Cryptography in the Bounded Quantum-Storage Model

Christian Schaffner

PhD Progress Report

BRICS

BRICS Ph.D. School
Department of Computer Science
University of Aarhus
Denmark

November 2005

Supervisors: Louis Salvail and Ivan Damgård

Abstract

This progress report presents the scientific results obtained in part A of my PhD studies at BRICS.

We initiate the study of two-party cryptographic primitives with unconditional security, assuming that the adversary's *quantum memory* is of bounded size. We show that Rabin oblivious transfer and bit commitment can be implemented in this model using protocols where honest parties need no quantum memory, whereas an adversarial player needs quantum memory of size at least $n/2$ in order to break the protocol, where n is the number of qubits transmitted. This is in sharp contrast to the classical bounded-memory model, where we can only tolerate adversaries with memory of size quadratic in honest players' memory size. Our protocols are efficient, non-interactive and can be implemented using today's technology.

In the last part of the report, some results of ongoing research and ideas for future research are presented. These results are concerned with the correct security definition of classical *1-2 OT*, a characterisation of the sender-privacy of classical *1-2 OT* and a security proof of a protocol for *1-2 OT* in the bounded quantum-storage model.

Contents

Chapter 1

Introduction

1.1 Purpose and Outline

This progress report presents the scientific results obtained in part A of my PhD studies at BRICS. The last two chapters give an outlook on upcoming work.

The report is organised as follows. The next section gives a short introduction to the world of unconditionally secure two-party computation. Chapter 2 describes notation and the tools needed from (quantum) information theory. Chapter 3 presents new entropic uncertainty relations based on min-entropy and their relation to prior work. These results are then used in Chapter 4 to prove the security of a protocol for Rabin oblivious transfer in the *quantum bounded-storage model* which we also define in this chapter. Using very similar techniques, we can prove secure a commitment scheme in the same model (Chapter 5). The last technical Chapter 6 summarizes the results obtained while trying to build *1-2 OT* in the bounded quantum storage model. Somewhat surprisingly, this research yielded two results about classical *1-2 OT*, one about correctly defining *1-2 OT* and the other about characterising the security requirements using balanced functions. All results in this chapter are still of preliminary nature. Most of the proofs are omitted or only sketched.

The results of Chapters 3, 4 and 5 have been published at the 46th IEEE Symposium on Foundations of Computer Science, FOCS 2005 [DFSS05a]. In Chapter 3, the general min-entropic uncertainty relation has been extended to more bases compared to the full version of the paper [DFSS05b]. Chapter 6 is a summary of three upcoming articles [CSSW05, DFSS05c, DFRSS05]. As those are still in preparation, just the main results are given. We refer to the articles for all the details.

1.2 Secure Two-Party Computation

It is well known that non-trivial two-party cryptographic primitives cannot be securely implemented if only error-free communication is available and there is no limitation assumed on the computing power and memory of the players. Fundamental examples of such primitives are bit commitment (BC) and oblivious transfer (OT). In BC, a committer C commits himself to a choice of a bit b by exchanging information with a verifier V. We want that V does not learn b (we say the commitment is hiding), yet C can later chose to reveal b in a convincing way, i.e., only the value fixed at commitment time will be accepted by V (we say the commitment is binding). In *Rabin OT*, a sender A sends a bit b to a receiver B by executing some protocol in such a way that B receives b with probability 1/2 and nothing with probability 1/2, yet A does not learn what was received.

Informally, BC is not possible with unconditional security since hiding means that when 0 is committed, exactly the same information exchange could have happened when committing to a 1. Hence, even if 0 was actually committed to, C could always compute a complete view of the protocol consistent with having committing to 1, and pretend that this was what he had in mind originally. A similar type of argument shows that OT is also impossible in this setting.

One might hope that allowing the protocol to make use of quantum communication would make a difference. Here, information is stored in qubits, i.e., in the state of two-level quantum mechanical systems, such as the polarization state of a single photon. It is well known that quantum information behaves in a way that is fundamentally different from classical information, enabling, for instance, unconditionally secure key exchange between two honest players. However, in the case of two mutually distrusting parties, we are not so fortunate: even with quantum communication, unconditionally secure BC and OT remain impossible [LC97, May97].

There are, however, several scenarios where these impossibility results do not apply, namely:

- if the computing power of players is bounded,
- if the communication is noisy,
- if the adversary is under some physical limitation, e.g., the size of the available memory is bounded.

The first scenario is the basis of many well known solutions based on plausible but unproven complexity assumptions, such as hardness of factoring or discrete logarithms. The second scenario has been used to construct both BC and OT protocols in various models for the noise [CK88, DFMS04, DKS99]. The third scenario is our focus here. In this model, OT and BC can be done using classical communication assuming, however, quite restrictive bounds on the adversary's memory size [CCM98, DHRS04], namely it can be at most quadratic in the memory size of honest players. Such an assumption is on the edge of being realistic, it would clearly be more satisfactory to have a larger separation between the memory size of honest players and that of the adversary. However, this was shown to be impossible [DM04].

In [DFSS05a], we study for the first time what happens if instead we consider protocols where quantum communication is used and we place a bound on the adversary's *quantum* memory size. There are two reasons why this may be a good idea: first, if we do not bound the classical memory size, we avoid the impossibility result of [DM04]. Second, the adversary's goal typically is to obtain a certain piece of classical information, however, converting quantum information to classical by measuring may irreversibly destroy information, and we may be able to arrange it such that the adversary cannot afford to loose information this way, while honest players can.

It turns out that this is indeed possible: we present protocols for both BC and OT in which n qubits are transmitted, where honest players need *no quantum memory*, but where the adversary must store at least $n/2$ qubits to break the protocol. We emphasize that no bounds are assumed on the adversary's computing power, nor on his classical memory. This is clearly much more promising than the classical case, not only from a theoretical point of view, but also in practice: while sending qubits and measuring them immediately as they arrive is well within reach of current technology, storing even a single qubit for more than a fraction of a second is a formidable technological challenge. Furthermore, we show that our protocols also work in a non-ideal setting where we allow the quantum source to be imperfect and the quantum communication to be noisy.

Our protocols are non-interactive, only one party sends information when doing OT, commitment or opening. Furthermore, the commitment protocol has the interesting property that the only message is sent to the committer, i.e., it is possible to commit while only *receiving* information. Such a scheme clearly does not exist without a bound on the committer's memory, even under computational assumptions and using quantum communication: a corrupt committer could always store (possibly quantumly) all the information sent, until opening time, and only then follow the the honest committer's algorithm to figure out what should be sent to convincingly open a 0 or a 1. Note that in the classical bounded-storage model, it is known how to do time-stamping that is non-interactive in our sense: a player can time-stamp a document while only receiving information [MSTS04]. However, no reasonable BC or protocol that time-stamps a bit exist in this model. It is straightforward to see that any such protocol can be broken by an adversary with classical memory of size twice that of an honest player, while our protocol requires no memory for the honest players and remains secure against any adversary not able to store more than half the size of the quantum transmission.

We also note that it has been shown earlier that BC is possible using quantum communication, assuming a different type of physical limitation, namely a bound on the size of coherent measurement that can be implemented [Sal98]. This limitation is incomparable to ours: it does not limit the total size of the memory, instead it limits the number of bits that can be simultaneously operated on to produce a classical result. Our adversary has a limit on the total memory size, but can measure all of it coherently. The protocol from [Sal98] is interactive, and requires a bound on the maximal measurement size that is sublinear in n.

On the technical side, we use privacy amplification against quantum adversaries by Renner and König [RK05] together with a proof technique by Shor and Preskill [SP00] where we purify the actions of honest players. This makes no difference from the adversary's point of view, but makes proofs go through more easily. We combine this with a new technical result that may be seen as a new type of uncertainty relation involving min-entropy (see Chapter 3).

After having established the possibility of secure Rabin oblivious transfer, we want to build the somewhat more practical primitive *1-2 OT* in the bounded quantum-storage model. In (chosen) *1-2 OT*, sender A holds two bits B_0, B_1 and receiver B can choose which bit he wants to receive. A secure protocol assures that a cheating sender $\widetilde{\mathsf{A}}$ does not learn B's choice bit (*receiver-privacy*) and a cheating $\widetilde{\mathsf{B}}$ learns only one of the two bits (*sender-privacy*). It turns out that already in the classical case, correctly defining the security of this seemingly simple primitive is a non-trival task. In [CSSW05], we adapt the definition of secure two-party computation of [Gol04] to the unconditional-secure case and derive from that a sufficient and complete definition of classical *1-2 OT*. In [DFSS05c], we establish a simple criterion using two-balanced functions for sender-privacy of *1-2 OT*. This characterisation is most practical when used in combination with privacy amplification and yields some more efficient (analyses of) reductions to weaker primitives.

In [DFRSS05], we will prove a quantum version of the characterisation of sender-privacy of classical *1-2 OT* and use that to prove secure a protocol for *1-2 OT* in the bounded quantum storage model.

1.3 Acknowledgements

First of all, I would like to greatly thank my supervisors Louis Salvail and Ivan Damgård. They were and still are doing an excellent job!

I am grateful to my (upcoming) co-authors Claude Crépeau, Serge Fehr, Renato Renner, George Savvides and Jürg Wullschleger for a lot of inspiring discussions.

A lot of thanks go to Claude Crépeau for hosting my visit at McGill University in Montreal from June to December 2005. I thank the DAIMI PhD committee for allowing me to postpone my qualification exam in order to spend formidable six months in this beautiful city. Special thanks go to my colocataire Jürg Wullschleger. Thanks to the McGill lab and everyone at Université de Montréal for creating such a nice atmosphere for doing quantum research.

Furthermore, I like to thank the whole BRICS staff for their well-working and always friendly support and my (ex) BRICS fellows for the great time.

Last but not least, I thank my family and Andrea for their great moral support.

I acknowledge financial support by the Project SECOQC, which is part of the 6th Framework Programme of the European Union.

Chapter 2

Preliminaries

2.1 Notation

For a set $I = \{i_1, i_2, \ldots, i_\ell\} \subseteq \{1, \ldots, n\}$ and a n-bit string $x \in \{0,1\}^n$, we define $x|_I := x_{i_1} x_{i_2} \cdots x_{i_\ell}$. For $x \in \{0,1\}^n$, $B^{\delta n}(x)$ denotes the set of all n-bit strings of Hamming distance at most δn from x. Note that the number of elements in $B^{\delta n}(x)$ is the same for all x, we denote it by $B^{\delta n} := |B^{\delta n}(x)|$. For a probability distribution Q over n-bit strings and a set $L \subseteq \{0,1\}^n$, we abbreviate the (overall) probability of L with $Q(L) := \sum_{x \in L} Q(x)$. All logarithms in this report are binary. We denote by $h(p)$ the binary entropy function $h(p) := -p \log p - (1-p) \log(1-p)$ with success probability p. We denote by $negl(n)$ any function of n smaller than any polynomial provided n is sufficiently large.

The basis $\{|0\rangle, |1\rangle\}$ denotes the computational or rectilinear or "+"-basis for the two-dimensional Hilbert space $\mathbb{C}^2$. 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 $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Measuring a qubit in the $+$-basis (resp. $\times$-basis) means applying the measurement described by projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ (resp. projectors $|0\rangle_\times\langle 0|_\times$ and $|1\rangle_\times\langle 1|_\times$). When the context requires it, we write $|0\rangle_+$ and $|1\rangle_+$ instead of $|0\rangle$ respectively $|1\rangle$; and for any $x \in \{0,1\}^n$ and $\theta \in \{+, \times\}$, we write $|x\rangle_\theta = \bigotimes_{i=1}^n |x_i\rangle_\theta$. If we want to choose the $+$ or $\times$-basis according to the bit $b \in \{0,1\}$, we write $\{+, \times\}_{[b]}$.

2.2 (Quantum) Probability Theory

As basis for the security definitions and proofs of our protocols, we are using the formalism introduced in [RK05], which we briefly summarize here.

2.2.1 Random Variables and Random States

Classical random variables $X, Y, \ldots$ have (joint) distributions $P_X, P_Y, P_{XY}, \ldots$ over finite domains $\mathcal{X}, \mathcal{Y}, \mathcal{X} \times \mathcal{Y}, \ldots$. Henceforth, we use UNIF to denote a random variable with range $\{0,1\}$, uniformly distributed and independent of anything else. We say that X, Y and Z form a *Markov-chain*, denoted

$$X \leftrightarrow Y \leftrightarrow Z,$$

if X and Z are independent, given Y. Such a chain is always symmetric and equivalent to the condition that $P_{Z|XY} = P_{Z|Y}$, or $I(X; Z|Y) = 0$, where I is the conditional mutual information.

A *random state* $\boldsymbol{\rho}$ is a random variable with distribution $P_{\boldsymbol{\rho}}$, whose range is the set of density operators[1] of a fixed Hilbert space. The view of an observer (which is ignorant of the value of $\boldsymbol{\rho}$) is given by the quantum system described by the density operator $[\boldsymbol{\rho}] := \sum_\rho P_{\boldsymbol{\rho}}(\rho)\rho$. In general, for any event $\mathcal{E}$, we define $[\boldsymbol{\rho}|\mathcal{E}] := \sum_\rho P_{\boldsymbol{\rho}|\mathcal{E}}(\rho)\rho$. If $\boldsymbol{\rho}$ is dependent on some classical random variable X, with joint distribution $P_{X\boldsymbol{\rho}}$, we also write ρ_x instead of $[\boldsymbol{\rho}|X = x]$. Note that ρ_x is a density operator (for any fixed x) whereas ρ_X is again a random state. The overall quantum system is then given by $[\{X\} \otimes \boldsymbol{\rho}] = \sum_x P_X(x)\,\{x\} \otimes \rho_x$, where $\{x\} := |x\rangle\langle x|$ is the *state representation* of x and $\{X\}$ the corresponding random state. Obviously, $[\{X\} \otimes \boldsymbol{\rho}] = [\{X\}] \otimes [\boldsymbol{\rho}]$ if and only if ρ_X is independent of X, where the latter in particular implies that no information on X can be learned by observing only $\boldsymbol{\rho}$. By slight abuse of notation, we usually simply write X instead of $\{X\}$.

2.2.2 Distances

For two density matrices ρ and σ, we define the *trace distance* as $\delta(\rho, \sigma) := \frac{1}{2}\operatorname{tr}(|\rho - \sigma|)$. For classical random variables X and Y this reduces to the *variational distance* $\delta([\{X\}], [\{Y\}]) := \frac{1}{2}\operatorname{tr}(|[\{X\}] - [\{Y\}]|) = \frac{1}{2}\sum_x |P_X(x) - P_Y(x)|$. We define the *distance from uniform* given a random state $\boldsymbol{\rho}$ as follows

$$d(X \mid \boldsymbol{\rho}) := \delta\left([\{X\} \otimes \boldsymbol{\rho}], [\{\textsc{unif}\}] \otimes [\boldsymbol{\rho}]\right).$$

If $[\{X\} \otimes \boldsymbol{\rho}] \approx_\varepsilon [\{X\}] \otimes [\boldsymbol{\rho}]$, i.e. $[\{X\} \otimes \boldsymbol{\rho}]$ and $[\{X\}] \otimes [\boldsymbol{\rho}]$ are ε-close in terms of their trace distance, then the real system $[\{X\} \otimes \boldsymbol{\rho}]$ "behaves" as the ideal system $[\{X\}] \otimes [\boldsymbol{\rho}]$ except with probability ε [RK05] in that for any evolution of the system no observer can distinguish the real from the ideal one with advantage greater than $\varepsilon/2$ (or ε, depending on the exact definition of advantage). In this sense, if $d(X \mid \boldsymbol{\rho}) \leq \varepsilon$ holds, X can be used as a perfect key which is secure against an adversary holding $\boldsymbol{\rho}$ except with probability ε.

2.2.3 Entropies

When reviewing the privacy amplification theorem from [RK05], we briefly address the generalization of the classical *Rényi entropy* $H_\alpha(X)$ of order α of a random variable X to the Rényi entropy $S_\alpha(\rho)$ of order α of a density operator ρ. Otherwise, though, we are only using the classical Rényi entropy of order ∞, commonly known as the *min-entropy* $H_\infty(X) = -\log \max_x P_X(x)$.

In Section 6.2, we briefly use smooth Renyi entropy $H_\infty^\varepsilon(X)$ and its chain rule, we refer to [RW05, Ren05] for details.

2.3 Hash Functions and Balanced Functions

Let ℓ be an arbitrary positive integer.

Definition 2.3.1 (two-balanced function). *A binary function $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ is called* two-balanced *if for any $s_0, s_1 \in \{0,1\}^\ell$, the functions $\beta(s_0, \cdot)$ and $\beta(\cdot, s_1)$ are balanced (in the usual sense), i.e.,*

$$\left|\{\varsigma_1 \in \{0,1\}^\ell : \beta(s_0, \varsigma_1) = 0\}\right| = 2^\ell/2 \quad \text{and} \quad \left|\{\varsigma_0 \in \{0,1\}^\ell : \beta(\varsigma_0, s_1) = 0\}\right| = 2^\ell/2\,.$$

[1]A density operator is a hermitian matrix with non-negative eigenvalues and trace equal to one.

In case $\ell = 1$, the XOR is a two-balanced function, and up to addition of a constant the XOR is the *only* two-balanced function.

A class $\mathcal{F}$ of hash functions from, say, $\{0,1\}^n$ to $\{0,1\}^\ell$ is *two-universal* if for any pair $x, y \in \{0,1\}^n$ with $x \neq y$

$$\big|\{f \in \mathcal{F} : f(x) = f(y)\}\big| \leq \frac{|\mathcal{F}|}{2^\ell}. \tag{2.1}$$

Several two-universal classes of hashing functions are such that evaluating and picking a function uniformly and at random in $\mathcal{F}$ can be done efficiently [CW77, WC79].

We call $\mathcal{F}$ a *strongly* two-universal class of hash functions, if for any distinct $x, y \in \{0,1\}^n$ the two random variables $F(x)$ and $F(y)$ are independent and uniformly distributed (over $\{0,1\}^\ell$), where the random variable F represents the random choice of a function in $\mathcal{F}$.

Proposition 2.3.2. *Let $\mathcal{F}_0$ and $\mathcal{F}_1$ be two classes of strongly two-universal hash functions from $\{0,1\}^{n_0}$ respectively $\{0,1\}^{n_1}$ to $\{0,1\}^\ell$, and let $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ be a two-balanced function. Consider the class $\mathcal{F}$ of all functions $f : \{0,1\}^{n_0} \times \{0,1\}^{n_1} \to \{0,1\}$ with $f(x_0, x_1) = \beta(f_0(x_0), f_1(x_1))$ where $f_0 \in \mathcal{F}_0$ and $f_1 \in \mathcal{F}_1$. Then, $\mathcal{F}$ is strongly two-universal.*

Proof: Fix distinct $x = (x_0, x_1)$ and $x' = (x'_0, x'_1)$ in $\{0,1\}^{n_0} \times \{0,1\}^{n_1}$. Assume without loss of generality that $x_1 \neq x'_1$. Fix $f_0 \in \mathcal{F}_0$, and set $s_0 = f_0(x_0)$ and $s'_0 = f_0(x'_0)$. By assumption on $\mathcal{F}_1$, the random variables $F_1(x_1)$ and $F_1(x'_1)$ are independently uniformly distributed over $\{0,1\}^\ell$ (where F_1 represents the random choice for $f_1 \in \mathcal{F}_1$). By the assumption on β, this implies that $\beta(f_0(x_0), F_1(x_1))$ and $\beta(f_0(x'_0), F_1(x'_1))$ are independently uniformly distributed (over $\{0,1\}$). This holds no matter how f_0 is chosen, and thus proves the claim. $\square$

As a side remark, it is easy to see that the claim does not hold in general for ordinary (as opposed to strongly) two-universal classes: if $n_0 = n_1 = \ell$ and $\mathcal{F}_0$ and $\mathcal{F}_1$ both only contain the identity function $id : \{0,1\}^\ell \to \{0,1\}^\ell$ (and thus are two-universal), then $\mathcal{F}$ consisting of the function $f(x_0, x_1) = \beta(id(x_0), id(x_1)) = \beta(x_0, x_1)$ is obviously not two-universal.

2.4 Privacy Amplification

Let $\mathcal{F}$ be a two-universal class of hashing functions from $\{0,1\}^n$ to one bit.

Theorem 2.4.1 ([RK05]). *Let X be distributed over $\{0,1\}^n$, and let $\boldsymbol{\rho}$ be a random state of q qubits[2]. Let F be the random variable corresponding to the random choice (with uniform distribution and independent from X and $\boldsymbol{\rho}$) of a member of a two-universal class of hashing functions $\mathcal{F}$. Then*

$$\begin{aligned}\delta([F(X) \otimes F \otimes \boldsymbol{\rho}], [\text{UNIF}] \otimes [F \otimes \boldsymbol{\rho}]) &\leq \frac{1}{2} 2^{-\frac{1}{2}(S_2([\{X\} \otimes \boldsymbol{\rho}]) - S_0([\boldsymbol{\rho}]) - 1)} \\ &\leq \frac{1}{2} 2^{-\frac{1}{2}(H_\infty(X) - q - 1)}. \end{aligned} \tag{2.2}$$

The first inequality is the original theorem from [RK05], and (2.2) follows by observing that $S_2([\{X\} \otimes \boldsymbol{\rho}]) \geq H_2(X) \geq H_\infty(X)$. In this paper, we only use this weaker version of the theorem.

[2]Remember that $\boldsymbol{\rho}$ can be correlated with X in an arbitrary way. In particular, we can think of $\boldsymbol{\rho}$ as an attempt to store the n-bit string X in q qubits.

Note that if the rightmost term of (2.2) is negligible, i.e. say smaller than $2^{-\varepsilon n}$, then this situation is $2^{-\varepsilon n}$-close to the ideal situation where $F(X)$ is perfectly uniform and independent of $\boldsymbol{\rho}$ and F. In particular, the situations $F(X) = 0$ and $F(X) = 1$ are statistically indistinguishable given $\boldsymbol{\rho}$ and F [FvdG99].

The following lemma is a direct consequence of Theorem 2.4.1. In Section 5.3, this lemma will be useful for proving the binding condition of our commitment scheme. Recall that for $X \in \{0,1\}^n$, $B^{\delta n}(X)$ denotes the set of all n-bit strings at Hamming distance at most δn from X and $B^{\delta n} := |B^{\delta n}(X)|$ is the number of such strings.

Lemma 2.4.2. *Let X be distributed over $\{0,1\}^n$, let $\boldsymbol{\rho}$ be a random state of q qubits and let $\hat{X}$ be a guess for X given $\boldsymbol{\rho}$. Then, for all $\delta < \frac{1}{2}$ it holds that*

$$\Pr\left[\hat{X} \in B^{\delta n}(X)\right] \leq 2^{-\frac{1}{2}(H_\infty(X)-q-1)+\log(B^{\delta n})}.$$

In other words, given a quantum memory of q qubits arbitrarily correlated with a classical random variable X, the probability to find $\hat{X}$ at Hamming distance at most δn from X where $nh(\delta) < \frac{1}{2}(H_\infty(X) - q)$ is negligible.

Proof: Here is a strategy to try to bias $F(X)$ when given $\hat{X}$ and $F \in_R \mathcal{F}$: Sample $X' \in_R B^{\delta n}(\hat{X})$ and output $F(X')$. Note that, using p_{succ} as a short hand for the probability $\Pr\left[\hat{X} \in B^{\delta n}(X)\right]$ to be bounded,

$$\begin{aligned}\Pr\left[F(X') = F(X)\right] &= \frac{p_{\text{succ}}}{B^{\delta n}} + \left(1 - \frac{p_{\text{succ}}}{B^{\delta n}}\right)\frac{1}{2} \\ &= \frac{1}{2} + \frac{p_{\text{succ}}}{2 \cdot B^{\delta n}},\end{aligned}$$

where the first equality follows from the fact that if $X' \neq X$ then, as $\mathcal{F}$ is two-universal, $\Pr\left[F(X) = F(X')\right] = \frac{1}{2}$. Since the probability of correctly guessing a binary $F(X)$ given F and $\boldsymbol{\rho}$ is always upper bounded by $\frac{1}{2} + \delta([F(X) \otimes F \otimes \boldsymbol{\rho}], [\text{UNIF}] \otimes [F \otimes \boldsymbol{\rho}])$, in combination with Theorem 2.4.1, the above results in

$$\frac{1}{2} + \frac{p_{\text{succ}}}{2 \cdot B^{\delta n}} \leq \frac{1}{2} + \frac{1}{2} 2^{-\frac{1}{2}(H_\infty(X)-q-1)}$$

and the claim follows immediately. $\square$

Chapter 3

Entropic Uncertainty Relations

3.1 Prior Work

One of the first things that comes to the mind of non-experts when quantum mechanics is the subject is Heisenberg's uncertainty principle [Hei27]. A lot of people remember to have heard of the fact that the laws of quantum mechanics do not allow us to simultaneously exactly determine two "incompatible" properties of a quantum system, for example the position *and* the speed of a particle.

In the same spirit, but phrased in terms of entropy of probability distributions, *entropic uncertainty relations* lowerbound the uncertainty we have when measuring a quantum state in two or more "incompatible", i.e. non-orthogonal, bases.

Definition 3.1.1 (mutually unbiased bases). *Two bases $\mathcal{B}^0 := \{|a_i\rangle\}_{i=1}^N$ and $\mathcal{B}^1 := \{|b_j\rangle\}_{j=1}^N$ of the complex Hilbert space $\mathbb{C}^N$ of dimension $N := 2^n$ are called* mutually unbiased *if*

$$\forall i,j \in \{1,\ldots,N\} : |\langle a_i|b_j\rangle|^2 = \frac{1}{N} = 2^{-n}.$$

More $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$ bases of this space $\mathbb{C}^N$ are called mutually unbiased*, if every pair of them is mutually unbiased.*

Stephen Wiesner showed in 1970 in one of the first articles about quantum cryptography that there are at least m mutually unbiased bases in a Hilbert space of dimension $2^{(m-1)!/2}$. Later, optimal constructions of $N+1$ mutually unbiased bases in a Hilbert space of dimension N were shown by Ivanović when N is prime [Ivo81] and by William Wootters and Brian Fields for N a prime power [WF89] (in particular, for $N = 2^n$ in the case of n qubits). Nice constructions based on the stabiliser formalism can be found in the article by Jay Lawrence, Časlav Brukner, and Anton Zeilinger [LBZ02] or in Thomas Brochmann Pedersen's PhD thesis [Ped05].

For a density matrix ρ describing the state of n qubits, let $Q^0(\cdot), Q^1(\cdot), \ldots, Q^M(\cdot)$ be the probability distributions over n-bitstring when measuring ρ in bases $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$, respectively. In the notation from above, we have $Q^0(i) = \langle a_i|\rho|a_i\rangle$ and $Q^1(j) = \langle b_j|\rho|b_j\rangle$.

David Deutsch proved one of the first entropic uncertainty relations for two bases using Shannon entropy [Deu83]. For mutually unbiased bases, the uncertainty relation reads

$$H(Q^0) + H(Q^1) \geq -2\log\frac{1}{2}(1 + \frac{1}{\sqrt{N}}).$$

A much stronger bound was first conjectured by Kraus [Kra87] and later proved by Maassen and Uffink [MU88]

$$H(Q^0) + H(Q^1) \geq \log N = n. \tag{3.1}$$

Intuitively, these bounds assure that if you know the outcome of measuring ρ in basis $\mathcal{B}^0$ pretty well, you have big uncertainty when measuring in the other basis $\mathcal{B}^1$.

Different results are known for complete sets of $N+1$ mutually unbiased bases of $\mathbb{C}^N$. All of them are based on a surprising geometrical result by Larsen [Lar90].

Theorem 3.1.2 ([Lar90]). *Let $Q^0, \ldots, Q^N$ be the $N+1$ distributions obtained by measuring state ρ in mutually unbiased bases $\mathcal{B}^0, \ldots, \mathcal{B}^N$. Then,*

$$\sum_{i=0}^{N} \pi(Q^i) = 1 + \operatorname{tr}(\rho^2), \tag{3.2}$$

where $\pi(Q) = \sum_x Q(x)^2$ denotes the collision probability of a distribution Q.

For a pure state $\rho = |\psi\rangle\langle\psi|$, $\operatorname{tr}(\rho^2) = 1$ holds and the right hand side of (3.2) equals 2. In this case, using Jensen's inequality, Sánchez-Ruiz[SR95] derives the following lower-bound on the sum of the collision entropies

$$\sum_{i=0}^{N} H_2(Q^i) = \sum_{i=0}^{N} -\log(\pi(Q^i)) \geq -(N+1)\log\left(\frac{\sum_{i=0}^{N}\pi(Q^i)}{N+1}\right) = (N+1)\log\left(\frac{N+1}{2}\right).$$

In cryptographic settings, we are interested in uncertainty relations over (possibly) incomplete sets of bases $\mathcal{B}^0, \ldots, \mathcal{B}^M$ with $1 \leq M \leq N$. The current state-of-the-art bound was independently obtained in [DPS04] and [Aza04] by subtracting the upper bound of the entropy in the bases not included in the sum:

$$\sum_{i=0}^{M} \pi(Q^i) \leq 2 - \frac{(N+1-(M+1))}{N} = \frac{N+M}{N}. \tag{3.3}$$

Theorem 3.1.3. *For $1 \leq M \leq N$, let $Q^0, \ldots, Q^M$ be the $M+1$ distributions obtained by measuring the pure state $|\psi\rangle$ in mutually unbiased bases $\mathcal{B}^0, \ldots, \mathcal{B}^M$.*

$$\sum_{i=0}^{M} H_2(Q^i) \geq (M+1)\log\left(\frac{N(M+1)}{N+M}\right). \tag{3.4}$$

Proof:

$$\begin{aligned}\sum_{i=0}^{M} H_2(Q^i) &= \sum_{i=0}^{M} -\log(\pi(Q^i)) \\ &\geq -(M+1)\log\left(\frac{\sum_{i=0}^{M}\pi(Q^i)}{M+1}\right) \geq (M+1)\log\left(\frac{N(M+1)}{N+M}\right).\end{aligned}$$

□

Notice that all the lower bounds on the collision entropy mentioned above imply bounds on the Shannon entropy because $H(Q) \geq H_2(Q)$, but do not say anything about the min-entropy $H_\infty(Q)$. In the following section, we derive entropic uncertainty relations involving min-entropies.

3.2 New Uncertainty Relations

For simplicity, we assume that $\mathcal{B}^0$ is the "computational" or $+$-basis and $\mathcal{B}^1$ the "diagonal" or $\times$-basis; the corresponding probabilities are Q^+ and $Q^\times$. We want to derive uncertainty relations in the flavor of the previous section, i.e. we want to show that these two distributions cannot *both* be "very far from uniform". One way to express this is to say that a distribution is very non-uniform if one can identify a subset of outcomes that has much higher probability than for a uniform choice. Intuitively, the theorem below says that such sets cannot be found for both measurements.

Theorem 3.2.1. *Let the density matrix ρ^A describe the state of a n-qubit register A. Let $Q^+(\cdot)$ and $Q^\times(\cdot)$ be the respective distributions of the outcome when register A is measured in the $+$-basis respectively the $\times$-basis. Then, for any two sets $L^+ \subset \{0,1\}^n$ and $L^\times \subset \{0,1\}^n$ it holds that*

$$Q^+(L^+) + Q^\times(L^\times) \leq \left(1 + \sqrt{2^{-n}|L^+||L^\times|}\right)^2 .$$

Proof: We can purify register A by adding a register B, such that the state of the composite system is pure. It can then be written as $|\psi\rangle^{AB} = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle^A |\varphi_x\rangle^B$ for some complex amplitudes α_x and normalised state vectors $|\varphi_x\rangle$.

Clearly, $Q^+(x) = |\alpha_x|^2$. To give a more explicit form of the distribution $Q^\times$, we apply the Hadamard transformation to register A:

$$(H^{\otimes n} \otimes \mathbb{1}^B)|\psi\rangle = \sum_{z\in\{0,1\}^n} |z\rangle \otimes \sum_{x\in\{0,1\}^n} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\alpha_x|\varphi_x\rangle$$

and obtain

$$Q^\times(z) = \left| \sum_{x\in\{0,1\}^n} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\alpha_x|\varphi_x\rangle \right|^2 .$$

Let $\overline{L}^+$ denote the complement of L^+ and p its probability $Q^+(\overline{L}^+)$. We can now split the sum in $Q^\times(z)$ in the following way:

$$\begin{aligned}
Q^\times(z) &= \left| \sum_{x\in\{0,1\}^n} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\alpha_x|\varphi_x\rangle \right|^2 \\
&= \left| \sqrt{p}\sum_{x\in\overline{L}^+} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\frac{\alpha_x}{\sqrt{p}}|\varphi_x\rangle + \sum_{x\in L^+} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\alpha_x|\varphi_x\rangle \right|^2 \\
&= \left| \sqrt{p}\cdot\zeta_z|\upsilon_z\rangle + \sum_{x\in L^+} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\alpha_x|\varphi_x\rangle \right|^2
\end{aligned}$$

where $|\upsilon_z\rangle$ is defined as follows: For the normalised state $|\upsilon\rangle := \sum_{x\in\overline{L}^+} \frac{\alpha_x}{\sqrt{p}}|x\rangle|\varphi_x\rangle$, $\zeta_z|\upsilon_z\rangle$ is the z-component of the state $H^{\otimes n}|\upsilon\rangle = \sum_z \zeta_z|z\rangle \otimes |\upsilon_z\rangle$. It therefore holds that $\sum_z |\zeta_z|^2 = 1$.

To upperbound the amplitudes provided by the sum over L^+, we notice that the amplitude is maximized when all unit vectors $|\varphi_x\rangle$ point in the same direction and when $(-1)^{x\cdot z}\alpha_x = |\alpha_x|$. More formally,

$$\begin{aligned}
\left|\sum_{x\in L^+} 2^{-\frac{n}{2}}(-1)^{x\cdot z}\alpha_x|\varphi_x\rangle\right| &\leq 2^{-\frac{n}{2}} \sum_{x\in L^+} |\alpha_x| \\
&\leq 2^{-\frac{n}{2}}\sqrt{|L^+|}\sqrt{\sum_{x\in L^+}|\alpha_x|^2} \qquad (3.5) \\
&\leq 2^{-\frac{n}{2}}\sqrt{|L^+|},
\end{aligned}$$

where (3.5) is obtained from the Cauchy-Schwarz inequality. Using ℓ^+ and $\ell^\times$ as shorthands for $|L^+|$ respectively $|L^\times|$, we conclude that

$$\begin{aligned}
Q^\times(L^\times) &= \sum_{z\in L^\times} Q^\times(z) \\
&\leq \sum_{z\in L^\times}\left(|\sqrt{p}\cdot\zeta_z|\upsilon_z\rangle| + 2^{-\frac{n}{2}}\sqrt{\ell^+}\right)^2 \\
&\leq p\sum_{z\in L^\times}|\zeta_z|^2 + 2\cdot 2^{-\frac{n}{2}}\sqrt{\ell^+}\sum_{z\in L^\times}|\zeta_z| + \ell^\times\cdot 2^{-n}\ell^+ \\
&\leq p + 2\cdot 2^{-\frac{n}{2}}\sqrt{\ell^+}\sqrt{\ell^\times\sum_{z\in L^\times}|\zeta_z|^2} + 2^{-n}\ell^+\ell^\times \qquad (3.6) \\
&\leq p + 2\sqrt{2^{-n}\ell^+\ell^\times} + 2^{-n}\ell^+\ell^\times \\
&= 1 - Q^+(L^+) + 2\sqrt{2^{-n}\ell^+\ell^\times} + 2^{-n}\ell^+\ell^\times. \qquad (3.7)
\end{aligned}$$

Inequality (3.6) follows again from Cauchy-Schwarz while in (3.7), we use the definition of p. The claim of the proposition follows after re-arranging the terms. □

This theorem yields a meaningful bound as long as $|L^+|\cdot|L^\times| < (\sqrt{2}-1)^2\cdot 2^n$, e.g. if L^+ and $L^\times$ both contain less than $2^{n/2}$ elements. If for $r \in \{+,\times\}$, L^r contains only the n-bit string with the maximal probability of Q^r, we obtain as a corollary a slightly weaker version of a known relation (see (9) in [MU88]).

Corollary 3.2.2. *Let q_∞^+ and $q_\infty^\times$ be the maximal probabilities of the distributions Q^+ and $Q^\times$ from above. It then holds that $q_\infty^+ \cdot q_\infty^\times \leq \frac{1}{4}(1+c)^4$ where $c = 2^{-n/2}$.*

Theorem 3.2.1 can be inductively generalised to $M+1$ mutually unbiased bases where $1 \leq M \leq N$ as seen in the previous section.

Theorem 3.2.3. *Let the density matrix ρ^A describe the state of a n-qubit register A and let for $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$ be mutually unbiased bases of register A. Let $Q^0(\cdot), Q^1(\cdot), \ldots, Q^M(\cdot)$*

be the distributions of the outcome when register A is measured in bases $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$, respectively. Then, for any sets $L^0, L^1, \ldots, L^M \subset \{0,1\}^n$, it holds that

$$\sum_{i=0}^{M} Q^i(L^i) \leq 1 - \binom{M+1}{2} + \sum_{0 \leq j < k \leq M} \left(1 + \sqrt{2^{-n}|L^j||L^k|}\right)^2. \tag{3.8}$$

Proof: Like in the proof of Theorem 3.2.1, we can purify register A by adding a register B. The composite state can then be written as $|\psi\rangle^{AB} = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle^A |\varphi_x\rangle^B$ for some complex amplitudes α_x and normalised state vectors $|\varphi_x\rangle$.

We prove the statement by induction over M: For $M = 1$, by applying an appropriate unitary transform to the whole system, we can assume without loss of generality that $\mathcal{B}^0$ is the standard $+$-basis.

Let us denote by T the matrix of the basis change from $\mathcal{B}^0$ to $\mathcal{B}^1$. As the inner product between states $|\phi\rangle \in \mathcal{B}^0$ and $|\phi'\rangle \in \mathcal{B}^1$ is always $|\langle\phi|\phi'\rangle| = 2^{-n/2}$, it follows that all entries of T are complex numbers of the form $2^{-n/2} \cdot e^{i\lambda}$ for real $\lambda \in \mathbb{R}$.

It is easy to verify that the same proof as for Theorem 3.2.1 applies after replacing the Hadamard transform $H^{\otimes n}$ on the sender's part by T and using the above observation about the entries of T.

For the induction step from M to $M+1$, we define $p := Q^0(\overline{L}^0)$, $|\upsilon\rangle := \sum_{x \in \overline{L}^0} \frac{\alpha_x}{\sqrt{p}} |x\rangle|\varphi_x\rangle$, and let $\zeta_z^j |\upsilon_z^j\rangle$ be the z-component of the state $|\upsilon\rangle$ transformed into basis $\mathcal{B}^j$. As in the proof of Theorem 3.2.1, using ℓ_i as a short hand for $\left|L^i\right|$, it follows:

$$\begin{aligned}
\sum_{i=1}^{M} Q^i(L^i) &= \sum_{i=1}^{M} \sum_{z \in L^i} Q^i(z) \\
&\leq \sum_{i=1}^{M} \sum_{z \in L^i} \left(\sqrt{p}\,\left|\zeta_z^i|\upsilon_z^i\rangle\right| + 2^{-n/2}\sqrt{\ell_0}\right)^2 \\
&\leq p \cdot \sum_{i=1}^{M} \sum_{z \in L^i} |\zeta_z^i|^2 + \sum_{i=1}^{M} \left(2 \cdot \sqrt{2^{-n}\ell_0\ell_i} + 2^{-n}\ell_0\ell_i\right) \\
&\leq p \cdot \sum_{i=1}^{M} P^i(L^i) + \sum_{i=1}^{M} \left(1 - \sqrt{2^{-n}\ell_0\ell_i}\right)^2 - M
\end{aligned}$$

where the distributions P^i are obtained by measuring register A of the normalised state $|\upsilon\rangle$ in the mutually unbiased bases $\mathcal{B}^1, \mathcal{B}^2, \ldots, \mathcal{B}^M$. We apply the induction hypothesis to the sum of $P^i(L^i)$:

$$\begin{aligned}\sum_{i=1}^{M} Q^i(L^i) &\leq p \cdot \sum_{i=1}^{M} P^i(L^i) + \sum_{i=1}^{M} \left(1 + \sqrt{2^{-n}\ell_0\ell_i}\right)^2 - M \\ &\leq \left[1 - Q^0(L^0)\right] \left[\sum_{1 \leq j < k \leq M} \left(1 + \sqrt{2^{-n}\ell_j\ell_k}\right)^2 + 1 - \binom{M}{2} \right] \\ &\quad + \sum_{i=1}^{M} \left(1 - \sqrt{2^{-n}\ell_0\ell_i}\right)^2 - M \\ &\leq -Q^0(L^0) + 1 - \binom{M+1}{2} + \sum_{0 \leq j < k \leq M} \left(1 + \sqrt{2^{-n}\ell_j\ell_k}\right)^2\end{aligned}$$

where the last inequality follows by observing that the term in the right bracket is at least 1 and rearranging the terms. This completes the induction step and the proof of the proposition. □

If we aim for an entropic uncertainty relation involving min-entropies, we consider the case where the sets L^i consist only of the n-bit string with the maximal probability. For each i, we call this string x_i with probability $q^i_\infty := Q^i(x_i)$. Just applying Theorem 3.2.3 yields a meaningful lowerbound on the sum of the min-entropies for up to $M \leq 2^{(1/4-\varepsilon)n}$ mutually unbiased bases:

$$\sum_{i=0}^{M} H^i_\infty \geq (M+1)\left(\log(M+1) - negl(n)\right).$$

The reason why it does not work for larger M is that there are $\binom{M+1}{2} \sim M^2$ summands containing $2^{-n/2}$ in (3.8) which is not negligible anymore. The following slightly more careful analysis proceeds along the lines of the proofs of Theorem 3.2.1 and Theorem 3.2.3, but is tailored for this special case. It yields a more precise result which holds for up to $M \leq 2^{n/2}$ bases.

For the normalised state $|\upsilon\rangle := \sum_{z \neq x_0} \frac{\alpha_z}{\sqrt{1-q^0_\infty}} |z\rangle|\varphi_z\rangle$, $\zeta_i|\upsilon_i\rangle$ is the x_i-component of the state $|\upsilon\rangle$ in basis $\mathcal{B}^i$. Formally, if T is the basis transform from $\mathcal{B}^0$ to $\mathcal{B}^i$, then $T|\upsilon\rangle =$

$\sum_z \zeta_z|z\rangle \otimes |\upsilon_z\rangle$ and $\zeta_i|\upsilon_i\rangle := \zeta_{x_i}|\upsilon_{x_i}\rangle$. For two bases, we obtain

$$\begin{aligned}
q^1_\infty &= \left| \sum_{z\in\{0,1\}^n} 2^{-\frac{n}{2}}(-1)^{z\cdot x_1}\alpha_z|\varphi_z\rangle \right|^2 \\
&= \left| \sqrt{1-q^0_\infty} \sum_{z\neq x_0} 2^{-\frac{n}{2}}(-1)^{z\cdot x_1} \frac{\alpha_z}{\sqrt{1-q^0_\infty}}|\varphi_z\rangle + 2^{-\frac{n}{2}}(-1)^{x_0\cdot x_1}\alpha_{x_0}|\varphi_{x_0}\rangle \right|^2 \\
&\leq \left(\sqrt{1-q^0_\infty}\,|\zeta_1|\upsilon_1\rangle| + 2^{-\frac{n}{2}}\,|(-1)^{x_0\cdot x_1}\alpha_{x_0}|\varphi_{x_0}\rangle| \right)^2 \\
&= \left(\sqrt{1-q^0_\infty}\,|\zeta_1| + 2^{-\frac{n}{2}}\sqrt{q^0_\infty} \right)^2 \\
&= (1-q^0_\infty)|\zeta_1|^2 + \underbrace{2\sqrt{(1-q^0_\infty)q^0_\infty}}_{\leq 1} 2^{-n/2}|\zeta_1| + 2^{-n}q^0_\infty \\
&\leq (1-q^0_\infty)|\zeta_1|^2 + 2^{-n/2}|\zeta_1| + 2^{-n}q^0_\infty.
\end{aligned} \tag{3.9}$$

Hence, we have

$$q^0_\infty + q^1_\infty \leq 1 + 2^{-n/2} + 2^{-n} = (1 + \frac{1}{2}2^{-n/2} + O(2^{-n}))^2 \tag{3.10}$$

In the same way as (3.9), we can derive

$$q^2_\infty \leq (1-q^0_\infty)|\zeta_2|^2 + 2^{-n/2}|\zeta_2| + 2^{-n}q^0_\infty$$

Adding this to (3.9), we obtain

$$q^1_\infty + q^2_\infty \leq (1-q^0_\infty)(|\zeta_1|^2 + |\zeta_2|^2) + 2^{-n/2}(|\zeta_1| + |\zeta_2|) + 2\cdot 2^{-n}q^0_\infty. \tag{3.11}$$

Note that $|\zeta_1|^2$ and $|\zeta_2|^2$ are the probabilities to obtain the n-bit strings x_1 and x_2 when measuring $|\upsilon\rangle$ in the mutually unbiased bases $\mathcal{B}^1$ and $\mathcal{B}^2$ and therefore, we can use (3.10) to upperbound this probability:

$$|\zeta_1|^2 + |\zeta_2|^2 \leq 1 + 2^{-n/2} + 2^{-n} \text{ and } |\zeta_1| + |\zeta_2| \leq \sqrt{2}(1 + \frac{1}{2}2^{-n/2} + O(2^{-n})).$$

Using these bounds in (3.11) yields

$$\begin{aligned}
q^0_\infty + q^1_\infty + q^2_\infty &\leq 1 + 2^{-n/2} + 2^{-n} + 2^{-n/2}(\sqrt{2}(1 + \frac{1}{2}2^{-n/2} + O(2^{-n}))) + q^0_\infty(2^{-n} - 2^{-n/2}) \\
&= 1 + 2^{-n/2}(\sqrt{2}+1) + 2^{-n}(\frac{\sqrt{2}}{2} + 1) + O(2^{-3n/2}) + q^0_\infty(2^{-n} - 2^{-n/2}) \\
&\leq (1 + 2^{-n/2}\frac{\sqrt{2}+1}{2} + O(2^{-n}))^2
\end{aligned}$$

We continue this process to obtain

$$\sum_{i=0}^{3} q_\infty^i \leq 1 + 2^{-n/2}(\sqrt{2}+1) + 2^{-n}(\frac{\sqrt{2}}{2}+1) + O(2^{-3n/2})$$
$$+ 2^{-n/2}(\sqrt{3}(1+\frac{\sqrt{2}+1}{2}2^{-n/2}+O(2^{-n}))) + q_\infty^0(2^{-n}(3-\frac{\sqrt{2}}{2}-1) - 2^{-n/2}(\sqrt{2}+1))$$
$$= 1 + 2^{-n/2}(\sqrt{3}+\sqrt{2}+1) + 2^{-n}(\sqrt{3}\frac{\sqrt{2}+1}{2}+\frac{\sqrt{2}}{2}+1) + O(2^{-3n/2})$$
$$+ q_\infty^0(2^{-n}(2-\frac{\sqrt{2}}{2}) - 2^{-n/2}(\sqrt{2}+1))$$
$$= (1 + 2^{-n/2}\frac{\sqrt{3}+\sqrt{2}+1}{2} + O(2^{-n}))^2$$

For general $M \in \mathbb{N}$, we have

$$\sum_{i=0}^{M} q_\infty^i \leq 1 + 2^{-n/2}\kappa_M + 2^{-n}\mu_M + O(2^{-3n/2}) + q_\infty^0(2^{-n}(M-\kappa_{M-1}) - 2^{-n/2}(\mu_{M-1})), \quad (3.12)$$

where the constants κ_M and λ_M can be seen by a iterative derivation as above to be

$$\kappa_M = \sum_{j=1}^{M}\sqrt{j} \quad \text{and} \quad \mu_M = \sum_{k=1}^{M}\frac{\sqrt{k}}{2}\kappa_{k-1} = \sum_{k=1}^{M}\frac{\sqrt{k}}{2}\sum_{j=1}^{k-1}\sqrt{j}.$$

For $M \to \infty$, they grow according to $\kappa_M \sim \frac{2}{3}M^{3/2} + O(\sqrt{M})$ and $\mu_M \sim \frac{1}{9}M^3 + O(M^2)$. Hence, for large enough M, the last q_∞^0-term in (3.12) is always negative, because $M < \kappa_M$ for large enough M. Therefore, we end up with the asymptotics

$$\sum_{i=0}^{M} q_\infty^i \leq 1 + 2^{-n/2}\left(\frac{2}{3}M^{3/2} + O(\sqrt{M})\right) + 2^{-n}\left(\frac{1}{9}M^3 + O(M^2)\right) + O(2^{-3n/2})$$

For the rest of the section, we assume that $M \leq 2^{(\frac{1}{2}-\varepsilon)n}$ and therefore, $O(\sqrt{M/N})$ and $O(M^2/N)$ are negligible in n. We get

$$\sum_{i=0}^{M} q_\infty^i \leq \frac{N + 2\frac{1}{3}\sqrt{NM^3} + \frac{1}{9}M^3 + negl(n)}{N} = \frac{(\sqrt{N}+\frac{1}{3}M^{3/2})^2 + negl(n)}{N}$$

As in the proof of Theorem 3.1.3, we use Jensen's inequality to conclude

$$\sum_{i=0}^{M} H_\infty^i(Q^i) = \sum_{i=0}^{M} -\log(q_\infty^i)$$
$$\geq -(M+1)\log\left(\frac{\sum_{i=0}^{M} q_\infty^i}{M+1}\right) \geq (M+1)\log\left(\frac{N(M+1)}{(\sqrt{N}+\frac{1}{3}M^{3/2})^2 + negl(n)}\right).$$

To summarize, we obtained

Theorem 3.2.4. *For an $\varepsilon > 0$, let $1 \leq M \leq 2^{(\frac{1}{2}-\varepsilon)n}$. The matrix ρ^A describes the state of a n-qubit register A and $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$ are mutually unbiased bases of register A. Let $Q^0(\cdot), Q^1(\cdot), \ldots, Q^M(\cdot)$ be the distributions of the outcome when ρ^A is measured in bases $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$. We denote by H^i_∞ the min-entropy of distribution Q^i. Then,*

$$\sum_{i=0}^{M} H^i_\infty \geq (M+1) \log \left(\frac{N(M+1)}{(\sqrt{N} + \frac{1}{3}M^{3/2})^2 + negl(n)} \right).$$

For $1 \leq M \leq 2^{(\frac{1}{3}-\varepsilon)n}$, this simplifies to

$$\sum_{i=0}^{M} H^i_\infty \geq (M+1) \left(\log(M+1) - negl(n) \right).$$

Chapter 4

Rabin Oblivious Transfer

4.1 The Definition

A protocol for Rabin Oblivious Transfer (*Rabin OT*) between sender Alice and receiver Bob allows Alice to send a bit b through an erasure channel to Bob. Each transmission delivers b or an erasure with probability $\frac{1}{2}$. Intuitively, a protocol for *Rabin OT* is secure if

- sender Alice gets no information on whether b was received or not, no matter what she does, and
- receiver Bob gets no information about b with probability at least $\frac{1}{2}$, no matter what he does.

In this report, we are considering quantum protocols for *Rabin OT*. This means that while in- and outputs of the honest senders are classical, described by random variables, the protocol may contain quantum computation and quantum communication, and the view of a dishonest player is quantum, and is thus described by a random state.

Any such (two-party) protocol is specified by a family $\{(\mathsf{A}_n, \mathsf{B}_n)\}_{n>0}$ of pairs of interactive quantum circuits (i.e. interacting through a quantum channel). Each pair is indexed by a security parameter $n > 0$, where A_n and B_n denote the circuits for sender Alice and receiver Bob, respectively. In order to simplify the notation, we often omit the index n, leaving the dependency on it implicit.

For the formal definition of the security requirements of a *Rabin OT* protocol, let us fix the following notation. Let B denote the binary random variable describing A's input bit b, and let A and B' denote the binary random variables describing B's two output bits, where the meaning is that A indicates whether the bit was received or not. Furthermore, for a dishonest sender $\widetilde{\mathsf{A}}$ (respecively $\widetilde{\mathsf{B}}$) let $\boldsymbol{\rho}_{\widetilde{\mathsf{A}}}$ ($\boldsymbol{\rho}_{\widetilde{\mathsf{B}}}$) denote the random state describing $\widetilde{\mathsf{A}}$'s ($\widetilde{\mathsf{B}}$'s) view of the protocol. Note that for a fixed candidate protocol for *Rabin OT*, and for a fixed input distribution P_B, depending on whether we consider two honest A and B, a dishonest $\widetilde{\mathsf{A}}$ and an honest B, or an honest A and a dishonest $\widetilde{\mathsf{B}}$, the corresponding joint distribution $P_{BAB'}$, $P_{\boldsymbol{\rho}_{\widetilde{\mathsf{A}}}AB'}$ respectively $P_{B\boldsymbol{\rho}_{\widetilde{\mathsf{B}}}}$ is uniquely determined.

Definition 4.1.1. *A two-party (quantum) protocol* (A, B) *is a* **(statistically) secure *Rabin OT*** *if the following holds.*

Correctness: *For honest* A *and* B

$$\Pr\left[B = B' | A = 1\right] \geq 1 - negl(n) .$$

Privacy: *For any* $\widetilde{\mathsf{A}}$
$$\delta([A \otimes \boldsymbol{\rho}_{\widetilde{\mathsf{A}}}], [\text{UNIF}] \otimes [\boldsymbol{\rho}_{\widetilde{\mathsf{A}}}]) \leq negl(n)\,.$$

Obliviousness: *For any* $\widetilde{\mathsf{B}}$ *there exists an event* $\mathcal{E}$ *with* $P[\mathcal{E}] \geq \frac{1}{2} - negl(n)$ *such that*
$$\delta([B \otimes \boldsymbol{\rho}_{\widetilde{\mathsf{B}}}|\mathcal{E}], [B] \otimes [\boldsymbol{\rho}_{\widetilde{\mathsf{B}}}|\mathcal{E}]) \leq negl(n)\,.$$

If any of the above trace distances equals 0, then the corresponding property is said to hold **perfectly**. *If one of the properties only holds with respect to a restricted class* $\mathfrak{A}$ *of* $\widetilde{\mathsf{A}}$*'s respectively* $\mathfrak{B}$ *of* $\widetilde{\mathsf{B}}$*'s, then this property is said to hold and the protocol is said to be secure* **against** $\mathfrak{A}$ *respectively* $\mathfrak{B}$.

Privacy requires that the joint quantum state is essentially the same as when A is uniformly distributed and independent of the senders's view, and obliviousness requires that there exists some event which occurs with probability at least $\frac{1}{2}$ (the event that the receiver does not receive the bit) and under which the joint quantum state is essentially the same as when B is distributed (according to P_B) independently of the receiver's view.

4.2 The Protocol

We introduce a quantum protocol for *Rabin OT* that will be shown perfectly private (against any sender) and statistically oblivious against any quantum memory-bounded receiver.

The protocol is very simple (see Figure 4.1): A picks $x \in_R \{0,1\}^n$ and sends to B n qubits in state either $|x\rangle_+$ or $|x\rangle_\times$ each chosen with probability $\frac{1}{2}$. B then measures all received qubits either in the rectilinear or in the diagonal basis. With probability $\frac{1}{2}$, B picked the right basis and gets x, while any $\widetilde{\mathsf{B}}$ that is forced to measure part of the state (due to a memory bound) can only have full information on x in case the $+$-basis was used *or* in case the $\times$-basis was used (but not in both cases). Privacy amplification using any two-universal class of hashing functions $\mathcal{F}$ allows to obtain a proper *Rabin OT*. (In order to avoid aborting, we specify that if a dishonest $\widetilde{\mathsf{A}}$ refuses to participate, or sends data in incorrect format, then B samples its output bits a and b' both at random in $\{0,1\}$.)

QOT(b)**:**

1. A picks $x \in_R \{0,1\}^n$, and $r \in_R \{+,\times\}$.
2. A sends $|\psi\rangle := |x\rangle_r$ in basis r to B.
3. B picks $r' \in_R \{+,\times\}$ and measures all qubits of $|\psi\rangle$ in basis r'. Let $x' \in \{0,1\}^n$ be the result.
4. A announces r, $f \in_R \mathcal{F}$, and $s := b \oplus f(x)$.
5. B outputs $a := 1$ and $b' := s \oplus f(x')$ if $r' = r$ and else $a := 0$ and $b' := 0$.

Figure 4.1. Protocol for Rabin QOT

As we shall see in Section 4.4, the security of the QOT protocol against receivers with bounded-size quantum memory holds as long as the bound applies before Step 4 is reached.

An equivalent protocol is obtained by purifying the sender's actions. Although QOT is easy to implement, the purified or EPR-based version depicted in Figure 4.2 is easier to prove secure. A similar approach was taken in the Shor-Preskill proof of security for the BB84 quantum key distribution scheme [SP00].

EPR-QOT(b):

1. A prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. A sends one half of each pair to B and keeps the other halves.
3. B picks $r' \in_R \{+, \times\}$ and measures all received qubits in basis r'. Let $x' \in \{0,1\}^n$ be the result.
4. A picks $r \in_R \{+, \times\}$, and measures all kept qubits in basis r. Let $x \in \{0,1\}^n$ be the outcome. A announces r, $f \in_R \mathcal{F}$, and $s := b \oplus f(x)$.
5. B outputs $a := 1$ and $b' := s \oplus f(x')$ if $r' = r$ and else $a := 0$ and $b' := 0$.

Figure 4.2. Protocol for EPR-based Rabin QOT

Notice that while QOT requires no quantum memory for honest players, quantum memory for A seems to be required in EPR-QOT. The following Lemma shows the strict equivalence between QOT and EPR-QOT.

Lemma 4.2.1. QOT *is secure if and only if* EPR-QOT *is secure.*

The proof follows easily after observing that A's choices of r and f, together with the measurements all commute with B's actions. Therefore, they can be performed right after Step 1 with no change for B's view. Modifying EPR-QOT that way results in QOT.

Lemma 4.2.2. EPR-QOT *is perfectly private.*

Proof: It is straightforward to verify that no information about whether B has received the bit is leaked to any sender $\widetilde{\mathsf{A}}$, since B does not send anything, i.e. EPR-QOT is non-interactive! □

4.3 Modeling Dishonest Receivers

We model dishonest receivers in EPR-QOT under the assumption that the maximum size of their quantum storage is bounded. These adversaries are only required to have bounded quantum storage when they reach Step 4 in EPR-QOT. Before that, the adversary can store and carry out quantum computations involving any number of qubits. Apart from the restriction on the size of the quantum memory available to the adversary, no other assumption is made. In particular, the adversary is not assumed to be computationally bounded and the size of its classical memory is not restricted.

Definition 4.3.1. *The set $\mathfrak{B}_\gamma$ denotes all possible quantum dishonest receivers $\{\widetilde{\mathsf{B}}_n\}_{n>0}$ in* QOT *or* EPR-QOT *where for each $n > 0$, $\widetilde{\mathsf{B}}_n$ has quantum memory of size at most γn when Step 4 is reached.*

In general, the adversary $\widetilde{\mathsf{B}}$ is allowed to perform any quantum computation compressing the n qubits received from A into a quantum register M of size at most γn when Step 4 is reached. More precisely, the compression function is implemented by some unitary transform C acting upon the quantum state received and an ancilla of arbitrary size. The compression is performed by a measurement that we assume in the computational basis without loss of generality. Before starting Step 4, the adversary first applies a unitary transform C:

$$2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle \otimes C|x\rangle|0\rangle \mapsto 2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle \otimes \sum_y \alpha_{x,y} |\varphi_{x,y}\rangle^M |y\rangle^Y,$$

where for all x, $\sum_y |\alpha_{x,y}|^2 = 1$. Then, a measurement in the computational basis is applied to register Y providing classical outcome y. The result is a quantum state in register M of size γn qubits. Ignoring the value of y to ease the notation, the re-normalized state of the system is now in its most general form when Step 4 is reached:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \otimes |\varphi_x\rangle^M,$$

where $\sum_x |\alpha_x|^2 = 1$.

4.4 Security against Dishonest Receivers

In this section, we show that EPR-QOT is secure against any dishonest receiver having access to a quantum storage device of size strictly smaller than half the number of qubits received at Step 2.

In our setting, we use Theorem 3.2.1 to lowerbound the overall probability of strings with small probabilities in the following sense. For $0 \leq \gamma + \kappa \leq 1$, define

$$S^+ := \left\{x \in \{0,1\}^n : Q^+(x) \leq 2^{-(\gamma+\kappa)n}\right\} \text{ and}$$
$$S^\times := \left\{z \in \{0,1\}^n : Q^\times(z) \leq 2^{-(\gamma+\kappa)n}\right\}$$

to be the sets of strings with small probabilities and denote by $L^+ := \overline{S}^+$ and $L^\times := \overline{S}^\times$ their complements. (Here's the mnemonic: S for the strings with Small probabilities, L for Large.) Note that for all $x \in L^+$, we have that $Q^+(x) > 2^{-(\gamma+\kappa)n}$ and therefore $|L^+| < 2^{(\gamma+\kappa)n}$. Analogously, we have $|L^\times| < 2^{(\gamma+\kappa)n}$. For the ease of notation, we abbreviate the probabilities that strings with small probabilities occur as follows: $q^+ := Q^+(S^+)$ and $q^\times := Q^\times(S^\times)$. The next corollary now immediately follows from Theorem 3.2.1.

Corollary 4.4.1. *Let $\gamma + \kappa < \frac{1}{2}$. For the probability distributions Q^+, $Q^\times$ and the sets S^+, $S^\times$ defined above, we have*

$$q^+ + q^\times := Q^+(S^+) + Q^\times(S^\times) \geq 1 - \mathit{negl}(n).$$

Theorem 4.4.2. *For all $\gamma < \frac{1}{2}$,* QOT *is secure against $\mathfrak{B}_\gamma$.*

Proof: After Lemmata 4.2.1 and 4.2.2, it remains to show that EPR-QOT is oblivious against $\mathfrak{B}_\gamma$. Since $\gamma < \frac{1}{2}$, we can find $\kappa > 0$ with $\gamma + \kappa < \frac{1}{2}$. Consider a dishonest receiver in EPR-QOT $\widetilde{\mathsf{B}}$ with quantum memory of size γn.

Using the notation from Section 4.1, we show that there exists an event $\mathcal{E}$ such that $P[\mathcal{E}] \geq \frac{1}{2} - negl(n)$ as well as $\delta([B \otimes \boldsymbol{\rho}_{\widetilde{\mathsf{B}}}|\mathcal{E}], [B] \otimes [\boldsymbol{\rho}_{\widetilde{\mathsf{B}}}|\mathcal{E}]) \leq negl(n)$, as required by the obliviousness condition of Definition 4.1.1. Let X denote the random variable describing the outcome x of A's measurement (in basis r) in Step 4 of EPR-QOT. We implicitely understand the distribution of X to be conditioned on the classical outcome y of the measurement $\widetilde{\mathsf{B}}$ performs, as described in Section 4.3. We define $\mathcal{E}$ to be the event $X \in S^r$. Note that $\mathcal{E}$ is independent of B and thus $[B|\mathcal{E}] = [B]$. Furthermore, due to the uniform choice of r, and using Corollary 4.4.1, $P[\mathcal{E}] = \frac{1}{2}(q^+ + q^\times) \geq \frac{1}{2} - negl(n)$.

In order to show the second condition, we have to show that whenever $\mathcal{E}$ occurs, the dishonest receiver cannot distinguish the situation where $B = 0$ is sent from the one where $B = 1$ is sent. As the bit B is masked by the output of the hash function $F(X)$ in Step 4 of EPR-QOT (where the random variable F represents the random choice for f), this is equivalent to distinguish between $F(X) = 0$ and $F(X) = 1$. This situation is exactly suited for applying Theorem 2.4.1, which says that $F(X) = 0$ is indistinguishable from $F(X) = 1$ whenever the right-hand side of (2.2) is negligible.

In the case $r = +$, we have

$$H_\infty(X|X \in S^+) = -\log\left(\max_{x\in S^+} \frac{Q^+(x)}{q^+}\right)$$
$$\geq -\log\left(\frac{2^{-(\gamma+\kappa)n}}{q^+}\right) = \gamma n + \kappa n + \log(q^+). \tag{4.1}$$

If $q^+ \geq 2^{-\frac{\kappa}{2}n}$ then $H_\infty(X|X \in S^+) \geq \gamma n + \frac{\kappa}{2}n$ and indeed the right-hand side of (2.2) decreases exponentially when conditioning on $X \in S^+$. The corresponding holds for the case $r = \times$.

Finally, if $q^+ < 2^{-\frac{\kappa}{2}n}$ (or similarly $q^\times < 2^{-\frac{\kappa}{2}n}$) then instead of as above we define $\mathcal{E}$ as the *empty event* if $r = +$ and as the event $X \in S^\times$ if $r = \times$. It follows that $P[\mathcal{E}] = \frac{1}{2} \cdot q^\times \geq \frac{1}{2} - negl(n)$ as well as $H_\infty(X|\mathcal{E}) = H_\infty(X|X \in S^\times) \geq \gamma n + \kappa n + \log(q^\times) \geq \gamma n + \frac{\kappa}{2}n$ (for n large enough), both by Corollary 4.4.1 and the bound on q^+. □

4.5 Weakening the Assumptions

Observe that QOT requires error-free quantum communication, in that a transmitted bit b, that is encoded by the sender and measured by the receiver using the same basis, is always received as b. And it requires a perfect quantum source which on request produces *one* qubit in the right state, e.g. *one* photon with the right polarization. Indeed, in case of noisy quantum communication, an honest receiver in QOT is likely to receive an incorrect bit, and the obliviousness of QOT is vulnerable to imperfect sources that once in while transmit more than one qubit in the same state: a malicious receiver $\widetilde{\mathsf{B}}$ can easily determine the basis $r \in \{+, \times\}$ and measure all the following qubits in the right basis. However, current technology only allows to approximate the behavior of single-photon sources and of noise-free quantum communication. It would be preferable to find a variant of QOT that allows to weaken the technological requirements put upon the honest participants.

In this section, we present such a protocol based on BB84 states [BB84], BB84-QOT (see Figure 4.3). The security proof follows essentially by adapting the security analysis of QOT in a rather straightforward way, as will be discussed later.

Let us consider a quantum channel with an error probability $\phi < \frac{1}{2}$, i.e., ϕ denotes the probability that a transmitted bit b, that is encoded by the sender and measured by the receiver using the same basis, is received as $1 - b$. In order not to have the security rely on any level of noise, we assume the error probability to be zero when considering a *dishonest* receiver. Also, let us consider a quantum source which produces two or more qubits (in the same state), rather than just one, with probability $\eta < 1 - \phi$. We call this the (ϕ, η)-weak quantum model.

In order to deal with noisy quantum communication, we need to do error-correction without giving the adversary too much information. This setting is known under the name of *information-reconciliation* from the theory of information-theoretic key agreement [CK78, Mau93]. Alice and Bob start with (correlated) values W and W', respectively. Alice wants to send to Bob the minimal information $S(W)$ such that Bob can reconstruct W from $S(W)$ and W'. Recently, such encodings $S(W)$ were called *secure sketches* [DRS04]. A (ℓ, m, ϕ)-secure sketch[1] is a randomized function $S : \{0,1\}^\ell \to \{0,1\}^*$ such that (1) for any $w \in \{0,1\}^\ell$ and for w' received from w by flipping each bit (independently) with probability ϕ, the string w can be recovered from w' and $S(w)$ except with negligible probability (in ℓ), and (2) for all random variables W over $\{0,1\}^\ell$, the "average min-entropy" of W given $S(W)$ is at least $H_\infty(W) - m$. We would like to point out that the notion of average min-entropy used in [DRS04] and here differs slightly from the standard notion $H_\infty(W|S(W))$, but it implies that for any $\Delta > 0$, the probability that $S(W)$ takes on a value y such that $H_\infty(W|S(W) = y) \geq H_\infty(W) - m - \Delta$ is at least $1 - 2^{-\Delta}$ (which is sufficient for our purpose).

Consider the protocol BB84-QOT in the (ϕ, η)-weak quantum model shown in Figure 4.3. For simplicity, we assume n to be even. The protocol uses a $(\frac{n}{2}, \alpha\frac{n}{2}, \phi)$-secure sketch S. We will argue later that α can be chosen arbitrarily close to (but greater than) $h(\phi)$. Like before, the memory bound in BB84-QOT applies before Step 4.

BB84-QOT (b)**:**

1. A picks $x \in_R \{0,1\}^n$ and a random index set $I_+ \subset_R \{1, \ldots, n\}$ of size $\frac{n}{2}$ and sets $I_\times := \{1, \ldots, n\} \setminus I_+$.
2. For $i = 1, 2, \ldots, n$: If $i \in I_+$, A sends $|x_i\rangle_+$ to B. If otherwise $i \in I_\times$, A sends $|x_i\rangle_\times$.
3. B picks $r' \in_R \{+, \times\}$ and measures all qubits in basis r'. Let $x' \in \{0,1\}^n$ be the result.
4. A picks $r \in_R \{+, \times\}$ and announces r, I_r, $y := S(x|_{I_r})$, $f \in_R \mathcal{F}_{n/2}$, and $s := b \oplus f(x|_{I_r})$.
5. B can recover $x|_{I_r}$ from $x'|_{I_r}$ and y, and outputs $a := 1$ and $b' := s \oplus f(x|_{I_r})$ if $r' = r$ and else $a := 0$ and $b' := 0$.

Figure 4.3. Protocol for the BB84 version of Rabin QOT

By the properties of a secure sketch, it is obvious that B receives the correct bit b if $r' = r$, except with negligible probability. Also, since there is no communication from B to A, BB84-QOT is clearly private. Similar as for protocol QOT, in order to argue about obliviousness

[1] Note that our definition of a secure sketch differs slightly from the one given in [DRS04].

we compare BB84-QOT with a purified version shown in Figure 4.4. BB84-EPR-QOT runs in the $(\phi, 0)$-weak quantum model, and the imperfectness of the quantum source assumed in BB84-QOT is simulated by A in BB84-EPR-QOT so that there is no difference from B's point of view. We would like to point out that the way A chooses the set I_r is more complicated than necessary; this is for proof-technical reasons, as will be clear later.

BB84-EPR-QOT (b):

1. A prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Additionally, A samples $\theta \in \{+, \times\}^n$ such that $\theta_i = +$ for exactly $\frac{n}{2}$ indices i, and A initializes $I'_+ := \emptyset$ and $I'_\times := \emptyset$.
2. For every $i \in \{1, \ldots, n\}$, A does the following. With probability $1 - \eta$ A sends one half of the i-th pair to B and keeps the other half. While with probability η A replaces I'_{θ_i} by $I'_{\theta_i} \cup \{i\}$ and sends two or more qubits in the same state $|x_i\rangle_{\theta_i}$ to B where $x_i \in_R \{0, 1\}$.
3. B picks $r' \in_R \{+, \times\}$ and measures all received qubits in basis r'. Let $x' \in \{0, 1\}^n$ be the result.
4. A picks a random index set $J \subset_R \{1, \ldots, n\} \setminus (I'_+ \cup I'_\times)$ of size $(1 - \eta - \varepsilon)n/2$ (where $\varepsilon > 0$ is sufficiently small). Then, A picks $r \in_R \{+, \times\}$, chooses a random index set $I_r \subset \{1, \ldots, n\}$ of size $\frac{n}{2}$ subject to $J \cup I'_r \subseteq I_r$ (respectively aborts if that is not possible) and for each $i \in I_r \setminus I'_r$ measures the corresponding qubit in basis r. Let x_i be the corresponding outcome, and let $x|_{I_r}$ be the collection of all x_i's with $i \in I_r$. A announces r, I_r, $y = S(x|_{I_r})$, $f \in_R \mathcal{F}n/2$, and $s = b \oplus f(x|_{I_r})$.
5. B can recover $x|_{I_r}$ from $x'|_{I_r}$ and y, and outputs $a := 1$ and $b' := s \oplus f(x|_{I_r})$, if $r' = r$ and else $a := 0$ and $b' := 0$.

Figure 4.4. Protocol for EPR-based Rabin QOT, BB84 version

The security equivalence between BB84-QOT (in the (ϕ, η)-weak quantum model) and BB84-EPR-QOT (in the $(\phi, 0)$-weak quantum model) is omitted here as it follows essentially along the same lines as in Section 4.2. The main difference here is that additionally one has to argue that the distribution of the "imperfectly generated qubits" (within the sets I_+ and $I_\times$) is the same as in BB84-QOT. As a matter of fact, it is not perfectly the same, but it is obviously the same conditioned on the event that the number of "imperfectly generated qubits" with basis $+$ and the number of those with basis $\times$ are both at most $(\eta + \varepsilon)n/2$ (in which case A does not abort in BB84-EPR-QOT). This event, though, happens with overwhelming probability by Bernstein's law of large numbers. This is good enough.

Theorem 4.5.1. *In the (ϕ, η)-weak quantum model,* BB84-QOT *is secure against $\mathfrak{B}_\gamma$ for any $\gamma < \frac{1-\eta}{4} - \frac{h(\phi)}{2}$ (if parameter α is appropriately chosen).*

Proof Sketch: It remains to show that BB84-EPR-QOT is oblivious against $\mathfrak{B}_\gamma$ (in the $(\phi, 0)$-weak quantum model). The reasoning goes exactly along the lines of the proof of Theorem 4.4.2, except that we restrict our attention to those i's which are in J. Write

$n' = |J| = (1-\eta-\varepsilon)n/2$, and let γ' be such that $\gamma n = \gamma' n'$, i.e., $\gamma' = 2\gamma/(1-\eta-\varepsilon)$. It then follows as in the proof of Theorem 4.4.2 that

$$\begin{aligned} H_\infty\big(X|_J \big| X|_J \in S^+\big) &\geq \gamma' n' + \kappa n' + \log(q^+) \\ &= \gamma n + \kappa(1-\eta-\varepsilon)n/2 + \log(q^+). \end{aligned}$$

Property (2) of a secure sketch then implies that, except with negligible probability, y is such that

$$\begin{aligned} &H_\infty\big(X|_{I_r} \big| X|_J \in S^+, S(X|_{I_r}) = y\big) \\ &\qquad \geq \gamma n + \kappa(1-\eta-\varepsilon)n/2 + \log(q^+) - \alpha n/2 - \varepsilon n. \end{aligned}$$

Similar as in the proof of Theorem 4.4.2, one can consider the cases $q^+ \geq 2^{-\varepsilon n}$ and $q^+ < 2^{-\varepsilon n}$, and in both cases argue that the min-entropy in question is larger than $\gamma n + \varepsilon n$ (which then completes the proof by referring to Theorem 2.4.1) if $\kappa(1-\eta-\varepsilon) > \alpha + 4\varepsilon$, where $\varepsilon > 0$ may be arbitrarily small and κ has to satisfy $\kappa < \frac{1}{2} - \gamma' = \frac{1}{2} - 2\gamma/(1-\eta-\varepsilon)$. This can be achieved (by choosing ε appropriately) if $\alpha < \kappa(1-\eta) < (1-\eta)/2 - 2\gamma$, which can be achieved (by choosing κ appropriately) if

$$\gamma < \frac{1-\eta}{4} - \frac{\alpha}{2}\,.$$

By the assumed restriction on γ, this inequality can be satisfied if α is chosen arbitrarily close to $h(\phi)$. But this follows in a straightforward way from a result in [DRS04], where it is shown that every (efficiently decodable) error correcting code induces an (efficient) secure sketch (with related parameters), combined with the fact that for every $\alpha > h(\phi)$ there exists an efficiently decodable code of large enough length ℓ, with rate $R = 1-\alpha$ and which (except with negligible probability) corrects errors introduced with probability ϕ (see [Cré97] and the reference therein). □

Chapter 5

Quantum Commitment Scheme

In this section, we present a BC scheme from a committer C with bounded quantum memory to an unbounded receiver V. The scheme is peculiar since in order to commit to a bit, the committer does not send anything. During the committing stage information only goes from V to C. The security analysis of the scheme uses similar techniques as the analysis of EPR-QOT.

5.1 The Protocol

The objective of this section is to present a bounded quantum-memory BC scheme COMM (see Figure 5.1). Intuitively, a commitment to a bit b is made by measuring random BB84-states in basis $\{+, \times\}_{[b]}$.

COMM(b):

1. V picks $x \in_R \{0,1\}^n$ and $r \in_R \{+, \times\}^n$.
2. V sends x_i in the corresponding bases $|x_1\rangle_{r_1}, |x_2\rangle_{r_2}, \ldots, |x_n\rangle_{r_n}$ to C.
3. C commits to the bit b by measuring all qubits in basis $\{+, \times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
4. To open the commitment, C sends b and x' to V.
5. V verifies that $x_i = x'_i$ for those i where $r_i = \{+, \times\}_{[b]}$. V accepts if and only if this is the case.

Figure 5.1. Protocol for quantum commitment

As for the OT-protocol of Section 4.2, we present an equivalent EPR-version of the protocol that is easier to analyze (see Figure 5.2).

Lemma 5.1.1. COMM *is secure if and only if* EPR-COMM *is secure.*

Proof: The proof uses similar reasoning as the one for Lemma 4.2.1. First, it clearly makes no difference, if we change Step 5 to the following:

EPR-COMM(b)**:**

1. V prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. V sends one half of each pair to C and keeps the other halves.
3. C commits to the bit b by measuring all received qubits in basis $\{+, \times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
4. To open the commitment, C sends b and x' to V.
5. V measures all his qubits in basis $\{+, \times\}_{[b]}$ and obtains $x \in \{0,1\}^n$. He chooses a random subset $I \subseteq \{1, \ldots, n\}$. V verifies that $x_i = x'_i$ for all $i \in I$ and accepts if and only if this is the case.

Figure 5.2. Protocol for EPR-based quantum commitment

5'. V chooses the subset I, measures all qubits with index in I in basis $\{+, \times\}_{[b]}$ and all qubits not in I in basis $\{+, \times\}_{[1-b]}$. V verifies that $x_i = x'_i$ for all $i \in I$ and accepts if and only if this is the case.

Finally, we can observe that the view of C does not change if V would have done his choice of I and his measurement already in Step 1. Doing the measurements at this point means that the qubits to be sent to C collapse to a state that is distributed identically to the state prepared in the original scheme. The EPR-version is therefore equivalent to the original commitment scheme from C's point of view. □

It is clear that EPR-COMM is hiding, i.e., that the commit phase reveals no information on the committed bit, since no information is transmitted to V at all. Hence we have

Lemma 5.1.2. EPR-COMM *is perfectly hiding.*

5.2 Modeling Dishonest Committers

A dishonest committer $\widetilde{\mathsf{C}}$ with bounded memory of at most γn qubits in EPR-COMM can be modeled very similarly to the dishonest OT-receiver $\widetilde{\mathsf{B}}$ from Section 4.3: $\widetilde{\mathsf{C}}$ consists first of a circuit acting on all n qubits received, then of a measurement of all but at most γn qubits, and finally of a circuit that takes the following input: a bit b that $\widetilde{\mathsf{C}}$ will attempt to open, the γn qubits in memory, and some ancilla in a fixed state. The output is a string $x' \in \{0,1\}^n$ to be sent to V at the opening stage.

Definition 5.2.1. *We define $\mathfrak{C}_\gamma$ to be the class of all committers $\{\widetilde{\mathsf{C}}_n\}_{n>0}$ in* EPR-COMM *that, at the start of the opening phase (i.e. at Step 4), have a quantum memory of size at most γn qubits.*

We adopt the binding condition for quantum BC from [DMS00]:

Definition 5.2.2. *A (quantum) BC scheme is* **(statistically) binding** *against $\mathfrak{C}$ if for all $\{\widetilde{\mathsf{C}}_n\}_{n>0} \in \mathfrak{C}$, the probability $p_b(n)$ that $\widetilde{\mathsf{C}}_n$ opens $b \in \{0,1\}$ with success satisfies*

$$p_0(n) + p_1(n) \leq 1 + negl(n).$$

In the next section, we show that EPR-COMM is binding against $\mathfrak{C}_\gamma$ for any $\gamma < \frac{1}{2}$.

5.3 Security Proof of the Commitment Scheme

Note that the first three steps of EPR-QOT and EPR-COMM (i.e. before the memory bound applies) are exactly the same! This allows us to reuse Corollary 4.4.1 and the analysis of Section 4.4 to prove the binding property of EPR-COMM.

Theorem 5.3.1. *For any $\gamma < \frac{1}{2}$,* COMM *is perfectly hiding and statistically binding against $\mathfrak{C}_\gamma$.*

The proof is given below. It boils down to showing that essentially $p_0(n) \leq 1 - q^+$ and $p_1(n) \leq 1 - q^\times$. The binding property then follows immediately from Corollary 4.4.1. The intuition behind $p_0(n) \leq 1 - q^+ := 1 - Q^+(S^+)$ is that a committer has only a fair chance in opening to 0 if x measured in $+$-basis has a large probability, i.e., $x \notin S^+$. The following proof makes this intuition precise by choosing the ε and δ's correctly.

Proof: It remains to show that EPR-COMM is binding against $\mathfrak{C}_\gamma$. Let $\kappa > 0$ be such that $\gamma + \kappa < \frac{1}{2}$. For the parameters κ and γ considered here, define Q^+, S^+ and q^+ as well as $Q^\times$, $S^\times$ and $q^\times$ as in Section 4.4. Furthermore, let $0 < \delta < \frac{1}{2}$ be such that $h(\delta) < \kappa/2$, where h is the binary entropy function, and choose $\varepsilon > 0$ small enough such that $h(\delta) < (\kappa - \varepsilon)/2$. This guarantees that $B^{\delta n} \leq 2^{(\kappa-\varepsilon)n/2}$ for all (sufficiently large) n. For every n we distinguish between the following two cases. If $q^+ \geq 2^{-\varepsilon n/2}$ then

$$H_\infty(X|X \in S^+) \geq \gamma n + \kappa n + \log(q^+) \geq \gamma n + \Big(\kappa - \frac{\varepsilon}{2}\Big)n$$

where the first inequality is argued as in (4.1). Applying Lemma 2.4.2, it follows that any guess $\hat{X}$ for X satisfies

$$\Pr\big[\hat{X} \in B^{\delta n}(X) \,|\, X \in S^+\big] \leq 2^{-\frac{1}{2}(H_\infty(X|X\in S^+)-\gamma n-1)+\log(B^{\delta n})} \leq 2^{-\frac{\varepsilon}{4}n+\frac{1}{2}}.$$

However, if $\hat{X} \notin B^{\delta n}(X)$ then sampling a random subset of the positions will detect an error except with probability not bigger than $2^{-\delta n}$. Hence,

$$\begin{aligned} p_0(n) &= (1 - q^+) \cdot p_{0|X\notin S^+} + q^+ \cdot p_{0|X\in S^+} \\ &\leq 1 - q^+ + q^+ \cdot \big(2^{-\delta n}(1 - 2^{-\frac{\varepsilon}{4}n+\frac{1}{2}}) + 2^{-\frac{\varepsilon}{4}n+\frac{1}{2}}\big). \end{aligned}$$

If on the other hand $q^+ < 2^{-\varepsilon n/2}$ then trivially

$$p_0(n) \leq 1 = 1 - q^+ + q^+ < 1 - q^+ + 2^{-\varepsilon n/2}.$$

In any case we have $p_0(n) \leq 1 - q^+ + negl(n)$.

Analogously, we derive $p_1(n) \leq 1 - q^\times + negl(n)$ and conclude that

$$p_0(n) + p_1(n) \leq 2 - q^+ - q^\times + negl(n) \leq 1 + negl(n), \tag{5.1}$$

where (5.1) is obtained from Corollary 4.4.1. □

5.4 Weakening the Assumptions

As argued earlier, assuming that a party can produce single qubits (with probability 1) is not reasonable given current technology. Also the assumption that there is no noise on the quantum channel is impractical. It can be shown that a straightforward modification of COMM remains secure in the (ϕ, η)-weak quantum model as introduced in Section 4.5, with $\phi < \frac{1}{2}$ and $\eta < 1 - \phi$.

Let COMM' be the modification of COMM where in Step 5 V accepts if and only if $x_i = x_i'$ for all *but about a ϕ-fraction* of the i where $r_i = \{+, \times\}_{[b]}$. More precisely, for all but a $(\phi + \varepsilon)$-fraction, where $\varepsilon > 0$ is sufficiently small.

Theorem 5.4.1. *In the (ϕ, η)-weak quantum model,* COMM' *is perfectly hiding and it is binding against $\mathfrak{C}_\gamma$ for any γ satisfying $\gamma < \frac{1}{2}(1 - \eta) - 2h(\phi)$.*

Proof Sketch: Using Bernstein's law of large numbers, one can argue that for *honest* C and V, the opening of a commitment is accepted except with negligible probability. The hiding property holds using the same reasoning as in Lemma 5.1.2. And the binding property can be argued essentially along the lines of Theorem 5.3.1, with the following modifications. Let J denote the set of indices i where V succeeds in sending a single qubit. We restrict the analysis to those i's which are in J. By Bernstein's law of large numbers, the cardinality of J is about $(1 - \eta)n$ (meaning within $(1 - \eta \pm \varepsilon)n$), except with negligible probability. Thus, restricting to these i's has the same effect as replacing γ by $\gamma/(1 - \eta)$ (neglecting the $\pm\varepsilon$ to simplify notation). Assuming that $\widetilde{\mathsf{C}}$ knows every x_i for $i \notin J$, for all x_i's with $i \in J$ he has to be able to guess all but about a $\phi/(1 - \eta)$-fraction correctly, in order to be successful in the opening. However, $\widetilde{\mathsf{C}}$ succeeds with only negligible probability if

$$\phi/(1 - \eta) < \delta\,.$$

Additionally, δ must be such that

$$h(\delta) < \frac{\kappa}{2} \qquad \text{with} \qquad \frac{\gamma}{1 - \eta} + \kappa < \frac{1}{2}\,.$$

Both restrictions on δ hold (respectively can be achieved by choosing κ appropriately) if

$$2\,h\!\left(\frac{\phi}{1 - \eta}\right) + \frac{\gamma}{1 - \eta} < \frac{1}{2}\,.$$

Using the fact that $h(\nu p) \leq \nu h(p)$ for any $\nu \geq 1$ and $0 \leq p \leq \frac{1}{2}$ such that $\nu p \leq 1$, this is clearly satisfied if $2h(\phi) + \gamma < \frac{1}{2}(1 - \eta)$. This proves the claim. $\square$

Chapter 6

1-2 Oblivious Transfer

This chapter presents current research trying to build a more practical variant of oblivious tranfer, (chosen) 1-out-of-2 oblivious transfer in the bounded quantum storage model. Trying to achieve this goal has turned out to be fruitful for different results, also in the classical world.

In Section 6.1.1, we argue that it is a nontrivial task to correctly define the security of classical *1-2 OT* and that a simulation-based approach seems to be the best to give a correct definition. In Section 6.1.2, we characterize the sender-privacy of *1-2 OT* using two-balanced functions. This is very useful for reductions using privacy amplification with strongly two-universal hash functions. Finally, in Section 6.2, we present a protocol for *1-2 OT* in the bounded quantum storage model and sketch its security proof.

We stress again, that all results presented in this chapter are of *preliminary nature* and represent the main ideas of upcoming articles or is research in progress. For proofs and all details, we refer to [CSSW05, DFSS05c, DFRSS05].

6.1 Classical *1-2* Oblivious Transfer

6.1.1 The Definition

1-2 Oblivious Transfer, *1-2 OT* for short, is a two-party primitive which allows a sender to send two bits (or, more generally, strings) B_0 and B_1 to a receiver, who is allowed to learn one of the two, according to his choice C, such that, informally, the receiver only learns B_C but not B_{1-C} (called *sender-privacy*, the sender's other input stays private), while at the same time the sender does not learn C (called *receiver-privacy*).

It turns out that correctly formalising the seemingly very simple concept of "knowing only one of two bits" is a nontrivial task. There are many examples in the literature where *1-2 OT* is not correctly defined (e.g. [BCW03]). An additional binary random variable D has to be introduced to indicate the bit the receiver knows. Most of the security definitions are incomplete, because they do not require this D to be independent of the original inputs B_0, B_1. In most of the cases, the protocols proposed are still secure, but it is clearly desirable to have a correct security definition and complete proofs. But what is the correct security definition?

The first thing one would try is to formalize the intuitive security requirements for a protocol. In the case of *1-2 OT*, one would say that a protocol is secure, if it is correct, i.e. it does what it is supposed to, as long as people behave honestly, it is sender-private and it is receiver-private as explained above. The difficulty in the case of *1-2 OT* is to correctly formalize sender-privacy. There are many examples (of other primitives) in cryptographic history where this approach (miserably) failed, because it lies in the nature of security, that it is very difficult to list *all* security requirements needed such that a protocol behaves well in a given environment. Newly proposed protocols (that were mathematically proven to fulfill all the security requirements the designer could think of) were easily broken by exploiting another security breach that the designer was not aware of.

Security history teaches us that there is a better way to obtain good security definitions. To circumvent the problem of listing all the security requirements, people started to *compare* their protocols to "ideal functionalities" that perform the specified task in a perfect way. Real protocols run in a certain model and a certain environment. The model is fixed and specifies for example the communication abilities (synchronous/asynchronous channels etc.), the computing power of the players, their memory size, whether they can process quantum information etc. The environment however is active, it can for example choose inputs for the players, receive outputs, specifiy random tapes etc. We can then imagine the real protocol replaced with the ideal functionality (that has the same interfaces to the environment) and we call a protocol *secure*, if these two situations cannot be distinguished (by the environment). Such a security definition has the great advantage that we can replace a secure protocol with the ideal functionality (because this cannot be distinguished) and in this way get rid of the internals of the original protocol. Normally, this allows to prove composition theorems and using them, to build modular cryptographic protocols that have much simpler security proofs.

The ideas sketched above were for the first time formally defined and elaborated by Beaver [Bea91]. Nowadays, two successful and popular frameworks are the Universally Composable framework by Canetti [Can01] and the framework of Reactive Simulatability of Backes, Pfitzmann and Waidner [BPW04]. In the quantum setting, models with composition theorems are independent works of Ben-Or and Mayers [BM02, BM04] and Unruh [Unr02].

A simpler framework that allows for sequential composition is given in Chapter 7 of Goldreich's book [Gol04]. In [CSSW05], we start from this model and tailor it for unconditionally secure two-party computation. By requiring that the output distribution of a real protocol with a dishonest player is the same as the distribution obtained when the same dishonest player acts with the ideal functionality, we can derive information-theoretic security requirements for the real protocol. In fact, we are able to show equivalence between simulation-security and our information-theoretic requirements. In other words, we can be sure that the list of requirements we obtain is complete to allow for sequential composition.

In order to be able to have sequential composition, we need to model the environment of the protocol. We do this by giving an auxiliary input Z to the dishonest player that contains all the information this player has gathered up to the execution of the protocol. Intuitively, if a protocol remains secure for whatever Z the dishonest player knows (e.g. from previous executions) it can be run again, and hence, composed.

In the special case of *1-2 OT*, we obtain the following definition.

Definition 6.1.1 (*1-2 OT*). *In a 1-2 OT protocol between sender* A *and receiver* B, A *has inputs* $B_0, B_1 \in \{0,1\}$ *and* B *holds a choice bit* $C \in \{0,1\}$. Z *denotes the auxiliary input for the dishonest player. We call the protocol* secure, *if it fulfills the three following requirements:*

Correctness: *If both players honestly follow the protocol,* B *outputs* B_C *and* A *has no ouput.*

Sender-privacy: *If* A *is honest, then for any (possibly dishonest)* $\widetilde{\mathsf{B}}$ *with view* W, *there* *exists a random variable D with range $\{0,1\}$ such that* A *has no output and*[1]

$$B_0, B_1 \leftrightarrow Z, C \leftrightarrow D \quad \text{and} \quad B_0, B_1 \leftrightarrow Z, C, D, B_D \leftrightarrow W.$$

Receiver-privacy: *If* B *is honest, then for any (possibly dishonest)* $\widetilde{\mathsf{A}}$ *with view V, it holds that*

$$C \leftrightarrow Z, B_0, B_1 \leftrightarrow V.$$

All information-theoretically secure constructions of *1-2 OT* protocols we are aware of in fact do implicitly build a variant of *1-2 OT*, which we call (sender-)randomized *1-2 OT*. A Randomized *1-2 OT*, or *Rand 1-2 OT* for short, essentially coincides with an (ordinary) *1-2 OT*, except that the two bits B_0 and B_1 are not *input* by the sender but generated uniformly at random during the protocol and *output* to the sender. *1-2 OT* can be constructed from a *Rand 1-2 OT*: the sender can use the randomly generated B_0 and B_1 to one-time-pad encrypt his input bits for the *1-2 OT*, and send the masked bits to the receiver.

To goal is now to formalize *Rand 1-2 OT* in such a way that it as much as possible minimizes and simplifies the security restraints, while at the same time still being sufficient for *1-2 OT* as defined above. This is achieved by the following definition.

Definition 6.1.2 (*Rand 1-2 OT*). *In a Rand 1-2 OT protocol between sender* A *and receiver* B, A *has no inputs* B *holds a choice bit $C \in \{0,1\}$. Z denotes the auxiliary input for the dishonest player. We call the protocol* secure *if it fulfills the three following requirements:*

Correctness: *If both players honestly follow the protocol,* A *outputs two bits $B_0, B_1 \in \{0,1\}$ and* B *outputs B_C.*

Sender-privacy: *If* A *is honest, then for any (possibly dishonest)* $\widetilde{\mathsf{B}}$ *with view W, there exists a random variable D with range $\{0,1\}$ such that* A *outputs $B_0, B_1 \in \{0,1\}$ and*

$$P_{B_{1-D}|Z,C,D,B_D,W} = P_{\text{UNIF}}$$

Receiver-privacy: *If* B *is honest, then for any (possibly dishonest)* $\widetilde{\mathsf{A}}$ *with view V on the protocol, it holds that*

$$C \leftrightarrow Z \leftrightarrow V.$$

Errors: In the case of a non-perfect protocol, we say that a protocol is *secure with an error ε*, if for all inputs, the distribution of the output has a statistical distance of at most ε from the output of a perfectly secure protocol.

In the following, we only consider the perfect scenario which suffices to get the important ideas.

Strings: We note that the above definitions can easily be extended to handle oblivious transfer of *strings*. In a *1-2 String OT*, the sender inputs two *strings* (of the same length), and the receiver is allowed to learn one of the two and only one of the two. Formally, for any positive integer ℓ, we can define a *1-2 ℓ-String OT* and a *Rand 1-2 ℓ-String OT* along the lines of Definition 6.1.1 respectively Definition 6.1.2 above, just by replacing the binary random variables B_0 and B_1 (as well as UNIF) by random variables S_0 and S_1 (and UNIF^{ℓ}) with range $\{0,1\}^{\ell}$. *Rand 1-2 ℓ-String OT* yields a proper *1-2 String OT* in the same way as before.

[1] Recall that the Markov chain $X \leftrightarrow Y \leftrightarrow Z$ holds, iff X and Z are independent, given Y.

6.1.2 Characterising Sender-Privacy

Trying to achieve the goal of building *1-2 OT* in the bounded quantum-storage model (see Section 6.2), we have developped a tool for characterising the sender-privacy of *Rand 1-2 OT* using balanced functions. The beauty of this approach is that balanced functions go well with strongly two-universal hash functions that are used for privacy amplification (as seen in Proposition 2.3.2). Before giving the characterisation of the general case, we investigate the case of Bit *1-2 OT*.

It is well known (and it follows from the condition for sender-privacy) that in a (*Rand*) *1-2 OT* the receiver B should in particular learn no information on the XOR $B_0 \oplus B_1$ of the two bits. The following proposition shows that this is not only necessary for the sender-privacy but also *sufficient*.

Theorem 6.1.3. *The sender-privacy condition for a Rand 1-2 OT is satisfied for a particular (possibly dishonest) receiver $\widetilde{\mathsf{B}}$ with auxiliary input Z and view W if and only if*

$$P_{B_0 \oplus B_1|ZW} = P_{\text{UNIF}}.$$

Before going into the proof (which is surprisingly simple), consider the following example. Assume a candidate protocol for *Rand 1-2 OT*, such that for a certain dishonest receiver, conditioned on the auxiliary input and the view of the receiver, (B_0, B_1) is $(0,0)$ with probability $\frac{1}{2}$, and $(0,1)$ and $(1,0)$ each with probability $\frac{1}{4}$. Then obviously the condition on the XOR from Theorem 6.1.3 is satisfied; on the other hand it appears as if the receiver has some joint information on B_0 and B_1 which is forbidden by a (*Rand*) *1-2 OT*. But that is not so. We can split the event $(B_0, B_1) = (0,0)$ into two disjoint subsets (subevents) $\mathcal{E}_0$ and $\mathcal{E}_1$ such that each has probability $\frac{1}{4}$, and then we define D by setting $D = 0$ if $\mathcal{E}_0$ or $(B_0, B_1) = (0,1)$, and $D = 1$ if $\mathcal{E}_1$ or $(B_0, B_1) = (1,0)$. Then, obviously, conditioned on $D = d$, the bit B_{1-d} is uniformly distributed from the receiver's point of view, even when given B_d.

Proof: The "only if" implication is well known and straightforward. For the "if" implication, let z and w be any values with $P_{ZW}(z,w) > 0$. The non-normalized distribution $P_{B_0B_1ZW}(\cdot,\cdot,z,w)$ can be expressed as depicted in the left table in Figure 6.1, with $a+b+c+d = P_{ZW}(z,w)$ and, by assumption, $a+d = b+c$. Due to symmetry, we may assume that $a \leq b$. Then we can define D by extending $P_{B_0B_1,Z,W}(\cdot,\cdot,z,w)$ to $P_{B_0B_1,D,Z,W}(\cdot,\cdot,\cdot,z,w)$ as depicted in the right two tables in Figure 6.1. $P_{B_0B_1,D,Z,W}(\cdot,\cdot,\cdot,z,w)$ is indeed an extension since by assumption $c + (b-a) = d$.

a	b
c	d

$P_{B_0B_1,Z,W}(\cdot,\cdot,z,w)$

a	a
c	c

$P_{B_0B_1D,Z,W}(\cdot,\cdot,0,z,w)$

0	$b-a$
0	$b-a$

$P_{B_0B_1D,Z,W}(\cdot,\cdot,1,z,w)$

Figure 6.1. Distributions $P_{B_0B_1,Z,W}(\cdot,\cdot,z,w)$ and $P_{B_0B_1D,Z,W}(\cdot,\cdot,\cdot,z,w)$

It is now obvious that $P_{B_0B_1DZ,W}(\cdot,\cdot,0,z,w) = \frac{1}{2}P_{B_0DZW}(\cdot,0,z,w)$ and $P_{B_0B_1DZ,W}(\cdot,\cdot,1,z,w) = \frac{1}{2}P_{B_1DZW}(\cdot,1,z,w)$, which finishes the proof. $\square$

The obvious question is whether there is a natural generalization of Theorem 6.1.3 to *Rand 1-2 String OT*. Note that the straightforward generalization of the XOR-condition in Theorem 6.1.3, requiring that any receiver has no information on the bit-wise XOR of the two strings, is clearly too weak, and does not imply sender-privacy for *Rand 1-2 String OT*: for instance the receiver could know the first half of the first string and the second half of the second string.

Instead of that, we are considering *two-balanced functions* as defined in Definition 2.3.1. In case $\ell = 1$, the XOR is a two-balanced function, and up to addition of a constant it is the *only* one. Based on this notion of two-balanced functions, sender-privacy of *Rand 1-2 String OT* can be characterized as follows.

Theorem 6.1.4. *The sender-privacy condition for a Rand 1-2 ℓ-String OT is satisfied for a particular (possibly dishonest) receiver $\widetilde{\mathsf{B}}$ with view W if and only if*

$$P_{\beta(S_0,S_1)|W} = P_{\text{UNIF}}.$$

for every two-balanced function β.

The non-perfect version of this theorem handling the error probabilities and its technically rather involved proof can be found in [DFSS05c]. In the next section, we sketch a classical application of Theorem 6.1.4 and in Section 6.2, we explain how to use it as basis for the security proof of a protocol in the bounded quantum storage model.

6.1.3 Reducing *1-2 OT* to Other Primitives

A great deal of effort has been put into constructing protocols for *1-2 (String) OT* based on physical assumptions like (various models for) noisy channels [CK88, DKS99, DFMS04, CMW04] or a memory bounded adversary [CCM98, Din01, DHRS04], as well as into reducing *1-2 (String) OT* to (seemingly) weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, *1-2 GOT* and *1-2 UOT* [Cré87, BC97, Cac98, Wol00, BCW03]. Note that the latter three flavors of *OT* are weaker than *1-2 OT* in that the (dishonest) receiver has more freedom in choosing the sort of information he wants to get about the sender's input bits B_0 and B_1: B_0, B_1 or $B_0 \oplus B_1$ in case of *1-2 XOT*, $g(B_0, B_1)$ for an arbitrary one-bit-output function g in case of *1-2 GOT*, and an arbitrary (probabilistic) Y with mutual information $I(B_0B_1;Y) \leq 1$ in case of *1-2 UOT*.[2]

All these reductions of *1-2 OT* to weaker versions follow a specific construction design (which is also at the core of the *1-2 OT* protocols based on noisy channels or a memory-bounded adversary). By repeated (independent) executions of the underlying primitive, A transfers a randomly chosen bit string $X = (X_0, X_1) \in \{0,1\}^n \times \{0,1\}^n$ to B such that: (1) depending on his choice bit C, the honest B knows either X_0 or X_1, (2) any A has no information on which part of X B learned, and (3) any A has some uncertainty in X. Then, this is completed to a *Rand 1-2 OT* by means of privacy amplification [BBCM95, HILL99]: A samples two functions f_0 and f_1 from a two-universal class $\mathcal{F}$ of hash functions, sends them to B, and outputs $S_0 = f_0(X_0)$ and $S_1 = f_1(X_1)$, and B outputs $S_C = f_C(X_C)$. Finally, the *Rand 1-2 OT* is transformed into a *1-2 OT* in the obvious way.

Correctness and receiver-privacy of this construction are clear, they follow immediately from (1) and (2). How easy or hard it is to prove sender-privacy depends heavily on the

[2] As a matter of fact, reduceability has been proven for any bound on $I(B_0B_1;Y)$ strictly smaller than 2.

underlying primitive. In case of *Rabin OT* it is rather straightforward. In case of *1-2 XOT* and the other weaker versions, this is non-trivial. The problem is that since B might know $X_0 \oplus X_1$, it is not possible to argue that there exists $d \in \{0,1\}$ such that B's uncertainty on X_{1-d} is large when given X_d. This, though, would be necessary in order to finish the proof by simply applying the privacy amplification theorem. We argue that, independent of the underlying primitive, sender-privacy follows as a simple consequence of Theorem 6.1.4, our characterisation from last section, and Proposition 2.3.2, the observation regarding the composition of two-balanced functions with strongly two-universal hash functions.

Briefly, sender-privacy for a construction as sketched above can be argued as follows. The only restriction is that $\mathcal{F}$ needs to be *strongly* two-universal. From the independent repetitions of the underlying weak *OT* (*Rabin OT*, *1-2 XOT*, *1-2 GOT* or *1-2 UOT*) it follows that B has "high" collision entropy in X. Hence, for any two-balanced function β, we can apply the privacy amplification theorem [BBCM95, HILL99] to the (strongly) two-universal hash function $\beta(f_0(\cdot), f_1(\cdot))$ and argue that $\beta(f_0(X_0), f_1(X_1))$ is close to uniform for randomly chosen f_0 and f_1. Sender-privacy then follows immediately from Theorem 6.1.4.

More details and a quantitative comparison of this approach to other reductions can be found in [DFSS05c].

6.2 *1-2 OT* in the Bounded Quantum-Storage Model

6.2.1 The Definition

In this section, we are considering quantum protocols for *Rand 1-2 ℓ-String OT*. For convenience, the formalism of Section 4.1 is repeated here. In- and outputs of the honest players are classical, described by random variables, the protocol may contain quantum computation and quantum communication, and the view of a dishonest player is quantum, and is thus described by a random state. Any such two-party protocol is specified by a family $\{(\mathsf{A}_n, \mathsf{B}_n)\}_{n>0}$ of pairs of interactive quantum circuits (i.e. interacting through a quantum channel). Each pair is indexed by a security parameter $n > 0$, where A_n and B_n denote the circuits for sender Alice and receiver Bob, respectively. In order to simplify the notation, we often omit the index n, leaving the dependency on it implicit.

Ideally, we would like to extend the work of [CSSW05] sketched in Section 6.1.1 to quantum protocols. In such a setting, the auxiliary input of the dishonest player (which can be thought of as the environment the protocol runs in) will be a random quantum state and it is not clear if everything can be translated in the straightforward way from the classical case. It is current research to further investigate this point. In the following, we assume that also in the quantum setting, it is sufficient to build *Rand 1-2 ℓ-String OT* which can then be transformed into a proper *1-2 String OT* by the classical reduction. As a first try, we ignore the auxiliary input for the dishonest player (and therefore give up composition issues for now) and give a formal definition analogous to the classical one.

Let us fix the following notation: Let C denote the binary random variable describing B's choice bit and let S_0, S_1 denote the ℓ-bit long random variables describing A's output strings. Furthermore, for a dishonest sender $\widetilde{\mathsf{A}}$ (respecively $\widetilde{\mathsf{B}}$) let $\boldsymbol{\rho}_{\widetilde{\mathsf{A}}}$ ($\boldsymbol{\rho}_{\widetilde{\mathsf{B}}}$) denote the random state describing $\widetilde{\mathsf{A}}$'s ($\widetilde{\mathsf{B}}$'s) complete view of the protocol. Note that for a fixed candidate protocol for *Rand 1-2 ℓ-String OT*, and for a fixed input distribution P_C, depending on whether we consider a dishonest $\widetilde{\mathsf{A}}$ and an honest B, or an honest A and a dishonest $\widetilde{\mathsf{B}}$, the corresponding joint distribution $P_{\boldsymbol{\rho}_{\widetilde{\mathsf{A}}} S_C}$ respectively $P_{S_0 S_1 \boldsymbol{\rho}_{\widetilde{\mathsf{B}}}}$ is uniquely determined.

Definition 6.2.1 (Quantum *Rand 1-2 OT*). *In a (quantum) Rand 1-2 OT protocol between sender* A *and receiver* B, A *has no inputs* B *holds a choice bit* $C \in \{0,1\}$. *We call the protocol* secure *if it fulfills the three following requirements:*

Correctness: *If both players honestly follow the protocol,* A *outputs two bitstrings* $S_0, S_1 \in \{0,1\}^\ell$ *and* B *outputs* S_C.

Sender-privacy: *If* A *is honest, then for any (possibly dishonest)* $\widetilde{\mathsf{B}}$ *with view* $\boldsymbol{\rho}_{\widetilde{\mathsf{B}}}$, *there exists a random variable* D *with range* $\{0,1\}$ *such that* A *outputs* $S_0, S_1 \in \{0,1\}$ *and*

$$d(S_{1-D} \mid \{C\} \otimes \{D\} \otimes \{S_D\} \otimes \boldsymbol{\rho}_{\widetilde{\mathsf{B}}}) = 0$$

Receiver-privacy: *If* B *is honest, then for any (possibly dishonest)* $\widetilde{\mathsf{A}}$ *with view* $\rho_{\widetilde{\mathsf{A}}}$ *on the protocol, it holds that*

$$[\{C\} \otimes \boldsymbol{\rho}_{\widetilde{\mathsf{A}}}] = [\{C\}] \otimes [\boldsymbol{\rho}_{\widetilde{\mathsf{A}}}].$$

If one of the properties only holds with respect to a restricted class $\mathfrak{A}$ *of* $\widetilde{\mathsf{A}}$*'s respectively* $\mathfrak{B}$ *of* $\widetilde{\mathsf{B}}$*'s, then this property is said to hold and the protocol is said to be secure* **against** $\mathfrak{A}$ *respectively* $\mathfrak{B}$.

The same remarks about errors as for the classical Definition 6.2.1 apply. Furthermore, the definition can be extended to (quantum) *1-2 String OT*.

6.2.2 The Protocol

We introduce a quantum protocol for *Rand 1-2 ℓ-String OT* that we want to show perfectly receiver-private (against any sender) and statistically sender-private against any quantum memory-bounded receiver.

The simple protocol is described in Figure 6.2: A sends random BB84 states to the receiver B. Bob then measures all received qubits according to his choice bit C. Let $\mathcal{F}_{n/2}$ denote a class of *strongly two-universal* hash functions mapping the appropriate amount of bits (assumed to be $n/2$ for the rest) to ℓ bits. Alice picks randomly two hash functions from $\mathcal{F}_{n/2}$ and applies them to $x|_{I_+}$ and $x|_{I_\times}$ to obtain her output strings S_0 and S_1. She announces the encoding bases and the hash functions to Bob. Intuitively, a dishonest receiver Bob who cannot store all the qubits until the right bases are announced, cannot learn both strings simultanously. (In order to avoid aborting, we specify that if a dishonest $\widetilde{\mathsf{A}}$ refuses to participate, or sends data in incorrect format, then B samples its output string s_c uniformly at random in $\{0,1\}^\ell$.)

The security of the *Rand 1-2 ℓ-*QOT protocol against receivers with bounded-size quantum memory holds as long as the bound applies before Step 4 is reached. Exactly as in Section 6.2.2, Figure 6.3 describes a EPR-version EPR *Rand 1-2 ℓ-*QOT of *Rand 1-2 ℓ-*QOT which is securitywise equivalent. We omit the proofs here.

As for EPR-QOT, we have that EPR *Rand 1-2 ℓ-*QOT is perfectly receiver-private, because it is non-interactive, i.e. no information flows from B to A.

6.2.3 Security against Dishonest Receivers

We can model dishonest receivers in EPR *Rand 1-2 ℓ-*QOT exactly the same way as in Chapter 4 and reuse the class $\mathfrak{B}_\gamma$ from Definition 4.3.1. Our final goal is to proof the following theorem.

Rand 1-2 ℓ-QOT:

1. A picks $x \in_R \{0,1\}^n$ and a random index set of positions $I_+ \subset_R \{1,\ldots,n\}$ and defines $I_\times := \{1,\ldots,n\} \setminus I_+$.
2. For $i = 1,2,\ldots,n$: If $i \in I_+$, A sends $|x_i\rangle_+$ to B. If otherwise $i \in I_\times$, A sends $|x_i\rangle_\times$.
3. B measures all qubits in basis $[+,\times]_c$ where c is B's choice bit. Let $x' \in \{0,1\}^n$ be the result.
4. A picks two hash functions $f_0, f_1 \in_R \mathcal{F}_{n/2}$ and outputs $s_0 := f_0(x|_{I_+}), s_1 := f_1(x|_{I_\times})$. She announces $I_+, I_\times, f_0, f_1$ to B.
5. B outputs $s_c := f_c(x'|_{I_c})$.

Figure 6.2. Quantum Protocol for *Rand 1-2 ℓString OT*.

EPR *Rand 1-2 ℓ*-QOT:

1. A prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. A sends one half of each pair to B and keeps the other halves.
3. B measures all qubits in basis $[+,\times]_c$. Let $x' \in \{0,1\}^n$ be the result.
4. A picks a random index set of positions $I_+ \subset_R \{1,\ldots,n\}$ and defines $I_\times := \{1,\ldots,n\} \setminus I_+$. For $r \in \{+,\times\}$ and $i \in I_r$, she measures the ith qubit in basis r. Let $x \in \{0,1\}^n$ be the outcome. A picks two hash functions $f_0, f_1 \in_R \mathcal{F}_{n/2}$ and outputs $s_0 := f_0(x|_{I_+}), s_1 := f_1(x|_{I_\times})$. She announces $I_+, I_\times, f_0, f_1$ to B.
5. B outputs $s_c = f_c(x'|_{I_c})$.

Figure 6.3. Protocol for EPR-based *Rand 1-2 ℓString OT*.

Theorem 6.2.2. *For all $\gamma < \frac{1}{2}$,* EPR *Rand 1-2 ℓ*-QOT *is secure against $\mathfrak{B}_\gamma$.*

Proof Sketch: It remains to show the sender-privacy of EPR *Rand 1-2 ℓ*-QOT. The proof proceeds in three steps:

1. We prove that, even given the knowledge of the bases $I_+, I_\times$ and the hash functions, an entropic uncertainty relation assures that there is some uncertainty about the outcome of x. The difficulty in this step is that we don't know how Bob compressed his half of the EPR pairs and therefore, we have to handle arbitrary correlations between the bit-positions of x. Azuma's inequality is used to prove Theorem 6.2.3 below. This result might be a useful tool in other contexts as well: Whenever we have a certain amount of entropy for each single position Z_i given the previous history, Theorem 6.2.3 guarantees that this entropy accumulates over the whole string $Z_1, \ldots, Z_n$ in terms of smooth min-entropy (even when the Z_i are not independent).
2. In order to use our classical characterisation of sender-privacy with balanced functions from Section 6.1.2, we have to prove a quantum version of Theorem 6.1.4. It turns out

that using the Schmidt decomposition for pure bipartite quantum states, the quantum case reduces nicely to the classical one. The result is Theorem 6.2.5.

3. We conclude the proof by combining the two previous tools with the smooth-entropy version of privacy amplification against quantum adversaries (Theorem 6.2.6): Corollary 6.2.4 gives us enough smooth entropy such that a memory size of less than $n/2$ qubits is not enough to have information about $\beta(f_0(x|_{I_+}), f_1(x|_{I_\times}))$ for any balanced function β except with negligible probability. Hence, the conditions of Theorem 6.2.5 are fulfilled and sender-privacy holds (except with negligible probability).

□

Theorem 6.2.3. *Let $Z_1, \ldots, Z_n$ be n random variables (not necessarily independent) over alphabet $\mathcal{Z}$ and let $0 < \gamma < 1$. If there exist real numbers $h > 0$ such that for all $1 \leq i \leq n$ and $z_1, \ldots, z_{i-1} \in \mathcal{Z}$:*

$$H(Z_i | Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}) \geq h$$

then

$$H_\infty^\varepsilon(Z_1, \ldots, Z_n) \geq n(h - 2\gamma),$$

for $\varepsilon = \exp\left(\frac{-\gamma^2 n}{2(|\mathcal{Z}|^2 + 4\log^2(\frac{1}{\gamma}))}\right)$.

Corollary 6.2.4. *Let Θ_i indicate the basis in which Alice measures the ith qubit in* EPR *Rand 1-2 ℓ-*QOT *and let X_i be the outcome. For a $0 < \delta < 1$, there exists an ε exponentially small in n, such that*

$$H_\infty^\varepsilon(X_1, \ldots, X_n | \Theta_1, \ldots, \Theta_n) \geq n(\frac{1}{2} - \delta).$$

Proof Sketch: Define $Z_i := (X_i, \Theta_i)$. It holds that

$$\begin{aligned} &H(Z_i | Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}) \\ &\quad = H(X_i | \Theta_i, Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}) + H(\Theta_i | Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}) \\ &\quad \geq \frac{1}{2} + 1 = \frac{3}{2}, \end{aligned}$$

where the inequality holds because Θ_i is chosen uniformly at random and the entropic uncertainty relation by Maassen and Uffink (3.1) for one qubits yields

$$H(X_i | \Theta_i) = \frac{1}{2}\left(H(Q^+) + H(Q^\times)\right) \geq \frac{1}{2}.$$

Note that the uncertainty relation holds for arbitrary one-qubit states and therefore also for the state conditioned on the previous history $Z_1 = z_1, \ldots, Z_{i-1} = z_{i-1}$.

We then use Theorem 6.2.3 and the chain rule for smooth min-entropy to conlude:

$$\begin{aligned} &H_\infty^{\varepsilon+\varepsilon'}(X_1, \ldots, X_n | \Theta_1, \ldots, \Theta_n) \\ &\qquad > H_\infty^{\varepsilon'}((X_1, \Theta_1), \ldots, (X_n, \Theta_n)) - H_0(\Theta_1, \ldots, \Theta_n) - \log\left(\frac{1}{\varepsilon}\right) \\ &\qquad \geq n(\frac{3}{2} - \gamma) - n - \log\left(\frac{1}{\varepsilon}\right). \end{aligned}$$

Choosing the ε's and γ correctly as a function of δ yields the result. □

Theorem 6.2.5 (Quantum Balanced Function Theorem). *If for all balanced functions $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$, it holds that $d(\beta(S_0, S_1) \mid \boldsymbol{\rho}) = 0$, then there exists a random variable D such that*

$$d(S_{1-D} \mid \{S_D\} \otimes \{D\} \otimes \boldsymbol{\rho}) = 0.$$

Theorem 6.2.6 (Privacy Amplification [RK05]). *Let $\varepsilon > 0$, X be distributed over $\{0,1\}^n$, and let $\boldsymbol{\rho}$ be a random state of q qubits*[3]*. Let F be the random variable corresponding to the random choice (with uniform distribution and independent from X and $\boldsymbol{\rho}$) of a member of a two-universal class of hashing functions $\mathcal{F}$. Then*

$$\begin{aligned} d(F(X) \mid \{F\} \otimes \boldsymbol{\rho}]) &\leq \frac{1}{2} 2^{-\frac{1}{2}(H_\infty^\varepsilon([\{X\} \otimes \boldsymbol{\rho}]) - H_0^\varepsilon([\boldsymbol{\rho}]) - 1)} + 2\varepsilon \\ &\leq \frac{1}{2} 2^{-\frac{1}{2}(H_\infty^\varepsilon(X) - q - 1)} + 2\varepsilon. \end{aligned}$$

[3]Remember that $\boldsymbol{\rho}$ can be correlated with X in an arbitrary way. In particular, we can think of $\boldsymbol{\rho}$ as an attempt to store the n-bit string X in q qubits.

Chapter 7

Conclusion and Further Research

7.1 Conclusion

We have presented new entropic uncertainty relations based on min-entropy and shown how to construct *Rabin OT* and BC securely in the bounded quantum-storage model. Our protocols require no quantum memory for honest players and remain secure provided the adversary has only access to quantum memory of size bounded by a large fraction of all qubits transmitted. Such a gap between the amount of storage required for honest players and adversaries is not achievable by classical means. All our protocols are non-interactive and can be implemented using current technology. We have given an outline of current research concerning the security definition of classical *1-2 OT*, a characterisation of sender-privacy of classical *1-2 OT*, and we have sketched the security of a protocol for *1-2 OT* in the bounded quantum storage model.

It is interesting to note that it makes perfect sense to perform our protocols over short (lab-range) distances of some meters. This is in contrast to quantum key-distribution which only makes sense when the two parties are far enough apart, so that they cannot talk to each other using their voice nor physically exchange messages.

7.2 Further Research

Chapter 6 contains the main ideas of ongoing research. In the following, we list some ideas and possible extensions along these lines.

7.2.1 Entropic Uncertainty Relations

An error term (that we like to keep negligible) is inherent to the approach taken in Section 3.2 to develop uncertainty relations based on min-entropy. This error term is the barrier to extend the results to more than $2^{n/3}$ mutually unbiased bases. We think this error term can only be avoided by exploiting the enourmous symmetry in the setting (remember that geometry was also the key to Larsens Theorem 3.1.2). We conjecture that also for the sum of the max-probability holds (analogous to (3.3) for the collision probabilities) that for $1 \leq M \leq N$:

$$\sum_{i=0}^{M} q_{\infty}^{i} \leq 1 + \frac{M}{N},$$

which would be tight. If the system is in a basis-state of one of the mutually unbiased bases, the other probability distributions will all be uniform and therefore their maximal probabilities will be equal to $1/N$.

7.2.2 Rabin String OT

In Chapter 4, we only considered *Rabin OT* of one bit per invocation. Our technique can easily be extended to deal with string *Rabin OT*, essentially by using a class of two-universal functions with range $\{0,1\}^{\lambda n}$ rather than $\{0,1\}$, for some λ with $\gamma + \lambda < \frac{1}{2}$ (respectively $< \frac{1-\eta}{4} - \frac{h(\phi)}{2}$ for BB84-QOT).

7.2.3 Stronger Binding Condition and String Commitments

The binding condition given in Definition 5.2.2 is weaker than the classical one, where one would require that a bit b exists such that $p_b(n)$ is negligible. But it is the best that can be achieved for a general quantum adversary who can always commit to 0 and 1 in superposition. However, an adversary with bounded quantum storage cannot necessarily maintain a commitment in superposition since the memory compression may force a collapse. Indeed, using the new techniques from Section 6.2, we should be able to show that commitment schemes exist satisfying the stronger binding condition. COMM can easily be transformed into a *string* commitment scheme simply by committing bitwise, at the cost of a corresponding blow-up of the communication complexity. In order to prove this string commitment secure, though, it is necessary that COMM is secure with respect to the stronger security definition.

7.2.4 Better Memory Bounds

For the BB84-version BB84-QOT of the protocol QOT, which works under weakened physical assumptions, the tools from Section 6.2 might yield better memory bounds.

In all our security proves, we can not exceed memory bounds of $n/2$ qubits, whereas intuitively, these protocols are secure against adversaries with larger quantum memory. The reason for this barrier is that in the uncertainty relation established in Theorem 3.2.1, we are completly ignoring the form of the purification of the state of register A. Translated into the setting of *Rabin OT*, this means that we give Bob complete control over the combined state of the system (formally, over the complex coefficients α_x and the states $|\phi_x\rangle$ in $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle^A |\phi_x\rangle$) and we are not using the *structure*(i.e. its entropy) that is given by Bob's abilities to compress the original system by adjoining anzillas, unitarily transforming and partially measuring. Therefore, the limiting factor in the uncertainty relation is the coefficient of $2^{-n/2}$ stemming from the Hadamard-transformation over n qubits.

Similarly in Section 6.2, where we are simplifying matters by ignoring Bob's actions on his part of the system and achieve the bound of Corollary 6.2.4, which is the best we can hope for, because it's origin, the Maassen-Uffink relation (3.1) is optimal (equality holds for example for the basis-state $|0\rangle$).

To increase the memory bounds, we have to make use of the additional entropy in Bob's part of the system. We hope that better results can be achieved using the latest results about privacy amplification in the presence of quantum adversaries from [Ren05]. The clarity of the setting in the commitment scheme COMM might be a good starting point.

7.2.5 Quantum Composition Framework and Memory Bounds under Composition

In order to give the correct security definitions for quantum two-party protocols, it would be desirable to have a framework similar to the one in [Gol04] for quantum protocols. As mentioned in Section 6.2.1, the auxiliary input to a dishonest player describing the previous knowledge gathered will be a random quantum state. The difficulty in quantum UC frameworks like [BM04, Unr02] is that one has to keep track of whether and when measurements are performed. The mentioned frameworks are still at a formally very complicated stage and therefore, a simple solution seems to be difficult to achieve for the moment.

In a bounded-storage model, one has to ask what memory bounds mean and how they scale when composing protocols. Does the same bound have to hold for each single protocol? If a (quantum) adversary collects qubits over several protocols, when and which memory bound is needed to achieve security?

7.2.6 1-m *OT* and String Commitments

Using encodings into more than two mutually unbiased bases, we can think of protocols for 1-m *OT* or String Commitments along the lines of our protocols above, which are more efficient than via the standard reductions, but proving their security remains a open problem for now.

Bibliography

[Aza04] Adam Azarchs. *Entropic uncertainty relations for incomplete sets of mutually unbiased observables.* Available at http://arxiv.org/abs/quant-ph/0412083, 2004.

[BB84] Charles H. Bennett and Gilles Brassard. *Quantum cryptography: Public key distribution and coin tossing.* In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175–179, 1984.

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. *Generalized Privacy Amplification.* IEEE Transactions on Information Theory, 41:1915–1923, November 1995.

[BC97] Gilles Brassard and Claude Crepeau. *Oblivious Transfers and Privacy Amplification.* In Advances in Cryptology—CRYPTO '97, volume 1294 of Lecture Notes in Computer Science. Springer, 1997.

[BCW03] Gilles Brassard, Claude Crépeau, and Stefan Wolf. *Oblivious Transfer and Privacy Amplification.* Journal of Cryptology, 16(4), 2003.

[Bea91] Donald Beaver. *Foundations of Secure Interactive Computing.* In Advances in Cryptology—CRYPTO '91, volume 576 of Lecture Notes in Computer Science, pages 377–391. Springer, 1991.

[BM02] Michael Ben-Or and Dominic Mayers. *Quantum universal composability*, November 2002. Presentation at "Quantum Information and Cryptography" Workshop, slides online available at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/mayers/1/meta/aux/mayers.pdf.

[BM04] Michael Ben-Or and Dominic Mayers. *General security definition and composability for quantum and classical protocols*, September 2004. online available at http://xxx.lanl.gov/abs/quant-ph/0409062.

[BPW04] Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Secure asynchronous reactive systems.* Cryptology ePrint Archive, March 2004. Online available at http://eprint.iacr.org/2004/082.ps.

[Cac98] Christian Cachin. *On the Foundations of Oblivious Transfer.* In Advances in Cryptology—EUROCRYPT '98, volume 1403 of Lecture Notes in Computer Science. Springer, 1998.

[Can01] Ran Canetti. *Universally Composable Security: A New Paradigm for Cryptographic Protocols.* In 42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 136–145, 2001.

[CCM98] C. Cachin, C. Crépeau, and J. Marcil. *Oblivious Transfer with a Memory-Bounded Receiver.* In 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 493–502, 1998.

[CK78] I. Csiszár and J. Körner. *Broadcast channels with confidential messages.* IEEE Transactions on Information Theory, 24(3):339–348, May 1978.

[CK88] C. Crépeau and J. Kilian. *Achieving Oblivious Transfer Using Weakened Security Assumptions.* In 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 42–53, 1988.

[CMW04] Claude Crepeau, Kirill Morozov, and Stefan Wolf. *Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel.* In International Conference on Security in Communication Networks (SCN), volume 4 of Lecture Notes in Computer Science, 2004.

[Cré87] Claude Crépeau. *Equivalence between Two Flavours of Oblivious Transfers.* In Advances in Cryptology—CRYPTO '87, volume 293 of Lecture Notes in Computer Science. Springer, 1987.

[Cré97] Claude Crépeau. *Efficient Cryptographic Protocols Based on Noisy Channels.* In Advances in Cryptology—EUROCRYPT '97, volume 1233 of Lecture Notes in Computer Science, pages 306–317. Springer, 1997.

[CSSW05] Claude Crépeau, George Savvides, Christian Schaffner, and Jürg Wullschleger. *Unconditionally Secure Two-Party Computation.* `In preparation`, 2005.

[CW77] J. Lawrence Carter and Mark N. Wegman. *Universal classes of hash functions.* In 9th Annual ACM Symposium on Theory of Computing (STOC), pages 106–112, 1977.

[Deu83] David Deutsch. *Uncertainty in Quantum Measurements.* Physical Review Letters, 50(9):631–633, February 1983.

[DFMS04] Ivan B. Damgård, Serge Fehr, Kirill Morozov, and Louis Salvail. *Unfair Noisy Channels and Oblivious Transfer.* In Theory of Cryptography Conference (TCC), volume 2951 of Lecture Notes in Computer Science, pages 355–373. Springer, 2004.

[DFRSS05] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. *1-2 OT in the Bounded Quantum-Storage Model with Applications.* `In preparation`, 2005.

[DFSS05a] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. *Cryptography In the Bounded Quantum-Storage Model.* In 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 449–458, 2005.

[DFSS05b] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. *Cryptography In the Bounded Quantum-Storage Model.* Research Series RS-05-20, BRICS, Department of Computer Science, University of Aarhus (`www.brics.dk`), 2005.

[DFSS05c] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. *Oblivious Transfer and Balanced Functions.* `In preparation`, 2005.

[DHRS04] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. *Constant-Round Oblivious Transfer in the Bounded Storage Model.* In Theory of Cryptography Conference (TCC), volume 2951 of Lecture Notes in Computer Science, pages 446–472. Springer, 2004.

[Din01] Yan Zong Ding. *Oblivious Transfer in the Bounded Storage Model.* In Advances in Cryptology—CRYPTO '01, volume 2139 of Lecture Notes in Computer Science. Springer, 2001.

[DKS99] Ivan B. Damgård, Joe Kilian, and Louis Salvail. *On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions.* In Advances in Cryptology—EUROCRYPT '99, volume 1592 of Lecture Notes in Computer Science, pages 56–73. Springer, 1999.

[DM04] STEFAN DZIEMBOWSKI AND UELI M. MAURER. *On Generating the Initial Key in the Bounded-Storage Model.* In Advances in Cryptology—EUROCRYPT '04, volume 3027 of Lecture Notes in Computer Science, pages 126–137. Springer, 2004.

[DMS00] PAUL DUMAIS, DOMINIC MAYERS, AND LOUIS SALVAIL. *Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation.* In Advances in Cryptology—EUROCRYPT 2000, volume 1807 of Lecture Notes in Computer Science, pages 300–315. Springer, 2000.

[DPS04] IVAN B. DAMGÅRD, THOMAS B. PEDERSEN, AND LOUIS SALVAIL. *On the Key-Uncertainty of Quantum Ciphers and the Computational Security of One-way Quantum Transmission.* In Advances in Cryptology—EUROCRYPT '04, volume 3027 of Lecture Notes in Computer Science, pages 91–108. Springer, 2004.

[DRS04] YEVGENIY DODIS, LEONID REYZIN, AND ADAM SMITH. *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data.* In Advances in Cryptology—EUROCRYPT '04, volume 3027 of Lecture Notes in Computer Science, pages 523–540. Springer, 2004.

[FvdG99] CHRISTOPHER A. FUCHS AND JEROEN VAN DE GRAAF. *Cryptographic Distinguishability Measures for Quantum-Mechanical States.* IEEE Transactions on Information Theory, 45:1216–1227, 1999.

[Gol04] ODED GOLDREICH. Foundations of Cryptography, volume II: Basic Applications. Cambridge University Press, 2004.

[Hei27] WERNER HEISENBERG. *Schwankungserscheinungen und Quantenmechanik.* Zeitschrift für Physik, 40:501–506, 1927.

[HILL99] JOHAN HÅSTAD, RUSSELL IMPAGLIAZZO, LEONID A. LEVIN, AND MICHAEL LUBY. *A Pseudorandom Generator from any One-way Function.* SIAM Journal on Computing, 28(4), 1999.

[Ivo81] I D IVONOVIĆ. *Geometrical description of quantal state determination.* Journal of Physics A: Mathematical and General, 14(12):3241–3245, December 1981.

[Kra87] K. KRAUS. *Complementary observables and uncertainty relations.* Physical Review D, 35(10):3070–3075, May 1987.

[Lar90] U. LARSEN. *Superspace geometry: the exact uncertainty relationship between complementary aspects.* Journal of Physics A: Mathematical and General, 23(7):1041–1061, April 1990.

[LBZ02] JAY LAWRENCE, ČASLAV BRUKNER, AND ANTON ZEILINGER. *Mutually unbiased binary observable sets on N qubits.* Physical Review A, 65(3), February 2002.

[LC97] HONG-KWONG LO AND H. F. CHAU. *Is quantum bit commitment really possible?* Physical Review Letters, 78(17):3410–3413, April 1997.

[Mau93] UELI M. MAURER. *Protocols for Secret Key Agreement by Public Discussion Based on Common Information.* In CRYPTO92, pages 461–470, London, UK, 1993. Springer-Verlag.

[May97] DOMINIC MAYERS. *Unconditionally secure quantum bit commitment is impossible.* Physical Review Letters, 78(17):3414–3417, April 1997.

[MSTS04] TAL MORAN, RONEN SHALTIEL, AND AMNON TA-SHMA. *Non-interactive Timestamping in the Bounded Storage Model.* In Advances in Cryptology—CRYPTO '04, volume 3152 of Lecture Notes in Computer Science, pages 460–476. Springer, 2004.

[MU88] HANS MAASSEN AND JOS B. M. UFFINK. *Generalized entropic uncertainty relations.* Physical Review Letters, 60(12):1103–1106, March 1988.

[Ped05] Thomas B. Pedersen. Quantum Encryption Minimising Key Leakage under Known Plaintext Attacks. PhD thesis, Department of Computer Science, University of Aarhus, Denmark, 2005.

[Ren05] Renato Renner. Security of Quantum Key Distribution. PhD thesis, ETH Zürich, 2005.

[RK05] Renato Renner and Robert König. *Universally Composable Privacy Amplification Against Quantum Adversaries.* In Theory of Cryptography Conference (TCC), volume 3378 of Lecture Notes in Computer Science, pages 407–425. Springer, 2005.

[RW05] Renato Renner and Stefan Wolf. *Simple and Tight Bounds for Information Reconciliation and Privacy Amplification.* In Advances in Cryptology—ASIACRYPT 2005, Lecture Notes in Computer Science. Springer, 2005.

[Sal98] Louis Salvail. *Quantum Bit Commitment from a Physical Assumption.* In Advances in Cryptology—CRYPTO '98, volume 1462 of Lecture Notes in Computer Science, pages 338–353. Springer, 1998.

[SP00] P. W. Shor and J. Preskill. *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.* Physical Review Letters, 85(2):441–444, July 2000.

[SR95] Jorge Sánchez-Ruiz. *Improved bounds in the entropic uncertainty and certainty relations for complementary observables.* Physics Letters A, 201(2–3):125–131, May 1995.

[Unr02] Dominique Unruh. *Formal security in quantum cryptology.* Master's thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, December 2002. available at `http://www.unruh.de/DniQ/publications/quantum_security.ps.gz`.

[WC79] Mark N. Wegman and J. Lawrence Carter. *New Classes and Applications of Hash Functions.* In 20th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pages 175–182, 1979.

[WF89] William K. Wootters and Brian D. Fields. *Optimal state-determination by mutually unbiased measurements.* Annals of Physics, 191(2):363–381, 1989.

[Wol00] Stefan Wolf. *Reducing Oblivious String Transfer to Universal Oblivious Transfer.* In IEEE International Symposium on Information Theory (ISIT), 2000.