symmetric resource while satisfying the above discussed scenarios once asymmetry is evaded. On the other hand, we haven't proved not disproved such existence and we think this is a very interesting problem to consider as it would allow to lower requirements on level of trust in the shared resource. A care should be taken to ensure that once such implementation is found, it should weaken the extra assumptions introduced.

A careful reader might recall that symmetric shared resource called *common refer-*

ence string (crs) has been demonstrated to construct a composable bit commitment in computational security settings [6]. However, the proposed protocol has no known implementations that are secure against quantum computers, although this might change once hardness of lattice-based problems is proven for quantum devices. See Section 2.3.1 for more details.

Chapter 9

Conclusion and Future Work

In this project we defined bit commitment protocol and motivated the need for an implementation that would satisfy security and composability properties. Such protocol which uses an assymetric, inactive and non-interactive shared resource called Assymetric Quantum Beamer (AQB) has been defined in Chapter 7. It is a very simplified and surprisingly more "powerful" modification of protocol [19] as it does not rely on assumption of perfectly non-linear bijections. Its standalone security and security against the famous Lo & Chau attack [21] is carefully explained and its composability is proven in *Casual Boxes Framework*. We use our results from Chapter 6 to argue how it specifically evades Vilasini's et al. composability no-go theorem [31].

The project explores beyond just finding a specific implementation of the protocol as AQB is a strong assumption that requires a high level of trust by all involved parties. It might be possible to relax some of the assumptions and hence lower the level of trust required. The important property of AQB is its inactivity, i.e. that it acts only in the set-up stage before the actual protocol is run. Otherwise, we could just consider a trusted third party that would emulate the protocol. If Alice and Bob are able to ensure that the third party is not involved in the protocol during its runtime, the assumptions are weakened. In Chapter 6 we formally defined a shared resource and its properties *activity/inactivity*, *interactivity/non-interactivity*, *symmetry, asymmetry*, $(\varepsilon, \lambda, \rho)$-*effectiveness* considered in the project which are as general as possible to cover all possible shared resources and in Chapter 8 we argue which properties are necessary and which have a potential to be relaxed. In particular, we argue that a shared resource F is a necessary, but not yet sufficient assumption on its own to evade the Vilasini's et al. composability no-go theorem. On top of the assumption we require that:

- F is non-interactive
- F is $(\varepsilon, \lambda, \rho)$-effective such that

$$\frac{1}{4} \leq \lambda(1-\rho)$$

It is an open question whether the above assumptions are sufficient to construct composable secure bit commitment protocol. AQB has in addition the following properties

- F is asymmetric
- F is inactive

This result implies that almost every reasonable shared resource in a bit commitment protocol evades the composability no-go theorem which is a remarkable result. The more elaborated explanation is located at the beginning of Section 6.2.1.

It is not clear whether the above two properties are necessary. As discussed in Chapter 8, the asymmetric property of F is a strong assumption which might possibly get relaxed. In the protocol using AQB, the asymmetry property guarantees that Lo & Chau attack can get evaded since once Alice commits to a bit m, she knows the state $|m\rangle$ but she does not know the state $|m \oplus 1\rangle$ and hence up to a negligible probability she cannot prepare the required purification of the joint system state that would allow her to apply a unitary that would change her commitment towards $m \oplus 1$. Hence if symmetric property of F is assumed, there should be different assumption introduced that would evade Lo & Chau impossibility theorem. One of such plausible assumptions is relativistic constraint as discussed in Chapter 4 which however requires space-like separation of Alice's agents and poses a limit on a commitment time interval. Hence the pros and cons of such method, that on the other hand allows symmetric F, depend on practical needs. Existence of different appropriate assumption that would allow symmetric F and offer a greater level of practicability than the asymmetric assumption is unclear to us and is and is an interesting direction to explore.

Although the inactivity property did not have any particular use in our discussions, we do not think there is a more practical implementation of the shared resource than AQB which is active during the runtime of the protocol, although we do not completely rule out such possibility. For example, activity might turn out to be a useful assumption in achieving symmetry of F, although we have no indication of such case.

Furthermore, it is unclear whether there exists a better practical implementation of non-interactive, inactive, asymmetric and $(\varepsilon, \lambda, \rho)$-effective resource satisfying Theorem 6.2.1 than the AQB resource. For example, it is unclear whether quantum capabilities of the shared resource are required. If computational hardness of solving lattice based problems by quantum computers is proven then it is possible that there is a specific realization of the *common reference string* discussed in Section 2.3.1 that satisfies the above properties as well. However, if quantum capabilities are assumed, we believe we have found a very effective implementation of the shared resource as its security is exponentially proportional to its security parameter.

Appendices

Appendix A

The Abstract Cryptography Framework

In order to argue about security and composability of classical/quantum cryptographic protocols we are in need of a framework providing definitions of such security guarantees. *The Abstract Cryptography Framework* [4, 23] has been widely applied for this purpose [31, 5, 11, 28] and therefore to preserve compatibility with previous works our project adopts it as well. Extension to relativistic settings is possible via Casual Boxes Framework, see *Appendix B*. The basic building blocks of the *The Abstract Cryptography Framework* are *resources*, *converters* and *distinguishers*. We restrict our definitions to allow for only two-party protocols, called Alice and Bob by convention, which is sufficient for the scope of our project.

Definition A.0.1. A **resource** $\mathcal{R}$ is an abstract system with two *interfaces*, each of the accessible to a separate party.

Resources can be thought of as black boxes providing certain functionalities (e.g. a commitment functionality, communication channel,etc.) for the involved users.

Definition A.0.2. A **converter** is an abstract system with *inner* and *outer* interfaces. It emulates an operation performed by a user $\mathcal{U} \in \{Alice, Bob\}$ interacting with a resource $\mathcal{R}$. The inner interface is connected to the interface of a resource $\mathcal{R}$ devoted for the user $\mathcal{U}$ and the outer interface is made available for user $\mathcal{U}$.

Converters serve as an intermediate program between two interfaces.

The fundamental principle of the framework is that a combination of resources and converters constructs new resources. For example, Blum's protocol [2] constructs a coin flipping resource given bit commitment resource. In order to measure security of a constructed protocol we need an *ideal* reference protocol to allow for the comparison.

Definition A.0.3. Ideal functionality is a black box resource that provides a desired behavior.

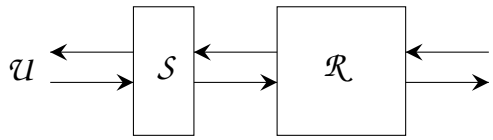


Figure A.1: Schematic depiction of a resource $\mathcal{R}$ and a connected converter $\mathcal{S}$ emulating operations of user $\mathcal{U}$. We write $\mathcal{S}_{\mathcal{U}}\mathcal{R}$ to denote the resulting resource. This can be simplified to $\mathcal{S}\mathcal{R}$ with convention that converters to the left of $\mathcal{R}$ belong to the user $\mathcal{U}$ and similarly the resources to the right belong to the user using right interface of $\mathcal{R}$.

We define a security of a constructed protocol $\mathcal{P}$ in terms of *distinguishability* from the corresponding ideal functionality $\mathcal{F}$.

Definition A.0.4. A **distinguisher** for resources $\mathcal{P}$ and $\mathcal{F}$ is an abstract system with two interfaces. An inside interface connects to either $\mathcal{P}$ or $\mathcal{F}$ and the outside interface produces a single bit providing a guess whether $\mathcal{P}$ or $\mathcal{F}$ is connected to the inside interface.

Definition A.0.5. A **distinguishing advantage** for a single distinguisher $\mathcal{D}$ for resources $\mathcal{P}$ and $\mathcal{F}$ is a pseudo-metric [29] defined as

$$d^{\mathcal{D}}(\mathcal{P},\mathcal{F}) = |P(\mathcal{D}(\mathcal{P}) = 0) - P(\mathcal{D}(\mathcal{F}) = 0)|$$

where $\mathcal{D}(\mathcal{P})$ is an output of $\mathcal{D}$ when connected to $\mathcal{P}$. A distinguishing advantage for a set of distinguishers $\mathbb{D}$ is defined by

$$d^{\mathbb{D}}(\mathcal{P},\mathcal{F}) = \sup_{\mathcal{D}\in\mathbb{D}} d^{\mathcal{D}}(\mathcal{P},\mathcal{F})$$

A security of a constructed resource $\mathcal{P}$ via protocol Π from an initial resource $\mathcal{R}$ is defined via probability of successfully distinguishing between $\mathcal{P}$ and ideal functionality $\mathcal{F}$ given set of all possible distiguishers relevant in the given settings. I.e. we might restrict the set of distinguishers to contain only computationally bounded distinguishers when proving computational security guarantees. Similarly, under different assumptions, computationally unbounded up to quantum distinguishers can be included. We argue about security of a constructed resource in three different settings: when both parties are honest, when Alice is dishonest and Bob is honest and vice-versa. The initial resources available to the players in the three cases are given by a tuple $\mathcal{R} = (R, R_A, R_B)$ where R_A is an initial resource available to a dishonest Alice and honest Bob, likely providing more functionalities to Alice. Similarly, the constructed resources are $\mathcal{P} = (\Pi_A R \Pi_B, R_A \Pi_B, \Pi_A R_B)$ where $\Pi = (\Pi_A, \Pi_B)$ is a tuple of converters emulating actions taken by Alice and Bob respectively. In case of a dishonest behaviour the protocol is removed from the corresponding interface of $\mathcal{R}$ since we do not know what steps the dishonest party follows. Most of the time $R_A\Pi_B$ and F_A can be trivially distinguished as dishonest Alice has no restrictions over her actions. Hence we limit the abilities of Alice by connecting a converter σ_A on her interface of F_A with the aim to make Alice weaker and hence possibly make the two systems indistinguishable. We shall call the converter in this setting a *simulator*. If $\sigma_A F_A$ is

indistinguishable from $R_A\Pi_B$ we can then safely use $R_A\Pi_B$ instead of $\Pi_A R\Pi_B$ since introducing the simulator σ_A only makes Alice weaker.

The security is hence defined via distinguishability between ($\Pi_A R\Pi_B$,$R_A\Pi_B$,$\Pi_A R_B$) and $\mathcal{F} = (F, F_A, F_B)$.

Definition A.0.6. A resource $\mathcal{F} = (F, F_A, F_B)$ is constructed within distance ε from $\mathcal{R} = (R, R_A, R_B)$ via protocol $\Pi = (\Pi_A, \Pi_B)$ with respect to a set of distinguishers $\mathbb{D}$ and set of simulators $\mathbb{S}$ if and only if

$$\begin{aligned} d^{\mathbb{D}}(\Pi_A R\Pi_B, F) &\leq \varepsilon \\ \exists \sigma_A \in \mathbb{S} : d^{\mathbb{D}}(R_A\Pi_B, \sigma_A F_A) &\leq \varepsilon \\ \exists \sigma_B \in \mathbb{S} : d^{\mathbb{D}}(\Pi_A R_B, \sigma_B F_B) &\leq \varepsilon \end{aligned}$$

We often abbreviate the above scenario to say $\mathcal{F}$ is ε-constructed from $\mathcal{R}$ by Π. There is also a convenient graphical representation of the conditions in Definition A.0.6 [31]:

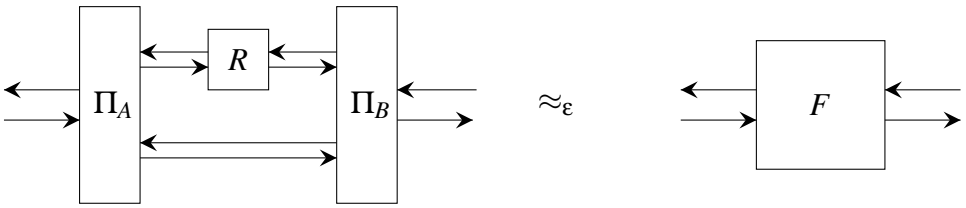


Figure A.2: $d^{\mathbb{D}}(\Pi_A R\Pi_B, F) \leq \varepsilon$

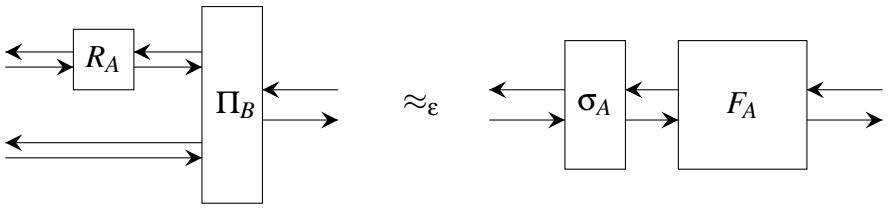


Figure A.3: $\exists \sigma_A : d^{\mathbb{D}}(R_A\Pi_B, \sigma_A F_A) \leq \varepsilon$

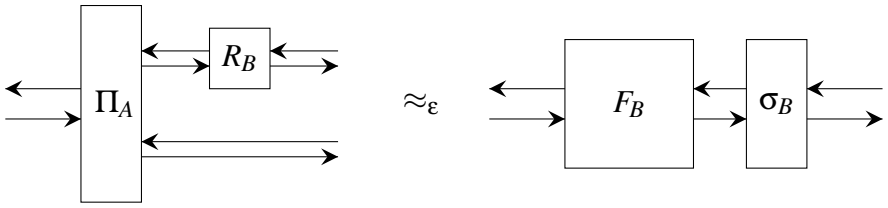


Figure A.4: $\exists \sigma_B : d^{\mathbb{D}}(\Pi_A R_B, F_B\sigma_B) \leq \varepsilon$

Appendix B

The Casual Boxes Framework

The *Abstract Cryptography Framework* (Appendix A) is unable to model relativistic cryptography. The extension is done via introducing *Causality condition* [31] which requires that outputs produced at a space-time point $\mathcal{P}$ can be dependent only on events inside the past lightcone of $\mathcal{P}$. The Minkowski-spacetime model is assumed.

In *Abstract Cryptography Framework* the classical/quantum messages exchanged through interfaces of *resources* and *converters* are points in a state space of the corresponding quantum system (classical system can be considered as a special case of the quantum system) that can be generally represented as a Hilbert space $\mathcal{H}$. A casual box is an extension of a *resource* where interfaces can carry arbitrary number (or a superposition of different numbers) of messages where each message is annotated with an ordering label from a countable, partially ordered set $\mathcal{T}$. The precedence operator $t_\alpha \prec t_\beta$ on messages (α, t_α) and (β, t_β) depicts that message β is in future light cone of α, see Figure B.1 for a schematic depiction.

Definition B.0.1. A **casual box** is a map from $\mathcal{H} \otimes l^2(\mathcal{T})$ to itself that respects causality condition where $l^2(\mathcal{T})$ is a sequence space induced by l^2 norm.

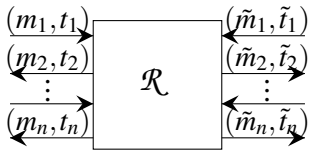
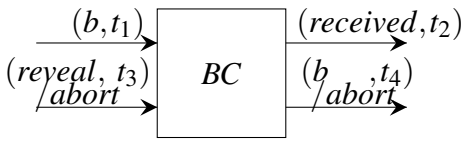


Figure B.1: A schematic depiction of a Casual box with an example of a defined partial order on messages $m_1, \ldots, m_n, \tilde{m}, \ldots \tilde{m}_n$.

The key property of Casual Boxes we shall need is composability. Indeed, in [27] a proof is provided that Casual Boxes can be arbitrarily composed with itself or other Casual Boxes while still providing security guarantees. The proof is complex and out of scope of this project report, although it has essential use in the proofs used in it.

B.1 Bit Commitment in Casual Boxes Framework

We define the ideal Bit Commitment functionality in honest case *BC* as a casual box



$$t_1 \prec t_2 \prec t_3 \prec t_4$$

Figure B.2: Bit Commitment Casual Box for honest Alice and honest Bob.

During the commitment phase, Alice inputs her chosen commitment bit b. Bob is then notified about Alice's action by a *received* message. Alice later on decides whether she reveals the bit b to Bob or whether she aborts the protocol. Note, that many implementations are feasible, for example, *abort* is triggered as well if Alice does not execute reveal phase in some specified space-time region. Bob then receives either the bit b or the *abort* message.

B.2 Biased Coin Flipping in Casual Boxes Framework

A p-biased coin flipping resource $\mathcal{CF}^p = (CF^p, CF_A^p, CF_B^p)$ outputs the same random bit c to both of the involved parties. If either party is dishonest, it has probability p of altering the coin flip outcome. Schematically, it is convenient to express the functionality in Casual Boxes as follows.

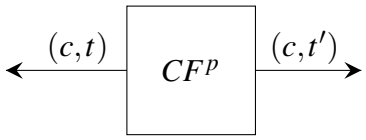
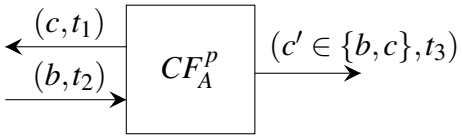
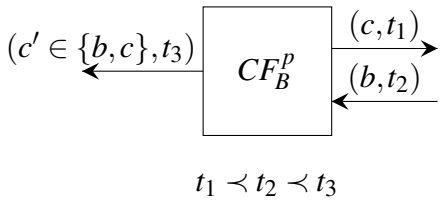


Figure B.3: Biased Coin Flipping Casual Box for honest Alice and honest Bob.



$$t_1 \prec t_2 \prec t_3$$

Figure B.4: Biased Coin Flipping Casual Box for dishonest Alice and honest Bob. $c' = b$ with probability p and $c' = c$ otherwise.



$$t_1 \prec t_2 \prec t_3$$

Figure B.5: Biased Coin Flipping Casual Box for honest Alice and dishonest Bob. $c' = b$ with probability p and $c' = c$ otherwise.

Bibliography

[1] Abhishek Banerjee and Alon Peikert, Chrisand Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 719–737, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[2] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, January 1983.

[3] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, oct 2018.

[4] Ran Canetti. A unified framework for analyzing security of protocols. *http://eprint. iacr. org/2000/067/*, 2000.

[5] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.

[6] Ran Canetti and Marc Fischlin. Universally composable commitments. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, pages 19–40, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[7] André Chailloux, María Naya-Plasencia, and André Schrottenloher. Cryptology eprint archive, report 2017/847. In *2017 International Conference on Computing, Networking and Communications (ICNC)*, pages 211–240, 11 2017.

[8] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Robust relativistic bit commitment. *Physical Review A*, 94, 08 2016.

[9] Sarah Croke and Adrian Kent. Security details for bit commitment by transmitting measurement outcomes. *Physical Review A*, 86, 08 2012.

[10] Grégory Demay and Ueli Maurer. Unfair coin tossing. *2013 IEEE International Symposium on Information Theory*, pages 1556–1560, 2013.

[11] Vedran Dunjko, Joseph F Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–425. Springer, 2014.

[12] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, June 1985.

[13] Elloá Guedes, Francisco de Assis, and BERNARDO LULA. Quantum attacks on pseudorandom generators. *Mathematical Structures in Computer Science*, 23, 06 2013.

[14] Shai Halevi and Silvio Micali. Practical and provably-secure commitment schemes from collision-free hashing. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 201–215, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[15] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, pages 411–428, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[16] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, Nov 2011.

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

[18] Joe Kilian. Founding crytpography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 20–31, New York, NY, USA, 1988. ACM.

[19] M. Lemus, P. Yadav, P. Mateus, N. Paunković, and A. Souto. On minimal assumptions to obtain a universally composable quantum bit commitment. In *2019 21st International Conference on Transparent Optical Networks (ICTON)*, pages 1–4, July 2019.

[20] Linxi Zhang, Nan Zhao, Changxing Pei, and Long Wang. A novel single agent quantum bit commitment scheme. In *2017 International Conference on Computing, Networking and Communications (ICNC)*, pages 126–130, 2017.

[21] Hoi-Kwong Lo and H. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78, 08 1998.

[22] Hristo Lulev. Overview of bit commitment schemes. *Bachelor Thesis*. Darmstadt University of Technology. Bachelor's thesis, Darmstadt University of Technology, 2007.

[23] Ueli Maurer and Renato Renner. Abstract cryptography. In *IN INNOVATIONS IN COMPUTER SCIENCE*. Tsinghua University Press, 2011.

[24] Dominic Mayers. The trouble with quantum bit commitment, 1996.

[25] Moni Naor. Bit commitment using pseudo-randomness. In Gilles Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 128–136, New York, NY, 1990. Springer New York.

[26] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[27] C. Portmann, C. Matt, U. Maurer, R. Renner, and B. Tackmann. Causal boxes: Quantum information-processing systems closed under composition. *IEEE Transactions on Information Theory*, 63(5):3277–3305, May 2017.

[28] Christopher Portmann. Quantum authentication with key recycling. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 339–368. Springer, 2017.

[29] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. *ArXiv*, abs/1409.3525, 2014.

[30] Dominique Unruh. Universally composable quantum multi-party computation. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 486–505, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[31] V Vilasini, Christopher Portmann, and Lídia del Rio. Composable security in relativistic quantum cryptography. *New Journal of Physics*, 21(4):043057, apr 2019.

[32] John Watrous. Lecture 15: quantum information revisited (continued). `https://cs.uwaterloo.ca/~watrous/LectureNotes/CPSC519.Winter2006/15.pdf`, 2016 (accessed March 25, 2020).