Converting the flavor of a quantum bit commitment

Frédéric Légaré

School of Computer Science
McGill University, Montréal

November, 2000

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Master of Science.

Résumé

Les résultats presentés dans le mémoire montrent comment on peut convertir une mise en gage de bit quantique statistiquement liante et calculatoirement camouflante en une mise en gage de bit quantique calculatoirement liante et statistiquement camouflante. Pour un paramètre de sécurité n, la construction de la mise en gage statistiquement camouflante requiert $O(n^2)$ appels à la mise en gage statistiquement liante. Une conséquence de la réduction est qu'une mise en gage de bit quantique calculatoirement liante et statistiquement camouflante peut se baser sur l'existence de n'importe quelle famille de fonctions à sens unique quantiques. On a découvert aucune réduction équivalente dans le monde classique.

Mots-clés: cryptographie quantique, mise en gage de bit, transfert inconscient, fonction à sens unique.

Abstract

The results presented in the thesis show how to convert a statistically binding but computationally concealing quantum bit commitment scheme into a computationally binding but statistically concealing scheme. For a security parameter n, the construction of the statistically concealing scheme requires $O(n^2)$ executions of the statistically binding scheme. As a consequence of the reduction, statistically concealing but computationally binding quantum bit commitments can be based upon any family of quantum one-way functions. Such a construction is not known to exist in the classical world.

Keywords: quantum cryptography, bit commitment, oblivious transfer, one-way function.

Remerciements

Je voudrais souligner l'apport de certaines personnes et organisations:

- Louis Salvail avec qui j'ai partagé les joies de la recherche ainsi que les moments moins agréables de la rédaction. Sans lui, je ne me serais pas rendu si loin; sans lui, mon mémoire ne serait pas ce qu'il est.
- Mon directeur de maîtrise, Claude Crépeau, qui a su orienter mes recherches et m'appuyer dans les différentes étapes de mes études de maîtrise.
- Zero-Knowledge Systems et, en particulier, Adam Shostack qui m'ont fourni temps et ressources pour terminer cet ouvrage.
- Paul Dumais, Christian Paquin et Jean-François Raymond qui m'ont apporté support moral et technique.
- Le Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Fonds FCAR) qui m'a permis de manger tout ce temps-là :).

- Mes parents, Monique et Robert, et ma copine, Caroline, que je me dois d'inclure, car s'il en était autrement, j'en entendrais parler longtemps :).

Merci!

Contents

Chapter 1

Introduction

Throughout human history, groups of individuals have tried to protect information while others have tried to gain access to it. These two opposing behaviors define the essence of cryptology and relate to cryptography and cryptanalysis respectively. More formally, cryptography is the study of mathematical techniques used to enforce information security. On the other hand, cryptanalysis is the study of mathematical techniques used to defeat cryptographic techniques and, more generally, information security services. Cryptology is simply the combination of both disciplines.

In 1969, for the first time quantum information processing was foreseen as a possible way to better accomplish cryptologic tasks [24]. It was the birth of quantum cryptology. Since then, outstanding contributions from quantum physics were made to both cryptography and cryptanalysis. Probably the most illustrious achievement in quantum cryptography was the discovery of a quantum key distribution protocol [2]. Using quantum information we can achieve an efficient QKD with unconditional security (i.e. do not depend on any computational assumption). On the other, quantum computation provided cryptanalysts with powerful tools such as an algorithm to factor or compute discrete logarithm efficiently [23]. Another remarkable result for quantum cryptanalysis was the quadratic speed-up for database search [13].

Researchers learned the hard way that quantum cryptography had also its limitations. In the beginning of the 90s, the scientific community was convince that bit commitment could be achieved with security relying solely on laws of quantum mechanics [5]. A bit commitment scheme is a cryptographic task involving two participants Alice and Bob. Alice wants to commit to a bit b but without Bob knowing the bit until she decides to open the commitment. We say a bit commitment protocol is binding if Alice is unable to change her mind and concealing if Bob cannot determine b before the opening of the commitment. A cold rain fell on the scientific community when unconditional security for quantum bit commitment was proven impossible [19, 20, 18].

Though unconditional security was impossible, one could still hope to base the security of quantum bit commitment on a computational assumption. A quantum one-way function must be easy to compute with a quantum computer but hard to invert even using quantum computations. Since there is a difference of power between classical and quantum computers, we do not have direct inclusion between the two respective sets of one-way functions. In computationally secure bit commitment, we have to sacrifice the unconditional security of only one of the two participants. Hence, there are two possible flavors: unconditionally binding and computationally concealing or computationally binding and unconditionally concealing. The two flavors allow different cryptographic applications. For example, computational zero-knowledge proofs [11, 12] can be constructed from unconditionally binding commitments whereas perfect zero-knowledge arguments [4] require unconditionally concealing commitments. Arguments can be used whenever the verifier is not restricted in computing power and proofs can be used whenever the prover has unlimited computing power. Arguments are preferable in some settings, since a dishonest prover for an argument must break the complexity assumption on-line in order to prove a false theorem, whereas a dishonest verifier involved in a computational zero-knowledge proof can spend unlimited time after the end of the protocol in order to extract additional knowledge. Classically, the two flavors seem to require different computational assumptions.

In the case of unconditionally binding commitments, the existence of a family of classical one-way function is sufficient. The reduction is divided into two parts: the existence of a one-way function implies the existence of a pseudo-random bit generator [15, 14] and the existence of a pseudo-random generator implies the existence of a unconditionally binding and computationally concealing bit commitment [21]. The two part proof also holds in the quantum setting.

For unconditionally concealing commitments, the weakest computational assumption for which a reduction was found is the existence of a family of classical one-way permutations [22]. However, the proof is not extendable to the quantum world [9]. Nevertheless, it was proven that computationally binding and unconditionally concealing quantum bit commitment can be based on any family of quantum one-way permutations [9]. Unfortunately, although we have candidates for quantum one-way functions [10], none of them is a permutation. It was still to be establish whether computationally binding and unconditionally concealing quantum bit commitment could rely on a weaker computational assumption, that is quantum one-way function.

New Results. Our main contribution consists in showing how any statistically binding quantum bit commitment scheme can be transformed into a statistically concealing one. Informally, statistical security is defined as unconditional security where an adversary is allowed a negligible probability of cheating (as opposition to perfect security). Our result relies heavily upon the QOT protocol for quantum 1-out-of-2 oblivious transfer [7, 6]. The QOT protocol can be seen as a construction of a secure quantum oblivious transfer from a black-box for bit commitment [7, 6, 25]. Therefore, unlike the classical case, there exists a black-box reduction of quantum oblivious transfer to bit commitment. The construction of a statistically concealing quantum bit commitment scheme is obtained by using the QOT protocol together with a statistically binding but otherwise computationally concealing commitment scheme (this commitment will be called *initial commitment* in the following). Using the QOT protocol that way, we construct a simple quantum commitment scheme that we show statistically concealing and computationally binding. The construction requires $O(n^2)$ executions of the initial commitment scheme for n a security parameter. As a by-product, we show that the QOT protocol is an oblivious transfer that statistically hides one out of the two bits sent and computationally conceals the receiver's selection bit whenever it is used together with statistically binding but computationally concealing commitments instead of perfect commitments given as black-boxes. This extends the security result for the QOT protocol of [7, 6, 25] to this case. Our reduction of an adversary for the concealing condition of the initial commitment scheme to an adversary for the binding condition of the resulting commitment scheme is an expected polynomial-time black-box reduction. Although quantum information has peculiar behaviors adding complexity to the security proofs of cryptographic protocols, we shall see that using quantum oblivious transfer as a primitive allows to return to an essentially classical situation. This might be of independent interest for the construction and analysis of complex quantum protocols.

One consequence of our result is that statistically concealing but computationally binding quantum commitment scheme can be based upon any quantum one-way function using Naor's construction [21] from pseudo-random generators. Only the ability to send and receive BB84 qubits [2] is required in order to get the new flavor. The scheme can therefore be implemented using current technology. Our result gives more evidence that computational security in 2-party quantum cryptography enjoys different properties than its classical counterpart [16].

The work presented in the thesis largely overlaps the content of a paper written in collaboration with Claude Crépeau and Louis Salvail and accepted for Eurocrypt 2001. Although the original ideas for the security proofs are mine, Claude Crépeau and Louis Salvail greatly contributed in developing and formalizing the reasoning.

Chapter 2

Preliminaries

2.1 Notations and Model of Computation

For simplicity, we shall often drop the security parameters associated with protocol executions. When protocols and adversaries are modeled as circuits they should be understood as infinite families of circuits, one circuit for each possible values of the security parameters. We define $poly(n) = \bigcup_{k \geq 0} O(n^k)$ as the set of all functions upper bounded by a positive polynomial. We say a positive function $f(n)$ is negligible if for all $p(n) \in poly(n)$ and n sufficiently large we have $f(n) < \frac{1}{p(n)}$. Accordingly, we say that a function $g(n)$ is overwhelming if $1 - g(n)$ is negligible.

Let $\mathcal{H}_n$ denote a n-dimensional Hilbert space, that is a complete inner product vector space over the complex numbers. The basis $\{|0\rangle, |1\rangle\}$ denotes the computational or rectilinear or "+" basis for $\mathcal{H}_2$. When the context requires, we write $|b\rangle_+$ to denote the bit b in the rectilinear basis. The diagonal basis, denoted "$\times$", is defined as $\{|0\rangle_\times, |1\rangle_\times\}$ where $|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The states $|0\rangle, |1\rangle, |0\rangle_\times$ and $|1\rangle_\times$ are the four BB84 states. For any $x \in \{0,1\}^n$ and $\theta \in \{+,\times\}^n$, the state $|x\rangle_\theta$ is defined as $\otimes_{i=1}^n |x_i\rangle_{\theta_i}$ where $\otimes$ denotes the tensor product. An orthogonal (or von Neumann) measurement of a quantum state in $\mathcal{H}_m$ is described by a set of m orthogonal projections $\mathcal{M} = \{\mathbb{P}_i\}_{i=1}^m$ acting in $\mathcal{H}_m$ thus satisfying $\sum_i \mathbb{P}_i = \mathbb{1}_m$ for $\mathbb{1}_m$ denoting the identity operator in $\mathcal{H}_m$. Each projection or equivalently each index $i \in \{1, \ldots, m\}$ is a possible classical outcome for $\mathcal{M}$.

We model quantum algorithms by quantum circuits built out of a universal set of quantum gates $\mathcal{UG} = \{\mathtt{CNot}, \mathtt{H}, \mathtt{R}_{\mathbb{Q}}\}$, where CNot denotes the controlled-NOT, H the one qubit Hadamard gate, and $\mathtt{R}_{\mathbb{Q}}$ is an arbitrary one qubit non-trivial rotation specified by a matrix containing only rational numbers [1]. The time-complexity of a quantum circuit C is the number of elementary gates $\|C\|_{\mathcal{UG}}$ in $\mathcal{C}$. In addition to the set of gates $\mathcal{UG}$, a quantum circuit is allowed to perform one kind of von Neumann measurement: $\mathcal{M}_+ = \{\mathbb{P}_0^+, \mathbb{P}_1^+\}$ where $\mathbb{P}_0^+ = |0\rangle\langle 0|$ and $\mathbb{P}_1^+ = |1\rangle\langle 1|$ are the two orthogonal projections of the computational basis. $\mathcal{M}_+$ is sometimes called the measurement in the *rectilinear* or *computational* basis. Another von Neumann measurement used by the receiver in the BB84 quantum coding scheme is the measurement in the *diagonal* basis $\mathcal{M}_\times = \{\mathbb{P}_0^\times, \mathbb{P}_1^\times\}$ for $\mathbb{P}_0^\times = \frac{1}{2}(|0\rangle + |1\rangle)^\dagger(|0\rangle + |1\rangle)$ and $\mathbb{P}_1^\times = \frac{1}{2}(|0\rangle - |1\rangle)^\dagger(|0\rangle - |1\rangle)$ where † denotes the transposed-complex conjugate operator. The Hadamard gate $\mathtt{H}$ is sufficient to build measurement $\mathcal{M}_\times \in \mathcal{UG}$ from $\mathcal{M}_+$ since $\mathcal{M}_\times = \{\mathtt{H}^\dagger\mathbb{P}_0^+\mathtt{H}, \mathtt{H}^\dagger\mathbb{P}_1^+\mathtt{H}\}$. If $|\Psi\rangle \in H_A \otimes H_B$ is a composite quantum state, we write $\mathbb{P}_x^A|\Psi\rangle$ (i.e. $\mathbb{P}_x^A \otimes \mathbb{1}^B|\Psi\rangle$) for the projector applied to the registers in H_A along the state $|x\rangle$ for $x \in \{0,1\}^{\mathrm{Dim}(H_A)}$. The classical output $L(|\Psi\rangle)$ of circuit L is the classical outcomes of all von Neumann measurements $\mathcal{M}_+$ taking place during the computation $L|\Psi\rangle$. If the circuit L accepts two input states of the form $|\Psi_0\rangle \otimes |\Psi_1\rangle$ we may write similarly $L(|\Psi_0\rangle, |\Psi_1\rangle)$ for the classical output.

A 2-party quantum protocol is a pair of interactive quantum circuits (A, B) applied to some initial product state $|x_A\rangle^A \otimes |x_B\rangle^B$ representing A's and B's inputs to the protocol neglecting to write explicitly the states of A's and B's registers that do not encode their respective input to the protocol (thus all in initial states $|0\rangle$). Also, we shall often write $|x_A\rangle^A|x_B\rangle^B$ for the product state without explicitly writing the tensor product $\otimes$. Since communication takes place between A and B, the complete circuit representing one protocol execution may have quantum gates in A and B acting upon the same quantum registers. We write $A \odot B$ for the complete quantum circuit when A is interacting with B. The final composite state $|\Psi_{final}\rangle$ obtained after the execution is written $|\Psi_{final}\rangle = (A \odot B)|x_A\rangle^A |x_B\rangle^B$. Protocols are to be understood, although not explicitly stated, as specified by families of circuits, one for each possible value of the security parameter n. If for a participant (adversary) $\mathcal{P}$ given 1^n as input there exists a classical Turing machine that efficiently computes the description of the circuit P_n to be run for security parameter n then $\mathcal{P}$ is said to be a *uniform* participant (adversary); that is $\mathcal{P}$ is modeled by a uniform family of quantum circuits. Otherwise, P is said to be non-uniform.

2.2 Cryptographic Primitives

The two relevant quantum primitives we shall use heavily in the following are quantum bit commitment and quantum oblivious transfer. They are defined as straightforward quantum generalizations of their classical counterparts.

2.2.1 Quantum Bit Commitment

A quantum bit commitment scheme is defined by two quantum protocols $((C^A, C^B), (O^A, O^B))$ where (C^A, C^B) is a pair of interactive quantum circuits for the committing stage and (O^A, O^B) is a pair of interactive quantum circuits for the opening stage (i.e. A being the committer and B the receiver). The committing stage generates the state $|\Psi_b\rangle = (C^A \odot C^B)|b\rangle^A|0\rangle^B$ upon which the opening stage is executed: $|\Psi_{final}\rangle = (O^A \odot O^B)|\Psi_b\rangle$. The binding condition of a quantum bit commitment is slightly more general than the usual classical definition. An adversary $\tilde{A} = (C^{\tilde{A}}, O^{\tilde{A}})$ is such that $|\tilde{\Psi}\rangle = (C^{\tilde{A}} \odot C^B)|0\rangle^{\tilde{A}}|0\rangle^B$ is generated during the committing stage. The dishonest opening circuit $O^{\tilde{A}}$ tries to open $b \in \{0,1\}$ given as an extra input bit $|b\rangle^{\tilde{A}}$. Given the final state $|\tilde{\Psi}_{final}\rangle = (O^{\tilde{A}} \odot O^B)|b\rangle^{\tilde{A}}|\tilde{\Psi}\rangle$ we define $s_b(n)$ as the probability to open b with success. More precisely, $s_b(n) = \|\mathbb{P}^B_{OK,b}|\tilde{\Psi}_{final}\rangle\|^2$ where $\mathbb{P}^B_{OK,b}$ is Bob's projection operator on the subspace leading to accept the opening of b. An adversary $\tilde{A}$ of the binding condition who can open $b = 0$ with probability at least $s_0(n)$ and open $b = 1$ with probability at least $s_1(n)$ will be called a $(s_0(n), s_1(n))$–*adversary against the binding condition.* We define the concealing and binding criteria similarly to [9]:

(computationally) binding: There exists no quantum $(s_0(n), s_1(n))$–adversary $\tilde{A}$ and positive polynomial $p(n)$ such that $s_0(n)+s_1(n) \geq 1+\frac{1}{p(n)}$ for n sufficiently large. The scheme is *computationally binding* if we add the restriction that $\|\tilde{A}\|_{\mathcal{UG}} \in poly(n)$.

(computationally) concealing: For every interactive quantum circuit $\tilde{C}^B$ for the committing stage, all quantum circuits $L^{\tilde{B}}$ acting only upon $\tilde{B}$'s registers, all positive polynomials $p(n)$ and n sufficiently large, $\mathrm{P}\left(L^{\tilde{B}}((C^A \odot C^{\tilde{B}})|b\rangle^A|0\rangle^{\tilde{B}}) = b\right) < \frac{1}{2} + \frac{1}{p(n)}$ where the probabilities are taken over $b \in_R \{0,1\}$. The scheme is *computationally concealing* if we add the restriction $\|C^{\tilde{B}}\|_{\mathcal{UG}} + \|L^{\tilde{B}}\|_{\mathcal{UG}} \in poly(n)$.

What we call concealing and binding is in fact statistically concealing and statistically binding respectively and not perfectly concealing and perfectly binding.

2.2.2 Quantum Oblivious Transfer

In the following, we shall restrict our attention to 1–2 quantum oblivious transfer (i.e. one-out-of-two oblivious transfer) [6, 8]. A 1–2 *quantum oblivious transfer protocol* involves a sender Alice holding input bits (b_0, b_1) and a receiver Bob holding input $c \in \{0,1\}$. Alice sends (b_0, b_1) to Bob in such a way that Bob receives only b_c and Alice does not get to know c. The receiver must not be able to find $b_{\overline{c}}$ for at at least one $\overline{c} \in \{0,1\}$ and even given b_c. More precisely, a protocol (A, B) for 1–2 quantum oblivious is such that $|\Psi(b_0, b_1, c)\rangle = (A \odot B)|b_0 b_1\rangle^A|c\rangle^B$ allows Bob to recover b_c from applying

$\mathcal{M}_+$ upon one of his registers. A protocol for 1–2 quantum oblivious transfer is *(computationally) secure* if it is both

(computationally) secure against the sender: For all quantum sender $\tilde{A}$, all quantum circuit $L^{\tilde{A}}$ acting only on $\tilde{A}$'s registers, all positive polynomials $p(n)$ and n sufficiently large, $\mathrm{P}\left(L^{\tilde{A}}((\tilde{A} \odot B)|00\rangle^{\tilde{A}}|c\rangle^{B}) = c\right) < \frac{1}{2} + \frac{1}{p(n)}$ where the probabilities are taken over $c \in_R \{0,1\}$. The security is *computational* if we add the restriction $\|L^{\tilde{A}}\|_{\mathcal{UG}} + \|\tilde{A}\|_{\mathcal{UG}} \in poly(n)$.

(computationally) secure against the receiver: For every quantum receiver $\tilde{B}$, all quantum circuits $L^{\tilde{B}}$ acting only on $\tilde{B}$'s registers, all positive polynomials $p(n)$ and n sufficiently large, there exists a random variable c with possible outcome 0 or 1 depending on $(A \odot \tilde{B})|b_0 b_1\rangle^{A}|0\rangle^{\tilde{B}}$ satisfying $\mathrm{P}\left(L^{\tilde{B}}((A \odot \tilde{B})|b_0 b_1\rangle^{A}|0\rangle^{\tilde{B}}, |b_c\rangle^{\tilde{B}}) = b_{\bar{c}}\right) < \frac{1}{2} + \frac{1}{p(n)}$ where the probabilities are taken over $b_0, b_1 \in_R \{0,1\}$. The security is *computational* if we add the restriction $\|\tilde{B}\|_{\mathcal{UG}} + \|L^{\tilde{B}}\|_{\mathcal{UG}} \in poly(n)$.

As for bit commitment, the security against the sender and the security against the receiver is not perfect but statistical.

2.3 Tools

Let $X \sim B(p)$ be a Bernoulli random variable with probability of success p (when $X = 1$). The following tools are used on multiple occasions in the security proofs presented in chapter 4.

2.3.1 Hybrid Argument

Let $\mathcal{X} = \{X_0, X_1, \ldots, X_n\}$ be a set of independent random variables $X_i \sim B(p_i)$ for $0 \leq i \leq n$. Then, there exist $0 \leq k < n$ such that,

$$|p_{k+1} - p_k| \geq \frac{|p_n - p_0|}{n}. \tag{2.1}$$

The result also holds without the absolute values, but is non-trivial only if $p_n > p_1$. This simple argument is also used in other cryptographic proofs [14].

2.3.2 Bernshtein's Law of Large Numbers

Theorem 2.3.1 (Bernshtein) *Let $X_1, X_2, \ldots, X_n \sim B(p)$ be independent random variables following a Bernoulli distribution with p as the probability parameter. Then for any $0 < \epsilon \leq p(1-p)$,*

$$\mathrm{P}\left(\left|\frac{\sum_{i=1}^{n} X_i}{n} - p\right| \geq \epsilon\right) \leq 2e^{-n\epsilon^2}$$

In particular, Bernshtein's law of large numbers ensures us that we can estimate the probability of an event with an error bounded by any polynomial except with negligible probability using a polynomial number of random variables. For example, if we want to estimate p with an error bounded by $\epsilon = \frac{1}{p(m)}$ then with $n = \lceil mp(m)^2 \rceil$ random variables we obtain a correctly bounded estimate with probability at least $1 - 2e^{-m}$.

2.3.3 Estimating Polynomial Variation

Suppose we have a quantum circuit $\mathtt{R_n}$ allowing to sample from a Bernoulli distribution with unknown parameter $p_n = q + \frac{1}{p(n)}$ where $0 \leq q < 1$ is a known constant and $p(n)$ is some positive polynomial. That is $\mathrm{P}\left(\mathtt{R_n} = 1\right) = p_n$ and $\mathrm{P}\left(\mathtt{R_n} = 0\right) = 1 - p_n$ independently for each execution of $\mathtt{R_n}$. The following classical procedure uses the quantum sampling circuit $\mathtt{R_n}$ as a black-box to provide a lower bound $\frac{1}{g_n}$ for $\frac{1}{p(n)}$ with overwhelming probability:

$\mathtt{LowBound}(\mathtt{R_n}, q, n)$

1. $\tilde{p}_n = 0$; $g_n = 1$;

2. `While` $\tilde{p}_n \leq q + \frac{2}{g_n}$ `Do`

    (a) $g_n = g_n n$;

(b) $sampling = ng_n^2$;

(c) $success = 0$;

(d) `For` $1 \leq i \leq sampling$ `Do` $success = success + \mathtt{R_n}$;

(e) $\tilde{p}_n = \frac{success}{sampling}$;

3. `Return:` $\frac{1}{g_n}$.

Lemma 2.3.2 *For n sufficiently large,* $\mathtt{LowBound}(\mathtt{R_n}, q, n)$ *returns $\frac{1}{g_n}$ such that $\frac{1}{n^2 p(n)} < \frac{1}{g_n} \leq \frac{1}{p(n)}$ except with probability $2^{-\alpha n}$ for $\alpha > 0$ constant and after calling $\mathtt{R}_n$ an expected $O(n^5 p(n)^2)$ times.*

Proof: For n sufficiently large, there exist a constant c such that

$$\frac{1}{n^{c+1}} < \frac{1}{p(n)} \leq \frac{1}{n^c}. \tag{2.2}$$

Hence, there exists at least one constant k such that for all $i \geq k+2$ and $j \leq k$

$$\frac{3}{n^i} < \frac{1}{p(n)} \leq \frac{1}{n^j}. \tag{2.3}$$

Let k' be the smallest constant satisfying (2.3).

By Bernshtein's law of large numbers, the obtained estimate $\tilde{p}_n(t)$ in the t-th repetition of step 2 has a bounded error $\frac{1}{g_n(t)} = \frac{1}{n^t}$ with probability at least $1-2e^{-n}$. So, for $j \leq k'$ we have with probability at least $1-2e^{-n}$

$$\tilde{p}_n(j) \leq q + \frac{1}{p(n)} + \frac{1}{n^j} \leq q + \frac{2}{n^j} = q + \frac{2}{g_n(j)} \tag{2.4}$$

and the number of repetition of step 2 is greater than k' with probability at least $(1-2e^{-n})^{k'}$. Moreover, for $i \geq k'+2$ we have again with probability at least $1-2e^{-n}$

$$\tilde{p}_n(i) \geq q + \frac{1}{p(n)} - \frac{1}{n^i} > q + \frac{2}{n^i} = q + \frac{2}{g_n(i)} \tag{2.5}$$

and so the probability of executing more than $k'+2$ repetitions of step 2 is lower then $2e^{-n}$. Hence the procedure will repeat step 2 either $k'+1$ or $k'+2$ and respectively output $\frac{1}{n^{k'+1}}$ or $\frac{1}{n^{k'+2}}$ except with negligible probability smaller than $2^{-\alpha n}$ for some $\alpha > 0$. By definition of k' we have that

$$\frac{1}{n^2 p(n)} \leq \frac{1}{n^{k'+2}}, \frac{1}{n^{k'+1}} < \frac{1}{p(n)}. \tag{2.6}$$

Hence, the number of calls to $\mathtt{R}_n$ in any of the first $k'+2$ rounds is at most $n^5 p(n)^2$ and since (2.5) the expected total number of calls to $\mathtt{R}_n$ is in $O(n^5 p(n)^2)$. □

2.3.4 Finding a Polynomial Drop Between Neighbors

Let $\mathcal{D}_m(\frac{1}{p(n)}) = \{p_i\}_{i=0}^m$ be a family of Bernoulli distributions with unknown parameters $0 \leq p_i \leq 1$ for every $0 \leq i \leq m$ and such that $p_{k^*} - p_{k^*+1} \geq \frac{1}{p(n)}$

for some $0 \leq k^* < m$. Let $\mathtt{S}$ be a quantum circuit such that $\mathrm{P}\left(\mathtt{S}|l\rangle = 1\right) = p_l$ and $\mathrm{P}\left(\mathtt{S}|l\rangle = 0\right) = 1 - p_l$ for all $0 \leq l \leq m$. That is, $\mathtt{S}$ is a quantum circuit allowing to sample from the Bernoulli distribution $B(p_l)$ given classical input $|l\rangle$. We would like to find κ that exhibits a polynomial drop $p_\kappa - p_{\kappa+1}$ similar to $p_{k^*} - p_{k^*}$. Algorithm `FindDrop` finds κ using the sampling circuit $\mathtt{S}$ as a black-box but is otherwise classical:

`FindDrop`$(\mathtt{S}, \frac{1}{p(n)}, n)$

1. $\tilde{p}_{-1} = 0; k = -1;$
2. `Loop:`
   (a) $k = k + 1$; $success = 0$;
   (b) `For` $i = 1$ `to` $\lceil 64mnp(n)^2 \rceil$ `Do` $success = success + \mathtt{S}|k\rangle$;
   (c) $\tilde{p}_k = success / \lceil 64mnp(n)^2 \rceil$;
3. `Until` $(\tilde{p}_{k-1} - \tilde{p}_k \geq \frac{3}{4p(n)})$ `or` $(k = m)$
4. `Return` κ=$k - 1$.

The returned value κ can now be shown to satisfy $p_\kappa - p_{\kappa+1} \geq \frac{1}{2}(p_{k^*} - p_{k^*+1})$ except with negligible probability. The algorithm is efficient in terms of $\|\mathtt{S}\|_{\mathcal{UG}}$, and parameters m and n.

Lemma 2.3.3 *Given a family of Bernoulli distributions* $\mathcal{D}_m(\frac{1}{p(n)}) = \{p_i\}_{i=1}^m$ *with sampling circuit* `S` *such that* $p_{k^*} - p_{k^*+1} \geq \frac{1}{p(n)}$ *for some* $0 \leq k^* \leq m-1$, *algorithm* `FindDrop`$(\mathtt{S}, \frac{1}{p(n)}, n)$ *returns* κ *such that* $p_\kappa - p_{\kappa+1} \geq \frac{1}{2p(n)}$ *except with negligible probability* $2^{-\alpha n}$ *for* $\alpha > 0$ *constant and after calling* `S` *at most* $(m+1)\lceil 64mnp(n)^2 \rceil \in O(m^2np(n)^2)$ *times.*

Proof: By Bernshtein's law of large numbers, $\tilde{p}_k$ as a bounded error $\frac{1}{8p(n)}$ with probability at least $1 - 2e^{-mn}$. So, with probability at least $(1 - 2e^{-mn})^{m+1}$ the estimate $\tilde{p}_k$ is within bounded errors $\frac{1}{8p(n)}$ of p_k for all $0 \leq k \leq m$. In that case, we have for $0 \leq i \leq m-1$ such that $p_i - p_{i+1} < \frac{1}{2p(n)}$

$$\tilde{p}_i - \tilde{p}_{i+1} \leq p_i - p_{i+1} + \frac{2}{8p(n)} < \frac{3}{4p(n)} \tag{2.7}$$

and also for $0 \leq j \leq m-1$ such that $p_j - p_{j+1} \geq \frac{1}{p(n)}$

$$\tilde{p}_j - \tilde{p}_{j+1} \geq p_j - p_{j+1} - \frac{2}{8p(n)} \geq \frac{3}{4p(n)}. \tag{2.8}$$

The algorithm `FindDrop` returns a bad κ whenever $p_\kappa - p_{\kappa+1} < \frac{1}{2p(n)}$ but $\tilde{p}_k - \tilde{p}_{\kappa+1} \geq \frac{3}{4p(n)}$ or whenever k^* could not be recognized. By equation 2.7 and 2.8, the probability p_e that `FindDrop` makes a mistake in the output satisfies $p_e \leq 1 - (1 - 2e^{-mn})^{m+1} \leq 2^{-\alpha n}$ for some $\alpha > 0$. The second inequality is easily obtained by expanding with the Newton's binomial theorem and bounding terms. $\square$

Chapter 3

Protocols

3.1 The QOT Protocol

The QOT protocol [7, 6] is based upon the BB84 quantum coding scheme [2]. If the receiver (Bob) of a random BB84 qubit $|s\rangle_\beta, s \in_R \{0,1\}, \beta \in_R \{+,\times\}$ measures it in basis $\hat{\beta} \in_R \{+,\times\}$ upon reception, then a noisy classical communication of bit s from Alice to Bob is implemented. Moreover, if later on Alice announces β, then Bob knows that he received s whenever $\beta = \hat{\beta}$ and an uncorrelated bit whenever $\beta \neq \hat{\beta}$. The QOT protocol amplifies this process in order to get a secure 1–2 oblivious transfer. In order to ensure that Bob measures the BB84 qubits upon reception, bit commitments are used. Bob commits upon each measurement basis[1] and measurement outcome right after the quantum transmission. Alice then verifies in random positions that

[1] The bases $\{+,\times\}$ are encoded in $\{0,1\}$.

Bob has really measured the transmitted qubits by testing that whenever $\beta = \hat{\beta}$ then Bob's classical outcome $r \in \{0, 1\}$ is such that $r = s$.

In the following, we assume that Alice and Bob have access to some bit commitment scheme $\mathtt{BBC}$ in order for Bob to commit upon the measurement bases of the received qubits together with the outcomes. Since the two commitments are made together, we write $\mathtt{BBC}(x, y)$ where $x \in \{+, \times\}$ and $y \in \{0, 1\}$ for the commitments of both the measurement basis and the measurement outcome. This simply means 2 sequential executions of $\mathtt{BBC}$, one for the commitment of x and the other the commitment of y. $\mathtt{BBC}$ may be given as a black-box for bit commitment or may be provided from some computational assumption. We denote by the $\mathtt{Open\text{-}BBC}(x, y)$ the opening stage of $\mathtt{BBC}(x, y)$. Protocol $\textsc{qot}(b_0, b_1)(c)$ achieves the oblivious transfer of bit b_c.

Protocol 1 (QOT$(b_0, b_1)(c)$)

1: *For* $1 \le i \le 2n$

- *Alice picks* $s_i \in_R \{0,1\}$, $\beta_i \in_R \{+, \times\}$
- *Alice sends to Bob a qubit* π_i *in state* $|s_i\rangle_{\beta_i}$
- *Bob picks a basis* $\hat{\beta}_i \in_R \{+, \times\}$, *measures* π_i *in basis* $\hat{\beta}_i$, *and obtains the outcome* $r_i \in \{0,1\}$

2: *For* $1 \le i \le n$

- *Bob runs* $\texttt{BBC}(\hat{\beta}_i, r_i)$ *and* $\texttt{BBC}(\hat{\beta}_{n+i}, r_{n+i})$ *with Alice*
- *Alice picks* $f_i \in_R \{0,1\}$ *and announces it to Bob*
- *Bob runs* $\texttt{Open-BBC}(\hat{\beta}_{nf_i+i}, r_{nf_i+i})$
- *Alice verifies that* $\beta_{nf_i+i} = \hat{\beta}_{nf_i+i} \Rightarrow s_{nf_i+i} = r_{nf_i+i}$, *otherwise she rejects the current execution*
- *if* $f_i = 0$ *then Alice sets* $\beta_i \leftarrow \beta_{n+i}$ *and* $s_i \leftarrow s_{n+i}$ *and Bob sets* $\hat{\beta}_i \leftarrow \hat{\beta}_{n+i}$ *and* $r_i \leftarrow r_{n+i}$

3: *Alice announces her choices of bases* $\beta_1, \beta_2, \ldots, \beta_n$ *to Bob*

4: *Bob chooses at random and announces two subsets of positions* $J_0, J_1 \subset \{1, 2, \ldots, n\}$, $|J_0| = |J_1| = \frac{n}{3}$, $J_0 \cap J_1 = \emptyset$, *and* $\forall i \in J_c, \beta_i = \hat{\beta}_i$.

5: *Alice computes and announces* $\hat{b}_0 = \bigoplus_{j \in J_0} s_j \oplus b_0$ *and* $\hat{b}_1 = \bigoplus_{j \in J_1} s_j \oplus b_1$

6: *Bob receives* $\langle \hat{b}_0, \hat{b}_1 \rangle$ *and computes* $b_c = \bigoplus_{i \in J_c} r_i \oplus \hat{b}_c$

Known Security Results. The correctness and the security of the QOT protocol against the sender (Alice) has been reduced to the concealing property of BBC in [3, 6]. The security against the receiver (Bob) has been provided by Yao in [25] given the commitment scheme BBC is binding. That is, given

BBC is a perfect black-box for bit commitment then QOT is secure against any dishonest Bob irrespectively of his computing power.

3.2 QBC Protocol using QOT

Given a binding but computationally concealing bit commitment scheme BBC in QOT the following commitment scheme will be shown concealing and computationally binding.

Protocol 2 (QBC(b))

1: QBC-COMMIT(b)

- *For* $1 \leq j \leq n$
  - *Alice prepares* $a_{0j} \in_R \{0,1\}$ *and* $a_{1j} = a_{0j} \oplus b$
  - *Bob prepares* $c_j \in_R \{0,1\}$
  - *Alice and Bob execute* QOT$(a_{0j}, a_{1j})(c_j)$ *and Bob receives the result* d_j

2: QBC-OPEN(b)

- *Alice announces* b
- *For* $1 \leq j \leq n$
  - *Alice announces* a_{0j} *and* a_{1j}
  - *Bob verifies that* $b = a_{0j} \oplus a_{1j}$ *and* $d_j = a_{c_j j}$

A commitment to bit b is done by sending through 1–2 oblivious transfers n pairs of bits $\{(a_{0j}, a_{1j})\}_{j=1}^{n}$ such that $a_{0j} \oplus a_{1j} = b$. The concealing condition depends on the security of the oblivious transfer against the receiver and the binding condition depends on the security against the sender. Intuitively, the QBC protocol appears concealing since for $1 \leq j \leq n$ Bob cannot obtain information on more than one of the two bits (a_{0j}, a_{1j}) input in the j-th QOT and so, cannot determine $b = a_{0j} \oplus a_{1j}$. Similarly, the QBC should be binding since for all $1 \leq j \leq n$ Alice needs to change the bit $a_{\bar{d}_j j}$ not selected by Bob in order to change her commitment.

3.3 More Notation

In the following we shall have to identify the variables generated during all calls to QOT in QBC. For that purpose, we use the following notation:

- π_i^j is the i-th qubit sent in the j-th call to QOT in QBC.
- $\beta_i^j \in \{+, \times\}$ is the basis β_i announced by Alice during the j-th execution of QOT in QBC. Note that since Alice is not necessarily honest, π_i^j can be different from $|0\rangle_{\beta_i^j}$ and $|1\rangle_{\beta_i^j}$.
- $\hat{\beta}_i^j \in \{+, \times\}$ is the basis used by Bob to measure π_i^j in the j-th call to QOT.
- $r_i^j \in \{0, 1\}$ is the outcome of Bob's measurement of π_i^j in basis $\hat{\beta}_i^j$.
- $\hat{r}_i^j \in \{0, 1\}$ is Carl's outcome for measurement of π_i^j in basis β_i^j.

- $J^j = (J_0^j, J_1^j)$ is the two sets of positions announced by Bob in the j-th execution of QOT.

We denote by bold lowercases the values for all executions at one glance: $\boldsymbol{\beta} = \{\beta_i^j\}_{i,j}, \hat{\boldsymbol{\beta}} = \{\hat{\beta}_i^j\}_{i,j}, \boldsymbol{r} = \{r_i^j\}_{i,j}$, and $\hat{\boldsymbol{r}} = \{\hat{r}_i^j\}_{i,j}$. We denote by $\hat{\boldsymbol{b}}_0 = \hat{b}_0^1, \ldots, \hat{b}_0^n$ and $\hat{\boldsymbol{b}}_1 = \hat{b}_1^1, \ldots, \hat{b}_1^n$ the bits announced by Alice at step 5 of each call to QOT. Similarly, we denote by $\boldsymbol{a} = (\boldsymbol{a}_0, \boldsymbol{a}_1) = (a_{01}, a_{11}), (a_{02}, a_{12}), \ldots, (a_{0n}, a_{1n}) \in \{0,1\}^{2n}$ Alice's announcements during the opening stage. We also denote $\boldsymbol{J}_0 = J_0^1, \ldots, J_0^n$ and $\boldsymbol{J}_1 = J_1^1, \ldots, J_1^n$ all sets announced by Bob and we write $\boldsymbol{J} = (\boldsymbol{J}_0, \boldsymbol{J}_1)$. Let $\boldsymbol{c} = c_1, \ldots, c_n$ be all selection bits used by Bob and let $\boldsymbol{d} = d_1, \ldots, d_n$ be all bits received by QOT. We write $\boldsymbol{J}_{\boldsymbol{c}} = J_{c_1}^1, J_{c_2}^2, \ldots, J_{c_n}^n$ for all set of positions corresponding to qubits measured by Bob in bases announced by Alice.

Chapter 4

Security Proofs

4.1 The Binding Condition

In the following section, we show that QBC is secure against any Alice (the sender) who cannot break the concealing condition of the inner commitment scheme BBC. BBC is used in the calls to QOT in order for Bob to commit on his measurements and outcomes.

Simplified Version of QOT. In our analysis of the binding condition of QBC, we shall assume that the opening of half of the commitments in step 2 of QOT doesn't occur. The opening of the commitments allows Alice to make sure that Bob measured the qubits received in QOT upon reception. This test is not relevant to the binding condition of QBC.

Protocol 3 ($\textsc{qot}^*(b_0, b_1)(c)$)

1: *...step 1 of protocol 3.1*

2: *For* $1 \leq i \leq n$

- *Bob runs* $\texttt{BBC}(\hat{\beta}_i, r_i)$ *and* $\texttt{BBC}(\hat{\beta}_{n+i}, r_{n+i})$ *with Alice*
- *Alice picks* $f_i \in_R \{0, 1\}$ *and announces it to Bob*
- *if* $f_i = 0$ *then Alice sets* $\beta_i \leftarrow \beta_{n+i}$ *and* $s_i \leftarrow s_{n+i}$ *and Bob sets* $\hat{\beta}_i \leftarrow \hat{\beta}_{n+i}$ *and* $r_i \leftarrow r_{n+i}$

3–6: *...as steps 3 to 6 in protocol 3.1*

We omit the proof of the following simple lemma:

Lemma 4.1.1 *If* $\textsc{qot}^*$ *is secure against the sender then* $\textsc{qot}$ *is secure against the sender.*

Throughout section 4.1, we shall assume tacitly calls to $\textsc{qot}^*$ in $\textsc{qbc}$ instead of calls to $\textsc{qot}$. This simplifies the analysis and according to lemma 4.1.1, it can be done without loss of generality.

4.1.1 How to Prove the Binding Condition

In order to show that $\textsc{qbc}$ is computationally binding, we introduce intermediary protocols that will allow us to bridge the security of the $\textsc{qbc}$ protocol with the known security of $\textsc{qot}$ given black-boxes for bit commitments. Let's consider the following four modified protocols:

U-QOT: Protocol QOT except that in step 2, Bob commits to random values. In other words, for $1 \leq i \leq n$, Bob runs $\mathtt{BBC}(u_{0i}, u_{1i})$ and $\mathtt{BBC}(u_{2i}, u_{3i})$ with $u_{0i}, u_{2i} \in_R \{+, \times\}$ and $u_{1i}, u_{3i} \in_R \{0, 1\}$.

M-QOT: The same as U-QOT but a third party named Carl, for $1 \leq i \leq n$, intercepts the i-th qubit π_i sent by Alice in step 1, measures in basis β_i (announced by Alice in step 3) and sends the resulting state to Bob.

U-QBC: Protocol QBC using U-QOT.

M-QBC: Protocol QBC using M-QOT.

The security against any dishonest sender in U-QOT and M-QOT is a direct consequence of the analysis provided in [6]. Since the commitments upon measurements do not carry any information about Bob's measurement, Alice cannot obtain any information about his selection bit c. The security is information-theoretic, no complexity assumption on Alice's computing power is required.

We reduce the security of the binding condition of QBC to the security of the concealing condition of BBC in two steps:

1. Using Lemmas 4.1.2 and 4.1.3, we conclude in Lemma 4.1.4 that U-QBC is binding. The modified protocol M-QBC is used for reducing

the security of U-QBC to the security of U-QOT. Carl's presence allows one to reduce the analysis to an essentially classical argument which becomes simpler than working from U-QBC directly.

2. Theorem 4.1.5 establishes the desired result using the fact that an adversary for the binding condition of QBC cannot be an adversary of U-QBC (Lemma 4.1.4). It is shown how to construct an adversary for the concealing condition of BBC given an adversary for the binding condition of QBC.

4.1.2 U-QBC is binding

In this section, we show that U-QBC is binding (Lemma 4.1.4) using Lemmas 4.1.2 and 4.1.3 as intermediary steps.

First, we show that an adversary against the binding condition of U-QBC can be transformed into an adversary against the binding condition of M-QBC.

Lemma 4.1.2 *If there exists a $(s_0(n), s_1(n))$-adversary $\tilde{A}$ against the binding condition of* U-QBC *there also exists a $(s_0(n), s_1(n))$-adversary A^* against the binding condition of* M-QBC*.*

Proof: We observe first that $\tilde{A}$'s announcement of $\boldsymbol{\beta}$ at step 3 of U-QOT commutes with step 2. That is, since only commitments to random values are received, $\tilde{A}$ can determine $\boldsymbol{\beta}$ without Bob's commitments. Moreover, $\tilde{A}$ could simulate the commitments on her own and then determine $\boldsymbol{\beta}$ before the qubits are sent to Bob at step 1. Let A^* be the quantum adversary that does that. If $\tilde{A}$ provides a $(s_0(n), s_1(n))$–advantage in U-QBC then so it is for A^*. We now show that A^* is also an adversary for the binding condition of M-QBC.

Now assume for simplicity and without loss of generality that, Bob in U-QBC or Bob and Carl in M-QBC wait until after Alice announces $\boldsymbol{a} = (\boldsymbol{a}_0, \boldsymbol{a}_1)$ before measuring all qubits received. It is easy to verify that this can always be done since nothing in the committing stage of U-QBC or M-QBC relies on those measurements' outcomes (i.e. since the commitments are made to random values). Clearly, postponing measurements do not influence Alice's probability of success at the opening stage.

Let $V = (\boldsymbol{\beta}, \boldsymbol{J}, \hat{\boldsymbol{b}}_0, \hat{\boldsymbol{b}}_1, \boldsymbol{c}, \boldsymbol{a})$ be the partial view in U-QBC or in M-QBC up to Alice's announcement of $\boldsymbol{a}$ (and b since for all $1 \leq j \leq n$, $a_{j0} \oplus a_{j1} = b$) in the opening stage. Let $\boldsymbol{V}_{\mathtt{U}}$ and $\boldsymbol{V}_{\mathtt{M}}$ be the random variable for the partial view in U-QBC and M-QBC respectively. By construction we have that for all $V = (\boldsymbol{\beta}, \boldsymbol{J}, \hat{\boldsymbol{b}}_0, \hat{\boldsymbol{b}}_1, \boldsymbol{c}, \boldsymbol{a})$, $\mathrm{P}\left(\boldsymbol{V}_{\mathtt{U}} = V\right) = \mathrm{P}\left(\boldsymbol{V}_{\mathtt{M}} = V\right)$. Moreover, we have that for all partial views V, the joint states $|\Psi_{\mathtt{U}}(V)\rangle$ for U-QBC and $|\Psi_{\mathtt{M}}(V)\rangle$ for

M-QBC satisfy $|\Psi_{\mathtt{U}}(V)\rangle = |\Psi_{\mathtt{M}}(V)\rangle$. Let $\mathcal{V}_b = \{(\boldsymbol{\beta}, \boldsymbol{J}, \hat{\boldsymbol{b}}_0, \hat{\boldsymbol{b}}_1, \boldsymbol{c}, \boldsymbol{a}) | (\forall 1 \leq j \leq n)[a_{j0} \oplus a_{j1} = b]\}$ be the set of partial views corresponding for Alice to open bit b. Given V, Bob's test will succeed if he gets $\boldsymbol{d} = \boldsymbol{a_c} = a_{1c_1}, a_{2c_2}, \ldots, a_{nc_n}$ after measuring the qubits in positions in $\boldsymbol{J_c}$ using Alice's bases β_i^j for all $i \in J_{c_j}^j$ and $j \in \{1, \ldots, n\}$. Let $\mathcal{M}_{test}(V) = \{\mathbb{Q}_{ok}^V, \mathbb{1} - \mathbb{Q}_{ok}^V\}$ be the measurement allowing Bob to test Alice's announcement when she unveils b given partial view $V \in \mathcal{V}_b$. $\mathbb{Q}_{ok}^V$ is the projection for the state of all qubits received in positions in $\boldsymbol{J_c}$ into the subspace corresponding to parity $d_j = a_{jc_j}$ for all $j \in \{1, \ldots, n\}$. More precisely, $\mathbb{Q}_{ok}^V = \bigotimes_{j=1}^n \sum_{x \in T(V,j)} \mathbb{P}_x^{\boldsymbol{\beta}(V,j)}$ where $T(V,j) = \{x \in \{0,1\}^{|J_{c_j}^j|} | \oplus_i x_i = a_{jc_j} \oplus \hat{b}_{c_j}^j\}$ and $\boldsymbol{\beta}(V,j) = \{\beta_i^j | i \in J_{c_j}^j\}$ for all $j \in \{1, \ldots, n\}$. Let $s_b'(n)$ be the probability of success when A^* opens b in M-QBC. We get that

$$
\begin{aligned}
s_b(n) &= \sum_{V \in \mathcal{V}_b} \mathrm{P}\left(\boldsymbol{V}_{\mathtt{U}} = V\right) \|\mathbb{Q}_{ok}^V |\Psi_{\mathtt{U}}(V)\rangle\|^2 \\
&= \sum_{V \in \mathcal{V}_b} \mathrm{P}\left(\boldsymbol{V}_{\mathtt{M}} = V\right) \|\mathbb{Q}_{ok}^V \mathbb{Q}_{ok}^V |\Psi_{\mathtt{M}}(V)\rangle\|^2 \\
&= s_b'(n)
\end{aligned} \tag{4.1}
$$

since the only difference between U-QBC and M-QBC is that in the former case both Carl and Bob measure the qubits in positions in $\boldsymbol{J_c}$ with the same measurement $\mathcal{M}_{test}$ (this is why we have $\mathbb{Q}_{ok}^V \mathbb{Q}_{ok}^V = \mathbb{Q}_{ok}^V$ in (4.1)). Carl's measurements for positions in $\boldsymbol{J}_{\overline{\boldsymbol{c}}}$ are irrelevant to the success probability. The result follows. $\square$

Next, we reduce the binding condition of M-QBC to the security against the sender in M-QOT. We show that from any successful adversary against the binding condition of M-QBC one can construct an adversary able to extract non-negligible information about Bob's selection bit in M-QOT. Carl's measurements in M-QBC allows one to use a classical argument for most of the reduction thus simplifying the proof that U-QBC is binding.

Lemma 4.1.3 *If there exists a $(s_0(n), s_1(n))$-adversary $\tilde{A} = (C^{\tilde{A}}, O^{\tilde{A}})$ for the binding condition of* M-QBC *with $s_0(n)+s_1(n) \geq 1+\frac{1}{p(n)}$ for some positive polynomial $p(n)$, then there also exists a cheating sender A^* for* M-QOT.

Proof: Let a'_{j0} and a'_{j1} be the two input bits for the j-th call to M-QOT computed according to Carl's outcomes $\hat{\boldsymbol{r}}$. Let $\boldsymbol{V}$ be the random variable for the joint view $(\boldsymbol{a}, \boldsymbol{a'}, \boldsymbol{d}, \boldsymbol{c})$ for an execution of the committing and the opening stages of M-QBC between $\tilde{A}$ and an honest receiver B and where $\tilde{A}$ is opening a random bit $b \in_R \{0,1\}$. Without loss of generality, we assume the announcements made by $\tilde{A}$ to be consistent, that is $a_{0i} \oplus a_{1i} = b$ for $1 \leq i \leq n$ when she opens bit b. Given $V = (\boldsymbol{a}, \boldsymbol{a'}, \boldsymbol{d}, \boldsymbol{c})$, we define the ordered set $S(V) = \{j | a'_{j0} \oplus a'_{j1} \neq a_{j0} \oplus a_{j1}\} \subseteq \{1, \ldots, n\}$ of calls to M-QOT for which given view V Alice's announcement of $\boldsymbol{a}$ disagree with Carl's outcomes $\boldsymbol{a'}$. Given the ordered set $S(V) = \{\sigma_1, \sigma_2, \ldots, \sigma_s\}$, let $X_j(V) \in \{0,1\}$ for $1 \leq j \leq s$ be defined as

$$X_j(V) = \begin{cases} 0 & \text{if } d_{\sigma_j} \neq a_{\sigma_j c_{\sigma_j}} \\ 1 & \text{if } d_{\sigma_j} = a_{\sigma_j c_{\sigma_j}}. \end{cases}$$

We let $X(V) = X_1(V), \ldots, X_{l(V)}(V)$ for $l(V) = \min\left(|S(V)|, \lceil \frac{n}{2} \rceil\right)$. Clearly, for $\tilde{A}$ to open with success given V, we must have $X(V) = 1^{l(V)}$. Note that $\mathrm{P}\left(|S(\boldsymbol{V})| \geq \frac{n}{2}\right) \geq \frac{1}{2}$ since for at least one choice of b, $|S(\boldsymbol{V})| \geq \frac{n}{2}$ given that $\boldsymbol{V}$ always describes a consistent opening. We easily get that

$$\begin{aligned} \mathrm{P}\left(X(\boldsymbol{V}) = 1^{\lceil \frac{n}{2} \rceil}\right) &= \mathrm{P}\left(X(\boldsymbol{V}) = 1^{l(\boldsymbol{V})}\right) - \mathrm{P}\left(X(\boldsymbol{V}) = 1^{l(\boldsymbol{V})} \ \wedge \ l(\boldsymbol{V}) < \frac{n}{2}\right) \\ &\geq \frac{1}{2}(s_0(n) + s_1(n)) - \frac{1}{2}\mathrm{P}\left(X(\boldsymbol{V}) = 1^{l(\boldsymbol{V})} \,|\, l(\boldsymbol{V}) < \frac{n}{2}\right) \\ &\geq \frac{1}{2p(n)}. \end{aligned} \tag{4.2}$$

Since $\sum_{x \in \{0,1\}^{\lceil \frac{n}{2} \rceil}} \mathrm{P}\left(X(\boldsymbol{V}) = x\right) \leq 1$, for n sufficiently large there exists a string $\hat{y}^0 \in \{0,1\}^{\lceil \frac{n}{2} \rceil}$ such that $\mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^0\right) \leq \frac{1}{4p(n)}$. Let ρ be the number of zeros in $\hat{y}^0$ and $R(\hat{y}^0) = \{r_1, r_2, \ldots, r_\rho\} \subseteq \{1, \ldots, \lceil \frac{n}{2} \rceil\}$ be the ordered set of positions $1 \leq r \leq \lceil \frac{n}{2} \rceil$ where $\hat{y}^0_r = 0$. We now define for $1 \leq j \leq \rho$ the hybrid strings $\hat{y}^j = \hat{y}^j_1 \hat{y}^j_2 \ldots \hat{y}^j_{\lceil \frac{n}{2} \rceil}$ between $\hat{y}^0$ and $1^{\lceil \frac{n}{2} \rceil}$:

$$\hat{y}^j_i = \begin{cases} 1 & \text{if } i = r_k \text{ for } k \leq j \\ \hat{y}^0_i & \text{Otherwise.} \end{cases}$$

Hence, $\mathrm{P}\left(X(\boldsymbol{V})=\hat{y}^{\rho}=1^{n}\right)-\mathrm{P}\left(X(\boldsymbol{V})=\hat{y}^{0}\right)\geq\frac{1}{4p(n)}$ and we conclude by an hybrid argument that there exist $1\leq k^{*}\leq\rho$ such that

$$\mathrm{P}\left(X(\boldsymbol{V})=\hat{y}^{k^{*}}\right)-\mathrm{P}\left(X(\boldsymbol{V})=\hat{y}^{k^{*}-1}\right)\geq\frac{1}{\rho 4p(n)}\geq\frac{1}{2(n+1)p(n)} \tag{4.3}$$

Note that $\hat{y}^{k^{*}}$ and $\hat{y}^{k^{*}-1}$ differs only by the bit in position $r_{k^{*}}$ where they respectively have a 1 and a 0.

A^{*} uses $\tilde{A}$ and $B=(C^{B},O^{B})$ in the following way: after choosing $h\in_{R}\{1,\ldots,n\}$, it makes $\tilde{A}$ interact with a simulated honest receiver B for M-QBC except for the h-th execution of M-QOT for which $\tilde{A}$ interacts with the targeted receiver for M-QOT. Let $V=(\boldsymbol{a},\boldsymbol{a'},\boldsymbol{d},\boldsymbol{c})$ be the view generated during the execution. Given A^{*}'s view, algorithm $L^{A^{*}}$ produces a guess $\tilde{c}$ for Bob's selection bit $c=c_{h}$ in M-QOT as follows:

- If $|S(V)|\geq\lceil\frac{n}{2}\rceil$, $h=\sigma_{r_{k^{*}}}$ and $\forall i\in\left\{1,\ldots,\lceil\frac{n}{2}\rceil\right\}\setminus\{r_{k^{*}}\},X_{i}(V)=\hat{y}_{i}^{k^{*}}$, then $\tilde{c}\in\{0,1\}$ is defined such that $a_{h\tilde{c}}=a'_{h\tilde{c}}$ (which necessarily exists since $h\in S(V)$),
- Otherwise, $\tilde{c}\in_{R}\{0,1\}$.

Let $\mathcal{T}(V)$ be the event of a successful test in the previous computation. Since independently $|S(V)|\geq\frac{n}{2}$ with probability at least $\frac{1}{2}$, $h=\sigma_{r_{k^{*}}}$ with probability $\frac{1}{n}$, and $\forall i \in \left\{1, \ldots, \lceil \frac{n}{2} \rceil\right\} \setminus \{r_{k^*}\}, X_i(V) = \hat{y}_i^{k^*}$ with probability $\mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*}\right) + \mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*-1}\right)$, we have that

$$\mathrm{P}\left(\mathcal{T}(\boldsymbol{V})\right) \geq \frac{\mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*}\right) + \mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*-1}\right)}{2n}. \tag{4.4}$$

Given $\mathcal{T}(V)$, the guess $\tilde{c}$ is the only value for Bob's selection bit c that would lead to $X(V) = \hat{y}^{k^*}$ instead of $X(V) = \hat{y}^{k^*-1}$ (the two strings are the only possible given $\mathcal{T}(V)$). We get

$$\mathrm{P}\left(\tilde{c} = c | \mathcal{T}(\boldsymbol{V})\right) = \frac{\mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*}\right)}{\mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*}\right) + \mathrm{P}\left(X(\boldsymbol{V}) = \hat{y}^{k^*-1}\right)}. \tag{4.5}$$

Following, (A^*, L^{A^*}) is a cheating sender for M-QOT since

$$\begin{aligned} \mathrm{P}\left(\tilde{c} = c\right) &= \frac{1}{2}(1 - \mathrm{P}\left(\mathcal{T}(\boldsymbol{V})\right)) + \mathrm{P}\left(\mathcal{T}(\boldsymbol{V})\right)\mathrm{P}\left(\tilde{c} = c | \mathcal{T}(\boldsymbol{V})\right) \\ &\geq \frac{1}{2} + \frac{1}{8n(n+1)p(n)}. \end{aligned} \tag{4.6}$$

□

Using Lemmas 4.1.1, 4.1.2 and 4.1.3 together with the fact that M-QOT is unconditionally secure against the sender [6], we get the desired result:

Lemma 4.1.4 *Protocol* U-QBC *is binding.*

As we shall see next, Lemma 4.1.4 helps a great deal in proving that QBC is computationally binding.

4.1.3 QBC is Binding when BBC is Concealing

In the following, we conclude that QBC is computationally binding whenever `BBC` is computationally concealing. We use the fact that U-QBC is binding (Lemma 4.1.4) in order to use any adversary against the binding condition of QBC as a distinguisher between random (U-QBC) and real (QBC) commitments for some hybrids between U-QBC and QBC.

Theorem 4.1.5 *If there exists a $(s_0(n), s_1(n))$-adversary $\tilde{A} = (C^{\tilde{A}}, O^{\tilde{A}})$ against the binding condition of* QBC *with $s_0(n)+s_1(n) \geq 1+\frac{1}{p(n)}$ for positive polynomial $p(n)$, then there exists a quantum receiver $C^{\tilde{B}}$ in* `BBC` *and a quantum algorithm $L^{\tilde{B}}$ such that $\mathrm{P}\left(L^{\tilde{B}}((C^A \odot C^{\tilde{B}})|b\rangle^A|0\rangle^{\tilde{B}}) = b\right) \geq \frac{1}{2}+\Omega(\frac{1}{n^4 p(n)})$ whenever $b \in_R \{0,1\}$ and where $C^{\tilde{B}}$ calls $\tilde{A}$ an expected $O(n^5 p(n)^2)$ times.*

Proof: Let $B = (C^B, O^B)$ be the circuits for the honest receiver in QBC and let $\mathcal{A}$ be an honest committer in `BBC`. Given $\tilde{A}$, we construct a receiver $C^{\tilde{B}}$ in `BBC` from which a bias for $\mathcal{A}$'s committed bit can be extracted. Remember that the only difference between U-QBC and QBC is that a honest receiver commits to random bits instead of his measurements and outcomes. There are $4n$ calls to `Commit-BBC` per QOT (U-QOT) for a total of $4n^2$ during the committing stage of QBC (U-QBC). Let's note as *significant* the committed bits specified by the protocol QOT (to measurements and outcomes) and as *random* the ones specified by the protocol U-QOT (to random bits). We describe hybrids in between QBC and U-QBC by letting the number of significant and random commitments vary. Let QBC^k be protocol QBC but where the first k commitments out of $4n^2$ are made to random values. We have that $\text{U-QBC} \equiv \text{QBC}^{4n^2}$ is binding whereas $\tilde{A}$ is a $(s_0(n), s_1(n))$–adversary for the binding condition of $\text{QBC}^0 \equiv \text{QBC}$. Let $s_b^k(n)$ be the probability that $\tilde{A}$ succeeds when opening $b \in \{0,1\}$ in QBC^k for $0 \leq k \leq 4n^2$. Defining $\hat{s}^k(n) = \frac{s_0^k(n)+s_1^k(n)}{2}$, we get that $\hat{s}^0(n) \geq \frac{1}{2} + \frac{1}{2p(n)}$ and $\hat{s}^{4n^2}(n) < \frac{1}{2} + \frac{1}{q(n)}$ for any $q(n) \in poly(n)$ (from Lemma 4.1.4), given n sufficiently large. By the hybrid argument, there exists $0 \leq k^* \leq 4n^2 - 1$ such that for n sufficiently large,

$$\hat{s}^{k^*}(n) - \hat{s}^{k^*+1}(n) \geq \frac{1}{9n^2 p(n)}. \tag{4.7}$$

Hence, $\mathcal{D}_{4n^2}(\frac{1}{9n^2p(n)}) = \{\hat{s}^i(n)\}_{i=0}^{4n^2}$ is a family of Bernoulli distributions that satisfies the condition of Lemma 2.3.3. The sampling circuit $\mathtt{S}$ is easy to construct given $\tilde{A}$ and B. Upon classical input $|l\rangle$ for $0 \leq l \leq 4n^2$, $\mathtt{S}$ runs $\tilde{A}$ and B except that the first l commitments sent from B to $\tilde{A}$ (using $\mathtt{BBC}$) are made to random values instead of the measurements $\hat{\boldsymbol{\beta}}$ and the outcomes $\boldsymbol{r}$. $\tilde{A}$ then opens a random bit $b \in_R \{0,1\}$. If B accepts the opening of b then

$\mathtt{S}(|l\rangle) = 1$ otherwise it returns $\mathtt{S}(|l\rangle) = 0$. Circuit $\mathtt{S}$ is therefore a sampling circuit for $\mathcal{D}_{4n^2}(\frac{1}{9n^2p(n)})$ such that $\|\mathtt{S}\|_{\mathcal{UG}} \in O(\|\tilde{A}\|_{\mathcal{UG}})$ assuming without loss of generality that $\|B\|_{\mathcal{UG}} \in O(\|\tilde{A}\|_{\mathcal{UG}})$.

We now construct the adversary $C^{\tilde{B}}$ for the concealing condition of $\mathtt{BBC}$ given $\tilde{A}$. In order to use algorithm $\mathtt{FindDrop}$ presented in section 2.3.4, $C^{\tilde{B}}$ must first determine a lower bound $\frac{1}{p'(n)}$ for the drop $\frac{1}{9n^2p(n)}$. This is done by finding a lower bound $\tilde{p}(n)$ for $\frac{1}{2p(n)}$ and then setting $p'(n) = \frac{5n^2}{\tilde{p}(n)}$. $C^{\tilde{B}}$ computes $\tilde{p}(n) = \mathtt{LowBound}(\mathtt{S}_0, \frac{1}{2}, n)$ where $\mathtt{LowBound}$ is the procedure described in section 2.3.3 and $\mathtt{S}_0$ is the circuit $\mathtt{S}$ with the input bits fixed to $|0\rangle$. According to Lemma 2.3.2, when n is sufficiently large $\mathtt{LowBound}$ returns $\tilde{p}(n)$ such that $\frac{1}{2n^2p(n)} \leq \tilde{p}(n) \leq \frac{1}{2p(n)}$ except with negligible probability and after an expected $O(n^5p(n)^2)$ calls to $\mathtt{S}_0$.

Now $C^{\tilde{B}}$ can use $\mathtt{FindDrop}(\mathtt{S}, \frac{1}{p'(n)}, n)$ with the family of distributions $\mathcal{D}_{4n^2}(\frac{1}{p'(n)}) = \{\hat{s}^i(n)\}_{i=0}^{4n^2}$ which exhibits a drop $\frac{1}{p'(n)}$ except with negligible probability. From Lemma 2.3.3, $C^{\tilde{B}}$ gets $0 \leq \kappa \leq 4n^2 - 1$ such that

$$\hat{s}^{\kappa}(n) - \hat{s}^{\kappa+1}(n) \geq \frac{1}{2p'(n)} \tag{4.8}$$

except with negligible probability. The value of κ is obtained after calling $\mathtt{S}$ (including the calls to $\mathtt{S}_0$ in $\mathtt{LowBound}$) an expected $O(n^5p(n)^2)$ times.

$C^{\tilde{B}}$ then uses κ for attacking the concealing condition of $\mathtt{BBC}$ in the following way: It makes $\tilde{A}$ and B interact (where $\tilde{A}$ opens $b \in_R \{0,1\}$) as in $\textsc{qbc}^{\kappa+1}$ except that the $(\kappa+1)$-th random commitment is provided by the committer $\mathcal{A}$ in $\mathtt{BBC}$. Let $b \in \{0,1\}$ be the bit committed by $\mathcal{A}$. Let $\boldsymbol{V}$ be the random variable for the view generated during the interaction between $\tilde{A}$ and B when $\tilde{A}$ opens the random bit. Let $c_{\kappa+1}(V) \in \{0,1\}$ be the bit that B would have committed if the $(\kappa+1)$-th commitment was significant. The distinguisher $L^{\tilde{B}}$ (which is classical given the view V) returns the guess $\tilde{b}$ for b the following way:

- If V is a successful opening then $\tilde{b} = c_{\kappa+1}(V)$,
- Otherwise, $\tilde{b} \in_R \{0,1\}$.

Let $\mathcal{V}_{ok}^{\kappa+1}$ be the set of views for $\textsc{qbc}^{\kappa+1}$ resulting in a successful opening and let $\mathcal{G}$ be the set of values κ for which (4.8) holds. We have $\hat{s}^{\kappa}(n) = \mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} | c_{\kappa+1}(\boldsymbol{V}) = b\right)$ and $\hat{s}^{\kappa+1}(n) = \frac{1}{2}\mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} | c_{\kappa+1}(\boldsymbol{V}) \neq b\right) + \frac{1}{2}\mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} | c_{\kappa+1}(\boldsymbol{V}) = b\right)$ which, using (4.8), leads to

$$\mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} \wedge c_{\kappa+1}(\boldsymbol{V}) \neq b\right) \leq \mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} \wedge c_{\kappa+1}(\boldsymbol{V}) = b\right) - \frac{1}{2p'(n)}. \tag{4.9}$$

Since we also have that $\mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1}\right) = \mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} \wedge c_{\kappa+1}(\boldsymbol{V}) \neq b\right) +$

$\mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} \wedge c_{\kappa+1}(\boldsymbol{V}) = b\right)$, we get

$$\begin{aligned}
\mathrm{P}\left(\tilde{b} = b | \kappa \in \mathcal{G}\right) &= \mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1} \wedge c_{\kappa+1}(\boldsymbol{V}) = b\right) + \frac{1}{2}\left(1 - \mathrm{P}\left(\boldsymbol{V} \in \mathcal{V}_{ok}^{\kappa+1}\right)\right) \\
&\geq \frac{1}{2}\left(1 + \frac{1}{2p'(n)}\right). \qquad (4.10)
\end{aligned}$$

Since $\mathrm{P}\left(\tilde{b} = b\right) \geq \mathrm{P}\left(\kappa \in \mathcal{G}\right) \mathrm{P}\left(\tilde{b} = b | \kappa \in \mathcal{G}\right)$ and $\mathrm{P}\left(\kappa \in \mathcal{G}\right) \geq 1 - 2^{-\alpha n}$ for some $\alpha > 0$ (Lemma 2.3.2) we finally get that $(C^{\tilde{B}}, L^{\tilde{B}})$ is an adversary for the concealing condition of `BBC` providing a bias in $\Omega(\frac{1}{p'(n)}) = \Omega(\frac{1}{n^4 p(n)})$ after calling $\tilde{A}$ an expected $O(n^5 p(n)^2)$ times. □

4.2 The Concealing Condition

In the following section, we show that QBC is concealing for any Bob (the receiver) who cannot break the binding condition of the inner commitment scheme `BBC`. `BBC` is used in the calls to QOT in order for Bob to commit on his measurements and outcomes.

4.2.1 QBC is Concealing when QOT is secure against the Receiver

We now reduce the concealing condition of QBC to the security of QOT against the receiver.

Lemma 4.2.1 *If there exists an interacting quantum circuit* $C^{\tilde{B}}$ *receiving for* `Commit-`QBC *and a quantum algorithm* $L^{\tilde{B}}$ *acting only on* $\tilde{B}$*'s registers such that* $\mathrm{P}\left(L^{\tilde{B}}((C^A \odot C^{\tilde{B}})|b\rangle^A|0\rangle^{\tilde{B}}) = b\right) \geq \frac{1}{2} + \frac{1}{p(n)}$ *for some positive polynomial* $p(n)$ *and an honest committing circuit* C^A *for* $b \in_R \{0,1\}$*, then there also exists a cheating receiver* (B^*, L^{B^*}) *for* QOT*.*

Proof: For the receiver $C^{\tilde{B}}$ and C^A described in the statement, we have $\mathrm{P}\left(L^{\tilde{B}}((C^A \odot C^{\tilde{B}})|1\rangle^A|0\rangle^{\tilde{B}}) = 1\right) - \mathrm{P}\left(L^{\tilde{B}}((C^A \odot C^{\tilde{B}})|0\rangle^A|0\rangle^{\tilde{B}}) = 1\right) \geq \frac{2}{p(n)}$. Let's define a modification of an honest committing circuit for QBC, noted $C^{\tilde{A}}$, which is the same as C^A but takes a string $\hat{f} \in \{0,1\}^n$ instead of a bit b and sends in the i-th call to QOT the bits $a_{0i} \in_R \{0,1\}$ and $a_{1i} = a_{0i} \oplus \hat{f}_i$ for $1 \leq i \leq n$. The circuit C^A with input b is equivalent to $C^{\tilde{A}}$ with input b^n. Once again, by an hybrid argument, there exists $1 \leq k^* \leq n$ such that

$$\begin{aligned}
&\mathrm{P}\left(L^{\tilde{B}}((C^{\tilde{A}} \odot C^{\tilde{B}})|1^{k^*}0^{n-k^*}\rangle^{\tilde{A}}|0\rangle^{\tilde{B}}) = 1\right) - \\
&\mathrm{P}\left(L^{\tilde{B}}((C^{\tilde{A}} \odot C^{\tilde{B}})|1^{k^*-1}0^{n-k^*+1}\rangle^{\tilde{A}}|0\rangle^{\tilde{B}}) = 1\right) \geq \frac{2}{np(n)}
\end{aligned} \tag{4.11}$$

With such a value k^*, B^* cheats an honest sender A' for QOT$(e_0, e_1)(0)$ in the following way: it makes $C^{\tilde{B}}$ interact with $C^{\tilde{A}}$ with input $(1^{k^*-1}?0^{n-k^*})$ for `Commit-`QBC except for the k^*-th call to QOT where it makes $C^{\tilde{B}}$ interact with the targeted sender A' with inputs $e_0, e_1 \in_R \{0,1\}$.

Then, knowing e_c for $c \in \{0,1\}$, we take the output of $L^{\tilde{B}}$, b' say, and compute a guess $e_c \oplus b'$ for $e_{\bar{c}}$. For this algorithm L^{B^*} we have

$$\begin{aligned} \mathrm{P}\left(L^{B^*}((A' \odot B^*)|e_0e_1\rangle^A|0\rangle^{B^*}, |e_c\rangle^{B^*}) = e_{\bar{c}}\right) &= \mathrm{P}\left(b' = e_0 \oplus e_1\right) \\ &\geq \frac{1}{2} + \frac{1}{np(n)} \end{aligned} \qquad (4.12)$$

where the probabilities are taken over $e_0, e_1 \in_R \{0,1\}$. □

4.2.2 QBC is Concealing when BBC is Binding

From Yao's result [25] and Lemma 4.2.1 it is straightforward to conclude that:

Theorem 4.2.2 *If* `BBC` *is binding then* QBC *is concealing.*

Chapter 5

Conclusion and Open Questions

Having shown in Theorem 4.1.5, that a computationally concealing BBC results in a computationally binding QBC and, in Theorem 4.2.2, that no adversary against the concealing condition of QBC exists, we conclude with our main result:

Theorem 5.0.3 *If* BBC *is binding and computationally concealing then* QBC *is concealing and computationally binding.*

For security parameter n, the reduction of an adversary $(C_n^{\tilde{B}}, L_n^{\tilde{B}})$ for the concealing condition of BBC to an adversary $\tilde{A}_n$ for the binding condition of QBC is expected polynomial-time black-box. If $\tilde{A}_n$ breaks the binding condition of QBC with $s_0(n) + s_1(n) \geq 1 + \frac{1}{p(n)}$ then the circuit $C_n^{\tilde{B}}$ is specified by a classical Turing machine calling $\tilde{A}_n$ at most $n^5 p(n)^2$ times except with negligible probability. $L_n^{\tilde{B}}$ then provides a polynomial bias on the committed bit through an almost trivial classical computation given as input $C^{\tilde{B}}$'s view. This guarantees that $(C_n^{\tilde{B}}, L_n^{\tilde{B}})$ satisfies $\|C_n^{\tilde{B}}\|_{\mathcal{UG}} + \|L_n^{\tilde{B}}\|_{\mathcal{UG}} \in O(n^5 p(n)\|\tilde{A}\|_{\mathcal{UG}})$ (using standard simulation techniques) thus breaking the concealing condition of `BBC` as defined in Sect. 2.2. The adversary $\{(C_n^{\tilde{B}}, L_n^{\tilde{B}})\}_{n>0}$ is specified by a uniform family of quantum circuits whenever $\{\tilde{A}_n\}_{n>0}$ is a uniform family[1]. Our reduction is therefore uniformity preserving [22]. It is an interesting open problem to find an exact polynomial-time black-box reduction.

One consequence of Theorem 5.0.3 is that concealing commitment schemes can be built from any quantum one-way function. We first observe that Naor's commitment scheme [21] is also secure against the quantum computer if the pseudo-random bit generator (PRBG) it is based upon is secure against the quantum computer. This follows from the fact that any quantum circuit able to distinguish between commitments to 0 and 1 is also able to distinguish a truly random sequence from a pseudo-random one. To complete the argument, we must make sure that given a quantum one-way function one can construct a PRBG resistant to quantum distinguishers. A tedious but not difficult exercise allows to verify that the classical construction of [14] results in a PRBG secure against quantum distinguishers given it is built

[1]Given 1^n, there exists a poly-time Turing machine that outputs the description of $(C_n^{\tilde{B}}, L_n^{\tilde{B}})$, namely one knowing $p(n)$.

from quantum one-way functions. We get the following corollary which is not known to hold in the classical case:

Corollary 5.0.4 *Both binding but computationally concealing and concealing but computationally biding quantum bit commitments can be constructed from quantum one-way functions.*

It would be interesting to find a concealing quantum bit commitment scheme directly constructed from one-way functions which improves the complexity of our construction. Is it possible to find a non-interactive concealing commitment scheme from the same complexity assumption or are such constructions inherently interactive? It is also unclear whether or not perfectly concealing schemes can be based upon any quantum one-way function.

Although we assumed in this thesis a perfect quantum channel, our construction should also work with noisy quantum transmission [3]. It would be nice to provide the analysis for this general case.

Bibliography

[1] Barenco, A., C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, "Elementary Gates for Quantum Computation", *Physical Review A*, vol. 52, no 5, November 1995, pp. 3457 – 3467.

[2] Bennett, C. H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, December 1984, pp. 175 – 179.

[3] Bennett, C. H., G. Brassard, C. Crépeau and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer", *Advances in Cryptology : CRYPTO '91 : Proceedings*, Lecture Notes in Computer Science, vol. 576, Springer-Verlag, August 1992, pp. 362 – 371.

[4] BRASSARD, G., D. CHAUM and C. CRÉPEAU, "Minimum Disclosure Proofs of Knowledge", *Journal of Computing and System Science*, vol. 37 , 1988, pp. 156 – 189.

[5] BRASSARD, G., C. CRÉPEAU, R. JOZSA and D. LANGLOIS, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 34th Annual IEEE Symposium on the Foundations of Computer Science*, November 1993, pp. 362 – 371.

[6] CRÉPEAU, C., "Quantum Oblivious Transfer", *Journal of Modern Optics*, vol. 41, no 12, December 1994, pp. 2445 – 2454.

[7] CRÉPEAU, C. and J. KILIAN, "Achieving oblivious transfer using weakened security assumptions", *Proceedings of 29th Annual IEEE Symposium on the Foundations of Computer Science*, October 1988, pp. 42 – 52.

[8] CRÉPEAU, C., "An Equivalence Between Two flavors of Oblivious Transfer", *Advances in Cryptology : CRYPTO '87 : Proceedings*, Lecture Notes in Computer Science, vol. 293, Springer-Verlag, 1987, pp. 350 – 354.

[9] Dumais, P., D. Mayers, and L. Salvail, "Perfectly Concealing Quantum Bit Commitment From Any Quantum One-Way Permutation", *Advances in Cryptology : EUROCRYPT '00 : Proceedings*, Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000, pp. 300 – 315.

[10] Fischer, J. B. and J. Stern, "An efficient pseudo-random generator provably as secure as syndrome decoding", *Advances in Cryptology : EUROCRYPT '96 : Proceedings*, Lecture Notes in Computer Science, vol. 1070, Springer-Verlag, 1996, pp. 245 – 255.

[11] Goldwasser, S., S. Micali and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems", *SIAM Journal on Computing*, vol. 18, 1989, pp. 186 – 208.

[12] Goldreich, O., S. Micali, and A. Wigderson,"Proofs that Yield Nothing but their Validity or All Language in NP Have Zero-Knowledge Proof Systems", *Journal of the ACM*, vol. 38, no 1, 1991, pp. 691 – 729.

[13] Grover, L. K., "Quantum mechanics helps in searching for a needle in a haystack", *Physical Review Letters*, vol. 79, no 2, 1997, pp. 325 – 328.

[14] HÅSTAD, J., R. IMPAGLIAZZO, L. LEVIN and M. LUBY "A pseudo-random generator from any one-way function", *SIAM Journal on Computing*, vol. 28, no 4, 1999, pp. 1364 – 1396.

[15] IMPAGLIAZZO, R., L. LEVIN, and L. LUBY, "Pseudo-Random Generation from One-Way Functions", *Proceedings of the 21st ACM Symposium on Theory of Computing*, 1989, pp. 12 – 24.

[16] IMPAGLIAZZO, R. and S. RUDICH, "Limits on Provable Consequences of One-Way Permutations", *Advances in Cryptology : CRYPTO '88 : Proceedings*, Lecture Notes in Computer Science, vol. 403, Springer-Verlag, 1989, pp. 2 – 7.

[17] KILIAN, J., "Founding cryptography on oblivious transfer", *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, 1998, pp. 20 – 31.

[18] LO, H.–K. and H. F. CHAU, "Is quantum Bit Commitment Really Possible?", *Physical Review Letters*, vol. 78, no 17, April 1997, pp. 3410 – 3413.

[19] MAYERS, D., "The Trouble With Quantum Bit Commitment", `http://xxx.lanl.gov/abs/quant-ph/9603015`, March 1996.

[20] Mayers, D., "Unconditionally Secure Quantum Bit Commitment is Impossible", *Physical Review Letters*, vol. 78, no 17, April 1997, pp. 3414 – 3417.

[21] Naor, M., "Bit Commitment Using Pseudo-Randomness", *Journal of Cryptology*, vol. 4, 1991, pp. 151 – 158.

[22] Naor, M., R. Ostrovsky, R. Ventkatesan, and M. Young, "Perfect Zero-Knowledge Arguments For NP Using Any One-Way Permutation", *Journal of Cryptology*, vol. 11, no 2, 1998, pp. 87 – 108.

[23] Shor, P., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing*, vol. 26, no 5, October 1997, pp. 1484 – 1509.

[24] Wiesner, S., "Conjugate coding", *Sigact News*, vol. 15, no 1, 1983, pp. 78 – 88; original manuscript written *circa* 1969.

[25] Yao, A. C., "Security of Quantum Protocols Against Coherent Measurements", *Proceedings of the 27th Annual ACM Symposium on Theory of Computing*, 1995, pp. 67 – 75.