Cryptography in the Bounded-Quantum-Storage Model

Christian Schaffner

PhD Dissertation

BRICS Research School
DAIMI – Department of Computer Science
University of Aarhus
Denmark

Cryptography in the Bounded-Quantum-Storage Model

A Dissertation
Presented to the Faculty of Science
of the University of Aarhus
in Partial Fulfillment of the Requirements for the
PhD Degree

by
Christian Schaffner
official version submitted: March 2, 2007

final version: September 3, 2007

Abstract

Cryptographic primitives such as oblivious transfer and bit commitment are impossible to realize if unconditional security is required against adversaries who are unbounded in running time and memory size. Therefore, it is a great challenge to come up with restrictions on the adversary's capabilities such that on one hand interesting cryptographic primitives become possible, but on the other hand the model is still realistic and as close to practice as possible.

The *bounded-quantum-storage model* is a prime example of such a cryptographic model. In this thesis, we initiate the study of cryptographic primitives with unconditional security under the sole assumption that the adversary's *quantum* memory is of bounded size.

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 to store *at least a large fraction* of the total number of transmitted qubits in order to break the protocol. This is in sharp contrast to the classical bounded-memory model, where we can only tolerate adversaries with memory of size polynomially larger than the honest players' memory size.

On the practical side, our protocols are efficient, non-interactive and can be adapted to cope with various kinds of noise in the transmission. In fact, they can be *implemented using today's technology*.

On the theoretical side, new *entropic uncertainty relations* involving min-entropy are established and used to prove the security of protocols in the bounded-quantum-storage model according to new strong security definitions. The uncertainty relations lower bound the min-entropy of the encoding used in most quantum-cryptographic protocols and therefore contribute to the understanding of the quantum effects which these protocols are based upon. The most direct way to make use of these lower bounds is by assuming a quantum-memory bound on the adversary. For instance, in the realistic setting of *Quantum Key Distribution (QKD)* against quantum-memory-bounded eavesdroppers, the uncertainty relation allows to prove the security of QKD protocols while tolerating considerably higher error rates compared to the standard model with unbounded adversaries.

In addition, though not directly related to the bounded-quantum-storage model, a classical result about unconditionally secure 1-out-of-2 Oblivious Transfer (*1-2 OT*) is obtained. It is pointed out that the standard security requirement for *1-2 OT* of bits, namely that the receiver only learns one of the bits sent, holds if and only if the receiver has no information on the XOR of the

two bits. This result generalizes to *1-2 OT* of strings, in which case the security can be characterized in terms of *binary linear functions*. More precisely, it is shown that the receiver learns only one of the two strings sent, if and only if he has no information on the result of applying any binary linear function which non-trivially depends on both inputs to the two strings. This result not only gives new insight into the nature of *1-2 OT*, but it in particular provides a *powerful tool for analyzing 1-2 OT protocols*. With this characterization at hand, the reducibility of *1-2 OT* of strings to a wide range of weaker primitives follows by a very simple argument.

Acknowledgements

I am grateful to everyone who helped and supported me during my PhD studies here in Århus.

First of all, I want to cordially thank my supervisors and co-authors Louis Salvail and Ivan Damgård and the whole cryptology group at DAIMI for providing an excellent environment for cryptographic research. Countless are the hours I have spent discussing scientific as well as non-scientific issues with Louis, *merci beaucoup*! I thank my other co-authors Claude Crépeau, Serge Fehr, Renato Renner, George Savvides and Jürg Wullschleger for many inspiring visits and discussions.

I appreciated very much being a PhD student in a well-organized and well-funded research group and to be able to work in a brand-new building with plenty of space, great infrastructure and always helpful and friendly staff and secretaries: Ellen, Hanne, Karen, Lene, Michael, and Uffe.

Studying in Århus has been a great experience mainly because of all the friends from the constantly changing "gang" of foreign and Danish fellows at DAIMI including Allan, Claudio, Claus, Doina, Gabi, Henrik, Jan, Jesper, Jooyong, Johan, Kevin, Michael, Mikkel, Mirka, Rune, Tord, Thomas M, Tomas, and Troels; but not to forget the ones who have left Denmark and are now spread around the world: Barnie, Christopher, Emanuela and Paolo, Fitzi, Gosia and Darek, Jens, Jesús, Karl, Kirill, Marco, Nelly and Antonio, Philipp, Thomas P, and Saurabh. I thank you all for the wonderful time, both at and off the table-soccer table. Special thanks to Gosia and Henrik for constructive comments on the introduction of this thesis and to Jürg and Serge for further comments.

I would also like to thank Claude Crépeau for hosting me for a fantastic summer half-year at McGill university in Montréal where I had the chance to meet many interesting people doing quantum research and experience the exciting spot where the francophone part of North America meets the anglophone rest of the continent.

I thank Prof. Andreas Winter from the University of Bristol and Prof. Stefan Wolf from ETH Zürich as well as Prof. Susanne Bødker from the University of Aarhus for agreeing to constitute the evaluation committee for my PhD thesis.

Last but not least, I want to express my gratitude to my family for their immense love and support from the distance. I am infinitely grateful for the great childhood they gave me which was and still is an invaluable source of self-confidence for me.

This research was partially supported by the EU Project SECOQC, No: FP6-2002-IST-1-506813.

Christian Schaffner,
Århus, March 2, 2007.

Contents

Chapter 1

Introduction

In the quest for interesting cryptographic models, bounding the quantum memory of adversarial players is a great assumption.

1.1 Cryptographic Models and Basic Primitives

It is a fascinating art to come up with *protocols*[1] that achieve a cryptographic task like encryption, authentication, identification, voting, secure function evaluation to name just a famous few. To define a notion of security for such protocols, one needs to specify a *cryptographic model*, i.e. an environment in which the protocol is run. The model states for example the number of honest and dishonest players, the allowed running time and amount of memory available to honest and dishonest players, how dishonest players are allowed to deviate from the protocol, the use of external resources like (quantum) communication channels or other already established cryptographic functionalities etc.

While coming up with more and more protocols for different models, cryptographers realized that some basic *primitives* (i.e. precisely defined cryptographic tasks) are useful as "benchmarks" of how powerful a particular cryptographic model is. An example is the two-party primitive *Oblivious Transfer* (*OT*). It comes in different flavors, but all of these variants are equivalent in the sense that anyone of them can be implemented using (possibly several instances of) an other. The *one-out-of-two* variant *1-2 OT* was originally introduced by Wiesner around 1970 (but only published much later in [Wie83]) in the very first paper about quantum cryptography, and later rediscovered by Even, Goldreich, and Lempel [EGL82]. It lets a sender Alice transmit two bits to a receiver Bob who can choose which of them to receive. A secure implementation of *1-2 OT* does not allow a dishonest sender to learn which of the two bits was received and it does not allow a dishonest receiver to learn any information about the second bit. It was a surprising insight when Kilian showed that this simple primitive is *complete* for two-party cryptography [Kil88]. In other words, a model in which *1-2 OT* can be securely implemented allows to implement any cryptographic functionality between two players[2]. Another variant we are con-

[1] A protocol consists of clear-cut instructions for the participating players.

[2] If the model can be reasonably extended to more players, this usually allows to implement

cerned with in this thesis was introduced by Rabin [Rab81] and is hence called Rabin Oblivious Transfer (*Rabin OT*). It is basically a "secure erasure channel": the sender Alice sends a bit which with probability one half is absorbed and with probability one half finds its way to the receiver Bob. The security requirements are the following: whatever a dishonest Alice does, she cannot find out whether the bit was received or not; and whatever a dishonest receiver does, he does not get any information about the bit with probability one half.

Yet another basic two-party primitive of interest is Bit Commitment (*BC*) which allows a player to commit himself to a choice of a bit b by communicating with a verifier. The verifier should not learn b (we say the commitment is *hiding*), yet the committer can later choose to reveal b in a convincing way, i.e. only the value fixed at commitment time will be accepted by the verifier (we say the commitment is *binding*). Bit Commitment is a fundamental building block of virtually every more complicated cryptographic protocol. Implementing secure *BC* with a secure *1-2 OT* at hand is not difficult[3]. On the other hand, there are cryptographic models allowing to securely implement *BC*, but not *1-2 OT*. Moran and Naor gave an example of such a model by assuming the physical device of a tamper-proof seal [MN05].

It is not hard to see that the two security requirements for *BC* are in a sense contradictory, so perfectly secure bit commitment cannot be implemented "from scratch", that is if only error-free communication is available and there is no limitation assumed on the computing power and memory of the players. The informal reason for this is that the hiding property implies that when 0 is committed to, exactly the same information exchange could have happened when committing to 1. Hence, even if 0 was actually committed to, the committer could always compute a complete view of the protocol consistent with having committed to 1, and pretend that this view was what he had in mind originally. By the reduction of *BC* to *1-2 OT* follows that also *1-2 OT* and many other cryptographic functionalities cannot be perfectly secure when built from scratch.

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. Quantum information behaves in a way that is fundamentally different from classical information, enabling, for instance, unconditionally secure key exchange between two honest players (so-called *Quantum Key Distribution*). However, in the case of two mutually distrusting parties, we are not so fortunate: even with quantum communication, unconditionally secure *BC* and *1-2 OT* remain impossible. This is the infamous impossibility result by Mayers and by Lo and Chau [May97, LC97].

For this reason, cryptographers have tried hard to exhibit more restricted models where these impossibility results do not apply. The high art in this pro-

---

secure multi-party protocols as well.

[3]To commit to a bit b, the committer sends random bits of parity b via (several instances of) *1-2 OT* and the verifier picks randomly one of the bits. To open, the committer sends all the random bits he was using, the verifier checks whether these are consistent with what he received.

cess is to find assumptions that are as realistic as possible – thus only minimally restricting the model, but still strong enough to allow for implementing interesting functionalities. There are at least three kinds of possible assumptions, namely

- bounding the computing power of players,
- using the noise in the communication channel,
- exploiting some physical limitation of the adversary, e.g., if 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. A term often used for such schemes is "computational security", meaning that it is *not impossible* for an adversary to behave dishonestly, but it is *computationally infeasible* for him to do so. Security proofs are usually done by reduction in the sense that breaking the security of the protocol would imply solving a hard problem like factoring the product of two large prime numbers. The second scenario has been used to construct both BC and OT protocols in various models for the noise by Crépeau, Kilian, Damgård, Salvail, Fehr, Morozov, Wolf, and Wullschleger [CK88, DKS99, DFMS04, CMW04, Wul07].

The third scenario is the focus of this thesis. In contrast to the first scenario, we deal with "unconditional security" where (depending on the task a protocol aims to achieve) an adversary has no way whatsoever to gain illegal information. Proofs are not done by reduction, but we can prove in information-theoretic terms that except with negligible probability, the adversary does not learn *any information* that is meant to remain secret.

1.2 Classical Bounded-Storage Model

In the classical bounded-storage model, we assume the players to use classical error-free communication and to be computationally unbounded, but on the other hand restrict the size of their memory. In the usual setting, there is a large random source R (often called the *randomizer*) which all players can access, but which is too large (or transmitted too quickly) to store as a whole. One can think of R as a deep-space radio source or a satellite broadcasting random bits at a very high rate.

When Maurer introduced the classical bounded-storage model in [Mau90], the goal was *secure message transmission*. He showed that two honest parties Alice and Bob sharing an initial key can expand that key unless the eavesdropper Eve can store more than a large fraction of the randomizer. The basic idea of the technique allowing Alice and Bob to get an advantage over Eve is that their initial secret key indexes some positions in the randomizer about which Eve has some uncertainty if she cannot store the whole randomizer. Therefore, the bits at these positions can be combined to yield more secure key bits and so to expand the initial key.

A line of subsequent work by Maurer, Cachin, Aumann, Ding, Rabin, Dziembowski, Lu, and Vadhan [Mau92, CM97, ADR02, DM04, Lu04, Vad04] improved this original protocol in terms of efficiency and security. Aumann, Ding and Rabin [ADR02] noticed that protocols in this model enjoy the property of "everlasting security" in the sense that the newly generated key remains secure even when the initial key is later revealed and Eve is no longer memory-bounded, under the sole condition that the original randomizer cannot be accessed any more. Ding [Din05] showed how to do error correction in the bounded-storage model and therefore how to cope with the situation when the honest parties do not have exactly the same view on the randomizer.

Cachin, Crépeau and Marcil illustrated the power of the bounded-storage model by exhibiting in [CCM98] a protocol for *1-2 OT*. Ding improved on this [Din01a] and later showed a constant-round protocol for oblivious transfer in joint work with Harnik, Rosen and Shaltiel [DHRS04].

All these protocols are shown secure as long as the adversary's memory size is at most quadratic in the memory size of the honest players. Considering the ease and low cost of storing massive amounts of classical data nowadays, it is questionable how practical such an assumption on the memory size of the players is. It would be clearly more satisfactory to have a larger than quadratic separation between the memory size of honest players and that of the adversary. However, this was shown to be impossible by Dziembowski and Maurer [DM04].

1.3 Contributions

In this section, we give an overview of the contributions of this thesis. The results about classical oblivious transfer described in Chapter 3 and summarized in Section 1.3.2 are joint work with Damgård, Fehr and Salvail [DFSS06]. All other results are based on two papers co-authored with Damgård, Fehr, Salvail and Renner: [DFSS05] and [DFR$^+$07]. A journal version of [DFSS05] is to appear in a special issue of the SIAM Journal of Computing [DFSS08].

1.3.1 Bounded-Quantum-Storage Model

In this thesis, we study for the first time 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 typical goal is to obtain a certain piece of classical information that we want to keep hidden from him. However, if he cannot store all the quantum information that is sent, he must convert some of it to classical information by measuring. This may irreversibly destroy information, and we may be able to arrange it in such a way that the adversary cannot afford to lose information this way, while honest players can.

It turns out that this can be achieved indeed: 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 a large fraction (typically $n/2$ or $n/4$) of the n transmitted qubits to break the protocol.

We emphasize that no bound is assumed on the adversary's computing power, nor on his classical memory. This is clearly much more satisfactory 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. We emphasize that what makes *OT* and *BC* possible in our model is not so much the memory bound per se, but rather the loss of information on the part of the adversary. Indeed, our results also hold if the adversary's memory device holds an arbitrary number of qubits, but is imperfect in certain ways.

All these factors make the assumption of bounded quantum memory a very attractive cryptographic model. On one hand, as for the classical bounded-storage model, it is simple to work with and yields beautiful theoretical results. On the other hand, it is much more reasonable to assume the difficulty of storing quantum information compared to storing classical one and hence, we are very close to the physical reality and get schemes that can actually be implemented!

1.3.2 Characterization of Security of Classical *1-2 OT*

While the task of formally defining unconditional security of classical protocols for *Rabin OT* and *BC* is well understood, capturing the security of *1-2 OT* in information-theoretic terms is considerably more delicate, as was pointed out by Crépeau, Savvides, Schaffner and Wullschleger [CSSW06]. For *1-2 OT* of bits, it is clear that the security for a honest sender against a cheating receiver guarantees that the receiver does not learn any information about the XOR of the two bits. Somewhat surprisingly, the converse is true as well, not having any information about the XOR of the two bits sent implies that we can point at one bit which the dishonest receiver does not know (given the other).

This idea can be generalized to *1-2 OT* of strings where the ignorance of the XOR becomes ignorance of the outcome of all Non-Degenerate Linear binary Functions (NDLFs) applied to the two strings sent. Such a characterization of sender-security in terms of NDLF composes well with *strongly two-universal hashing* and hereby yields a powerful technique to improve the analyses of the standard reductions from *1-2 OT* to weaker variants of *OT*.

As a historical side note, the original motivation for this classical characterization was the hope that it translates to the quantum setting and thereby yields a security proof of the *1-2 OT* scheme in the bounded-quantum-storage model. We will point out why this approach does *not* work.

1.3.3 Quantum Security Definitions and Protocols

When the players are allowed to use quantum communication, the output of a dishonest player is a quantum state even when the protocol implements a classical primitive. Therefore, security definitions for *Rabin OT*, *1-2 OT* and

BC have to be phrased in quantum terms. As an easy-to-use composability framework has not yet been established for quantum protocols[4], various *ad-hoc* security requirements are commonly used. The definitions in this thesis are the strongest so far proposed, and as they are based on the (classical) considerations in [CSSW06], we believe that they are best suited to provide *sequential composability.*

Most of the presented protocols in the bounded-quantum-storage model can be cast in a non-interactive form, i.e. only one party sends information when doing OT, commitment or opening. We show the following.

OT in the Bounded-Quantum-Storage Model: *There exist non-interactive protocols for Rabin OT and 1-out-of-2 Oblivious Transfer (1-2 OT) of ℓ-bit messages, secure in the bounded-quantum-storage model against adversaries with quantum-memory size at most $n/2 - \ell$ for Rabin OT and $n/4 - 2\ell$ for 1-2 OT. Here, n is the number of qubits transmitted in the protocol and ℓ can be a constant fraction of n. Honest players need no quantum memory at all.*

For the case of bit commitment, the standard definition of the binding property used in the quantum setting was introduced by Dumais, Mayers and Salvail [DMS00]. For $b \in \{0, 1\}$, let p_b denote the probability that a dishonest committer successfully opens the commitment to value b. The binding condition then requires that the sum of p_0 and p_1 does essentially not exceed 1. More formally, $p_0+p_1 \leq 1+negl(n)$ where $negl(n)$ stands for a term which is negligible in n such as 2^{-cn} (for a constant $c > 0$) which is exponentially small in n. This is to capture that a quantum committer can always commit to the values 0 and 1 in superposition. We call this notion *weakly binding* in the following. A shortcoming of this notion is that committing bit by bit is not guaranteed to yield a secure string commitment—the argument that one is tempted to use requires independence of the p_b's between the different executions, which in general does not hold.

Instead, we propose the following *strong binding* condition: After the commitment phase, there exists a binary random variable $D \in \{0, 1\}$ such that a dishonest committer cannot open the commitment to value D except with negligible probability. The point is that the distribution of D is not under control of the dishonest committer. We will point out that using this definition, we can easily derive the security of a string commitment from the security of the individual bits.

BC in the Bounded-Quantum-Storage Model: *There exists a protocol for bit commitment which is non-interactive. It is perfectly hiding and weakly binding in the bounded-quantum-storage model against dishonest committers with quantum-memory size at most $n/2$. It is strongly binding against memory sizes of at most $n/4$. Here, n is the number of qubits transmitted in the protocol. Honest players need no quantum memory at all.*

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

[4]Some rather complicated frameworks are known. They have been put forward by Ben-Or and Mayers [BM04] and Unruh [Unr02].

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 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 has been shown by Moran, Shaltiel and Ta-Shma [MST04] how to do time-stamping that is non-interactive in our sense: a player can time-stamp a document while only receiving information. However, no reasonable protocol for BC or for time-stamping a single bit exists 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 quantum memory for the honest players and remains secure against any adversary unable to store more than half the size of the quantum transmission.

We also note that it has been shown earlier by Salvail [Sal98] 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. 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 quantum 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 sub-linear in n.

1.3.4 Quantum Uncertainty Relations

A problem often encountered in quantum cryptography is the following: through some interaction between the players, a quantum state is generated and then measured by one of the players (we call her Alice in the following). Assuming Alice is honest, we want to know how unpredictable her measurement outcome is to the adversary. Once a lower bound on the adversary's uncertainty about Alice's measurement outcome is established, it is usually easy to prove the desired security property of the protocol. Many existing constructions in quantum cryptography have been proven secure following this paradigm.

Typically, Alice does not make her measurement in a fixed basis, but chooses at random from a set of different bases. These bases are usually chosen to be pairwise *mutually unbiased*, meaning that if the quantum state is such that the measurement outcome in one basis is fixed, then this implies that the uncertainty about the outcome of the measurement in the other basis is maximal. In this way, one hopes to keep the adversary's uncertainty high, even if the state is (partially) under the adversary's control.

An inequality that lower bounds the adversary's uncertainty in such a scenario is called an *uncertainty relation*. There exist uncertainty relations for different measures of uncertainty but cryptographic applications typically require the adversary's min-entropy to be bounded from below. Such uncertainty relations are the key ingredient in the security proofs of our protocols in the bounded-quantum-storage model.

In this thesis, we introduce new general and tight high-order entropic uncertainty relations. Since the relations are expressed in terms of lower bounds on the min-entropy or upper-bounds on large probabilities respectively, they are applicable to a large class of natural protocols in quantum cryptography.

The first uncertainty relation is concerned with the situation where a n-qubit state ρ is measured in one out of two mutually unbiased bases, say either in the computational basis (the $+$-basis) or in the diagonal basis (the $\times$-basis).

First Uncertainty Relation: *Let ρ be an arbitrary state of n qubits, and let $Q^+(\cdot)$ and $Q^\times(\cdot)$ be the respective probability distributions over $\{0,1\}^n$ of the outcome when ρ 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*

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

Another uncertainty relation is derived for situations where an n-qubit state ρ has each of its qubits measured in a random and independent basis sampled uniformly from a fixed set $\mathcal{B}$ of bases. $\mathcal{B}$ does not necessarily have to be mutually unbiased, but we assume a lower bound h—the so-called *average entropic uncertainty bound*—on the average Shannon entropy of the distribution P_ϑ, obtained by measuring an arbitrary one-qubit state in basis $\vartheta \in \mathcal{B}$, meaning that $\frac{1}{|\mathcal{B}|}\sum_\vartheta \mathrm{H}(P_\vartheta) \geq h$.

Second Uncertainty Relation (informal): *Let $\mathcal{B}$ be a set of bases with an average entropic uncertainty bound h as above. Let P_θ denote the probability distribution defined by measuring an arbitrary n-qubit state ρ in basis $\theta \in \mathcal{B}^n$. For a uniform choice $\Theta \in_R \mathcal{B}^n$, it holds except with negligible probability (over Θ and over P_θ) that*

$$\mathrm{H}_\infty(P_\theta \mid \Theta = \theta) \gtrsim nh. \tag{1.1}$$

Observe that (1.1) cannot be improved significantly since the min-entropy of a distribution is at most equal to the Shannon entropy. Our uncertainty relation is therefore asymptotically tight when the bound h is tight.

Any lower bound on the Shannon entropy associated to a set of measurements $\mathcal{B}$ can be used in (1.1). In the special case where the set of bases is $\mathcal{B} = \{+, \times\}$ (i.e. the two BB84 bases named after Bennett and Brassard who used them in the first quantum-key-distribution protocol [BB84]), h is known precisely using Maassen and Uffink's entropic relation [MU88], see (4.2). We get $h = \frac{1}{2}$ and (1.1) results in $\mathrm{H}_\infty(P_\theta \mid \Theta = \theta) \gtrsim \frac{n}{2}$. Uncertainty relations for the BB84 coding scheme are useful, since this coding is widely used in quantum cryptography. Its resilience to imperfect quantum channels, sources, and detectors is an important advantage in practice.

A major difference between the first and second uncertainty relation is that while both relations can be used to bound the min-entropy conditioned on an event, this event happens in the latter case with probability essentially 1 (on average) whereas the corresponding event from the first relation (defined in Corollary 4.17) only happens with probability about 1/2.

1.3.5 *QKD* against Quantum-Memory-Bounded Eavesdropper

We illustrate the versatility of our second uncertainty relation by applying it to Quantum-Key-Distribution (*QKD*) settings. *QKD* is the art of distributing a secret key between two distant parties, Alice and Bob, using only a completely insecure quantum channel and authentic classical communication. *QKD* protocols typically provide unconditional security, i.e., even an adversary with unlimited resources cannot get any information about the key. A major difficulty when implementing *QKD* schemes is that they require a low-noise quantum channel. The tolerated noise level depends on the actual protocol and on the desired security of the key. Because the quality of the channel typically decreases with its length, the maximum tolerated noise level is an important parameter limiting the maximum distance between Alice and Bob.

We consider a model in which the adversary has a limited amount of quantum memory to store the information she intercepts during the protocol execution. In this model, we show that the maximum tolerated noise level is larger than in the standard scenario where the adversary has unlimited resources. For *one-way QKD protocols* which are protocols where error-correction is performed non-interactively (i.e., a single classical message is sent from one party to the other), we show the following result:

QKD Against Quantum-Memory-Bounded Eavesdroppers: *Let $\mathcal{B}$ be a set of orthonormal bases of the two-dimensional Hilbert space $\mathcal{H}_2$ with average entropic uncertainty bound h. Then, a* one-way *QKD*-protocol *produces a secure key against eavesdroppers whose quantum-memory size is sublinear in the length of the raw key at a positive rate, as long as the bit-flip probability p of the quantum channel fulfills $h(p) < h$ where $h(\cdot)$ denotes the binary Shannon-entropy function.*

Although this result does not allow us to improve (compared to unbounded adversaries) the maximum error-rate for the BB84 protocol (the 4-state protocol), the 6-state (using three mutually unbiased bases) protocol can be shown secure against adversaries with memory bound sublinear in the secret-key length as long as the bit-flip error-rate is less than 17%. This improves over the maximal error-rate of 13% for this protocol against unbounded adversaries. We also show that the generalization of the 6-state protocol to more bases (not necessarily mutually unbiased) can be shown secure for a maximal error-rate up to 20% provided the number of bases is large enough. Note that the best known one-way protocol based on qubits is proven secure against general attacks for an error-rate of only up to roughly 14.1%, and the theoretical maximum is 16.3% [RGK05].

The quantum-memory-bounded eavesdropper model studied here is not comparable to other restrictions on adversaries considered in the literature (e.g. *individual attacks*, where the eavesdropper is assumed to apply independent measurements to each qubit sent over the quantum channel as considered by Fuchs, Gisin, Griffiths, Niu, Peres, and Lütkenhaus [FGG$^+$97, Lüt00]). In fact, these assumptions are generally artificial and their purpose is to simplify security proofs rather than to relax the conditions on the quality of the communication channel from which secure key can be generated. We believe that the quantum-memory-bounded eavesdropper model is more realistic.

1.4 Outline of the Thesis

In Chapter 2, we introduce notation and present some basic concepts from probability and quantum information theory like quantum states and various kinds of their entropies. We prepare the stage by reproducing and slightly extending the results about privacy amplification via two-universal hashing from Renner's PhD thesis [Ren05].

Chapter 3 is the only (almost) exclusively classical chapter. It introduces the different flavors of oblivious transfer and gives a characterization of the security for the sender of *1-2 OT* in terms of non-degenerate linear functions. It is cast in a stand-alone manner and the rest of the thesis can be understood without reading this chapter.

In Chapter 4, the basis for the security proofs of the following chapters is laid by establishing the quantum min-entropic uncertainty relations. The following Chapters 5 and 6 contain the quantum definitions, protocols and security proofs for *Rabin OT* and *1-2 OT*, respectively. Chapter 7 treats quantum bit commitment. Two flavors of the "binding property" are defined and the techniques from the two previous chapters are used to prove security in the bounded-quantum-storage model.

Chapter 8 is devoted to another application of the (second) uncertainty relation, quantum key distribution against a quantum-memory-bounded eavesdropper. The last Chapter 9 addresses some practical issues in greater detail and concludes.

A short summary of the notation, the bibliography and an index can be found at the end of the thesis.

1.5 Related Work

The classical bounded-storage model is described in Section 1.2. Besides work pointed out in the overview of the contributions in Section 1.3 above, it is worth mentioning that several protocols aiming at achieving quantum oblivious transfer have been proposed. After Wiesner's original conjugate-coding protocol [Wie83], Bennett, Brassard, Crépeau, and Skubiszewska proposed an interactive protocol for *1-2 OT* [BBCS91], whose security was subsequently analyzed by Crépeau [Cré94], Mayers, Salvail [MS94, May95], and Yao [Yao95]. The protocol from [BBCS91] is interactive and can be easily broken by a dishonest receiver with unbounded quantum memory. To ensure that the receiver actually performs a measurement, it was suggested to use (quantum) bit-commitment schemes such as [BCJL93] which were believed to be secure against such adversaries at this point in time. After the impossibility proofs of quantum bit-commitment by Lo and Chau [LC97], and Mayers [May97], and of oblivious transfer by Lo [Lo97], it became clear that assumptions are necessary in order to securely realize these primitives. Compared to these previous attempts, the protocols in this thesis are simpler, non-interactive, and provably secure according to stronger security definitions.

Work related to classical OT-reductions is referred to in the introductory sections to Chapter 3 in Sections 3.1 and 3.4.1. Previous work about quantum uncertainty relations is described in Section 4.2.

Chapter 2

Preliminaries

In this chapter, we introduce notation and basic concepts used throughout the rest of the thesis. In addition, most of the following chapters have an individual preliminary section introducing concepts that are exclusively used in those specific chapters.

This chapter does *not* give a thorough introduction to probability theory, information theory and quantum information processing, but we rather assume the reader familiar with the basic concepts from the standard literature like [CT91, NC00]. Instead, we give a specific overview of the concepts which are required for understanding this thesis.

2.1 Notation and Basic Tools

For a sequence of variables $x_1, \ldots, x_n$, we use the abbreviation $x^i := x_1, \ldots, x_i$ for the collection of variables up to index i, and we define $x^0 := \emptyset$ to be the empty string.

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 $x|_I := x_{i_1} x_{i_2} \cdots x_{i_\ell}$. It is sometimes convenient that all substrings of this form have the same length, irrespective of the actual size ℓ of the index set I. Therefore, we define the n-bit string $x|_I^\circ := x_{i_1} x_{i_2} \cdots x_{i_\ell} 0 \cdots 0$ to be the original substring padded with $n - \ell$ zeros.

Most logarithms in this thesis are with respect to base 2 and denoted by $\log(\cdot)$. However, when needed, $\ln(\cdot)$ denotes the natural logarithm to base e.

We write $\mathrm{B}^{\delta n}(x)$ for the ball of all n-bit strings at Hamming distance at most δn from x. Note that the number of elements in $\mathrm{B}^{\delta n}(x)$ is the same for all x, we denote it by $\mathrm{B}^{\delta n} := |\mathrm{B}^{\delta n}(x)|$. It is well known that $\mathrm{B}^{\delta n} \leq 2^{nh(\delta)}$, where

$$h(p) := -\big(p \cdot \log p + (1-p) \cdot \log(1-p)\big)$$

is the binary entropy function.

We denote by $negl(n)$ any function of n smaller than the inverse of any polynomial provided n is sufficiently large.

If we want to choose two symbols $+$ or $\times$ according to the bit $b \in \{0,1\}$, we write $[+, \times]_b$. The Kronecker delta function is defined as

$$\delta_{i,j} = \begin{cases} 1 & \text{if} \quad i = j, \\ 0 & \text{if} \quad i \neq j. \end{cases}$$

The indicator random variable $\mathbb{1}_{\mathcal{E}}$ equals 1, if the event $\mathcal{E}$ occurs and 0 else.

Definition 2.1 (convex/concave function) *A function $f : \mathbb{R} \to \mathbb{R}$ is* convex *on the interval $[a, b]$, if for any two points $x, y \in [a, b]$ and $0 \leq s \leq 1$, it holds that*

$$f(sx + (1-s)y) \leq sf(x) + (1-s)f(y).$$

Analogously, the function is concave *on $[a, b]$, if*

$$f(sx + (1-s)y) \geq sf(x) + (1-s)f(y).$$

Lemma 2.2 (Jensen's inequality) *Let $f : \mathbb{R} \to \mathbb{R}$ be a convex function on $\mathbb{R}$ and let $x_1, \ldots, x_n \in \mathbb{R}$. Let $p_1, \ldots, p_n \in [0, 1]$ be such that $\sum_i p_i = 1$. Then,*

$$f\left(\sum_{i=1}^{n} p_i x_i\right) \leq \sum_{i=1}^{n} p_i f(x_i)\,.$$

For $x_1 = x_2 = \ldots = x_n$, equality holds.

Lemma 2.3 (Cauchy-Schwarz inquality) *For real numbers $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, the following holds*

$$\left(\sum_{i=1}^{n} x_i \cdot y_i\right)^2 \leq \left(\sum_{i=1}^{n} x_i^2\right) \cdot \left(\sum_{i=1}^{n} y_i^2\right)\,.$$

Proof: Note that $\sum_{i=1}^{n} (x_i \cdot z + y_i)^2$ is a quadratic polynomial $a \cdot z^2 + bz + c$ without real roots unless all x_i/y_i are equal. Therefore, its discriminant $b^2 - 4ac$ is non-positive:

$$4\left(\sum_{i=1}^{n} x_i \cdot y_i\right)^2 - 4\left(\sum_{i=1}^{n} x_i^2\right) \cdot \left(\sum_{i=1}^{n} y_i^2\right) \leq 0\,.$$

□

2.2 Probability Theory

For a discrete probability space (Ω, P), we write $P[\mathcal{E}]$ for the probability of the event $\mathcal{E} \subset \Omega$, and we write P_X for the distribution of the random variable $X : \Omega \to \mathcal{X}$ taking values in the finite set $\mathcal{X}$. As is common practice, we do not refer to the probability space (Ω, P) but leave it implicitly defined by the joint probabilities of all considered events and random variables. For two random variables X and Y with joint distribution P_{XY} over $\mathcal{X} \times \mathcal{Y}$, the conditional probability distribution of X *given* Y is defined as $P_{X|Y}(x|y) := \frac{P_{XY}(x,y)}{P_Y(y)}$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ with $P_Y(y) > 0$. For a probability distribution Q over $\mathcal{X}$, we abbreviate the (overall) probability of a set $L \subseteq \mathcal{X}$ with $Q(L) := \sum_{x \in L} Q(x)$.

Let P and Q be two probability distributions over the same finite domain $\mathcal{X}$. The *variational distance*[1] $\delta\big(P,Q\big)$ between P and Q is defined as

$$\delta\big(P,Q\big) := \frac{1}{2} \sum_{x \in \mathcal{X}} \big|P(x) - Q(x)\big| \,.$$

Note that this definition makes sense also for *non-normalized* distributions, and indeed we define and use $\delta\big(P,Q\big)$ for arbitrary positive-valued functions P and Q with common domain. In case $\mathcal{X}$ is of the form $\mathcal{X} = \mathcal{U} \times \mathcal{V}$, we can expand $\delta\big(P,Q\big)$ to $\delta\big(P,Q\big) = \sum_u \delta\big(P(u,\cdot),Q(u,\cdot)\big) = \sum_v \delta\big(P(\cdot,v),Q(\cdot,v)\big)$. We write $P \approx_\varepsilon Q$ to denote that P and Q are ε-close, i.e., that $\delta\big(P,Q\big) \leq \varepsilon$.

By UNIF we denote a uniformly distributed binary random variable independent of anything else, such that $P_{\text{UNIF}}(b) = \frac{1}{2}$ for both $b \in \{0,1\}$, and UNIF^ℓ stands for ℓ independent copies of UNIF.

For a random variable R over the reals $\mathbb{R}$, its expected value is denoted by $\mathbb{E}[R]$.

Lemma 2.4 (Markov's inequality) *For a non-negative real random variable X and $\varepsilon > 0$, we have*

$$\Pr\left[X \geq \frac{\mathbb{E}[X]}{\varepsilon}\right] \leq \varepsilon \,.$$

Proof: For the indicator function $\mathbb{1}_\mathcal{E}$ which equals 1 if the event $\mathcal{E}$ occurs and 0 else, we observe that

$$\frac{\mathbb{E}[X]}{\varepsilon} \cdot \mathbb{1}_{\left\{X \geq \frac{\mathbb{E}[X]}{\varepsilon}\right\}} \leq X \,.$$

Taking the expected values on both sides, using linearity of the expectation and rearranging the terms yields the claim. □

Lemma 2.5 (Chernoff's inequality) *Let $X_1, \ldots, X_n$ be identically and independently distributed random variables with Bernoulli distribution, i.e. $X_i = 1$ with probability p and $X_i = 0$ with probability $1-p$. Then $S := \sum_{i=1}^n X_i$ has binomial distribution with parameters (n,p) and it holds that*

$$P\left[\, |S - pn| > \varepsilon n \,\right] \leq 2e^{-2\varepsilon^2 n} \,.$$

See [AS00] or [MP95] for a proof.

[1] also called *statistical* or *Kolmogorov* distance

2.3 Quantum Information Theory

In this section, we give a very brief introduction to the quantum notions we use in this thesis, we refer to [NC00, Ren05] for further explanations.

For any positive integer $d \in \mathbb{N}$, $\mathcal{H}_d$ stands for the complex Hilbert space of dimension d. Sometimes, we omit the dimension and simply write $\mathcal{H}$. The state of a quantum-mechanical system in $\mathcal{H}$ is described by a *density operator* ρ. A density operator ρ is normalized with respect to the trace norm ($\mathrm{tr}(\rho) = 1$), Hermitian ($\rho^* = \rho$) and has non-negative eigenvalues. $\mathcal{P}(\mathcal{H})$ denotes the set of all *density operators* acting on $\mathcal{H}$. $\mathbb{1}$ denotes the identity matrix (describing the fully mixed state) renormalized by the appropriate dimension.

A quantum state $\rho \in \mathcal{P}(\mathcal{H})$ is called *pure* if it is of the form $\rho = |\varphi\rangle\langle\varphi|$ for a (normalized) vector $|\varphi\rangle \in \mathcal{H}$.

A *positive operator-valued measurement (POVM)* is a family $M = \{E_x\}_{x\in\mathcal{X}}$ of non-negative operators such that $\sum_{x\in\mathcal{X}} E_x$ equals the identity matrix. The probability distribution P_X obtained when applying the POVM M to the quantum state ρ is defined as $P_X(x) := \mathrm{tr}(E_x\rho)$.

The general evolution (like unitary transforms, measurements, applying noise etc.) of a quantum system in state ρ can be described by a *quantum operation* $\mathcal{E}(\rho)$, which is a completely positive and trace-preserving map, i.e. $\mathcal{E}$ is linear and maps non-negative normalized operators $\rho \in \mathcal{P}(\mathcal{H})$ into non-negative normalized operators $\mathcal{E}(\rho) \in \mathcal{P}(\mathcal{H})$.

The notion of (variational) distance of two random variables can be naturally extended to the *trace distance* between two density operators $\rho, \sigma \in \mathcal{P}(\mathcal{H})$ defined by $\delta\big(\rho, \sigma\big) := \frac{1}{2}\,\mathrm{tr}(|\rho - \sigma|)$, where we define $|A| := \sqrt{A^*A}$ to be the positive square-root of A. As in the classical case, we write $\rho \approx_\varepsilon \sigma$ to denote that ρ and σ are ε-close, i.e. $\delta\big(\rho, \sigma\big) \leq \varepsilon$. The trace distance has an operational meaning in that the value $\frac{1}{2} + \frac{1}{2}\delta\big(\rho, \sigma\big)$ is the average success probability when distinguishing ρ from σ via a measurement. In fact, the relation to the classical variational distance becomes evident in $\delta\big(\rho, \sigma\big) = \max_M \delta\big(M(\rho), M(\sigma)\big)$ where the maximization is over all POVMs M and $M(\rho)$ refers to the probability distribution obtained when measuring ρ using M. Ruskai [Rus94] showed that the trace distance does not increase under (trace-preserving) quantum operations, formally $\delta\big(\rho, \sigma\big) \leq \delta\big(\mathcal{E}(\rho), \mathcal{E}(\sigma)\big)$ for any quantum operation $\mathcal{E}$.

The pair $\{|0\rangle, |1\rangle\}$ denotes the computational or rectilinear or "+" basis for the 2-dimensional Hilbert space $\mathcal{H}_2$. The diagonal or "×" basis is defined as $\{|0\rangle_\times, |1\rangle_\times\}$ where $|0\rangle_\times = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle_\times = (|0\rangle - |1\rangle)/\sqrt{2}$. The circular or "$\circlearrowleft$" basis consists of vectors $(|0\rangle + i|1\rangle)/\sqrt{2}$ and $(|0\rangle - i|1\rangle)/\sqrt{2}$. 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 $|1\rangle$. For a n-bit string $x \in \{0,1\}^n$, $|x\rangle_+$ stands for the state $\bigotimes_{i=1}^n |x_i\rangle_+ \in \mathcal{H}_{2^n}$ and analogous for $|x\rangle_\times$.

As mentioned above, the behavior of a quantum state in a register E is fully described by its density matrix ρ_E. We often consider cases where a quantum state may depend on some classical random variable X, in that it is described by the density matrix ρ_E^x if and only if $X = x$. For an observer who has only access to the register E but not to X, the behavior of the state is determined by the density matrix $\sum_x P_X(x)\rho_E^x$. The joint state, consisting of the *c*lassical X and the *q*uantum register E and therefore called *cq-state*, is described by the density matrix $\sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x$. In order to have more compact expressions, we use the following notation. We write

$$\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x \qquad \text{and} \qquad \rho_E = \mathrm{tr}_X(\rho_{XE}) = \sum_x P_X(x)\rho_E^x \,.$$

More general, for any event $\mathcal{E}$, we write

$$\rho_{XE|\mathcal{E}} = \sum_x P_{X|\mathcal{E}}(x)|x\rangle\langle x| \otimes \rho_E^x \quad \text{and} \quad \rho_{E|\mathcal{E}} = \mathrm{tr}_X(\rho_{XE|\mathcal{E}}) = \sum_x P_{X|\mathcal{E}}(x)\rho_E^x \,.$$

We also write $\rho_X = \sum_x P_X(x)|x\rangle\langle x|$ for the quantum representation of the classical random variable X (and similarly for $\rho_{X|\mathcal{E}}$). This notation extends naturally to quantum states that depend on several classical random variables (i.e. to ccq-states, cccq-states etc.). Given a cq-state ρ_{XE} as above, by saying that there exists a random variable Y such that ρ_{XYE} satisfies some condition, we mean that ρ_{XE} can be understood as $\rho_{XE} = \mathrm{tr}_Y(\rho_{XYE})$ for a ccq-state ρ_{XYE} that satisfies the required condition.

Obviously, $\rho_{XE} = \rho_X \otimes \rho_E$ holds if and only if the quantum part is independent of X (in that $\rho_E^x = \rho_E$ for any x), where the latter in particular implies that no information on X can be learned by observing only ρ_E. Furthermore, if ρ_{XE} and $\rho_X \otimes \rho_E$ are ε-close in terms of their trace distance $\delta\big(\rho,\sigma\big) = \frac{1}{2}\,\mathrm{tr}(|\rho-\sigma|)$, then the real system ρ_{XE} "behaves" as the ideal system $\rho_X \otimes \rho_E$ except with probability ε (as explained by Renner and König in [RK05]) in that for any evolution of the system no observer can distinguish the real from the ideal one with advantage greater than ε.

2.4 Entropies

2.4.1 Classical Rényi Entropy

Definition 2.6 *Let P be a probability distribution over the finite set $\mathcal{X}$ and $\alpha \in [0,\infty]$. The α-*order sum *of the probability distribution P is defined as $\pi_\alpha(P) := \sum_{x\in\mathcal{X}} P(x)^\alpha$.*

In the limits $\alpha \to \infty$ and $\alpha \to 0$, we set $\pi_\infty(P) := \max_{x\in\mathcal{X}} P(x)$ and $\pi_0(P) := |\{x \in \mathcal{X} : P(x) > 0\}$.

Definition 2.7 (Rényi entropy [Rén61]) *Let P be a probability distribution over the finite set $\mathcal{X}$ and $\alpha \in [0,\infty]$. The* Rényi entropy of order α *is defined as*

$$\mathrm{H}_\alpha(P) := \frac{1}{1-\alpha}\,\log\left(\pi_\alpha(P)\right) = -\log\Big(\big(\sum_{x\in\mathcal{X}} P(x)^\alpha\big)^{\frac{1}{\alpha-1}}\Big)\,.$$

In the limit $\alpha \to \infty$, we obtain the *min-entropy* $\mathrm{H}_\infty(P) = -\log\big(\max_{x\in\mathcal{X}} P(x)\big)$ and for $\alpha \to 0$, we obtain *max-entropy* $\mathrm{H}_0(P) = \log|\{x \in \mathcal{X} : P(x) > 0\}|$. Another important special case is the case $\alpha = 2$, also known as *collision probability* $\pi_2(P) = \sum_{x\in\mathcal{X}} P(x)^2$ and *collision entropy* $\mathrm{H}_2(P) = -\log\big(\sum_x P(x)^2\big)$.

For the limit $\alpha \to 1$, we can use Jensen's inequality (Lemma 2.2) with $p_x := P(x)$ to obtain

$$-\frac{1}{\alpha-1}\log\left(\sum_x p_x P(x)^{\alpha-1}\right) \leq -\sum_x p_x \log\left((P(x)^{\alpha-1})^{\frac{1}{\alpha-1}}\right) .$$

In the limit $\alpha \to 1$, all $P(x)^{\alpha-1}$ go to 1 and therefore, equality holds and we obtain the standard definition of *Shannon entropy* $\mathrm{H}(P) := -\sum_x P(x)\log P(x)$ as in [Sha48].

For a random variable X with probability distribution P_X, we will most often slightly abuse notation and use the common shortcut $\mathrm{H}_\alpha(X)$ instead of $\mathrm{H}_\alpha(P_X)$. For a fixed random variable X over the finite set $\mathcal{X}$, $\alpha \mapsto \mathrm{H}_\alpha(X)$ is a decreasing function on $[0,\infty]$:

$$\log|\mathcal{X}| \geq H_0(X) \geq \mathrm{H}(X) \geq \mathrm{H}_2(X) \geq H_\infty(X)\,,$$

with equality if and only if X is uniform over a subset of $\mathcal{X}$. Furthermore, we have that for $\alpha > 1$, $\pi_\alpha(X) = \sum_x P_X(x)^\alpha \geq \max_x P_X(x)^\alpha$ and therefore,

$$\mathrm{H}_\alpha(X) = \frac{1}{1-\alpha}\log\pi_\alpha(X) \leq \frac{1}{1-\alpha}\log\max_x P_X(x)^\alpha = \frac{\alpha}{1-\alpha}\log\max_x P_X(x)\,,$$

which implies the following relation between Rényi entropies of order $\alpha > 1$:

$$\frac{\alpha-1}{\alpha}\,\mathrm{H}_\alpha(X) \leq \mathrm{H}_\infty(X)\,. \tag{2.1}$$

Conditional Rényi entropy

The Rényi entropy $\mathrm{H}_\alpha(X|Y{=}y)$ of X given the event $Y = y$ is naturally defined as $\mathrm{H}_\alpha(X|Y=y) = \frac{1}{1-\alpha}\log\big(\sum_x P_{X|Y=y}(x)^\alpha\big)$. We can define the *conditional α-order sum of X given Y* and *conditional Rényi entropy* by

$$\pi_\alpha(X|Y) := \max_y \sum_x P_{X|Y=y}(x)^\alpha \quad \text{and} \quad \mathrm{H}_\alpha(X|Y) := \frac{1}{1-\alpha}\log(\pi_\alpha(X|Y))\,.$$

In the limits we have, $\pi_\infty(X|Y) = \max_{x,y} P_{X|Y=y}(x)$, $\pi_0(X|Y) = \max_y |\{x \in \mathcal{X} : P_{X|Y=y}(x) > 0\}|$. For the conditional min-, collision- and max-entropy, we get

$$\begin{aligned}
\mathrm{H}_\infty(X|Y) &:= \min_y \mathrm{H}_\infty(X|Y=y) = \min_{x,y} -\log P_{X|Y=y}(x),\\
\mathrm{H}_2(X|Y) &:= \min_y \mathrm{H}_2(X|Y=y) = \min_y -\log\left(\sum_x P_{X|Y=y}(x)^2\right),\\
\mathrm{H}_0(X|Y) &:= \max_y \mathrm{H}_0(X|Y=y) = \max_y \log|\{x \in \mathcal{X} : P_{X|Y=y}(x) > 0\}|.
\end{aligned}$$

In the limit $\alpha \downarrow 1$, we get $\mathrm{H}_{\downarrow 1}(X|Y) = \min_y \mathrm{H}(X|Y=y)$ and for $\alpha \uparrow 1$, we get $\mathrm{H}_{\uparrow 1}(X|Y) = \max_y \mathrm{H}(X|Y=y)$ which might be different. However, the standard definition of conditional Shannon entropy is neither of those, but "in between":

$$\mathrm{H}(X|Y) := \sum_y P_Y(y)\,\mathrm{H}(X|Y=y) = \sum_{x,y} P_{XY}(x,y)\log P_{X|Y=y}(y)\,.$$

We note that in the literature, $\mathrm{H}_\alpha(X|Y)$ is sometimes defined as average over Y, $\sum_y P_Y(y)\ \mathrm{H}_\alpha(X|Y{=}y)$, like for Shannon entropy. However, we define the more natural following notion. For $1 < \alpha < \infty$, we define the *average conditional* Rényi entropy $\tilde{\mathrm{H}}_\alpha(X|Y)$ as

$$\tilde{\mathrm{H}}_\alpha(X|Y) := -\log\Big(\sum_y P_Y(y)\big(\sum_x P_{X|Y}(x|y)^\alpha\big)^{\frac{1}{\alpha-1}}\Big)\,,$$

and as $\tilde{\mathrm{H}}_\infty(X|Y) = -\log\big(\sum_y P_Y(y)\max_x P_{X|Y}(x|y)\big)$ for $\alpha = \infty$. This notion is useful in particular because it has the property that if the *average* conditional Rényi entropy is large, then the conditional Rényi entropy is large with high probability:

Lemma 2.8 *Let $\alpha > 1$ (allowing $\alpha = \infty$) and $t \geq 0$. Then with probability at least $1 - 2^{-\kappa}$ (over the choice of y) $\mathrm{H}_\alpha(X|Y=y) \geq \tilde{\mathrm{H}}_\alpha(X|Y) - \kappa$.*

Proof: By definition of average conditional Rényi entropy, we have

$$2^{-\tilde{\mathrm{H}}_\alpha(X|Y)} = \mathbb{E}_y\left[(\pi_\alpha(X|Y=y))^{\frac{1}{\alpha-1}}\right]\,.$$

By the Markov's inequality (Lemma 2.4), we get that

$$\Pr_y\left[\pi_\alpha(X|Y=y)^{\frac{1}{\alpha-1}} \geq 2^{-\tilde{\mathrm{H}}_\alpha(X|Y)+\kappa}\right] \leq 2^{-\kappa}$$

and therefore, the probability (over y) that $\mathrm{H}_\alpha(X|Y=y) \leq \tilde{\mathrm{H}}_\alpha(X|Y) - \kappa$ is at most $2^{-\kappa}$. □

As long as $\alpha > 1$, the minimization (or average) over y is the same for all orders of Rényi entropy hence, Equation (2.1) translates to (average) conditional Rényi entropy:

Lemma 2.9 *For any $1 < \alpha < \infty$, we have*

$$\mathrm{H}_2(X|Y) \geq \mathrm{H}_\infty(X|Y) \geq \frac{\alpha-1}{\alpha}\,\mathrm{H}_\alpha(X|Y)$$
$$\tilde{\mathrm{H}}_2(X|Y) \geq \tilde{\mathrm{H}}_\infty(X|Y) \geq \frac{\alpha-1}{\alpha}\tilde{\mathrm{H}}_\alpha(X|Y).$$

Concavity

Lemma 2.10 *For $0 \leq \alpha \leq 1$, Rényi Entropy is a* concave entropic functional, *i.e., for $0 \leq s \leq 1$ and distributions P, Q, we have*

$$\mathrm{H}_\alpha(sP + (1-s)Q) \geq s\,\mathrm{H}_\alpha(P) + (1-s)\,\mathrm{H}_\alpha(Q)\,.$$

For the case of Shannon entropy, note that the function $f(p) := -p\log p$ has derivatives $f'(p) = -1 - \log p$ and $f''(p) = -1/p$ and $f''(p) \leq 0$ for $0 \leq p \leq 1$. Therefore, $f(p)$ is concave and we have

$$\begin{aligned}\mathrm{H}(sP + (1-s)Q) &= \sum_x f(sP(x) + (1-s)Q(x)) \geq \sum_x sf(P(x)) + (1-s)f(Q(x)) \\ &= s\sum_x f(P(x)) + (1-s)\sum_x f(Q(x)) = s\,\mathrm{H}(P) + (1-s)\,\mathrm{H}(Q).\end{aligned}$$

Higher-order Rényi entropy is not necessarily concave as the following example illustrates. Consider the distributions $P(x) = \delta_{x,0}$ and $Q(x) = 2^{-n}$ over $\{0,1\}^n$ with $\mathrm{H}_2(P) = 0$ and $\mathrm{H}_2(Q) = n$. For the equal mixture of these distributions holds $\mathrm{H}_2((P+Q)/2) = -\log(1/4) + O(2^{-n}) \approx 2 < n/2 = (\mathrm{H}_2(P) + \mathrm{H}_2(Q))/2$ for $n > 5$.

Fano's Inequality

Lemma 2.11 (Fano's Inequality) *Let $X \leftrightarrow Y \leftrightarrow X'$ be a Markov chain*[2]. *Then, for the error probability $p_e := P[X \neq X']$, it holds*

$$\mathrm{H}(X|Y) \leq h(p_e) + p_e \cdot \log(|\mathcal{X}| - 1)\,.$$

Proof: We denote by $E := \mathbb{1}_{\{X \neq X'\}}$ the indicator random variable of the event $\{X \neq X'\}$ that the guess was not successful. By the chain rule for Shannon entropy, we can write

$$\mathrm{H}(XE|Y) = \mathrm{H}(X|Y) + \mathrm{H}(E|XY) = \mathrm{H}(E|Y) + \mathrm{H}(X|EY)$$

We observe that $H(E|Y) \leq h(p_e)$, $\mathrm{H}(E|XY) \geq 0$ and

$$\mathrm{H}(X|EY) = (1-p_e)\,\mathrm{H}(X|\{X = X'\}Y) + p_e\,\mathrm{H}(X|\{X \neq X'\}Y) = p_e \log(|\mathcal{X}| - 1)$$

and the claim follows by rearranging the terms. □

2.4.2 Smooth Rényi Entropy

Smooth min- and max-entropies were introduced by Renner and Wolf in [Ren05, RW05][3]. They are families of entropy measures parametrized by non-negative

[2] Think of X' as guess of X based only on Y.

[3] The notion of *smoothing a probability distribution* was already used in [ILL89]. Furthermore, a different kind of *smooth Rényi entropy* (not equivalent to the ones used here) was introduced by Cachin [Cac97].

real numbers ε, called the *smoothness*. It is a generalization of the notions of conditional min- and max-entropy defined in the last section.

$$\mathrm{H}_\infty^\varepsilon(X|Y) := \max_{\mathcal{E}} \min_{x,y} -\log\left(\frac{P_{XY\mathcal{E}}(x,y)}{P_Y(y)}\right),$$
$$\mathrm{H}_0^\varepsilon(X|Y) := \min_{\mathcal{E}} \max_{y} \log\left|\{x \in \mathcal{X} : \frac{P_{XY\mathcal{E}}(x,y)}{P_Y(y)} > 0\}\right|$$

where the maximum/minimum ranges over all events $\mathcal{E}$ with probability $\Pr[\mathcal{E}] \geq 1-\varepsilon$. $P_{XY\mathcal{E}}(x,y)$ is the probability that $\mathcal{E}$ occurs and X, Y take values x, y. Hence, the "distribution" $P_{XY\mathcal{E}}$ is not normalized.

For a given distribution P_{XY}, it is easy to compute its smooth min-entropy (max-entropy), simply by cutting a maximum mass of ε off the largest (smallest) probabilities.

Informally, the statement $\mathrm{H}_\infty^\varepsilon(X) = r$ can be understood that the standard min-entropy of X is close to r, except with probability ε. As ε can be interpreted as an error probability, we typically require ε to be negligible in the security parameter.

The reason why we only define the min- and max-versions of smooth Rényi entropy is that it is shown in [RW05] that for example smooth Rényi entropy of order $\alpha > 1$ obeys

$$\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X|Y) + \frac{\log(1/\varepsilon')}{\alpha - 1} \geq \mathrm{H}_\alpha^\varepsilon(X|Y) \geq \mathrm{H}_\infty^\varepsilon(X|Y)\,.$$

and hence is equivalent to smooth min-entropy up to an additive term which depends on α and the smoothness ε'. An analogue statement holds for $\alpha < 1$ and smooth max-entropy. As pointed out in [RW05], for $\varepsilon = 0$ the relation above shows for example that $\mathrm{H}_2(X)$ cannot be larger than $\mathrm{H}_\infty^\varepsilon(X) + \log(1/\varepsilon)$ whereas for the non-smooth versions, we only know from Equation (2.1) that $\mathrm{H}_2(X) \leq 2\,\mathrm{H}_\infty(X)$.

Most importantly, smooth min- and max-entropy have an *operational meaning* as they provide the answer to two fundamental information-theoretic problems:

- $\mathrm{H}_\infty^\varepsilon(X|Y)$ is the maximum amount[4] of randomness that can be extracted from X and an independent random string R, such that except with probability ε, the extracted string looks completely uniform to an adversary who knows Y and learns R. This falls into the setting of privacy amplification, see Section 2.5 below.

- $\mathrm{H}_0^\varepsilon(X|Y)$ is the minimal length[4] of an encoding computed from X and some additional independent randomness R, such that except with probability ε, someone knowing Y and R can reconstruct X from the encoding. This is a data-compression problem which is often called *information reconciliation* or *error correction* in cryptographic settings.

[4]up to some small additive error term which depends logarithmically on ε

In [RW05], it is shown that smooth min- and max-entropies enjoy several Shannon-like properties such as the chain rule (see Lemma 2.12 below), sub-additivity $\mathrm{H}_\infty^\varepsilon(XY) \leq \mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X) + \mathrm{H}_0^{\varepsilon'}(Y)$ and monotonicity $\mathrm{H}_\infty^\varepsilon(X) \leq \mathrm{H}_\infty^\varepsilon(XY)$).

Lemma 2.12 (Chain Rule [RW05]) *For all $\varepsilon, \varepsilon' > 0$, we have*

$$\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X|Y) > \mathrm{H}_\infty^\varepsilon(XY) - \mathrm{H}_0(Y) - \log\left(\frac{1}{\varepsilon'}\right).$$

As a consequence of the asymptotic equipartition property (cf. [CT91]), smooth Rényi entropy is asymptotically equal to Shannon entropy in the following sense.

Lemma 2.13 ([RW05, HR06]) *Let $(X_1, Y_1), \ldots, (X_n, Y_n)$ be n independent pairs of random variables distributed according to P_{XY}. Then, for any $\alpha \neq 1$,*

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{\mathrm{H}_\alpha^\varepsilon(X^n|Y^n)}{n} = \mathrm{H}(X|Y).$$

Note that such a lemma does *not* hold at all for non-smooth Rényi entropies.

To provide some intuition about smooth min-entropy, the following lemma shows how to translate smooth min-entropy back to regular conditional min-entropy.

Lemma 2.14 *If $\mathrm{H}_\infty^\varepsilon(X|Y) = r$ then there exists an event $\mathcal{E}'$ such that $\Pr(\mathcal{E}') \geq 1 - 2\varepsilon$ and $\mathrm{H}_\infty(X|\mathcal{E}', Y{=}y) \geq r - 1$ for every y with $P_{Y\mathcal{E}'}(y) > 0$.*

Proof: By definition of smooth min-entropy, there exists an event $\mathcal{E}$ with $\Pr(\mathcal{E}) \geq 1 - \varepsilon$ and such that $\mathrm{H}_\infty(X\mathcal{E}|Y{=}y) \geq r$ for all y, and thus $P_{X\mathcal{E}|Y}(x|y) \leq 2^{-r}$ for all x and y. Define $\mathcal{E}'$ by setting for all x and y

$$P_{X\mathcal{E}'|Y}(x|y) := \begin{cases} P_{X\mathcal{E}|Y}(x|y) & \text{if } P_{\mathcal{E}|Y}(y) \geq \frac{1}{2} \\ 0 & \text{else} \end{cases}$$

Then obviously for any y with $P_{Y\mathcal{E}'}(y) > 0$ and thus $P_{\mathcal{E}'|Y}(y) = P_{\mathcal{E}|Y}(y) \geq \frac{1}{2}$,

$$P_{X|\mathcal{E}'Y}(x|y) = \frac{P_{X\mathcal{E}'|Y}(x|y)}{P_{\mathcal{E}'|Y}(y)} \leq \frac{2^{-r}}{P_{\mathcal{E}'|Y}(y)} \leq 2^{-r+1}\,.$$

Furthermore,

$$\begin{aligned} 1 - \varepsilon &\leq \Pr(\mathcal{E}) \\ &= \Pr(\mathcal{E}|P_{\mathcal{E}|Y}(Y) < \tfrac{1}{2}) \cdot \Pr(P_{\mathcal{E}|Y}(Y) < \tfrac{1}{2}) \\ &\quad + \Pr(\mathcal{E}|P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \cdot \Pr(P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \qquad (2.2) \\ &\leq \frac{1}{2}\Pr(P_{\mathcal{E}|Y}(Y) < \tfrac{1}{2}) + \Pr(P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \end{aligned}$$

from which follows that $\Pr(P_{\mathcal{E}|Y}(Y) < \frac{1}{2}) \leq 2\varepsilon$. Thus we can conclude that

$$\begin{aligned}\Pr(\mathcal{E}') &\geq \Pr(\mathcal{E}'|P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \cdot \Pr(P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \\ &\geq \Pr(\mathcal{E}|P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \cdot \Pr(P_{\mathcal{E}|Y}(Y) \geq \tfrac{1}{2}) \\ &\geq 1 - \varepsilon - \frac{1}{2}\Pr(P_{\mathcal{E}|Y}(Y) < \tfrac{1}{2}) \\ &\geq 1 - 2\varepsilon\end{aligned}$$

where the second-last inequality follows from (2.2), and noting (once more) that $\Pr(\mathcal{E}|P_{\mathcal{E}|Y}(Y) < \frac{1}{2}) < \frac{1}{2}$. □

2.4.3 Min-Entropy-Splitting Lemma

For proving reductions between variants of oblivious transfer in Section 3.4 and the security of *1-2 OT* in the bounded-quantum storage in Chapter 6, we will make use of the following min-entropy splitting lemma. Note that if the joint entropy of two random variables X_0 and X_1 is large, then one is tempted to conclude that at least one of X_0 and X_1 must still have large entropy, e.g. half of the original entropy. Whereas this is indeed true for Shannon entropy, it is in general not true for min-entropy. The following lemma, though, which first appeared in a preliminary version of [Wul07], shows that it *is* true in a randomized sense.

Lemma 2.15 (Min-Entropy-Splitting Lemma) *Let $\varepsilon \geq 0$, and let X_0, X_1 be random variables with $\mathrm{H}_\infty^\varepsilon(X_0X_1) \geq \alpha$ Then, there exists a random variable $C \in \{0,1\}$ such that $\mathrm{H}_\infty^\varepsilon(X_{1-C}C) \geq \alpha/2$.*

Proof: Below, we give the proof for $\varepsilon = 0$, i.e., for ordinary (non-smooth) min-entropy. The general claim for smooth min-entropy follows immediately by observing that the same argument also works for non-normalized distributions with a total probability smaller than 1.

We extend the probability distribution $P_{X_0X_1}$ as follows to $P_{X_0X_1C}$. Let $C = 1$ if $P_{X_1}(X_1) \geq 2^{-\alpha/2}$ and $C = 0$ otherwise. We have that for all x_1, $P_{X_1C}(x_1, 0)$ either vanishes or is equal to $P_{X_1}(x_1)$. In any case, $P_{X_1C}(x_1, 0) < 2^{-\alpha/2}$.

On the other hand, for all x_1 with $P_{X_1C}(x_1, 1) > 0$, we have that $P_{X_1C}(x_1, 1) = P_{X_1}(x_1) \geq 2^{-\alpha/2}$ and therefore, for all x_0,

$$P_{X_0X_1C}(x_0, x_1, 1) \leq 2^{-\alpha} = 2^{-\alpha/2} \cdot 2^{-\alpha/2} \leq 2^{-\alpha/2} P_{X_1}(x_1).$$

Summing over all x_1 with $P_{X_0X_1C}(x_0, x_1, 1) > 0$, and thus with $P_{X_1C}(x_1, 1) > 0$, results in

$$P_{X_0C}(x_0, 1) \leq \sum_{x_1} 2^{-\alpha/2} P_{X_1}(x_1) \leq 2^{-\alpha/2}.$$

This shows that $P_{X_{1-C}C}(x, c) \leq 2^{-\alpha/2}$ for all x, c. □

The corollary below follows rather straightforwardly by noting that (for normalized as well as non-normalized distributions) $\mathrm{H}_\infty(X_0X_1|Z) \geq \alpha$ holds exactly if $\mathrm{H}_\infty(X_0X_1|Z = z) \geq \alpha$ for all z, applying the Min-Entropy Splitting Lemma, and then using the chain rule, Lemma 2.12.

Corollary 2.16 *Let $\varepsilon \geq 0$ be given, and let X_0, X_1, Z be random variables with $\mathrm{H}_\infty^\varepsilon(X_0X_1|Z) \geq \alpha$. Then, there exists a binary random variable $C \in \{0,1\}$ such that for $\varepsilon' > 0$,*

$$\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X_{1-C}|ZC) \geq \alpha/2 - 1 - \log(1/\varepsilon').$$

2.4.4 Entropy of Quantum States

As pointed out in [RK05], Rényi entropy $\mathrm{H}_\alpha(\rho)$ can also be defined for a quantum state $\rho \in \mathcal{P}(\mathcal{H})$. For $\alpha \in [0,\infty]$ and $\rho \in \mathcal{P}(\mathcal{H})$, we have

$$\mathrm{H}_\alpha(\rho) := \frac{1}{1-\alpha}\log\left(\mathrm{tr}\left(\rho^\alpha\right)\right).$$

In the limit cases $\alpha \to 0$ and $\alpha \to \infty$, we obtain $\mathrm{H}_0(\rho) = \log(\mathrm{rank}(\rho))$ and $\mathrm{H}_\infty(\rho) = -\log\left(\lambda_{\max}(\rho)\right)$, where $\lambda_{\max}(\rho)$ denotes the maximum eigenvalue of ρ. For $\alpha = 2$, we obtain the *collision entropy* $\mathrm{H}_2(\rho) = -\log\left(\sum_i \lambda_i^2\right)$, where $\{\lambda_i\}_i$ are the eigenvalues of ρ.

For a classical random variable X encoded in $\rho_X = \sum_x P_X(x)|x\rangle\langle x|$, it holds that that $\mathrm{H}_\alpha(\rho_X) = \mathrm{H}_\alpha(X)$.

For deriving our version of the privacy-amplification theorem in the next section, we need the slightly more involved version of quantum conditional min-entropy from [Ren05].

Definition 2.17 ([Ren05]) *Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$. The min-entropy of ρ_{AB} relative to σ_B is*

$$\mathrm{H}_{\min}(\rho_{AB}|\sigma_B) := -\log\lambda$$

where λ is the minimum real number such that $\lambda\cdot\mathbb{1}_A\otimes\sigma_B - \rho_{AB}$ is non-negative.

The min-entropy of ρ_{AB} given $\mathcal{H}_B$ is

$$\mathrm{H}_{\min}(\rho_{AB}|B) := \sup_{\sigma_B}\mathrm{H}_{\min}(\rho_{AB}|\sigma_B)$$

where the supremum ranges over all $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$.

Similar to the classical case, the smooth version can be defined as follows.

Definition 2.18 ([Ren05]) *Let $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A\otimes\mathcal{H}_B)$, $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$, and $\varepsilon \geq 0$. The ε-smooth min-entropy of ρ_{AB} relative to σ_B is*

$$\mathrm{H}_{\min}^\varepsilon(\rho_{AB}|\sigma_B) := \sup_{\overline{\rho}_{AB}}\mathrm{H}_{\min}(\overline{\rho}_{AB}|\sigma_B)$$

where the supremum ranges over the set $\mathcal{B}^\varepsilon(\rho_{AB})$ containing all Hermitian, non-negative operators $\overline{\rho}_{AB}$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $\delta\big(\overline{\rho}_{AB}, \rho_{AB}\big) \leq 2\varepsilon$ and $\mathrm{tr}(\overline{\rho}_{AB}) \leq 1$.

The ε-smooth min-entropy given $\mathcal{H}_B$ is

$$\mathrm{H}_{\min}^\varepsilon(\rho_{AB}|B) := \sup_{\sigma_B}\mathrm{H}_{\min}^\varepsilon(\rho_{AB}|\sigma_B)$$

where the supremum ranges over all $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$.

To compute $\mathrm{H}^{\varepsilon}_{\min}(\rho_{XB}|\sigma_B)$ where ρ_{XB} is a cq-state, the supremum can be restricted to states $\overline{\rho}_{XB} \in \mathcal{B}^{\varepsilon}(\rho_{XB})$ which are classical on $\mathcal{H}_X$ as well [Ren05, Remark 3.2.4].

There is a chain rule for smooth min-entropy, proven in [Ren05, Lemma 3.2.9].

Lemma 2.19 ([Ren05]) *Let $\rho_{XUE} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_U \otimes \mathcal{H}_E)$, $\sigma_U \in \mathcal{P}(\mathcal{H}_U)$, and let $\sigma_E \in \mathcal{P}(\mathcal{H}_E)$ be the fully mixed state on the image of ρ_E, and let $\varepsilon \geq 0$. Then*

$$\mathrm{H}^{\varepsilon}_{\min}(\rho_{XUE}|\sigma_U) - \mathrm{H}_{\max}(\rho_E) \leq \mathrm{H}^{\varepsilon}_{\min}(\rho_{XUE}|\sigma_U \otimes \sigma_E).$$

The following two lemmas state that dropping a quantum register cannot increase the (smooth) min-entropy.

Lemma 2.20 *Let $\rho_{XUQ} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_U \otimes \mathcal{H}_Q)$ be a ccq-state. Then,*

$$\mathrm{H}_{\min}(\rho_{XUQ}|\rho_U) \geq \mathrm{H}_{\min}(\rho_{XU}|\rho_U).$$

Proof: For $\lambda := 2^{-\mathrm{H}_{\min}(\rho_{XU}|\rho_U)}$, we have by Definition 2.17 that $\lambda \cdot \mathbb{1}_X \otimes \rho_U - \rho_{XU} \geq 0$. Using that both X and U are classical, we derive that for all x, u, it holds $\lambda \cdot p_u - p_{xu} \geq 0$, where p_u and p_{xu} are shortcuts for the probabilities $P_U(u)$ and $P_{XU}(x,u)$. Let the normalized conditional operator $\overline{\rho}_Q^{x,u}$ be the quantum state conditioned on the event that $X = x$ and $U = u$, i.e.

$$\sum_{x,u} p_{xu}\, \overline{\rho}_Q^{x,u} \otimes |xu\rangle\langle xu| = \rho_{QXU}.$$

Then,

$$\sum_{x,u} \lambda \cdot p_u\, \overline{\rho}_Q^{x,u} \otimes |xu\rangle\langle xu| - p_{xu}\, \overline{\rho}_Q^{x,u} \otimes |xu\rangle\langle xu| \geq 0.$$

Because of $\overline{\rho}_Q^{x,u} \leq \mathbb{1}_Q$, we get

$$\sum_{x,u} \lambda \cdot p_u\, \mathbb{1}_Q \otimes |xu\rangle\langle xu| - p_{xu}\, \overline{\rho}_Q^{x,u} \otimes |xu\rangle\langle xu| \geq 0.$$

Therefore, $\lambda \cdot \mathbb{1}_{QX} \otimes \rho_U - \rho_{QXU} \geq 0$ holds, from which follows by definition that $\mathrm{H}_{\min}(\rho_{XUQ}|\rho_U) \geq -\log(\lambda)$. □

Lemma 2.21 *Let $\rho_{XUQ} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_U \otimes \mathcal{H}_Q)$ be a ccq-state and let $\varepsilon \geq 0$. Then*

$$\mathrm{H}^{\varepsilon}_{\min}(\rho_{XUQ}|\rho_U) \geq \mathrm{H}^{\varepsilon}_{\min}(\rho_{XU}|\rho_U).$$

Proof: After the remark after Definition 2.18 above, there exists $\sigma_{XU} \in \mathrm{B}^{\varepsilon}(\rho_{XU})$ classical on $\mathcal{H}_X \otimes \mathcal{H}_U$ such that $\mathrm{H}^{\varepsilon}_{\min}(\rho_{XU}|\rho_U) = \mathrm{H}_{\min}(\sigma_{XU}|\sigma_U)$. Because both X and U are classical, we can write $\sigma_{XU} = \sum_{x,u} p_{xu} |xu\rangle\langle xu|$ and extend it to obtain $\sigma_{XUQ} := \sum_{x,u} p_{xu} |xu\rangle\langle xu| \otimes \overline{\rho}_Q^{x,u}$. Lemma 2.20 from above yields $\mathrm{H}_{\min}(\sigma_{XU}|\sigma_U) \leq \mathrm{H}_{\min}(\sigma_{XUQ}|\sigma_U)$. We have by construction that $\delta\big(\sigma_{XUQ}, \rho_{XUQ}\big) = \delta\big(\sigma_{XU}, \rho_{XU}\big) \leq 2\varepsilon$. Therefore, $\sigma_{XUQ} \in \mathrm{B}^{\varepsilon}(\rho_{XUQ})$ and $\mathrm{H}_{\min}(\sigma_{XUQ}|\sigma_U) \leq \mathrm{H}^{\varepsilon}_{\min}(\rho_{XUQ}|\rho_U)$. □

2.5 Two-Universal Hashing and Privacy Amplification against Quantum Adversaries

2.5.1 History and Setting of Privacy Amplification

Assume two parties Alice and Bob share some information X which is only partly secure in the sense that an adversary Eve has some partial knowledge about it. *Privacy Amplification*, introduced by Bennett, Brassard, and Robert [BBR88], is the art of transforming this information X into a highly secure key K by public discussion. The honest parties want to end up with an almost uniformly distributed key K about which Eve has only negligible information given the communication.

A common way to achieve this is to have Alice pick a hash function f at random from a two-universal class of hashing functions (see next section for the definition), apply it to X and announce it to Bob, who applies it to X as well. Due to the randomizing properties of a two-universal function, the output $f(X)$ is close to uniformly distributed from Eve's point of view. As shown in [BBR88] and by Impagliazzo, Levin, Luby [ILL89] and Bennett, Brassard, Crépeau, and Maurer [BBCM95], the classical *privacy amplification theorem* or *left-over hash lemma* (see Corollary 2.27 below) states that if Eve has some classical knowledge W about X, a secure key of length roughly the uncertainty of Eve about X (measured in terms of min-entropy) can be extracted by two-universal hashing. It is pointed out in [RW05], that the maximum amount of extractable randomness is essentially given by the conditional smooth min-entropy $\mathrm{H}_\infty^\varepsilon(X|W)$.

It is interesting to investigate the case when Eve holds quantum information about X. This scenario has been considered by König, Maurer, and Renner [KMR05, RK05, Ren05] and the results reproduced below show that two-universal hashing works just as well against quantum as against classical adversaries.

We note that unlike in the classical case, where many other forms of randomness extractors are known, two-universal hashing is essentially the only way to perform privacy amplification against quantum adversaries.[5] This tool is one of the key ingredients in all protocols presented in this thesis. It has been widely used in other applications as well, for example in security proofs of quantum-key-distribution schemes by Christandl, Renner, Ekert, Kraus, and Gisin [CRE04, KGR05, RGK05, Ren05].

2.5.2 Two-Universal Hashing

An important tool we use is two-universal hashing.

Definition 2.22 *A class $\mathcal{F}_n$ of hashing functions from $\{0,1\}^n$ to $\{0,1\}^\ell$ is called* two-universal*, if for any pair $x, y \in \{0,1\}^n$ with $x \neq y$, and F uniformly*

[5] In a recent paper, König and Terhal [KT06] exhibit some extractors which work against quantum adversaries, but the parameters are far from the classical ones.

chosen from $\mathcal{F}_n$, it holds that

$$P\big[F(x) = F(y)\big] \leq \frac{1}{2^\ell}.$$

We can also define a slightly stronger notion of two-universality as follows:

Definition 2.23 *A class $\mathcal{F}_n$ of hashing functions from $\{0,1\}^n$ to $\{0,1\}^\ell$ is called* strongly two-universal, *if for any pair $x, y \in \{0,1\}^n$ with $x \neq y$, and F uniformly chosen from $\mathcal{F}_n$, the random variables $F(x)$ and $F(y)$ are independent and uniformly distributed over $\{0,1\}^\ell$.*

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

2.5.3 Privacy Amplification against Quantum Adversaries

In the following, we consider the situation where a hash function is picked randomly from $\mathcal{F}_n$ and applied to a classical value $X \in \{0,1\}^n$ which is correlated with a quantum register $\mathcal{H}_E$. Formally, starting with the cq-state $\rho_{XE} = \sum_{x\in\{0,1\}^n} P_X(x)\, |x\rangle\langle x| \otimes \rho_E^x$, we obtain

$$\rho_{F(X)FE} = \sum_{f\in\mathcal{F}_n} \sum_{z\in\{0,1\}^\ell} |z\rangle\langle z| \otimes |f\rangle\langle f| \otimes \sum_{x\in f^{-1}(z)} P_X(x)\, \rho_E^x. \tag{2.3}$$

The following privacy-amplification theorem in the presence of quantum adversaries was first derived in [RK05]. The version below is from [Ren05, Corollary 5.6.1][6].

Theorem 2.24 (Privacy Amplification [Ren05]) *Let $\rho_{XB} \in \mathcal{P}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a cq-state, where X takes values in $\{0,1\}^n$. Let $\mathcal{F}_n$ be a two-universal family of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$, and let $\varepsilon \geq 0$. Then, for the ccq-state $\rho_{F(X)FB}$ defined by (2.3), it holds*

$$\delta\big(\rho_{F(X)FB}, \mathbb{1} \otimes \rho_{FB}\big) \leq \varepsilon + \frac{1}{2} 2^{-\frac{1}{2}(\mathrm{H}^\varepsilon_{\min}(\rho_{XB}|B)-\ell)}.$$

For large parts of this thesis, slightly weaker forms of this theorem are used. These are derived in the following.

Corollary 2.25 *Let ρ_{XUE} be a ccq-state, where X takes values in $\{0,1\}^n$, U in the finite domain $\mathcal{U}$ and register E contains q qubits. Let $\mathcal{F}_n$ be a two-universal family of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$, and let $\varepsilon \geq 0$. Then, for the cccq-state $\rho_{F(X)FUE}$ defined analogous to (2.3), it holds*

$$\delta\big(\rho_{F(X)FUE}, \mathbb{1} \otimes \rho_{FUE}\big) \leq \frac{1}{2} 2^{-\frac{1}{2}\big(\mathrm{H}^\varepsilon_\infty(X|U)-q-\ell\big)} + \varepsilon. \tag{2.4}$$

[6]Note that in [Ren05], the distance from uniform is defined in terms of the trace-norm distance which is twice the variational distance used in this thesis.

Recall that by the definition of the trace-distance, we have that if the right-most term of (2.4) is negligible, i.e. say smaller than $2^{-\lambda n}$, then this situation is $2^{-\lambda n}$-close to the ideal situation where $F(X)$ is perfectly uniform and independent of F, U and E. In particular, replacing $F(X)$ by an independent and uniformly distributed bit results in a common state which essentially cannot be distinguished from the original one.

Proof: In our case, the quantum register B from Theorem 2.24 consists of a classical part U and a quantum part E. Denoting by σ_E the fully mixed state on the image of ρ_E, we only need to consider the term in the exponent to derive Theorem 2.25 as follows

$$\begin{aligned} \mathrm{H}^{\varepsilon}_{\min}(\rho_{XUE}|UE) &\geq \mathrm{H}^{\varepsilon}_{\min}(\rho_{XUE}|\rho_U \otimes \sigma_E) \\ &\geq \mathrm{H}^{\varepsilon}_{\min}(\rho_{XUE}|\rho_U) - \mathrm{H}_{\max}(\rho_E) && (2.5) \\ &\geq \mathrm{H}^{\varepsilon}_{\min}(\rho_{XU}|\rho_U) - \mathrm{H}_{\max}(\rho_E) && (2.6) \\ &= \mathrm{H}^{\varepsilon}_{\infty}(X|U) - q. \end{aligned}$$

The first inequality follows by Definition 2.18 of $\mathrm{H}^{\varepsilon}_{\min}$ as supremum over all σ_{UE}. Inequality (2.5) is the chain rule for smooth min-entropy (Lemma 2.19). Inequality (2.6) uses that the smooth min-entropy cannot decrease when dropping the quantum register which is proven in Lemma 2.21 from the last section. The last step follows by assumption about the quantum register and observing that the state ρ_{XU} is classical and the quantum Definition 2.18 therefore reduces to classical smooth min-entropy. □

The following corollary is a direct consequence of Corollary 2.25. In Chapter 7, this lemma will be useful for proving the binding condition of our commitment scheme. Recall that for $X \in \{0,1\}^n$, $\mathrm{B}^{\delta n}(X)$ denotes the set of all n-bit strings at Hamming distance at most δn from X and $\mathrm{B}^{\delta n} := |\mathrm{B}^{\delta n}(X)|$ is the number of such strings.

Corollary 2.26 *Let ρ_{XUE} be a ccq-state, where X takes values in $\{0,1\}^n$, U in the finite domain $\mathcal{U}$ and register E contains q qubits. Let $\hat{X}$ be a guess for X obtained by learning U and measuring E, and let $\varepsilon \geq 0$. Then, for all $\delta < \frac{1}{2}$ it holds that*

$$P\big[\hat{X} \in \mathrm{B}^{\delta n}(X)\big] \leq 2^{-\frac{1}{2}(\mathrm{H}^{\varepsilon}_{\infty}(X|U)-q-1)+\log(\mathrm{B}^{\delta n})} + 2\varepsilon \cdot \mathrm{B}^{\delta n}.$$

In other words, given some classical knowledge U and 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 $nh(\delta) < \frac{1}{2}(\mathrm{H}^{\varepsilon}_{\infty}(X|U)) - q)$ is small.

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

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

where the first equality follows from the fact that if $X' \neq X$ then, as $\mathcal{F}_n$ is two-universal, $P[F(X) = F(X')] = \frac{1}{2}$. Note that, given F and U and being allowed to measure E, the probability of correctly guessing a binary $F(X)$ is upper bounded by $\frac{1}{2} + \delta\big(\rho_{F(X)FUE}, \mathbb{1} \otimes \rho_{FUE}\big)$ [FvdG99]. In combination with Corollary 2.25 (with $\ell = 1$) the above results in

$$\frac{1}{2} + \frac{p_{\mathrm{succ}}}{2 \cdot \mathrm{B}^{\delta n}} \leq \frac{1}{2} + \frac{1}{2} 2^{-\frac{1}{2}(\mathrm{H}_\infty^\varepsilon(X|U) - q - 1)} + \varepsilon$$

and the claim follows by rearranging the terms. □

2.5.4 Classical Privacy Amplification

The classical privacy-amplification theorem follows as special case from the results above. When there is no quantum correlation, we (almost) recover the well-known classical *left-over hash lemma* [ILL89, BBCM95, HILL99]:

Corollary 2.27 *Let X be a random variable over $\{0,1\}^n$, and let F denote the uniform choice of a hash function in a two-universal family of hash functions $\mathcal{F}_n$ mapping from $\{0,1\}^n$ to $\{0,1\}^\ell$. Then*

$$\delta\big(P_{F(X)F}, P_{\mathrm{UNIF}^\ell} P_F\big) \leq \frac{1}{2} 2^{-\frac{1}{2}(\mathrm{H}_2(X) - \ell)} .$$

This corollary (with collision- instead of min-entropy in the exponent on the right-hand side) cannot immediately be derived from Theorem 2.24 above, but rather from its proof in [Ren05]. The reason for this is that the easiest way of proving both Theorem 2.24 and Corollary 2.27 is by directly considering collision entropy instead of min-entropy. On the other hand, relaxing the notion of collision entropy to smooth min-entropy gives the natural operative meaning (see Section 2.4.2) and interestingly, it only looks like we are losing something by doing that, but in fact this achieves optimality [RW05].

Chapter 3

Classical Oblivious Transfer

Most of the results presented in this chapter are published in [DFSS06].

3.1 Introduction and Outline

As already mentioned in Section 1.1, 1-out-of-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 his choice C. Informally, it is required that the receiver only learns B_C but not B_{1-C} (what we call security for the honest sender, hence *sender-security*), while at the same time the sender does not learn C (*receiver-security*). Interestingly, *1-2 OT* was introduced by Wiesner around 1970 (but only published much later [Wie83]) under the name of "multiplexing" in the context of quantum cryptography, and, inspired by [Rab81] where a different flavor was introduced, later re-discovered by Even, Goldreich and Lempel [EGL82].

1-2 OT turned out to be very powerful as Kilian [Kil88] showed it to be sufficient for secure general two-party computation. For this reason, much effort has been put into reducing *1-2 OT* to seemingly weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, etc. [Cré87, BC97, Cac98, Wol00, BCW03, CS06].

In this chapter, we focus on a slightly modified notion of *1-2 OT*, which we call *Randomized 1-2 OT*, *Rand 1-2 OT* for short, where the bits (or strings) B_0 and B_1 are not *in*put by the sender, but generated uniformly at random during the *Rand 1-2 OT* and then *out*put to the sender. It is still required that the receiver only learns the bit (or string) of his choice, B_C, whereas the sender does not learn any information on C. It is obvious that a *Rand 1-2 OT* can easily be turned into an ordinary *1-2 OT* simply by using the generated B_0 and B_1 to mask the actual input bits (or strings). Furthermore, all known constructions of unconditionally secure *1-2 OT* protocols make implicitly the detour via *Rand 1-2 OT*.

In a first step, we observe that the sender-security condition of a *Rand 1-2 OT* of *bits* is equivalent to requiring the XOR $B_0 \oplus B_1$ to be close to uniformly distributed from the receiver's point of view. The proof is very simple, and it is kind of surprising that—to the best of our knowledge—this has not been realized before. We then ask and answer the question whether there is a natural generalization of this result to *Rand 1-2 OT* of *strings*. Note that requiring the bit wise XOR of the two strings to be uniformly distributed is obviously not sufficient. We show that the sender-security for *Rand 1-2 OT* of strings can be characterized in terms of *non-degenerate linear functions* (bivariate binary linear functions which non-trivially depend on both arguments, as defined in Definition 3.3): sender-security holds if and only if the result of applying any non-degenerate linear function to the two strings is (close to) uniformly distributed from the receiver's point of view.

We then show the usefulness of this new understanding of *1-2 OT*. We demonstrate this on the problem of reducing *1-2 OT* to weaker primitives. Concretely, we show that the reducibility of an ordinary *1-2 OT* to weaker flavors via a non-interactive reduction follows by a trivial argument from our characterization of sender-security. This is in sharp contrast to the current literature: The proofs given by Brassard, Crépeau and Wolf [BC97, Wol00, BCW03] for reducing *1-2 OT* to *1-2 XOT*, *1-2 GOT* and *1-2 UOT* (we refer to Section 3.4 for a description of these flavors of *OT*) are rather complicated and tailored to a particular class of privacy-amplifying hash functions; whether the reductions also work for a less restricted class is left as an open problem [BCW03, page 222]. And, the proof given by Cachin [Cac98] for reducing *1-2 OT* to one execution of a general *UOT* is not only complicated, but also incorrect, as we will point out. Thus, our characterization of the condition for sender-security allows to simplify existing reducibility proofs and, along the way, to solve the open problem posed in [BCW03], as well as to improve the reduction parameters in most cases, but it also allows for new, respectively until now only incorrectly proven reductions. In recent work by Wullschleger [Wul07], the analysis of these reductions is further improved.

Furthermore, we extend our result and show how our characterization of *Rand 1-2 OT* in terms of non-degenerate linear functions translates to *1-n OT*.

As historical side note, we note that the original motivation for characterizing sender-security with the help of NDLFs was to prove sender-security of the quantum protocol for *1-2 OT* described in Chapter 6. We point out by an example in Section 3.6 at the end of this chapter why this approach does not work.

3.2 Defining *1-2 OT*

3.2.1 Randomized *1-2 OT* of Bits

Formally capturing the intuitive understanding of the security of *1-2 OT* is a non-trivial and subtle task. For instance requiring the sender's view to be independent of the receiver's choice bit C is too strong a requirement, since his input might already depend on C. The best one can hope for is that his view is independent of C *conditioned on his input* B_0, B_1. Security against a dishonest receiver is even more subtle. We refer to the security definition by Crépeau, Savvides, Schaffner and Wullschleger of [CSSW06], where it is argued that this definition is the "right" way to define unconditionally secure *1-2 OT*. In their model, a secure *1-2 OT* protocol is as good as an ideal *1-2 OT* functionality.

In this thesis, we will mainly focus on a slight modification of *1-2 OT*, which we call *Randomized 1-2 OT* (although *sender*-randomized *1-2 OT* would be a more appropriate, but also rather lengthy name). 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. This is formalized in Definition 3.1 below.

There are two main justifications for focusing on *Rand 1-2 OT*. First, an ordinary *1-2 OT* can easily 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 (as first realized by Beaver [Bea95]). For a formal proof of this we refer to the full version of [CSSW06]. And second, all information-theoretically secure constructions of *1-2 OT* protocols we are aware of in fact do implicitly build a *Rand 1-2 OT* and use the above reduction to achieve *1-2 OT*.

We formalize *Rand 1-2 OT* in such a way that it minimizes and simplifies as much as possible the security restraints, while at the same time remaining sufficient for *1-2 OT*.

Definition 3.1 (*Rand 1-2 OT*) *An ε-secure Rand 1-2 OT is a protocol between sender* S *and receiver* R*, with* R *having input $C \in \{0,1\}$ (while* S *has no input), such that for any distribution of C, the following properties hold:*

ε-Correctness: *For honest* S *and* R*,* S *has output $B_0, B_1 \in \{0,1\}$ and* R *has output B_C, except with probability ε.*

ε-Receiver-security: *For honest* R *and any (dishonest)* $\tilde{\mathsf{S}}$ *with output V,*

$$\delta\big(P_{CV}, P_C \cdot P_V\big) \leq \varepsilon.$$

ε-Sender-security: *For honest* S *and any (dishonest)* $\tilde{\mathsf{R}}$ *with output W, there exists a binary random variable D such that*

$$\delta\big(P_{B_{1-D}WB_DD}, P_{\text{UNIF}} \cdot P_{WB_DD}\big) \leq \varepsilon.$$

The condition for receiver-security simply says that S learns no information on C, and sender-security requires that there exists a choice bit D, supposed to be C, such that when given the choice D and the corresponding bit B_D, then the other bit, B_{1-D}, is completely random from R's point of view.

We would like to point out that the definition of *Rand 1-2 OT* given in [CSSW06] look syntactically slightly different than our Definition 3.1. However, it is not hard to see that they are actually equivalent. The main difference is that the definition in [CSSW06] involves an auxiliary input Z, which is given to the dishonest player, and receiver- and sender-security as we define them are required to hold *conditioned on Z* for any Z. Considering a *constant Z* immediately proves one direction of the claimed equivalence, and the other follows from the observation that if receiver- and sender-security as we define them hold for *any* distribution $P_{B_0B_1C}$ (respectively P_C), then they also hold for the conditional distribution $P_{B_0B_1C|Z=z}$ (respectively $P_{C|Z=z}$). The other difference is that in [CSSW06], in the condition for sender-security of *Rand 1-2 OT*, B_{1-D} is required to be random and independent of W, B_D, D *and* C. This of course implies our sender-security condition (which is without C), but it is also implied by our definition as C may be part of the output W. We feel that simplifying the definitions as we do, without changing their meaning, allows for an easier handling.

3.2.2 Randomized *1-2 OT* 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 and only one of the two. Formally, for any positive integer ℓ, *1-2 OT*$^\ell$ and *Rand 1-2 OT*$^\ell$ can be defined along the same lines as *1-2 OT* and *Rand 1-2 OT* of *bits*: the binary random variables B_0 and B_1 as well as UNIF in Definition 3.1 are simply replaced by random variables S_0 and S_1 and UNIF$^\ell$ with range $\{0,1\}^\ell$.

3.3 Characterizing Sender-Security

3.3.1 The Case of Bit *OT*

It is well known and it follows from sender-security that in a (*Rand*) *1-2 OT* the receiver R should in particular learn essentially 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 sender-security but also *sufficient*.

Theorem 3.2 *The condition for ε-sender-security for a Rand 1-2 OT is satisfied for a particular (possibly dishonest) receiver $\tilde{\mathsf{R}}$ with output W if and only if*

$$\delta\big(P_{(B_0\oplus B_1)W}, P_{\text{UNIF}} \cdot P_W\big) \leq \varepsilon\,.$$

Before going into the proof which is surprisingly simple, consider the following example. Assume a candidate protocol for *Rand 1-2 OT* and a dishonest receiver $\tilde{\mathsf{R}}$ which is able to output $W = 0$ if $B_0 = 0 = B_1$, $W = 1$ if $B_0 = 1 = B_1$ and $W = 0$ or 1 with probability 1/2 each in case $B_0 \neq B_1$. Then, it is easy to see that conditioned on, say, $W = 0$, (B_0, B_1) is $(0,0)$ with probability $\frac{1}{2}$, and $(0,1)$ and $(1,0)$ each with probability $\frac{1}{4}$, such that the condition on the XOR from Theorem 3.2 is satisfied. On the other hand, neither B_0 nor B_1 is uniformly distributed conditioned on $W = 0$, and 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. Indeed, the same view can be obtained when attacking an *ideal Rand 1-2 OT*: submit a random bit C to obtain B_C and output $W = B_C$. In the light of Definition 3.1, if $W = 0$ 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 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, even when given B_d. The corresponding holds if $W = 1$.

Proof: The "only if" implication is well-known and straightforward. For the "if" implication, we first argue the perfect case where $P_{(B_0 \oplus B_1)W} = P_{\text{UNIF}} \cdot P_W$. For any value w with $P_W(w) > 0$, the non-normalized distribution $P_{B_0B_1W}(\cdot,\cdot,w)$ can be expressed as depicted in the left table of Figure 3.1, where we write a for $P_{B_0B_1W}(0,0,w)$, b for $P_{B_0B_1W}(0,1,w)$, c for $P_{B_0B_1W}(1,0,w)$ and d for $P_{B_0B_1W}(1,1,w)$. Note that $a+b+c+d = P_W(w)$ and, by assumption, $a+d = b+c$. Due to symmetry, we may assume that $a \leq b$. We can then define D by extending $P_{B_0B_1W}(\cdot,\cdot,w)$ to $P_{B_0B_1DW}(\cdot,\cdot,\cdot,w)$ as depicted in the right two tables in Figure 3.1: $P_{B_0B_1DW}(0,0,0,w) = P_{B_0B_1DW}(0,1,0,w) = a$, $P_{B_0B_1DW}(1,0,0,w) = P_{B_0B_1DW}(1,1,0,w) = c$ etc. Important to realize is that $P_{B_0B_1DW}(\cdot,\cdot,\cdot,w)$ is indeed a valid extension since by assumption $c+(b-a) = d$.

a	b
c	d

$P_{B_0B_1W}(\cdot,\cdot,w)$

a	a
c	c

$P_{B_0B_1DW}(\cdot,\cdot,0,w)$

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

$P_{B_0B_1DW}(\cdot,\cdot,1,w)$

Figure 3.1: Distributions $P_{B_0B_1W}(\cdot,\cdot,w)$ and $P_{B_0B_1DW}(\cdot,\cdot,\cdot,w)$

It is now obvious that $P_{B_0B_1DW}(\cdot,\cdot,0,w) = \frac{1}{2}P_{B_0DW}(\cdot,0,w)$ as well as $P_{B_0B_1DW}(\cdot,\cdot,1,w) = \frac{1}{2}P_{B_1DW}(\cdot,1,w)$. This finishes the perfect case.

Concerning the general case, the idea is the same as above, except that one has to take some care in handling the error parameter $\varepsilon \geq 0$. As this does not give any new insight, and we anyway state and fully prove a more general result in Theorem 3.6, we skip this part of the proof.[1] □

3.3.2 The Case of String *OT*

The obvious question after the previous section is whether there is a natural generalization of Theorem 3.2 to *1-2 OT^ℓ* for $\ell \geq 2$. Note that the straightforward generalization of the XOR-condition in Theorem 3.2, 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-security for *Rand 1-2 OT^ℓ*: for instance the receiver could know the first half of the first string and the second half of the second string.

The Characterization

Let ℓ be an arbitrary positive integer.

Definition 3.3 *A function $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ is called a* non-degenerate linear function *(NDLF) if it is of the form*

$$\beta : (s_0, s_1) \mapsto \langle a_0, s_0 \rangle \oplus \langle a_1, s_1 \rangle$$

[1] Although the special case $\ell = 1$ in Theorem 3.6 is quantitatively slightly weaker than Theorem 3.2.

for two non-zero $a_0, a_1 \in \{0,1\}^\ell$, *i.e., if it is linear and non-trivially depends on both input strings.*

Even though this is the main notion we are using, the following more relaxed notion allows to make some of our claims slightly stronger.

Definition 3.4 *A binary function* $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ *is called* 2-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, meaning that* $\big|\{\sigma_1 \in \{0,1\}^\ell : \beta(s_0,\sigma_1) = 0\}\big| = 2^\ell/2$ *and* $\big|\{\sigma_0 \in \{0,1\}^\ell : \beta(\sigma_0, s_1) = 0\}\big| = 2^\ell/2$.

The following is easy to see and the proof is omitted.

Lemma 3.5 *Every non-degenerate linear function is 2-balanced.*

In case $\ell = 1$, the XOR is a NDLF and thus 2-balanced, and it is the *only* NDLF and up to addition of a constant the only 2-balanced function. Based on this notion of non-degenerate linear functions, sender-security of *Rand 1-2 String OT* can be characterized as follows.

Theorem 3.6 *The condition of* ε*-sender-security for a Rand 1-2 OT*$^\ell$ *is satisfied for a particular (possibly dishonest) receiver* $\tilde{\mathsf{R}}$ *with output* W *if*

$$\delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) \leq \varepsilon/2^{2\ell+1}$$

for every NDLF β, *and, on the other hand,* ε*-sender-security may be satisfied only if* $\delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) \leq \varepsilon$ *for every NDLF* β.

The number of NDLFs is exponential in ℓ, namely $(2^\ell - 1)^2$. Nevertheless, we show in Section 3.4 that this characterization turns out to be very useful. There, we will also argue that an exponential overhead in ℓ in the sufficient condition is unavoidable. The proof of Theorem 3.6 also shows that the set of NDLFs forms a minimal set of functions among all sets that imply sender-security. In this sense, our characterization is tight.

At first glance, Theorem 3.6 appears to be related to the so-called (information-theoretic) XOR-Lemma, commonly attributed to Vazirani [Vaz86] and nicely explained by Goldreich [Gol95], which states that a string is close to uniform if the XOR of the bits of any non-empty substring are. As far as we can see, neither follows Theorem 3.6 from the XOR-Lemma in an obvious way nor can it be proven by modifying the proof of the XOR-Lemma, as given in [Gol95].

Furthermore, we would like to point out that Theorem 4 in [BCW03] also provides a tool to analyze sender-security of *1-2 OT* protocols in terms of linear functions; however, the condition that needs to be satisfied is much stronger than for our Theorem 3.6: it additionally requires that one of the two strings is *a priori* uniformly distributed from the receiver's point of view.[2] This difference is crucial, because showing that one of the two strings is uniform (conditioned on

[2]Concretely, it is additionally required that every non-trivial parity of that string is uniform, but by the XOR-Lemma this is equivalent to the whole string being uniform.

the receiver's view) is usually technically involved and sometimes not even possible, as the example given after Theorem 3.2 shows. This is also demonstrated by the fact that the analysis in [BCW03] of the considered *1-2 OT* protocol is tailored to one particular class of privacy-amplifying hash functions, and it is stated as an open problem how to prove their construction secure when a different class of hash functions is used. The condition for Theorem 3.6, on the other hand, is naturally satisfied for typical constructions of *1-2 OT* protocols, as we shall see in Section 3.4. As a result, Theorem 3.6 allows for much simpler and more elegant security proofs for *1-2 OT* protocols, and, as a by-product, allows to solve the open problem from [BCW03]. We explain this in detail in Section 3.4, and the interested reader may well jump ahead and save the proof of Theorem 3.6 for later.

Proof of Theorem 3.6 ("only if" part)

We start with the proof for the "only if" part of Theorem 3.6. In fact, a slightly stronger statement is shown, namely that ε-sender-security implies $\delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) \le \varepsilon$ for any *2-balanced* function.

According to Definition 3.1, ε-sender-security for *Rand 1-2 OT* is satisfied for a receiver R with output W if there exists a random variable D with range $\{0,1\}$ such that

$$\frac{1}{2}\sum_{w,d,s_0,s_1} \big|P_{S_{1-D}S_DDW}(s_{1-d},s_d,d,w) - 2^{-\ell}P_{S_DDW}(s_d,d,w)\big| \le \varepsilon.$$

In order to upper bound

$$\delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) = \frac{1}{2}\sum_{w,b}\big|P_{\beta(S_0,S_1)W}(b,w) - \frac{1}{2}P_W(w)\big|$$

we expand the terms on the right hand side as follows.

$$\begin{aligned} P_{\beta(S_0,S_1)W}(b,w) &= \sum_d P_{\beta(S_0,S_1)DW}(b,d,w) \\ &= \sum_d \sum_{\substack{s_d,s_{1-d} \\ \beta(s_0,s_1)=b}} P_{S_{1-D}S_DDW}(s_{1-d},s_d,d,w) \end{aligned}$$

and

$$P_W(w) = \sum_d \sum_{s_d} P_{S_DDW}(s_d,d,w) = \sum_d 2^{-\ell+1} \cdot \sum_{\substack{s_d,s_{1-d} \\ \beta(s_0,s_1)=b}} P_{S_DDW}(s_d,d,w)$$

where the last equality holds because there are $2^{\ell-1}$ values for s_{1-d} such that $\beta(s_0,s_1) = b$, as β is a 2-balanced function. Using those two expansions we conclude that

$$\begin{aligned}
&\delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) \\
&\quad \leq \frac{1}{2}\sum_{w,b}\sum_{d}\sum_{\substack{s_d,s_{1-d}\\ \beta(s_0,s_1)=b}} \big|P_{S_{1-D}S_DDW}(s_{1-d},s_d,d,w) - 2^{-\ell}P_{S_DDW}(s_d,d,w)\big| \\
&\quad = \frac{1}{2}\sum_{w,d,s_0,s_1} \big|P_{S_{1-D}S_DDW}(s_{1-d},s_d,d,w) - 2^{-\ell}P_{S_DDW}(s_d,d,w)\big| \leq \varepsilon.
\end{aligned}$$

where the first inequality follows follows from the above expansions and the triangle inequality and the last inequality is our initial assumption. □

The "if" part, which is the interesting direction, is proven below.

The Case $\ell = 2$

We feel that in order to understand the proof of Theorem 3.6, it is useful to first consider the case $\ell = 2$. Let us focus on trying to develop a condition that is sufficient for *perfect* sender-security. Fix an arbitrary output w, and consider an arbitrary non-normalized probability distribution $P_{S_0S_1W}(\cdot,\cdot,w)$ of S_0 and S_1 when $W = w$. This is depicted in the left table of Figure 3.2, where we write a for $P_{S_0S_1W}(00,00,w)$, b for $P_{S_0S_1W}(00,01,w)$, etc. We may assume that $a \leq b,c,d$. We now extend this distribution to $P_{S_0S_1DW}(\cdot,\cdot,\cdot,w)$ similar as in the proof of Theorem 3.2. This is depicted in the two right tables in Figure 3.2. We verify what conditions $P_{S_0S_1W}(\cdot,\cdot,w)$ must satisfy such that $P_{S_0S_1DW}$ is indeed a valid extension, i.e., that $P_{S_0S_1DW}(\cdot,\cdot,0,w) + P_{S_0S_1DW}(\cdot,\cdot,1,w) = P_{S_0S_1W}(\cdot,\cdot,w)$.

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

$P_{S_0S_1W}(\cdot,\cdot,w)$

a	a	a	a
e	e	e	e
i	i	i	i
m	m	m	m

$P_{S_0S_1DW}(\cdot,\cdot,0,w)$

0	$b-a$	$c-a$	$d-a$
0	$b-a$	$c-a$	$d-a$
0	$b-a$	$c-a$	$d-a$
0	$b-a$	$c-a$	$d-a$

$P_{S_0S_1DW}(\cdot,\cdot,1,w)$

Figure 3.2: Distributions $P_{S_0S_1W}(\cdot,\cdot,w)$ and $P_{S_0S_1DW}(\cdot,\cdot,\cdot,w)$

For instance, looking at the second row and second column we get equation $e + (b - a) = f$. Altogether, we get the following system of equations.

$$\begin{array}{lll}
b+e=a+f & b+i=a+j & b+m=a+n \\
c+e=a+g & c+i=a+k & c+m=a+o \\
d+e=a+h & d+i=a+l & d+m=a+p
\end{array}$$

Note that if all these equations do hold for any w, then $P_{S_0S_1DW}(\cdot,\cdot,\cdot,\cdot)$ is well defined and satisfies $P_{S_0S_1DW}(\cdot,\cdot,0,\cdot) = \frac{1}{4}P_{S_0DW}(\cdot,0,\cdot)$ and $P_{S_0S_1DW}(\cdot,\cdot,1,\cdot) = \frac{1}{4}P_{S_1DW}(\cdot,1,\cdot)$, in other words, perfect sender-security holds.

The idea now is to show that the above equation system is equivalent to another equation system, in which every equation expresses that a certain NDLF applied to S_0 and S_1 is uniformly distributed when $W = w$, which holds by assumption.

For example, by adding all the equations in the original system while taking every second equation with negative sign, one gets the equation

$$b + d + e + g + j + l + m + o = a + c + f + h + i + k + n + p\,.$$

Define the function $\beta : \{0,1\}^2 \times \{0,1\}^2 \to \{0,1\}$ as follows. Let $\beta(s_0, s_1)$ be 0 if the entry which corresponds to (s_0, s_1) in the left table in Figure 3.2 appears on the left hand side of the above equation, and else we let $\beta(s_0, s_1)$ be 1. Then the above equation simply says that $\beta(S_0, S_1) = 0$ with the same probability as $\beta(S_0, S_1) = 1$ (when $W = w$). Note that it is crucial that in the above equation every variable a up to p occurs with multiplicity exactly 1. By comparing the function tables, it is now easy to verify that β coincides with the function $(s_0, s_1) \mapsto s_{02} \oplus s_{12}$, where s_{i2} denotes the second coordinate of $s_i \in \{0,1\}^2$, thus is a NDLF.

One can now show (and we are going to do this below for an arbitrary ℓ) that there are enough such equations, corresponding to NDLFs, such that these equations imply the original ones. This implies that if $\beta(S_0, S_1)$ is distributed uniformly and independently of W for every NDLF β, then the original equation system is satisfied (for any w), and thus $P_{S_0S_1DW}$ is well-defined.

Proof of Theorem 3.6 ("if" part).

First, we consider the perfect case: if $P_{\beta(S_0,S_1)W}$ *equals* $P_{\mathrm{UNIF}} \cdot P_W$ for every NDLF β, then sender-security for Rand *1-2 OT*$^\ell$ holds perfectly.

The Perfect Case: Since the case $\ell = 1$ is already settled, we assume that $\ell \geq 2$. We generalize the idea from the case $\ell = 2$. The main issue will be to transform the equations guaranteed by the assumption on the linear functions into the ones required for $P_{S_0S_1DW}(\cdot,\cdot,0,w) + P_{S_0S_1DW}(\cdot,\cdot,1,w) = P_{S_0S_1W}(\cdot,\cdot,w)$.

Fix an arbitrary output w of the receiver, and consider the non-normalized probability distribution $P_{S_0S_1W}(\cdot,\cdot,w)$. We use the variable p_{s_0,s_1} to refer to $P_{S_0S_1W}(s_0,s_1,w)$, and we write $\mathbf{o}$ for the all-zero string $(0,\ldots,0) \in \{0,1\}^\ell$. We assume that $p_{\mathbf{o},\mathbf{o}} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^\ell$; we show later that we may do so. We extend this distribution to $P_{S_0S_1DW}(\cdot,\cdot,\cdot,w)$ by setting

$$P_{S_0S_1DW}(s_0,s_1,0,w) = p_{s_0,\mathbf{o}} \quad \text{and} \quad P_{S_0S_1DW}(s_0,s_1,1,w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}} \tag{3.1}$$

for any strings $s_0, s_1 \in \{0,1\}^\ell$, and we collect the equations resulting from the condition that $P_{S_0S_1W}(\cdot,\cdot,w) = P_{S_0S_1DW}(\cdot,\cdot,0,w) + P_{S_0S_1DW}(\cdot,\cdot,1,w)$ needs to be satisfied: for any two $s_0, s_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$

$$p_{s_0,\mathbf{o}} + p_{\mathbf{o},s_1} = p_{\mathbf{o},\mathbf{o}} + p_{s_0,s_1}\,. \tag{3.2}$$

If all these equations do hold for any w, then as in the case of $\ell = 1$ or $\ell = 2$, the random variable D is well defined and $P_{S_{1-D}S_D WD} = P_{\text{UNIF}^\ell} \cdot P_{S_D WD}$ holds, since $P_{S_0 S_1 DW}(s_0, s_1, 0, w)$ does not depend on s_1 and $P_{S_0 S_1 DW}(s_0, s_1, 1, w)$ not on s_0.

We proceed by showing that the equations provided by the assumed uniformity of $\beta(S_0, S_1)$ for any β imply the equations given by (3.2). Consider an arbitrary pair $a_0, a_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$ and let β be the associated NDLF, i.e., such that $\beta(s_0, s_1) = \langle a_0, s_0 \rangle \oplus \langle a_1, s_1 \rangle$. By assumption, $\beta(S_0, S_1)$ is uniformly distributed, independent of W. Thus, for any fixed w, this can be expressed as

$$\sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle = \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} = \sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle \neq \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} , \tag{3.3}$$

where both summations are over all $\sigma_0, \sigma_1 \in \{0,1\}^\ell$ subject to the indicated respective properties. Recall, that this equality holds for any pair $a_0, a_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$. Thus, for fixed $s_0, s_1 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$, if we sum over all such pairs a_0, a_1 subject to $\langle a_0, s_0 \rangle = \langle a_1, s_1 \rangle = 1$, we get the equation

$$\sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1}} \sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle = \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} = \sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1}} \sum_{\substack{\sigma_0,\sigma_1: \\ \langle a_0,\sigma_0\rangle \neq \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} ,$$

which, after re-arranging the terms of the summations, leads to

$$\sum_{\sigma_0,\sigma_1} \sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1 \\ \langle a_0,\sigma_0\rangle = \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} = \sum_{\sigma_0,\sigma_1} \sum_{\substack{a_0,a_1: \\ \langle a_0,s_0\rangle = \langle a_1,s_1\rangle = 1 \\ \langle a_0,\sigma_0\rangle \neq \langle a_1,\sigma_1\rangle}} p_{\sigma_0,\sigma_1} . \tag{3.4}$$

We will now argue that, up to a constant multiplicative factor, equation (3.4) coincides with equation (3.2).

First, it is straightforward to verify that the variables $p_{\mathbf{o},\mathbf{o}}$ and p_{s_0,s_1} occur only on the left hand side, both with multiplicity $2^{2(\ell-1)}$ (the number of pairs a_0, a_1 such that $\langle a_0, s_0 \rangle = \langle a_1, s_1 \rangle = 1$), whereas $p_{s_0,\mathbf{o}}$ and $p_{\mathbf{o},s_1}$ only occur on the right hand side, with the same multiplicity $2^{2(\ell-1)}$.

Now, we argue that any other p_{σ_0,σ_1} equally often appears on the right and on the left hand side, and thus cancel out. Note that the set of pairs a_0, a_1, over which the summation runs on the left respectively the right hand side, can be understood as the set of solutions to a binary non-homogeneous linear equations system:

$$\begin{pmatrix} s_0 & 0 \\ 0 & s_1 \\ \sigma_0 & \sigma_1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \text{ respectively } \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} .$$

Also note that the two linear equation systems consist of three equations and involve at least 4 variables, because $a_0, a_1 \in \{0,1\}^\ell$ and $\ell \geq 2$. Therefore, using basic linear algebra, one is tempted to conclude that they both have solutions, and, because they have the same homogeneous part, they have the same number of solutions, equal to the number of homogeneous solutions. However, this is only guaranteed if the matrix defining the homogeneous part has full rank. In our situation, this is precisely the case if and only if $(\sigma_0, \sigma_1) \notin \{(\mathbf{o}, \mathbf{o}), (s_0, \mathbf{o}), (\mathbf{o}, s_1), (s_0, s_1)\}$, where those four exceptions have already been treated above. It follows that the equations (3.3), which are guaranteed by assumption, imply the equations (3.2).

It remains to justify the assumption that $p_{\mathbf{o},\mathbf{o}} \leq p_{\mathbf{o},s_1}$ for any s_1. In general, we choose $t \in \{0,1\}^\ell$ such that $p_{\mathbf{o},t} \leq p_{\mathbf{o},s_1}$ for any $s_1 \in \{0,1\}^\ell$, and we set $P_{S_0S_1DW}(s_0, s_1, 0, w) = p_{s_0,t}$ and $P_{S_0S_1DW}(s_0, s_1, 1, w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},t}$, resulting in the equation $p_{s_0,t} + p_{\mathbf{o},s_1} = p_{\mathbf{o},t} + p_{s_0,s_1}$ that needs to be satisfied for $s_0 \in \{0,1\}^\ell \setminus \{\mathbf{o}\}$ and $s_1 \in \{0,1\}^\ell \setminus \{t\}$. This equality, though, can be argued as for equation (3.2), which we did above, simply by replacing p_{σ_0,σ_1} on both sides of (3.3) by $p_{\sigma_0,\sigma_1 \oplus t}$ (where $\oplus$ is the bit wise XOR). We may safely do so: doing a suitable variable substitution and using linearity of the inner product, it is easy to see that this modified equation still expresses uniformity of $\beta(S_0, S_1)$. This concludes the proof for the perfect case.

THE GENERAL CASE: Now, we consider the general case where there exists some $\varepsilon > 0$ such that $\delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) \leq 2^{-2\ell-1}\varepsilon$ for any NDLF β. We use the observations from the perfect case but additionally keep track of the "error term".

For any w with $P_W(w) > 0$ and any NDLF β, set

$$\varepsilon_{w,\beta} = \delta\big(P_{\beta(S_0,S_1)W}(\cdot, w), P_{\text{UNIF}} \cdot P_W(w)\big) .$$

Note that $\sum_w \varepsilon_{w,\beta} = \delta\big(P_{\beta(S_0,S_1)W}, P_{\text{UNIF}} \cdot P_W\big) \leq 2^{-2\ell-1}\varepsilon$, independent of β. Fix now an arbitrary w with $P_W(w) > 0$. Then, (3.3) only holds up to an error of $2\varepsilon_{w,\beta}$, where β is the NDLF associated to a_0, a_1. As a consequence, Equation (3.4) only holds up to an error of $2\sum_\beta \varepsilon_{w,\beta}$ and thus (3.2) holds up to an error of $\delta_{s_0,s_1} = \frac{2}{2^{2\ell-2}} \sum_\beta \varepsilon_{w,\beta}$, where the sum is over the $2^{2\ell-2}$ functions associated to the pairs a_0, a_1 with $\langle a_0, s_0\rangle = \langle a_1, s_1\rangle = 1$. Note that δ_{s_0,s_1} depends on w, but the set of β's, over which the summation runs, does not. Adding up over all possible w's gives

$$\sum_w \delta_{s_0,s_1} = \frac{2}{2^{2\ell-2}} \sum_w \sum_\beta \varepsilon_{w,\beta} = \frac{2}{2^{2\ell-2}} \sum_\beta \sum_w \varepsilon_{w,\beta} \leq 2^{-2\ell}\varepsilon .$$

Since (3.2) only holds approximately, $P_{S_0S_1DW}$ as in (3.1) is not necessarily a valid extension, but close. This can obviously be overcome by instead setting

$$P_{S_0S_1DW}(s_0, s_1, 0, w) = p_{s_0,\mathbf{o}} \pm \delta'_{s_0,s_1} \quad \text{and}$$
$$P_{S_0S_1DW}(s_0, s_1, 1, w) = p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}} \pm \delta''_{s_0,s_1}$$

with suitably chosen $\delta'_{s_0,s_1}, \delta''_{s_0,s_1} \geq 0$ with $\delta'_{s_0,s_1} + \delta''_{s_0,s_1} = \delta_{s_0,s_1}$, and with suitably chosen signs "+" or "−".[3] Using that every $P_{S_0S_1DW}(s_0, s_1, 0, w)$ differs from $p_{s_0,\mathbf{o}}$ by at most δ'_{s_0,s_1}, it follows from a straightforward computation

[3] Most of the time, it probably suffices to correct one of the two, say, choose $\delta'_{s_0,s_1} = \delta_{s_0,s_1}$ and $\delta''_{s_0,s_1} = 0$; however, if for instance $p_{s_0,\mathbf{o}}$ and $p_{\mathbf{o},s_1} - p_{\mathbf{o},\mathbf{o}}$ are both positive but $P_{S_0S_1W}(s_0, s_1, w) = 0$, then one has to correct both.

that $\delta\big(P_{S_{1-D}S_D DW}(\cdot,\cdot,0,w), P_{\text{UNIF}}P_{S_D DW}(\cdot,0,w)\big) \leq \sum_{s_0,s_1} \delta'_{s_0,s_1}$. The corresponding holds for $P_{S_0S_1DW}(\cdot,\cdot,1,w)$. It follows that

$$\delta\big(P_{S_{1-D}S_D WD}, P_{\text{UNIF}}P_{S_D WD}\big) \leq \sum_w \sum_{s_0,s_1} (\delta'_{s_0,s_1} + \delta''_{s_0,s_1}) = \sum_{s_0,s_1} \sum_w \delta_{s_0,s_1} \leq \varepsilon$$

which concludes the proof. □

3.4 Applications

In this section we will show the usefulness of Theorem 3.6 for the construction of *1-2 OT*$^\ell$, based on weaker primitives like a noisy channel or other flavors of *OT*. In particular, we will show that the reducibility of *1-2 OT* to any weaker flavor of *OT* follows as a simple argument using Theorem 3.6.

3.4.1 Reducing *1-2 OT*$^\ell$ to Independent Repetitions of Weak *1-2 OT*s

Background

A great deal of effort has been put into constructing protocols for *1-2 OT*$^\ell$ based on physical assumptions like various models for noisy channels [CK88, DKS99, DFMS04, CMW04] or a memory bounded adversary [CCM98, Din01b, DHRS04], as well as into reducing *1-2 OT*$^\ell$ to (seemingly) weaker flavors of *OT*, like *Rabin OT*, *1-2 XOT*, *1-2 GOT* and *1-2 UOT* [Cré87, BC97, Cac98, Wol00, BCW03, CS06, Wul07]. 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 XOR-OT* (which is abbreviated by *1-2 XOT*), $g(B_0, B_1)$ for an arbitrary one-bit-output function g in case of *1-2 Generalized-OT (1-2 GOT)*, and an arbitrary probabilistic Y with mutual information $I(B_0B_1;Y) \leq 1$ in case of *1-2 Universal-OT (1-2 UOT)*.[4]

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, S transfers a randomly chosen bit string $X = (X_0, X_1) \in \{0,1\}^n \times \{0,1\}^n$ to R such that:

1. depending on his choice bit C, the honest R knows either X_0 or X_1,
2. any $\tilde{\mathsf{S}}$ has no information on which part of X R learned, and
3. any $\tilde{\mathsf{R}}$ has some uncertainty in X.

[4] As a matter of fact, reducibility has been proven for any bound on $I(B_0B_1;Y)$ strictly smaller than 2. Note that there is some confusion in the literature in what a *Universal OT*, *UOT* is: In [BC97, Wol00, BCW03], a *UOT* takes as input two *bits* and the receiver is doomed to have at least one bit or any other non-trivial amount of *Shannon* entropy on them; we denote this by *1-2 UOT*. Whereas in [Cac98], a *UOT* takes as input two *strings* and the receiver is doomed to have some *Rényi* entropy of order $\alpha > 1$ on them. We address this latter notion in more detail in Section 3.4.2.

Then, this is completed to a *Rand 1-2 OT* by means of privacy amplification (cf. Section 2.5): S samples two functions f_0 and f_1 from a two-universal class $\mathcal{F}$ of hash functions, sends them to R, and outputs $S_0 = f_0(X_0)$ and $S_1 = f_1(X_1)$, and R outputs $S_C = f_C(X_C)$. Finally, the *Rand 1-2 OT* is transformed into an ordinary *1-2 OT* in the obvious way.

Correctness and receiver-security of this construction are clear, they follow immediately from 1. and 2. How easy or hard it is to prove sender-security depends heavily on the 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 R might know $X_0 \oplus X_1$, it is not possible to argue that there exists $d \in \{0,1\}$ such that R'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 (Corollary 2.27). This difficulty is overcome in [BC97, BCW03] by tailoring the proof to a particular two-universal class of hash functions, namely the class of all *linear* hash functions. Whether the reduction also works for a less restricted class of hash functions is left in [BC97, BCW03] as an open problem, which we solve here as a side result. Using a smaller class of hash functions would allow for instance to reduce the communication complexity of the protocol.

In [CS06], the difficulty is overcome by giving up on the simplicity of the reduction. The cost of two-way communication allowing for interactive hashing is traded for better reduction parameters. We would like to emphasize that these parameters are incomparable to ours, because a different reduction is used, whereas our approach provides a *better analysis* of the common non-interactive reductions.

The New Approach

We argue that, independent of the underlying primitive, sender-security follows as a simple consequence of Theorem 3.6, in combination with a simple observation regarding the composition of non-degenerate linear (respectively, more general, 2-balanced) functions with strongly two-universal hash functions, stated in Proposition 3.7 below.

Recall Definition 2.23 of strong two-universality. A class $\mathcal{F}$ of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$ is *strongly two-universal*, if for any distinct $x, x' \in \{0,1\}^n$ the two random variables $F(x)$ and $F(x')$ 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 3.7 *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 2-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.*[5]

[5] 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 not 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 independent and 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 independent and uniformly distributed over $\{0,1\}$. This holds no matter how f_0 is chosen, and thus proves the claim. □

Now, briefly, sender-security 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 $\tilde{\mathsf{R}}$ has "high" collision entropy in X. Hence, for any NDLF β, we can apply the privacy-amplification Theorem 2.27 with 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-security then follows immediately from Theorem 3.6.

We save the quantitative analysis (Theorem 3.8) for next section, where we consider a reduction of *1-2 OT* to the weakest kind of *OT*: to *one* execution of a *UOT*. Based on this, we compare in Section 3.4.3 the quality of the analysis of the above reductions based on Theorem 3.6 with the results in [BCW03]. It turns out that our analysis is tighter for *1-2 GOT* and *1-2 UOT*, whereas the analysis in [BCW03] is tighter for *1-2 XOT*; but in all cases, our analysis is much simpler and, we believe, more elegant.

3.4.2 Reducing *1-2 OT*$^\ell$ to One Execution of *UOT*

In this section, we use the definition and some elementary properties of Rényi entropy introduced in Section 2.4.1.

Universal Oblivious Transfer

Probably the weakest flavor of *OT* is the *Universal OT* (*UOT*) as it was introduced by Cachin in [Cac98], in that it gives the receiver the most freedom in getting information on the string X. Formally, for a finite set $\mathcal{X}$ and parameters $\alpha > 1$ (allowing $\alpha = \infty$) and $r > 0$, an (α, r)-*UOT*$(\mathcal{X})$ works as follows: the sender inputs $x \in \mathcal{X}$, and the receiver may choose an arbitrary conditional probability distribution $P_{Y|X}$ with the only restriction that for a uniformly distributed X it must satisfy $\mathrm{H}_\alpha(X|Y) \geq r$. The receiver then gets as output y, sampled according to the distribution $P_{Y|X}(\cdot|x)$, whereas the sender gets no information on the receiver's choice for $P_{Y|X}$. Note that a *1-2 UOT* is a limit case of this kind of *UOT* since "*1-2 UOT* = $(1,1)$-*UOT*$(\{0,1\}^2)$".

The crucial property of such an *UOT* is that the input is not restricted to two bits, but may be two bit-*strings*; this potentially allows to reduce *1-2 OT* to *one* execution of a *UOT*, rather than to many independent executions of the same primitive as for the 1-2 flavors of *OT* mentioned above. Indeed, following the design principle discussed in Section 3.4.1, it is straightforward to come up with a candidate protocol for *1-2 OT*$^\ell$ which uses *one* execution of a (α, r)-*UOT*$(\mathcal{X})$ with $\mathcal{X} = \{0,1\}^n \times \{0,1\}^n$. The protocol is given in Figure 3.3, where $\mathcal{F}$ is a strongly two-universal class of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$.

OT2UOT(c)**:**

1. S and R run (α, r)-*UOT*$(\mathcal{X})$: S inputs a random $x = (x_0, x_1) \in \mathcal{X} = \{0,1\}^n \times \{0,1\}^n$, R inputs $P_{Y|X}$ with $P_{Y|X}(x'_c|(x'_0, x'_1)) = 1$ for any (x'_0, x'_1), and as a result R obtains $y = x_c$.
2. S samples independent random $f_0, f_1 \in \mathcal{F}$, sends f_0 and f_1 to R, and outputs $s_0 = f_0(x_0)$ and $s_1 = f_1(x_1)$.
3. R computes and outputs $s_c = f_c(y)$.

Figure 3.3: Protocol *OT2UOT* for *Rand1-2 OT*$^\ell$.

In [Cac98] it is claimed that, for appropriate parameters, protocol *OT2UOT* is a secure *Rand 1-2 OT*$^\ell$, respectively, the resulting protocol for *1-2 OT* is secure. However, we argue below that the proof given is not correct and it is not obvious how to fix it. In Theorem 3.8 we then show that its security follows easily from Theorem 3.6.

A Flaw in the Security Proof

In [Cac98] the security of protocol *OT2UOT* is argued as follows. Using rather complicated *spoiling-knowledge techniques*, it is shown that, conditioned on the receiver's output (which we suppress to simplify the notation) at least one out of $\mathrm{H}_\infty(X_0)$ and $\mathrm{H}_\infty(X_1|X_0 = x_0)$ is "large" (for any x_0), and, similarly, at least one out of $\mathrm{H}_\infty(X_1)$ and $\mathrm{H}_\infty(X_0|X_1{=}x_1)$. Since collision entropy is lower bounded by min-entropy, it then follows from the privacy amplification theorem that at least one out of $\mathrm{H}(F_0(X_0)|F_0)$ and $\mathrm{H}(F_1(X_1)|F_1, X_0{=}x_0)$ is close to ℓ, and similarly, one out of $\mathrm{H}(F_1(X_1)|F_1)$ and $\mathrm{H}(F_0(X_0)|F_0, X_1{=}x_1)$. It is then claimed that this proves *OT2UOT* secure.

We argue that this very last implication is not correct. Indeed, what is proven about the entropy of $F_0(X_0)$ and $F_1(X_1)$ does not exclude the possibility that both entropies $\mathrm{H}(F_0(X_0)|F_0)$ and $\mathrm{H}(F_1(X_1)|F_1)$ are maximal, but that $\mathrm{H}(F_0(X_0) \oplus F_1(X_1)|F_0, F_1) = 0$. This would allow the receiver to learn the bit wise XOR $S_0 \oplus S_1$, which is clearly forbidden by the condition of sender-security.

Also note that the proof does not use the fact that the two functions F_0 and F_1 are chosen *independently*. However, if they are chosen to be the same, then the protocol is clearly insecure: if the receiver asks for $Y = X_0 \oplus X_1$, and if $\mathcal{F}$ is a class of *linear* two-universal hash functions, then $\tilde{\mathsf{R}}$ obviously learns $S_0 \oplus S_1$.

Reducing *1-2 OT*$^\ell$ to *UOT*

The following theorem guarantees the security of *OT2UOT* for an appropriate choice of the parameters. The only restriction we have to make is that $\mathcal{F}$ needs to be a *strongly* two-universal class of hash function.

Theorem 3.8 *Let $\mathcal{F}$ be a* strongly *two-universal class of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$. Then OT2UOT reduces a $2^{-\kappa}$-secure Rand 1-2 OT$^\ell$ to a perfect $(2,r)$-UOT$(\{0,1\}^{2n})$ with $n \geq r \geq 4\ell + 2\kappa + 1$.*

Using the bounds from Lemma 2.9 on the different orders of Rényi entropy, the reducibility of *1-2 OT*$^\ell$ to (α, r)-*UOT*$(\mathcal{X})$ follows immediately for *any* $\alpha > 1$.

Informally, sender-security of the protocol *OT2UOT* is argued as for the reduction of *1-2 OT* to *Rabin OT*, *1-2 XOT* etc., discussed in Section 3.4.1, simply by using Proposition 3.7 in combination with the privacy amplification Theorem 2.27, and applying Theorem 3.6. The formal proof given below additionally keeps track of the error term.

From this proof it also becomes clear that the exponential (in ℓ) overhead in Theorem 3.6 is unavoidable. Indeed, a sub-exponential overhead would allow ℓ in Theorem 3.8 to be super-linear in n, which of course is nonsense.

Proof: By the definition of conditional collision entropy, we have that for all y, $\mathrm{H}_2(X|Y=y) \geq r \geq 4\ell + 2\kappa + 1$. Fix an arbitrary y and consider any NDLF $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$. Let F_0 and F_1 be the random variables that represent the random choices of f_0 and f_1, and set $B = \beta(F_0(X_0), F_1(X_1))$. In combination with Proposition 3.7, privacy amplification (Corollary 2.27) guarantees that

$$\delta\big(P_{BF_0F_1|Y=y}, P_{\mathrm{UNIF}} P_{F_0F_1|Y=y}\big) \leq 2^{-\frac{1}{2}(\mathrm{H}_2(X|Y=y)+1)} \leq 2^{-\frac{1}{2}(4\ell+2\kappa+2)} = 2^{-2\ell-\kappa-1}.$$

It now follows that

$$\begin{aligned}\delta\big(P_{\beta(S_0,S_1)W}, P_{\mathrm{UNIF}} \cdot P_W\big) &= \delta\big(P_{BF_0F_1Y}, P_{\mathrm{UNIF}} P_{F_0F_1Y}\big)\\ &= \sum_y \delta\big(P_{BF_0F_1|Y=y}, P_{\mathrm{UNIF}} P_{F_0F_1|Y=y}\big) P_Y(y) \leq 2^{-\kappa}/2^{2\ell+1}\,.\end{aligned}$$

Sender-security as claimed now follows from Theorem 3.6. □

The min-entropy splitting Lemma 2.15 and a larger (not necessarily strongly) two-universal class of hash functions can alternatively be used to show the security of the reduction protocol *OT2UOT* without the use of NDLFs. We do this here for illustration purposes because the same technique is used in the security proof of *1-2 OT* in the bounded-quantum-storage model in Chapter 6. After the execution of a perfect (∞, r)-*UOT*$(\{0,1\}^{2n})$, we have $\mathrm{H}_\infty(X_0X_1|Y) \geq r$ and Lemma 2.15 yields the existence of a random variable $D \in \{0,1\}$ such that $\mathrm{H}_\infty(X_{1-D}D|Y) \geq r/2$ and therefore also $\mathrm{H}_\infty(X_{1-D}DS_D|Y) \geq r/2$. By the chain rule (Lemma 2.12) and setting $\varepsilon := 2^{-\kappa-1}$, we get $\mathrm{H}_\infty^\varepsilon(X_{1-D}|DS_DY) \geq r/2 - 1 - \ell - \kappa - 1$. Hence to get a $2^{-\kappa}$-secure *Rand 1-2 OT*$^\ell$ via the privacy amplification theorem (Corollary 2.25), we need $r/2 - \ell - \kappa - 2 > 2\kappa + \ell$ which gives slightly worse parameters than in Theorem 3.8, namely $n \geq r \geq 4\ell + 4\kappa + 4$.

3.4.3 Quantitative Comparisons To Related Work

Subsequent to [DFSS06], Wullschleger improved the min-entropy splitting technique described in the last paragraph. In [Wul07], it is shown that the protocol *OT2UOT* reduces a $2^{-\kappa}$-secure *Rand 1-2* OT^ℓ to a perfect (∞, r)-$UOT(\{0,1\}^{2n})$ if $n \geq r \geq 2\ell + 6\kappa + 6\log(3)$. So, *Rand 1-2* OT^ℓ of strings of length ℓ roughly half of the receivers min-entropy r can be obtained, which is asymptotically optimal for this reduction-protocol. Technically, the result is essentially obtained by using the min-entropy splitting approach sketched at the end of last section and a more careful case distinction. The random variable $D \in \{0,1\}$ pointing to the "known" string X_D is basically defined as in Lemma 2.15, but for the case when both X_0, X_1 have high min-entropy, a new *distributed* left-over hash lemma is used to show that both S_0 and S_1 are close to uniform and therefore close to independent (and hence, the pointer D can be chosen arbitrarily in this case).

In the following, we compare the simple reduction of *1-2* OT^ℓ to n executions of *1-2 XOT*, *1-2 GOT* and *1-2 UOT*, respectively, using our analysis based on Theorem 3.6 together with the quantitative statement given in Theorem 3.8, with the results achieved in [BCW03].[6] The quality of the analysis of a reduction is given by the *reduction parameters* c_{len}, c_{sec} and c_{const} such that the *1-2* OT^ℓ is guaranteed to be $2^{-\kappa}$-secure as long as $n \geq c_{\text{len}} \cdot \ell + c_{\text{sec}} \cdot \kappa + c_{\text{const}}$. The smaller these constants are, the better is the analysis of the reduction. The comparison of these parameters is given in Figure 3.4. We focus on c_{len} and c_{sec} since c_{const} is not really relevant, unless very large.

	1-2 XOT		*1-2 GOT*		*1-2 UOT*	
	c_{len}	c_{sec}	c_{len}	c_{sec}	c_{len}	c_{sec}
BCW [BCW03]	2	2	4.8	4.8	14.6	14.6
this work [DFSS06]	4	2	4	3	13.2	10.0
subsequent [Wul07]	2	6	2	7	6.7	23.3

Figure 3.4: Comparison of the reduction parameters.

The parameters in the first line can easily be extracted from Theorems 5, 7 and 9 of [BCW03], where in Theorem 9 $p_e \approx 0.19$. The parameters in the second line corresponding to the reduction to *1-2 XOT* follow immediately from Theorem 3.8, using the fact that in *one* execution of a *1-2 XOT*, the receiver's conditional collision entropy on the sender's two input bits is at least 1.

Determining the parameters of the reductions to *1-2 GOT* and *1-2 UOT* requires a little more work. We first determine the *average* conditional min-entropy $\tilde{\mathrm{H}}_\infty(X|Y)$ of one instance of *1-2 GOT* and *1-2 UOT*. In the case of *1-2 GOT*, $\tilde{\mathrm{H}}_\infty(X|Y)$ can easily be seen to be at least 1 (for example by in-

[6] As mentioned earlier, these results are incomparable to the parameters achieved in [CS06], where *interactive* reductions are used.

spection of Table 2 in [BCW03]). For one execution of *1-2 UOT*, the receiver's average Shannon entropy is at least 1. Therefore, it follows from Fano's Inequality (Lemma 2.11) that his average guessing probability is at most $1 - p_e$ with $p_e \approx 0.19$ as above, and thus his average conditional min-entropy is at least $-\log(1 - p_e) \approx 0.3$.

We use Lemma 2.8 to lower bound the (regular) conditional min-entropy $\mathrm{H}_\infty(X|Y = y)$ except with probability $2^{-\kappa-1}$ and use Theorem 3.8 with security parameter $2^{-\kappa-1}$ which together yields a $2^{-\kappa}$ secure *Rand 1-2 OT*$^\ell$. To apply Theorem 3.8, we require $\mathrm{H}_2(X|Y = y) \geq \mathrm{H}_\infty(X|Y = y) \geq 4\ell + 2\kappa + 3$ and to obtain this by Lemma 2.8, we need $\tilde{\mathrm{H}}_\infty(X|Y) \geq 4\ell + 3\kappa + 4$.

This yields $c_{\mathrm{len}} = 4, c_{\mathrm{sec}} = 3$ for *1-2 GOT* and $c_{\mathrm{len}} \approx 4/0.3$ and $c_{\mathrm{sec}} \approx 3/0.3$ for *1-2 UOT*. The derivation of the parameters for [Wul07] is analogous.

3.5 Extension to *1-n OT*$^\ell$

In this section we extend our characterization of sender-security of *Rand 1-2 OT* to *Rand 1-n OT*. We use the following notation. For a sequence of random variables $S_0, S_1, \ldots, S_{n-1}$ and indices $i, j \in \{0, \ldots, n-1\}$, we denote by $\overline{S_{i,j}}$ the sequence of variables $\{S_k : k \in \{0, \ldots, n-1\} \setminus \{i, j\}\}$ with all indices except i and j. Similarly, $\overline{S_i}$ denotes all variables but the ith.

Definition 3.9 (*Rand 1-n OT*$^\ell$) *An ε-secure Rand 1-n OT is a protocol between* S *and* R*, with* R *having input $C \in \{0, 1, \ldots, n-1\}$ (while* S *has no input), such that for any distribution of C, the following properties hold:*

ε-Correctness: *For honest* S *and* R*,* S *has output $S_0, S_1, \ldots, S_{n-1} \in \{0,1\}^\ell$ and* R *outputs S_C, except with probability ε.*

ε-Receiver-security: *If* R *is honest then for any (possibly dishonest) $\tilde{\mathsf{S}}$ with output V,*

$$\delta\big(P_{CV}, P_C \cdot P_V\big) \leq \varepsilon.$$

ε-Sender-security: *If* S *is honest then for any (possibly dishonest) $\tilde{\mathsf{R}}$ with output W, there exists a random variable D with range $\{0, 1, \ldots, n-1\}$ such that*

$$\delta\big(P_{\overline{S_D} W S_D D}, P^{n-1}_{\mathrm{UNIF}^\ell} \cdot P_{W S_D D}\big) \leq \varepsilon.$$

Analogous to the *1-2 OT*-case we want for sender-security that there exists a choice D, such that when given the corresponding string (or bit) S_D all the other strings (or bits) look completely random from R's point of view.

Recall that for the characterization of sender-security in the case of *1-2 OT*, it is sufficient that $P_{\beta(S_0,S_1)W} = P_{\mathrm{UNIF}} \cdot P_W$ for every NDLF β. In a first attempt one might try to characterize the sender-security of *1-n OT* using linear functions β that non-trivially depend on n arguments. In the case of *1-3 OT* of bits, the only linear function of this kind is the XOR of the three bits, but it can be easily verified that the requirement that $B_0 \oplus B_1 \oplus B_2$ is uniform does *not* imply sender-security in the sense defined above. Instead, as we will see below, sufficient requirements are that the XOR of *every pair of bits* is uniform *when given the value of the third.*

Theorem 3.10 *The condition for ε-sender-security for a Rand 1-n OT$^\ell$ is satisfied for a particular (possibly dishonest) receiver $\tilde{\mathsf{R}}$ with output W, if for all $i \neq j \in \{0, \dots, n-1\}$*

$$\delta\big(P_{\beta(S_i,S_j)W\overline{S_{i,j}}}, P_{\text{UNIF}} \cdot P_{W\overline{S_{i,j}}}\big) \leq \nu$$

for every NDLF β, where $\nu = \varepsilon/(2^{2\ell}n(n-1))$.

Proof: We first consider and prove the perfect case.

THE PERFECT CASE: Like in the proof of Theorem 3.6, we fix an output w of the receiver and consider the non-normalized probability distribution $P_{S_0 \dots S_{n-1}W}(\cdot, \dots, \cdot, w)$. We use the variable $p_{s_0,\dots,s_{n-1}}$ to refer to the value $P_{S_0 \dots S_{n-1}W}(s_0, \dots, s_{n-1}, w)$ and $\mathbf{o}$ for the all-zero string $(0, \dots, 0) \in \{0,1\}^\ell$. We use bold font to denote a collection of strings $\mathbf{s} := (s_0, s_1, \dots, s_{n-1}) \in \{0,1\}^{\ell n}$, and we write $\overline{\mathbf{s}_i}$ for $(s_0, \dots, s_{i-1}, s_{i+1}, \dots, s_{n-1})$, the collection $\mathbf{s}$ without s_i. Finally, for a collection $\mathbf{t} = (t_0, \dots, t_{k-1}) \in \{0,1\}^{\ell k}$ of arbitrary size k, we define sets of indices with one (respectively two) non-zero substrings:

$$\begin{aligned}
\mathcal{S}_1(\mathbf{t}) &:= \{(\mathbf{o}, \dots, \mathbf{o}, t_i, \mathbf{o}, \dots, \mathbf{o}) : i \in \{0, \dots, k-1\}\} \\
\mathcal{S}_2(\mathbf{t}) &:= \{(\mathbf{o}, \dots, \mathbf{o}, t_i, \mathbf{o}, \dots, \mathbf{o}, t_j, \mathbf{o}, \dots, \mathbf{o}) : i < j \in \{0, \dots, k-1\}\}
\end{aligned}$$

where the t_i (and t_j) are at ith (and jth) position. As in the proof of Theorem 3.6, we assume for the clarity of exposition that for all $i \in \{0, \dots, n-1\}$ and $s_i \in \{0,1\}^\ell$, it holds that $p_{\mathbf{o},\dots,\mathbf{o}} \leq p_{\mathbf{o},\dots,\mathbf{o},s_i,\mathbf{o},\dots,\mathbf{o}}$ (where s_i is at position i). For symmetry reasons, the general case can be handled along the same lines.

We extend the distribution $P_{S_0 \dots S_{n-1}W}(\cdot, \dots, \cdot, w)$ similarly to (3.1): for every $\mathbf{s} \in \{0,1\}^{\ell n}$, we set

$$\begin{aligned}
P_{S_0 \dots S_{n-1}DW}(s_0, \dots, s_{n-1}, 0, w) &:= p_{s_0,\mathbf{o},\dots,\mathbf{o}}, \\
P_{S_0 \dots S_{n-1}DW}(s_0, \dots, s_{n-1}, 1, w) &:= p_{\mathbf{o},s_1,\mathbf{o},\dots,\mathbf{o}} - p_{\mathbf{o},\dots,\mathbf{o}}, \\
&\vdots \\
P_{S_0 \dots S_{n-1}DW}(s_0, \dots, s_{n-1}, n-2, w) &:= p_{\mathbf{o},\dots,s_{n-2},\mathbf{o}} - p_{\mathbf{o},\dots,\mathbf{o}}, \\
P_{S_0 \dots S_{n-1}DW}(s_0, \dots, s_{n-1}, n-1, w) &:= p_{\mathbf{o},\dots,\mathbf{o},s_{n-1}} - p_{\mathbf{o},\dots,\mathbf{o}}.
\end{aligned}$$

In order to show that this is a valid extension, we have to show that for every $\mathbf{s} \in \{0,1\}^{\ell n}$

$$p_{\mathbf{s}} = \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - (n-1)p_{\mathbf{o},\dots,\mathbf{o}}. \tag{3.5}$$

If this holds, then the random variable D is well defined, and the $\overline{S_D}$ are uniformly distributed given D, S_D and W.

We now show that (3.5) follows from the assumed uniformity property that $P_{\beta(S_i,S_j)W|\overline{S_{i,j}}=\overline{\mathbf{s}_{i,j}}} = P_{\text{UNIF}} \cdot P_{W|\overline{S_{i,j}}=\overline{\mathbf{s}_{i,j}}}$ for every non-degenerate linear function β and any $i \neq j$. This is done by induction on n. The case $n = 2$ is covered by the proof of Theorem 3.6, and by induction assumption we may assume that it also holds for $n-1$. Let us fix some $\mathbf{s} \in \{0,1\}^{\ell n}$ and $i \in \{0,\dots,n-1\}$. It is easy to see that the assumed uniformity property on $S_0,\dots,S_{n-1},W$ implies the corresponding uniformity property on $\overline{S_i},W$ when conditioning on $S_i = s_i$, and therefore, by induction assumption and "multiplying out the conditioning",

$$p_{\mathbf{s}} = \sum_{\mathbf{t}} p_{\mathbf{t}} - (n-2) p_{\mathbf{o},\dots,\mathbf{o},s_i,\mathbf{o},\dots,\mathbf{o}} \,. \tag{3.6}$$

where the sum is over all $\mathbf{t} \in \{0,1\}^{\ell n}$ with $t_i = s_i$ and $\overline{\mathbf{t}_i} \in \mathcal{S}_1(\overline{\mathbf{s}_i})$. Summing all the equations over $i \in \{0,\dots,n-1\}$ yields

$$n \cdot p_{\mathbf{s}} = 2 \sum_{\mathbf{t} \in \mathcal{S}_2(\mathbf{s})} p_{\mathbf{t}} - (n-2) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} \,. \tag{3.7}$$

By a similar reasoning we can also derive from the case $n = 2$ that equations of type (3.2) hold conditioned on the event that all but two of the S_i's are zero. More formally, we have that for all $i < j \in \{0,\dots,n-1\}$,

$$p_{\mathbf{o},\dots,\mathbf{o},s_i,\mathbf{o},\dots,\mathbf{o},s_j,\mathbf{o},\dots,\mathbf{o}} = p_{\mathbf{o},\dots,\mathbf{o},s_i,\mathbf{o},\dots,\mathbf{o}} + p_{\mathbf{o},\dots,\mathbf{o},s_j,\mathbf{o},\dots,\mathbf{o}} - p_{\mathbf{o},\dots,\mathbf{o}}. \tag{3.8}$$

Summing these equations over all $i < j \in \{0,\dots,n-1\}$ yields

$$\sum_{\mathbf{t} \in \mathcal{S}_2(\mathbf{s})} p_{\mathbf{t}} = (n-1) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - \binom{n}{2} p_{\mathbf{o},\dots,\mathbf{o}} \tag{3.9}$$

We conclude by substituting (3.9) into (3.7) as follows

$$\begin{aligned} n \cdot p_{\mathbf{s}} &= 2 \sum_{\mathbf{t} \in \mathcal{S}_2(\mathbf{s})} p_{\mathbf{t}} - (n-2) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} \\ &= 2 \left((n-1) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - \binom{n}{2} p_{\mathbf{o},\dots,\mathbf{o}} \right) - (n-2) \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} \\ &= n \sum_{\mathbf{t} \in \mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - n(n-1) p_{\mathbf{o},\dots,\mathbf{o}}, \end{aligned}$$

which is equation (3.5) after dividing by n, and thus finishes the induction step and the claim for $\varepsilon = 0$.

THE GENERAL CASE: For the non-zero error case, we follow the above argument, but keep track of the error. For technical reasons, we assume that the S_i's are independent and uniformly distributed, and we assume that the assumed uniformity property with respect to NDLFs holds conditioned on $\overline{S_{i,j}} = \overline{\mathbf{s}_{ij}}$ for *any* $\overline{\mathbf{s}_{ij}}$, not just on average, i.e., $\delta\big(P_{\beta(S_i,S_j)W|\overline{S_{i,j}}=\overline{\mathbf{s}_{ij}}}, P_{\text{UNIF}} \cdot P_{W|\overline{S_{i,j}}=\overline{\mathbf{s}_{ij}}}\big) \leq \nu$

for any $\overline{\mathbf{s}_{ij}} \in \{0,1\}^{\ell(n-2)}$. We show at the end of the proof how to argue in general. Write

$$\delta_{\mathbf{s}} = \Big| \sum_{\mathbf{t}\in\mathcal{S}_1(\mathbf{s})} p_{\mathbf{t}} - (n-1)p_{\mathbf{o},\ldots,\mathbf{o}} - p_{\mathbf{s}}\Big|$$

such that (3.5) holds up to the error $\delta_{\mathbf{s}}$. Note that $\delta_{\mathbf{s}}$ depends on w; we also write $\delta_{\mathbf{s}}(w)$ to make this dependency explicit. We will argue, following the induction proof, that

$$\sum_{w,\mathbf{s}} \delta_{\mathbf{s}}(w) \le n(n-1)\cdot 2^{2\ell}\cdot \nu = \varepsilon\,.$$

The proof can then be completed analogue to the proof of Theorem 3.6 by "correcting" the values for $P_{S_0\ldots S_{n-1}DW}$'s appropriately.

By the proof of Theorem 3.6, the claimed inequality holds in case $n = 2$. For the induction step, note that by induction assumption, (3.6) holds up to $\delta_{\overline{\mathbf{s}_i}}(w)P_{S_i}(s_i)$ where

$$\sum_{w,\overline{\mathbf{s}_i}} \delta_{\overline{\mathbf{s}_i}}(w) \le (n-1)(n-2)\cdot 2^{2\ell}\cdot\nu\,.$$

Furthermore, from the case $n = 2$ it follows that Equation (3.8) holds up to $\delta_{s_i,s_j}(w)P_{\overline{S_{ij}}}(\mathbf{o}\cdots\mathbf{o})$, where

$$\sum_{w,s_i,s_j} \delta_{s_i,s_j}(w) \le 2^{2\ell+1}\cdot\nu$$

and, by the additional assumption posed on the S_i's, $P_{\overline{S_{ij}}}(\mathbf{o}\cdots\mathbf{o}) = 2^{-(n-2)\ell}$. It follows that (3.5) holds up to

$$\delta_{\mathbf{s}} = \frac{1}{n}\Big(\sum_i \delta_{\overline{\mathbf{s}_i}}P_{S_i}(s_i) + 2\sum_{i<j}\delta_{s_i,s_j}P_{\overline{S_{ij}}}(\mathbf{o}\cdots\mathbf{o})\Big)$$

such that

$$\begin{aligned}\sum_{w,\mathbf{s}}\delta_{\mathbf{s}}(w) &= \frac{1}{n}\Big(\sum_i\sum_{w,\overline{\mathbf{s}_i}}\delta_{\overline{\mathbf{s}_i}}(w)\sum_{s_i}P_{S_i}(s_i) + 2\sum_{i<j}\sum_{\overline{\mathbf{s}_{ij}}}\sum_{w,s_i,s_j}\delta_{s_i,s_j}(w)P_{\overline{S_{ij}}}(\mathbf{o}\cdots\mathbf{o})\Big)\\ &\le (n-1)(n-2)\cdot 2^{2\ell}\cdot\nu + (n-1)\cdot 2^{(n-2)\ell}\cdot 2^{2\ell+1}\cdot 2^{-(n-2)\ell}\cdot\nu\\ &= \big((n-1)(n-2)\cdot 2^{2\ell} + 2\cdot(n-1)\cdot 2^{2\ell}\big)\cdot\nu\\ &\le n(n-1)\cdot 2^{2\ell}\cdot\nu = \varepsilon\,.\end{aligned}$$

It remains to argue the case where the S_i's are not independent uniformly distributed and/or the assumed uniformity property holds only on average over the $\overline{\mathbf{s}_{ij}}$'s. We first argue that we may indeed assume without loss of generality that the S_i's are random: We consider $\tilde{S}_0,\ldots,\tilde{S}_{n-1},\tilde{W}$ defined as $\tilde{S}_i = S_i \oplus R_i$ and $\tilde{W} = [W, R_0,\ldots,R_{n-1}]$ for independent and uniformly distributed R_i's in $\{0,1\}^{\ell}$. It is easy to see that the assumed uniformity condition with respect to NDLFs on $S_0,\ldots,S_{n-1},W$ implies the corresponding uniformity condition on

$\tilde{S}_0, \ldots, \tilde{S}_{n-1}, \tilde{W}$ with the same "error" ν, and it is obvious that the $\tilde{S}_i$'s are independent and uniformly distributed. Furthermore, it is easy to see that ε-sender-security for $\tilde{S}_0, \ldots, \tilde{S}_{n-1}, \tilde{W}$ implies ε-sender-security for $S_0, \ldots, S_{n-1}, W$ with the same ε. Thus it suffices to prove the claim for the case of random S_i's.

Finally, in order to reason that we may assume that the uniformity property holds conditioned on every $\overline{\mathbf{s}_{ij}}$, where we now may already assume that the S_i's are random due to the above observation, we again consider $\tilde{S}_0, \ldots, \tilde{S}_{n-1}, \tilde{W}$ defined as above. It is not hard to verify that due to this randomization and since the S_i's are random, the average near-uniformity of $\beta(S_i, S_j)$ translates to a "worst-case" near-uniformity of $\beta(\tilde{S}_i, \tilde{S}_j)$ with the same ν. □

3.6 *1-2 OT* in a Quantum Setting

As briefly mentioned in the introductory Section 3.1, the results of this chapter were originally motivated by the idea of using them to prove sender-security in the bounded-quantum-storage model of the *1-2 OT*-protocol presented later in Chapter 6. For this protocol, we can use a quantum uncertainty relation to show a lower bound on the min-entropy of the n-bit string X transmitted by the sender using a quantum encoding.

If we had a quantum version of Theorem 3.6 at hand, we could use privacy amplification against quantum adversaries (Theorem 2.25) to prove sender-security against quantum-memory-bounded receivers. Unfortunately, the example below shows that such a quantum version of Theorem 3.6 cannot exist.

In the case of a dishonest quantum receiver $\tilde{\mathsf{R}}$, the final state of a quantum protocol for *Rand 1-2 OT* is given by the ccq-state $\rho_{S_0 S_1 \tilde{\mathsf{R}}}$. The condition for ε-sender-security given in Definition 6.1 requires the existence of a random variable $D \in \{0,1\}$ such that

$$\delta\big(\rho_{S_{1-D} S_D D \tilde{\mathsf{R}}}, \mathbb{1} \otimes \rho_{S_D D \tilde{\mathsf{R}}}\big) \leq \varepsilon\,.$$

This coincides with the classical Definition 3.1, except that the dishonest receiver's output is a quantum state, and closeness is measured in terms of the trace-norm distance.

A quantum analogue of Theorem 3.6 would state that this condition is fulfilled if for every NDLF β,

$$\delta\big(\rho_{\beta(S_0,S_1)\tilde{\mathsf{R}}}, \mathbb{1} \otimes \rho_{\tilde{\mathsf{R}}}\big) \leq \varepsilon'$$

where ε' is comparable to the classical parameter $\varepsilon/2^{2\ell+1}$.

Consider now the following example for *1-2 OT* of bits B_0, B_1. We define the ccq-state $\rho_{B_0 B_1 \tilde{\mathsf{R}}}$ as follows: Let

$$\begin{aligned}\rho_{B_0 B_1 \tilde{\mathsf{R}}} := \frac{1}{4}\big(&|00\rangle\langle 00| \otimes |0\rangle\langle 0| \;+\; |11\rangle\langle 11| \otimes |1\rangle\langle 1| \\ &+ |01\rangle\langle 01| \otimes |+\rangle\langle +| \;+\; |10\rangle\langle 10| \otimes |-\rangle\langle -|\big),\end{aligned}$$

where $|+\rangle\langle +|$ and $|-\rangle\langle -|$ are the projectors onto the states $|+\rangle := |0\rangle_\times = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle := |1\rangle_\times = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

For this state, it is clear that the XOR $B_0 \oplus B_1$ is perfectly hidden from the dishonest receiver holding $\rho_{\tilde{\mathsf{R}}}$, i.e.

$$\delta\big(\rho_{(B_0 \oplus B_1)\tilde{\mathsf{R}}}, \mathbb{1} \otimes \rho_{\tilde{\mathsf{R}}}\big) = 0 \,.$$

On the other hand, $\tilde{\mathsf{R}}$ can determine the bit of his choice by measuring in the Breitbart basis $\{\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle, \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle\}$ if he is interested in the first bit, or by measuring in the Breitbart basis rotated by 45 degrees if he wants to obtain the second bit. It is easy to see that such a measurement succeeds in yielding the correct bit with probability $\cos(\pi/8)^2 \approx 0.85$. This precludes the existence of a pointer variable $D \in \{0, 1\}$ such that perfect sender-security in the sense of Definition 6.1 holds.

It is unclear how that difficulty can be overcome, but it is clear from the simple example above, that a statement like in Theorem 3.6 with comparable parameters cannot hold. Therefore, the alternative approach via the entropy-splitting Lemma 2.15 (outlined at the end of Section 3.4.2) will be taken in Chapter 6 to show sender-security.

Chapter 4

Quantum Uncertainty Relations

Quantum uncertainty relations are the fundamental tool for the security analysis of protocols in the bonded-quantum-storage model presented later in this thesis. We start off with some preliminary tools in Section 4.1 and proceed to the history of uncertainty relations in Section 4.2. Then, we derive new high-order entropic uncertainty relations for two (Section 4.3) and more (Section 4.4) mutually unbiased bases. In the last Section 4.5, we investigate the situation where for each qubit, a basis is picked independently at random from a set of bases.

The results in this chapter are based on joint work with Damgård, Fehr, Salvail and Renner which appeared in [DFSS08, DFR+07].

4.1 Preliminaries

4.1.1 Operators and Norms

For a linear operator A on the complex Hilbert space $\mathcal{H}$, we define the *operator norm*

$$\|A\| := \sup_{\langle x|x\rangle=1} \|Ax\|$$

for the Euclidian norm $\|x\| := \sqrt{\langle x|x\rangle}$ of the vector $|x\rangle \in \mathcal{H}$. When A is Hermitian, i.e. the complex conjugate transpose H^* and H coincide, we have

$$\|A\| = \lambda_{\max}(A) := \max\{|\lambda_j| : \lambda_j \text{ an eigenvalue of } A\}.$$

From an equivalent definition of the norm $\|A\| = \sup_{\langle y|y\rangle=\langle x|x\rangle=1} |\langle y|A|x\rangle|$, it is easy to see that $\|A^*\| = \|A\|$. For two Hermitian matrices A and B, we have that $\|AB\| = \|(AB)^*\| = \|B^*A^*\| = \|BA\|$. The operator norm is *unitarily invariant*, i.e. for all unitary U, V, $\|A\| = \|UAV\|$ holds. It is easy to show that

$$\left\| \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right\| = \max\{\|A\|, \|B\|\}.$$

Lemma 4.1 *Let X, Y be any two $n \times n$ matrices such that the products XY and YX are Hermitian. Then, we have*

$$\|XY\| = \|YX\|$$

Proof: For any two $n \times n$ matrices X and Y, XY and YX have the same eigenvalues, see e.g. [Bha97, Exercise I.3.7]. Therefore, $\|XY\| = \lambda_{\max}(XY) = \lambda_{\max}(YX) = \|YX\|$. □

A linear operator P such that $P^2 = P$ and $P^* = P$ is called an *orthogonal projector.*

Proposition 4.2 *Let A and B be two orthogonal projectors. Then it holds that $\|A + B\| \leq 1 + \|AB\|$.*

Proof: We adapt a technique by Kittaneh [Kit97] to our case. Define two 2×2-block matrices X and Y as follows

$$X := \begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad Y := \begin{pmatrix} A & 0 \\ B & 0 \end{pmatrix}.$$

Using $A^2 = A$ and $B^2 = B$, we compute

$$XY := \begin{pmatrix} A+B & 0 \\ 0 & 0 \end{pmatrix} \text{ and } YX := \begin{pmatrix} A & AB \\ BA & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} + \begin{pmatrix} 0 & AB \\ BA & 0 \end{pmatrix}.$$

As A and B are Hermitian, so are $A + B$, AB, BA, XY and YX as well. We use Lemma 4.1 and the triangle inequality to obtain

$$\left\| \begin{pmatrix} A+B & 0 \\ 0 & 0 \end{pmatrix} \right\| = \left\| \begin{pmatrix} A & AB \\ BA & B \end{pmatrix} \right\| \leq \left\| \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right\| + \left\| \begin{pmatrix} 0 & AB \\ BA & 0 \end{pmatrix} \right\|.$$

Using the unitary invariance of the operator norm to permute the columns in the rightmost matrix and the facts that $\|A\| = \|B\| = 1$ as well as $\|AB\| = \|BA\|$, we conclude that

$$\|A + B\| \leq 1 + \|AB\|.$$

□

A nice feature of this block-matrix technique is that it generalizes easily to more projectors.

Proposition 4.3 *For orthogonal projectors $A_0, A_1, A_2, \ldots, A_M$, it holds that*

$$\left\| \sum_{i=0}^{M} A_i \right\| \leq 1 + M \cdot \max_{0 \leq i < j \leq M} \|A_i A_j\|. \tag{4.1}$$

Proof: Defining

$$X := \begin{pmatrix} A_0 & A_1 & \cdots & A_M \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad Y := \begin{pmatrix} A_0 & 0 & \cdots & 0 \\ A_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ A_M & 0 & \cdots & 0 \end{pmatrix}$$

yields

$$XY = \begin{pmatrix} A_0 + A_1 + \ldots + A_M & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and}$$

$$YX = \begin{pmatrix} A_0 & A_0A_1 & \cdots & A_0A_M \\ A_1A_0 & A_1 & \cdots & A_1A_M \\ \vdots & \vdots & \ddots & \vdots \\ A_MA_0 & A_MA_1 & \cdots & A_M \end{pmatrix}$$

The matrix YX can be additively decomposed into $M + 1$ matrices according to the following pattern

$$YX = \begin{pmatrix} * & & & & \\ & * & & & \\ & & \ddots & & \\ & & & * & \\ & & & & * \end{pmatrix} + \begin{pmatrix} 0 & * & & & \\ & 0 & & & \\ & & \ddots & \ddots & \\ & & & 0 & * \\ * & & & & 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 & & & & * \\ * & 0 & & & \\ & \ddots & \ddots & & \\ & & & 0 & \\ & & & * & 0 \end{pmatrix}$$

where the asterisk stand for entries of YX and for $i = 0, \ldots, M$ the ith asterisk-pattern after the diagonal pattern is obtained by i cyclic shifts of the columns of the diagonal pattern. Entries without asterisk are zero.

As in the proof of Proposition 4.2, XY and YX are Hermitian and we use Lemma 4.1, the triangle inequality, the unitary invariance of the operator norm and the facts that for all $i \neq j : \|A_i\| = 1$, $\|A_iA_j\| = \|A_jA_i\|$ to obtain the desired statement (4.1). □

4.1.2 Azuma's Inequality

As we will exclusively use the concentration result at the end of this section, we only give an informal definition of martingales. We refer to [AS00] or [MP95] for a more detailed treatment.

Definition 4.4 *A sequence of real random variables $X_0, X_1, \ldots$ is a martingale sequence, if for all $i = 1, 2, \ldots$, it holds $\mathbb{E}[X_i | X_0, \ldots, X_{i-1}] = X_{i-1}$.*

Theorem 4.5 (Azuma's inequality [Azu67]) *Let $X_0, X_1, \ldots$ be a martingale sequence such that for each k, $|X_k - X_{k-1}| \leq c_k$, where c_k may depend on k. Then, for all $t \geq 0$ and any $\tau > 0$,*

$$\Pr[X_t - X_0 \geq \tau] \leq \exp\left(-\frac{\tau^2}{2\sum_{k=1}^t c_k^2}\right) .$$

The theorem is often stated as two-sided bound with absolute values:

$$\Pr\left[|X_t - X_0| \geq \tau\right] \leq 2\exp\left(-\frac{\tau^2}{2\sum_{k=1}^t c_k^2}\right) ,$$

but the one-sided version fits our purposes better.

Definition 4.6 *A sequence of real-valued random variables* $R_1, \ldots, R_n$ *is called a* martingale difference sequence *if for every* i *and every* $r_1, \ldots, r_{i-1} \in \mathbb{R}$*:* $\mathbb{E}[R_i | R_1 = r_1, \ldots, R_{i-1} = r_{i-1}] = 0$.

Note that for an arbitrary sequence of real random variables $S_0, S_1, \ldots \in \mathbb{R}$, defining $R_n := \sum_{i=1}^n S_i - \mathbb{E}[S_i | S^{i-1}]$ (with $R_0 := 0$) yields a martingale difference sequence $R_0, R_1, \ldots$.

The following lemma follows directly from Azuma's Theorem 4.5.

Corollary 4.7 *Let* $R_1, \ldots, R_n$ *be a martingale difference sequence such that* $|R_i| \leq c$ *for every* $1 \leq i \leq n$*. Then, for any* $\lambda > 0$,

$$\Pr\left[\sum_i R_i \geq \lambda n\right] \leq \exp\big(-\frac{\lambda^2 n}{2c^2}\big).$$

Proof: Set $\tau := \lambda n$, $X_0 := 0$, and for $n \geq 1$, $X_n := \sum_{i=1}^n R_i$ in Theorem 4.5. □

4.1.3 Mathematical Tools

The following two purely analytical lemmas will be used to bound some error terms.

Lemma 4.8 *For any* $0 < x < 1/e$ *such that* $y := x \log(1/x) < 1/4$*, it holds that* $x > \frac{y}{4 \log(1/y)}$.

Proof: Define the function $x \mapsto f(x) = x \log(1/x)$. It holds that $f'(x) = \frac{d}{dx} f(x) = \log(1/x) - \log e$, which shows that f is bijective in the interval $(0, 1/e)$, and thus the inverse function $f^{-1}(y)$ is well defined for $y \in (0, \log(e)/e)$, which contains the interval $(0, 1/4)$. We are going to show that $f^{-1}(y) > g(y)$ for all $y \in (0, 1/4)$, where $g(y) = \frac{y}{4 \log(1/y)}$. Since both $f^{-1}(y)$ and $g(y)$ converge to 0 for $y \to 0$, it suffices to show that $\frac{d}{dy} f^{-1}(y) > \frac{d}{dy} g(y)$; respectively, we will compare their reciprocals. For any $x \in (0, 1/e)$ such that $y = f(x) = x \log(1/x) < 1/4$

$$\frac{1}{\frac{d}{dy} f^{-1}(y)} = f'(f^{-1}(y)) = \log(1/x) - \log(e)$$

and

$$\frac{d}{dy} g(y) = \frac{1}{4}\left(\frac{1}{\log(1/y)} + \frac{1}{\ln(2) \log(1/y)^2}\right)$$

such that

$$\begin{aligned}
\frac{1}{\frac{d}{dy} g(y)} &= 4\,\frac{\ln(2)\log(1/y)^2}{\ln(2)\log(1/y) + 1} = 4\,\frac{\log(1/y)}{1 + \frac{1}{\ln(2)\log(1/y)}} \\
&> 2 \log\Big(\frac{1}{y}\Big) = 2 \log\Big(\frac{1}{x \log(1/x)}\Big) \\
&= 2\big(\log(1/x) - \log\log(1/x)\big)
\end{aligned}$$

where for the inequality we are using that $y < 1/4$ so that $\ln(2)\log(1/y) > 2\ln(2) = \ln(4) > 1$. Defining the function

$$h(z) := z - 2\log(z) + \log(e)$$

and showing that $h(z) > 0$ for all $z > 0$ finishes the proof, as then

$$0 < h\big(\log(1/x)\big) \leq \frac{1}{\frac{d}{dy}g(y)} - \frac{1}{\frac{d}{dy}f^{-1}(y)}$$

which was to be shown. For this last claim, note that $h(z) \to \infty$ for $z \to 0$ and for $z \to \infty$, and thus the global minimum is at z_0 with $h'(z_0) = 0$. $h'(z) = 1 - 2/(\ln(2)z)$ and thus $z_0 = 2/\ln(2) = 2\log(e)$, and hence the minimum of $h(z)$ equals $h(z_0) = 3\log(e) - 2\log\big(2\log(e)\big)$, which turns out to be positive. □

Lemma 4.9 *For any* $0 < x < 1/4$*, it holds that* $\exp(-\frac{x^2}{32(2-\log(x))^2}) < 2^{-x^4/32}$.

Proof: Note that $\exp(-\frac{x^2}{32(2-\log(x))^2}) = 2^{-\frac{\log(e)}{32}\frac{x^2}{(2-\log(x))^2}}$. Therefore, it suffices to show that $x^4 \leq \frac{x^2}{(2-\log(x))^2}$ or equivalently that the function $x \mapsto f(x) := x^2(2-\log(x))^2$ is smaller than 1 for $0 < x < 1/4$. It holds that $f(0) = 0$ and $f(1/4) = 1$ and it is easy to see that f is a continuous increasing function, e.g. by verifying that for the first derivative

$$\frac{d}{dx}f(x) = 2x\,(2-\log(x))\left(2 - \log(x) - \frac{1}{\ln(2)}\right) > 0$$

holds for $0 < x < 1/4$. □

4.2 History and Previous Work

4.2.1 Mutually Unbiased Bases

Definition 4.10 (Mutually Unbiased Bases (MUBs)) *Two orthonormal 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* $\mathcal{H}_N$ *of dimension* $N := 2^n$ *are called* mutually unbiased *if*

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

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

Wiesner showed in 1970 in one of the first articles about quantum cryptography [Wie83] 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 Wootters and Fields for N a prime power [WF89] (in particular, for $N = 2^n$ in the case of n qubits). A nice construction based on the stabilizer formalism can be found in the article by Lawrence, Brukner, and Zeilinger [LBZ02]. It turned out to be an intriguing question to determine the maximal number of mutually unbiased bases in other dimensions, already the case $N = 6$ is still open [Eng03].

For a density matrix ρ describing the state of n qubits, let $Q^0_\rho(\cdot), Q^1_\rho(\cdot), \dots, Q^M_\rho(\cdot)$ be the probability distributions over n-bit strings when measuring ρ in bases $\mathcal{B}^0, \mathcal{B}^1, \dots, \mathcal{B}^M$, respectively. For instance, for basis $\mathcal{B}^0 = \{|a_i\rangle\}_{i=1}^N$ and basis $\mathcal{B}^1\{|b_j\rangle\}_{j=1}^N$, we have $Q^0_\rho(i) = \langle a_i|\rho|a_i\rangle$ and $Q^1_\rho(j) = \langle b_j|\rho|b_j\rangle$. We leave out the state ρ in the subscript when it is clear from the context.

4.2.2 Uncertainty Relations Using Shannon Entropy

The history of uncertainty relations starts with Heisenberg who showed that the outcomes of two non-commuting observables applied to a quantum state are not easy to predict simultaneously [Hei27]. However, Heisenberg only speaks about the variance of the measurement results, and his result was shown to have several shortcomings by Deutsch [Deu83] and Hilgevood and Uffink [HU88]. More general forms of uncertainty relations were proposed by Bialynicki-Birula and Mycielski in [BBM75] and by Deutsch [Deu83] to resolve these problems. The new relations were called *entropic uncertainty relations*, because they are expressed using Shannon entropy instead of the statistical variance.

For mutually unbiased bases, Deutsch's relation reads

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

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

$$\mathrm{H}(Q^0) + \mathrm{H}(Q^1) \geq \log N = n. \tag{4.2}$$

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

Note that for entropic bounds using *Shannon entropy*, it is sufficient to state them for pure states. They then automatically hold for mixed state by concavity.

Lemma 4.11 *If* $\mathrm{H}(Q^0_{|\varphi\rangle}) + \mathrm{H}(Q^1_{|\varphi\rangle}) \geq k$ *holds for all pure states* $|\varphi\rangle \in \mathcal{H}$*, then* $\mathrm{H}(Q^0_\rho) + \mathrm{H}(Q^1_\rho) \geq k$ *holds for all (possibly mixed) states* $\rho \in \mathcal{P}(\mathcal{H})$*.*

Proof: Let $\rho = \sum_x \lambda_x |\varphi_x\rangle\langle\varphi_x|$ the spectral composition of a mixed state. We then have for $i = 0, 1$ that $Q^i_\rho = \sum_x \lambda_x Q^i_{|\varphi_x\rangle}$ and therefore by concavity of the Shannon entropy (Lemma 2.10)

$$\mathrm{H}(Q^0_\rho) + \mathrm{H}(Q^1_\rho) \geq \sum_x \lambda_x \left(\mathrm{H}(Q^0_{|\varphi_x\rangle}) + \mathrm{H}(Q^1_{|\varphi_x\rangle}) \right) \geq k.$$

□

Although a bound on Shannon entropy can be helpful in some cases, it is usually not good enough in cryptographic applications. The main tool to reduce the adversary's information—privacy amplification by two-universal hashing—requires a bound on the adversary's min-entropy (in fact collision entropy), see Section 2.5. As $H(Q) \geq H_\alpha(Q)$ for $\alpha > 1$, higher-order entropic bounds are generally weaker, but imply bounds for Shannon entropy as well.

4.2.3 Higher-Order Entropic Uncertainty Relations

Different results are known for *complete sets* of $N+1$ mutually unbiased bases of $\mathcal{H}_N$. All of them are based on the following surprising geometrical result by Larsen.

Theorem 4.12 ([Lar90]) *Let $Q_\rho^0, \ldots, Q_\rho^N$ be the $N+1$ distributions obtained by measuring state ρ in mutually unbiased bases $\mathcal{B}^0, \ldots, \mathcal{B}^N$ of the Hilbert space $\mathcal{H}_N$. Then,*

$$\sum_{i=0}^{N} \pi_2(Q_\rho^i) = 1 + \operatorname{tr}(\rho^2), \tag{4.3}$$

where $\pi_2(Q) = \sum_x Q(x)^2$ denotes the collision probability of a distribution Q (cf. Definition 2.6).

For a pure state $\rho = |\psi\rangle\langle\psi|$, $\operatorname{tr}(\rho^2) = 1$ holds and the right hand side of (4.3) equals 2. In this case, using that $x \mapsto -\log(x)$ is a convex function, Sánchez-Ruiz [Sán95] applies Jensen's inequality (Lemma 2.2) to derive the following lower-bound on the sum of the collision entropies

$$\begin{aligned}\sum_{i=0}^{N} \mathrm{H}_2(Q^i) &= \sum_{i=0}^{N} -\log(\pi_2(Q^i)) \\ &\geq -(N+1)\log\left(\frac{\sum_{i=0}^{N}\pi_2(Q^i)}{N+1}\right) = (N+1)\log\left(\frac{N+1}{2}\right).\end{aligned}$$

Because of the lack of convexity of higher-order Rényi entropy, we cannot immediately extend an uncertainty relation for pure states to mixed states. On the other hand, the following lemma shows that uncertainty relations based on upper bounds of high-order *probability sums* for pure states also hold for mixed states and therefore translate to entropy lower bounds for mixed states.

Lemma 4.13 *Let $\alpha \in (1, \infty]$. If $\sum_{i=0}^{M} \pi_\alpha(Q_{|\varphi\rangle}^i) \leq c$ for all pure states $|\varphi\rangle$, then for all mixed states ρ,*

$$\sum_{i=0}^{M} \mathrm{H}_\alpha(Q_\rho^i) \geq (M+1)\log\left(\frac{M+1}{c}\right).$$

Equality holds for a state ρ for which $\pi_\alpha(Q_\rho^i) = \frac{c}{M+1}$ for all i.

Proof: As $x \mapsto x^\alpha$ is convex for $\alpha > 1$, $\pi_\alpha(\cdot)$ is a convex functional. Therefore, for a mixed state $\rho = \sum_x \lambda_x |\varphi_x\rangle\langle\varphi_x|$, we have $Q^i_\rho = \sum_x \lambda_x Q^i_{|\varphi_x\rangle}$ and

$$\sum_{i=0}^{M} \pi_\alpha(Q^i_\rho) \leq \sum_{i=0}^{M} \sum_x \lambda_x \pi_\alpha(Q^i_{|\varphi_x\rangle}) \leq \sum_x \lambda_x \sum_{i=0}^{M} \pi_\alpha(Q^i_{|\varphi_x\rangle}) \leq c.$$

Just as above follows by Jensen's inequality (Lemma 2.2) that

$$\begin{aligned}\sum_{i=0}^{M} \mathrm{H}_\alpha(Q^i_\rho) &= \sum_{i=0}^{M} -\log(\pi_\alpha(Q^i_\rho)) \\ &\geq -(M+1)\log\left(\frac{\sum_{i=0}^{M} \pi_\alpha(Q^i_\rho)}{M+1}\right) \geq (M+1)\log\left(\frac{M+1}{c}\right).\end{aligned}$$

Jensen's inequality is tight if the values $\pi_\alpha(Q^i_\rho)$ are all equal. □

For 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 by Damgård, Salvail and Pedersen [DPS04] and Azarchs [Aza04] by subtracting the minimal amount of collision probability ($1/N$) in the bases not included in the sum:

$$\sum_{i=0}^{M} \pi_2(Q^i_{|\varphi\rangle}) \leq 2 - \frac{(N+1-(M+1))}{N} = \frac{N+M}{N}. \tag{4.4}$$

By Lemma 4.13, this yields

$$\sum_{i=0}^{M} \mathrm{H}_2(Q^i_\rho) \geq (M+1)\log\left(\frac{N(M+1)}{N+M}\right). \tag{4.5}$$

As mentioned above, all lower bounds on the collision entropy from this section imply bounds on the Shannon entropy because $H(Q) \geq H_2(Q)$, but do not tell us anything about the min-entropy $H_\infty(Q)$. In the rest of this chapter, we derive entropic uncertainty relations involving *min-entropy.*

Uncertainty relations in terms of Rényi entropy have also been studied in a different context by Bialynicki-Birula [BB06].

4.3 Two Mutually Unbiased Bases

In this section, we consider the situation where a n-qubit state is measured in one out of two mutually unbiased bases of $\mathcal{H}_{2^n}$. Without loss of generality, we assume these two bases to be the n-fold tensor product of the computational basis $+^{\otimes n}$ and of the diagonal basis $\times^{\otimes n}$, in this section simply called +- and $\times$-basis.

We show that two distributions obtained by measuring in two mutually unbiased bases cannot *both* be "very far from uniform". One way to characterize non-uniformity of a distribution is to 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 simultaneously for *both* measurements.

Theorem 4.14 *Let ρ be an arbitrary state of n qubits, and let $Q^+(\cdot)$ and $Q^\times(\cdot)$ be the respective distributions of the outcome when ρ 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*

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

Proof: We define the two orthogonal projectors

$$A := \sum_{x \in L^+} |x\rangle\langle x| \quad \text{and} \quad B := \sum_{y \in L^\times} H^{\otimes n}|y\rangle\langle y|H^{\otimes n}.$$

Using the spectral decomposition of $\rho = \sum_w \lambda_w |\varphi_w\rangle\langle\varphi_w|$, we have

$$\begin{aligned} Q^+(L^+) + Q^\times(L^\times) &= \operatorname{tr}(A\rho) + \operatorname{tr}(B\rho) \\ &= \sum_w \lambda_w \left(\operatorname{tr}(A|\varphi_w\rangle\langle\varphi_w|) + \operatorname{tr}(B|\varphi_w\rangle\langle\varphi_w|)\right) \\ &= \sum_w \lambda_w \left(\langle\varphi_w|A|\varphi_w\rangle + \langle\varphi_w|B|\varphi_w\rangle\right) \\ &= \sum_w \lambda_w \langle\varphi_w|(A+B)|\varphi_w\rangle \\ &\leq \|A+B\| \leq 1 + \|AB\|, \end{aligned}$$

where the last line is Proposition 4.2. To conclude, we show that $\|AB\| \leq 2^{-n/2}\sqrt{|L^+||L^\times|}$. Note that an arbitrary state $|\psi\rangle = \sum_z \lambda_z H^{\otimes n}|z\rangle$ can be expressed with coordinates λ_z in the diagonal basis. Then, with the sums over x and y understood as over $x \in L^+$ and $y \in L^\times$, respectively,

$$\begin{aligned} \big\|AB|\psi\rangle\big\| &= \Big\|\sum_{x,y} |x\rangle\langle x|H^{\otimes n}|y\rangle\langle y|H^{\otimes n}|\psi\rangle\Big\| = 2^{-n/2}\Big\|\sum_{x,y} |x\rangle\,\langle y|H^{\otimes n}|\psi\rangle\Big\| \\ &= 2^{-n/2}\Big\|\sum_x |x\rangle\Big\| \cdot \Big|\sum_y \lambda_y\Big| \leq 2^{-n/2}\sqrt{|L^+|}\sum_y |\lambda_y| \leq 2^{-n/2}\sqrt{|L^+||L^\times|}, \end{aligned}$$

The second equality holds since $\langle x|H^{\otimes n}|y\rangle = 2^{-n/2}$ are mutually unbiased, the first inequality follows from Pythagoras and the triangle inequality, and the last inequality follows from Cauchy-Schwarz (Lemma 2.3). This implies $\|AB\| \leq 2^{-n/2}\sqrt{|L^+||L^\times|}$ and finishes the proof. □

This theorem yields a meaningful bound as long as $|L^+| \cdot |L^\times| < 2^n$, for instance if L^+ and $L^\times$ both contain less than $2^{n/2}$ elements. The relation is tight in the sense that for the Hadamard-invariant state

$$|\varphi\rangle = \left(|0\rangle^{\otimes n} + (H|0\rangle)^{\otimes n}\right)/\sqrt{2(1+2^{-n/2})}$$

and $L^+ = L^\times = \{0^n\}$, it is straightforward to verify that $Q^+(L^+) = Q^\times(L^\times) = (1+2^{-n/2})/2$ and therefore $Q^+(L^+) + Q^\times(L^\times) = 1 + 2^{-n/2}$. Another state that achieves equality (for n even) is $|\varphi\rangle = |0\rangle^{\otimes n/2} \otimes (H|0\rangle)^{\otimes n/2}$ with $L^+ = \{0^{n/2}x | x \in \{0,1\}^{n/2}\}$ and $L^\times = \{x0^{n/2} | x \in \{0,1\}^{n/2}\}$. We get that $Q^+(L^+) = Q^\times(L^\times) = 1$ and thus $Q^+(L^+) + Q^\times(L^\times) = 2 = 1 + 2^{-n/2}\sqrt{2^n}$.

If for $r \in \{+,\times\}$, L^r contains only the n-bit string with the maximal probability of Q^r, we obtain a known tight relation (see (9) in [MU88]).

Corollary 4.15 *Let q_∞^+ and $q_\infty^\times$ be the maximal probabilities of the distributions Q^+ and $Q^\times$ from above. It then holds that $q_\infty^+ + q_\infty^\times \leq 1 + c$ and therefore also $q_\infty^+ \cdot q_\infty^\times \leq \frac{1}{4}(1+c)^2$ where $c = 2^{-n/2}$.*

Equality is achieved for the same state $|\varphi\rangle = \left(|0\rangle^{\otimes n} + (H|0\rangle)^{\otimes n}\right)/\sqrt{2(1+2^{-n/2})}$ as above.

Using Lemma 4.13, the following corollary is obtained.

Corollary 4.16 *For all quantum states ρ of n qubits, it holds that*

$$\mathrm{H}_\infty(Q_\rho^+) + \mathrm{H}_\infty(Q_\rho^\times) \geq 2(1 - \log(1 + 2^{-n/2})).$$

There exists a quantum state achieving equality.

The following corollary plays the crucial role in the security proofs of protocols in the bounded-quantum-storage model presented in the following chapters of this thesis.

Corollary 4.17 *Let R be a random variable over $\{+, \times\}$, and let X be the outcome when ρ is measured in basis R, such that $P_{X|R}(x|r) = Q^r(x)$. Then, for any $\lambda < \frac{1}{2}$ there exists $\kappa > 0$ and an event $\mathcal{E}$ such that*

$$P[\mathcal{E}|R{=}+] + P[\mathcal{E}|R{=}\times] \geq 1 - 2^{-\kappa n}$$

and thus $P[\mathcal{E}] \geq \frac{1}{2} - 2^{-\kappa n}$ in case R is uniform, and such that

$$\mathrm{H}_\infty(X|R{=}r, \mathcal{E}) \geq \lambda n$$

for $r \in \{+, \times\}$ with $P_{R|\mathcal{E}}(r) > 0$.

Proof: Choose $\kappa > 0$ such that $\lambda + 2\kappa < \frac{1}{2}$, and define

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

to be the sets of strings with small probabilities and denote by $L^+ := \overline{S}^+$ and $L^\times := \overline{S}^\times$ their complements[1]. Note that for all $x \in L^+$, we have that $Q^+(x) > 2^{-(\lambda+\kappa)n}$ and therefore $|L^+| < 2^{(\lambda+\kappa)n}$. Analogously, we have $|L^\times| < 2^{(\lambda+\kappa)n}$. For ease of notation, we abbreviate the probabilities that strings with small probabilities occur with $q^+ := Q^+(S^+)$ and $q^\times := Q^\times(S^\times)$. It follows immediately from the choice of κ and Theorem 4.14 that

$$q^+ + q^\times \geq 1 - 2^{-n/2} \cdot 2^{(\lambda+\kappa)n} \geq 1 - 2^{-\kappa n}.$$

We define $\mathcal{E}$ to be the event $X \in S^R$. Then $P[\mathcal{E}|R{=}+] = P[X \in S^+|R{=}+] = q^+$ and similarly $P[\mathcal{E}|R = \times] = q^\times$, and thus the first claim follows immediately. Furthermore, if R is uniformly distributed, then

$$\begin{aligned} P[\mathcal{E}] &= P[\mathcal{E}|R{=}+]P_R(+) + P[\mathcal{E}|R{=}\times]P_R(\times) \\ &= \frac{1}{2}(q^+ + q^\times) \geq \frac{1}{2} - 2^{-\kappa n}/2 \geq \frac{1}{2} - 2^{-\kappa n}. \end{aligned}$$

[1]Here's the mnemonic: S for the strings with *S*mall probabilities, L for *L*arge.

Regarding the second claim, in case $R = +$, we have

$$\begin{aligned}\mathrm{H}_\infty(X|R{=}{+},\mathcal{E}) &= -\log\left(\max_{x\in S^+}\frac{Q^+(x)}{q^+}\right)\\ &\geq -\log\left(\frac{2^{-(\lambda+\kappa)n}}{q^+}\right) = \lambda n + \kappa n + \log(q^+).\end{aligned}$$

Thus, if $q^+ \geq 2^{-\kappa n}$ then indeed $\mathrm{H}_\infty(X|R{=}{+}, X \in S^+) \geq \lambda n$. The corresponding holds for the case $R = \times$.

Finally, if $q^+ < 2^{-\kappa n}$ (or similarly $q^\times < 2^{-\kappa n}$) then instead of the 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 $P[\mathcal{E}|R{=}{+}] = 0$ and $P[\mathcal{E}|R{=}\times] = q^\times \geq 1 - 2^{-\kappa n}$, as well as $\mathrm{H}_\infty(X|R{=}\times,\mathcal{E}) = \mathrm{H}_\infty(X|R{=}\times, X \in S^\times) \geq \lambda n + \kappa n + \log(q^\times) \geq \lambda n$ (for n large enough), both by the bound on $q^+ + q^\times$ and on q^+, whereas $P_{R|\mathcal{E}}(+) = 0$. □

4.4 More Mutually Unbiased Bases

In this section, we generalize the uncertainty relation derived in Section 4.3 to more than two mutually unbiased bases. Such uncertainty relations over more than two, but not all mutually unbiased bases in terms of min-entropy may be of independent interest, see the discussion at the end of Section 4.2.

Theorem 4.18 *Let the density matrix ρ describe the state of n qubits and let $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$ be mutually unbiased bases of $\mathcal{H}_{2^n}$. Let $Q^0(\cdot), Q^1(\cdot), \ldots, Q^M(\cdot)$ be the distributions of the outcome when ρ 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*

$$\sum_{i=0}^{M} Q^i(L^i) \leq\ 1 + M\cdot 2^{-n/2} \max_{0\leq i<j\leq M} \sqrt{|L^i||L^j|}.$$

Proof: Except of using Proposition 4.3 instead of Proposition 4.2, the proof is analogous to the one of Theorem 4.14. □

As in Corollary 4.16, we derive an uncertainty relation about the sum of the min-entropies of up to $2^{n/2}$ distributions.

Corollary 4.19 *For an $\varepsilon > 0$, let $0 < M < 2^{\frac{n}{2}-\varepsilon n}$. For $i = 0,\ldots,M$, let $\mathrm{H}_\infty(Q^i)$ be the min-entropies of the distributions Q^i from the theorem above. Then,*

$$\sum_{i=0}^{M} \mathrm{H}_\infty(Q^i) \geq (M+1)\big(\log(M+1) - \mathit{negl}(n)\big).$$

Proof: For $i = 0,\ldots,M$, we denote by q^i_∞ the maximal probability of Q^i and let L^i be the set containing only the n-bit string x with this maximal probability q_∞^i. Theorem 4.18 together with the assumption about M assures $\sum_{i=0}^{M} q_\infty^i \leq 1 + negl(n)$. By Lemma 4.13 follows

$$\sum_{i=0}^{M} \mathrm{H}_\infty(Q^i) \geq (M+1)\big(\log(M+1) - negl(n)\big).$$

□

4.5 Independent Bases for Each Subsystem

So far, we have focused on the case of an n-qubit state $\rho \in \mathcal{P}(\mathcal{H}_{2^n})$ measured in two or more mutually unbiased bases of $\mathcal{H}_{2^n}$. In this section, we investigate the case when each of the n qubits is measured in an individual basis, picked independently and uniformly from $\{+, \times\}$, i.e. ρ is measured in basis $\Theta \in_R \{+, \times\}^n$.

More generally, our result holds for a state $\rho \in \mathcal{H}_d^{\otimes n}$ of n quantum systems—each d-dimensional—which are measured in an individual basis, picked independently and uniformly from a set $\mathcal{B}$ of basis of $\mathcal{H}_d$, see Theorem 4.22.

4.5.1 A Classical Tool

We start our derivation with a classical information-theoretic tool which itself might be of independent interest.

Theorem 4.20 *Let $Z_1, \ldots, Z_n$ be n random variables (not necessarily independent) over alphabet $\mathcal{Z}$. If there exists a real number $h > 0$ such that for all $1 \leq i \leq n$ and $z_1, \ldots, z_{i-1} \in \mathcal{Z}$:*

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

then for any $0 < \lambda < \frac{1}{2}$

$$\mathrm{H}_\infty^\varepsilon(Z_1, \ldots, Z_n) \geq (h - 2\lambda)n,$$

where $\varepsilon = \exp\big(-\frac{\lambda^2 n}{32 \log(|\mathcal{Z}|/\lambda)^2}\big)$.

If the Z_i's are independent and have Shannon entropy at least h, it is known (see Lemma 2.13) that the smooth min-entropy of $Z_1, \ldots, Z_n$ is at least nh for large enough n. Informally, Theorem 4.20 guarantees that when the independence-condition is relaxed to a lower bound on the Shannon entropy of Z_i *given any previous history*, then we still have (almost) nh bits of min-entropy except with negligible probability ε.

The proof idea is to use Azuma's inequality in the form of Corollary 4.7 for cleverly chosen R_i's. The main trick is that for a random variable Z over $\mathcal{Z}$, we can define another random variable $S := \log P_Z(Z)$ over $\mathbb{R}$ with expected value $\mathbb{E}[S] = \sum_{z \in \mathcal{Z}} P_Z(z) \cdot \log P_Z(z) = \mathrm{H}(Z)$ equal to the Shannon entropy of Z, which allows us to make the connection with the assumption about the Shannon entropy.

Proof: Recall that the superscript means $Z^i := (Z_1, \ldots, Z_i)$ for any $i \in \{1, \ldots, n\}$, and similarly for other sequences. We want to show that

$$\Pr\left[P_{Z^n}(Z^n) \geq 2^{-(h-2\lambda)n}\right] \leq \varepsilon$$

for ε as claimed in Theorem 4.20. This means that $P_{Z^n}(z^n)$ is smaller than $2^{-(h-2\lambda)n}$ except with probability at most ε (over the choice of z^n), and therefore implies the claim $H_\infty^\varepsilon(Z^n) \geq (h-2\lambda)n$ by the definition of smooth min-entropy from Section 2.4.2. Note that $P_{Z^n}(Z^n) \geq 2^{-(h-2\lambda)n}$ is equivalent to

$$\sum_{i=1}^{n} \Big(\log\big(P_{Z_i|Z^{i-1}}(Z_i|Z^{i-1})\big) + h \Big) \geq 2\lambda n \tag{4.6}$$

which is of suitable form to apply Azuma's inequality (Corollary 4.7).

Consider first an arbitrary sequence $S_1, \ldots, S_n$ of real-valued random variables. We assume the S_i's to be either all positive or all negative. Define a new sequence $R_1, \ldots, R_n$ of random variables by putting $R_i := S_i - \mathbb{E}[S_i|S^{i-1}]$. It is straightforward to verify that $\mathbb{E}[R_i|R^{i-1}] = 0$, i.e., $R_1, \ldots, R_n$ forms a martingale difference sequence. Thus if for any i, $|S_i| \leq c$ for some c, and thus $|R_i| \leq c$, Azuma's inequality guarantees that

$$\Pr\left[\sum_{i=1}^{n} \Big(S_i - \mathbb{E}\big[S_i|S^{i-1}\big]\Big) \geq \lambda n\right] \leq \exp\left(-\frac{\lambda^2 n}{2c^2}\right). \tag{4.7}$$

We now put $S_i := \log P_{Z_i|Z^{i-1}}(Z_i|Z^{i-1})$ for $i = 1, \ldots, n$. Note that $S_1, \ldots, S_n \leq 0$. It is easy to see that the bound on the conditional entropy of Z_i from Theorem 4.20 implies that $\mathbb{E}[S_i|S^{i-1}] \leq -h$. Indeed, for any $z^{i-1} \in \mathcal{Z}^{i-1}$, we have $\mathbb{E}\big[\log P_{Z_i|Z^{i-1}}(Z_i|Z^{i-1})|Z^{i-1} = z^{i-1}\big] = -\mathrm{H}(Z_i|Z^{i-1} = z^{i-1}) \leq -h$, and thus for any subset $\mathcal{E}$ of $\mathcal{Z}^{i-1}$, and in particular for the set of z^{i-1}'s which map to a given s^{i-1}, it holds that

$$\begin{aligned}\mathbb{E}\big[S_i|Z^{i-1} \in \mathcal{E}\big] &= \sum_{z^{i-1}\in\mathcal{E}} P_{Z^{i-1}|Z^{i-1}\in\mathcal{E}}(z^{i-1}) \cdot \mathbb{E}\big[\log P_{Z_i|Z^{i-1}}(Z_i|Z^{i-1})|Z^{i-1} = z^{i-1}\big] \\ &\leq -h\,. \end{aligned} \tag{4.8}$$

As a consequence, the bound on the probability of (4.7) in particular bounds the probability of the event (4.6), even with λn instead of $2\lambda n$. A problem though is that we have no upper bound c on the $|S_i|$'s. Because of that, we now consider a modified sequence $\tilde{S}_1, \ldots, \tilde{S}_n$ defined by $\tilde{S}_i := \log P_{Z_i|Z^{i-1}}(Z_i|Z^{i-1})$ if $P_{Z_i|Z^{i-1}}(Z_i|Z^{i-1}) \geq \delta$ and $\tilde{S}_i := 0$ otherwise, where $\delta > 0$ will be determined later. This gives us a bound like (4.7) but with an explicit c, namely $c = \log(1/\delta)$. Below, we will argue that $\mathbb{E}\big[\tilde{S}_i|\tilde{S}^{i-1}\big] - \mathbb{E}\big[S_i|\tilde{S}^{i-1}\big] \leq \lambda$ by the right choice of δ; the claim then follows from observing that

$$\begin{aligned}\tilde{S}_i - \mathbb{E}\big[\tilde{S}_i|\tilde{S}^{i-1}\big] &\geq S_i - \mathbb{E}\big[\tilde{S}_i|\tilde{S}^{i-1}\big] \\ &\geq S_i - \mathbb{E}\big[S_i|\tilde{S}^{i-1}\big] - \lambda \\ &\geq S_i + h - \lambda,\end{aligned}$$

where the last inequality follows from (4.8). Regarding the claim $\mathbb{E}\big[\tilde{S}_i|\tilde{S}^{i-1}\big] - \mathbb{E}\big[S_i|\tilde{S}^{i-1}\big] \leq \lambda$, using a similar argument as for (4.8), it suffices to show that $\mathbb{E}\big[\tilde{S}_i|\tilde{Z}^{i-1}{=}z^{i-1}\big] - \mathbb{E}\big[S_i|\tilde{Z}^{i-1}{=}z^{i-1}\big] \leq \lambda$ for any z^{i-1}:

$$
\begin{aligned}
&\mathbb{E}\big[\tilde{S}_i|\tilde{Z}^{i-1}{=}z^{i-1}\big] - \mathbb{E}\big[S_i|\tilde{Z}^{i-1}{=}z^{i-1}\big] \\
&\quad = -\sum_{z_i} P_{Z_i|Z^{i-1}}(z_i|z^{i-1}) \log(P_{Z_i|Z^{i-1}}(z_i|z^{i-1})) \\
&\quad \leq |\mathcal{Z}|\delta \log(1/\delta)
\end{aligned}
$$

where the summation is over all $z_i \in \mathcal{Z}$ with $P_{Z_i|Z^{i-1}}(z_i|z^{i-1}) < \delta$, and where the inequality holds as long as $\delta \leq 1/e$, as can easily be verified. Thus, we let $0 < \delta < 1/e$ be such that $|\mathcal{Z}|\delta \log(1/\delta) = \lambda$. Using the mathematical Lemma 4.8, we have that $\delta > \frac{\lambda/|\mathcal{Z}|}{4\log(|\mathcal{Z}|/\lambda)}$ and derive that $c^2 = \log(1/\delta)^2 = \lambda^2/(\delta|\mathcal{Z}|)^2 < 16\log(|\mathcal{Z}|/\lambda)^2$, which gives us the claimed bound ε on the probability. □

4.5.2 Quantum Uncertainty Relations

We now state and prove the new entropic uncertainty relation in its most general form. A special case will then be introduced (Corollary 4.23) and used in the security analysis of the *1-2 OT*-protocols we consider in Chapter 6.

Definition 4.21 *Let $\mathcal{S}$ be a finite set of orthonormal bases in the d-dimensional Hilbert space $\mathcal{H}_d$. We call $h \geq 0$ an* average entropic uncertainty bound *for $\mathcal{S}$ if every state in $\mathcal{H}_d$ satisfies $\frac{1}{|\mathcal{S}|}\sum_{\vartheta\in\mathcal{S}} \mathrm{H}(P_\vartheta) \geq h$, where P_ϑ is the distribution obtained by measuring the state in basis ϑ.*

Note that by the convexity of the Shannon entropy H, a lower bound for all *pure* states in $\mathcal{H}_d$ suffices to imply the bound for all (possibly mixed) states.

Theorem 4.22 *Let $\mathcal{S}$ be a set of orthonormal bases in $\mathcal{H}_d$ with an average entropic uncertainty bound h, and let $\rho \in \mathcal{P}(\mathcal{H}_d^{\otimes n})$ be an arbitrary quantum state. Let $\Theta = (\Theta_1, \ldots, \Theta_n)$ be uniformly distributed over $\mathcal{S}^n$ and let $X = (X_1, \ldots, X_n)$ be the outcome when measuring ρ in basis Θ, distributed over $\{0, \ldots, d-1\}^n$. Then for any $0 < \lambda < \frac{1}{2}$*

$$\mathrm{H}^\varepsilon_\infty(X|\Theta) \geq (h - 2\lambda)\, n$$

with $\varepsilon = \exp\Big(-\frac{\lambda^2 n}{32(\log(|\mathcal{S}|\cdot d/\lambda))^2}\Big)$.

Proof: Define $Z_i := (X_i, \Theta_i)$ and $Z^i := (Z_1, \ldots, Z_i)$. Let $z^{i-1} \in \mathcal{S}^{i-1}$ be arbitrary. Then

$$\mathrm{H}(Z_i|Z^{i-1}{=}z^{i-1}) = \mathrm{H}(X_i|\Theta_i, Z^{i-1}{=}z^{i-1}) + \mathrm{H}(\Theta_i|Z^{i-1}{=}z^{i-1}) \geq h + \log|\mathcal{S}|,$$

where the inequality follows from the fact that Θ_i is chosen uniformly at random and from the definition of h. Note that h lower bounds the average entropy for any system in $\mathcal{H}_d$, and thus in particular for the ith subsystem of ρ, with all previous d-dimensional subsystems measured. Theorem 4.20 thus implies that

$H^{\varepsilon}_{\infty}(X\Theta) \geq (h + \log|\mathcal{B}| - 2\lambda)n$ for any $0 < \lambda < \frac{1}{2}$ and for ε as claimed. We conclude that

$$H^{\varepsilon}_{\infty}(X \mid \Theta) \geq H^{\varepsilon}_{\infty}(X\Theta) - n\log|\mathcal{B}| \geq (h - 2\lambda)n \ ,$$

where the first inequality follows from the equality

$$P_{X\mathcal{E}|\Theta}(x|\theta) = P_{X\Theta\mathcal{E}}(x,\theta)/P_{\Theta}(\theta) = |\mathcal{B}|^n \cdot P_{X\Theta\mathcal{E}}(x,\theta)$$

for all x and θ and any event $\mathcal{E}$, and from the definition of (conditional) smooth entropy. □

For the special case where $\mathcal{S} = \{+,\times\}$ is the set of BB84 bases, we can use the uncertainty relation of Maassen and Uffink [MU88] (see Equation (4.2)) which, using our terminology, states that $\mathcal{S}$ has average entropic uncertainty bound $h = \frac{1}{2}$. Theorem 4.22 together with Lemma 4.9 then immediately gives the following corollary.

Corollary 4.23 *Let $\rho \in \mathcal{P}(\mathcal{H}_2^{\otimes n})$ be an arbitrary n-qubit quantum state. Let $\Theta = (\Theta_1,\ldots,\Theta_n)$ be uniformly distributed over $\{+,\times\}^n$ and $X = (X_1,\ldots,X_n)$ be the outcome when measuring ρ in basis Θ. Then for any $0 < \lambda < \frac{1}{4}$*

$$H^{\varepsilon}_{\infty}(X|\Theta) \geq \left(\tfrac{1}{2} - 2\lambda\right)n$$

where $\varepsilon = 2^{-\frac{\lambda^4}{32}n}$.

Maassen and Uffink's relation being optimal means there exists a quantum state ρ—namely the product state of eigenstates of the subsystems, e.g. $\rho = |0\rangle\langle 0|^{\otimes n}$—for which $H(X|\Theta) = \frac{n}{2}$. On the other hand, we have shown that $(\frac{1}{2} - \lambda)n \leq H^{\varepsilon}_{\infty}(X|\Theta)$ for $\lambda > 0$ arbitrarily close to 0. For the product state ρ, the X are independent and we know from Lemma 2.13 that $H^{\varepsilon}_{\infty}(X|\Theta)$ approaches $H(X|\Theta) = \frac{n}{2}$. It follows that the relation cannot be significantly improved even when considering Rényi entropy of order $1 < \alpha < \infty$.

Another tight corollary is obtained if we consider the set of measurements $\mathcal{S} = \{+,\times,\circlearrowleft\}$ (see Section 2.3 for the definition of the circular basis $\circlearrowleft$). In [Sán93], Sánchez-Ruiz shows that for this $\mathcal{S}$, the average entropic uncertainty bound

$$h = \frac{2}{3} \tag{4.9}$$

is optimal. It implies that $H^{\varepsilon}_{\infty}(X|\Theta) \gtrsim H(X|\Theta) = \frac{2n}{3}$ for negligible ε.

4.5.3 The Overall Average Entropic Uncertainty Bound

In the this section, we compute the average uncertainty bound for the set of *all bases* of a d-dimensional Hilbert space. Let $\mathcal{U}(d)$ be the set of unitaries on $\mathcal{H}_d$. Moreover, let dU be the normalized Haar measure on $\mathcal{U}(d)$, i.e.,

$$\int_{\mathcal{U}(d)} f(VU)dU = \int_{\mathcal{U}(d)} f(UV)dU = \int_{\mathcal{U}(d)} f(U)dU \ ,$$

for any $V \in \mathcal{U}(d)$ and any integrable function f, and $\int_{\mathcal{U}(d)} dU = 1$. (Note that the normalized Haar measure dU exists and is unique.)

Let $\{\omega_1, \ldots, \omega_d\}$ be a fixed orthonormal basis of $\mathcal{H}_d$, and let $\mathcal{S}_{\text{all}} = \{\vartheta_U\}_{U \in \mathcal{U}(d)}$ be the family of bases $\vartheta_U = \{U\omega_1, \ldots, U\omega_d\}$ with $U \in \mathcal{U}(d)$. The set $\mathcal{S}_{\text{all}}$ consist of *all* orthonormal basis of $\mathcal{H}_d$. We generalize Definition 4.21, the average entropic uncertainty bound for a finite set of bases, to the *infinite* set $\mathcal{S}_{\text{all}}$.

Definition 4.24 *We call h_d an* overall average entropic uncertainty bound *in $\mathcal{H}_d$ if every state in $\mathcal{H}_d$ satisfies*

$$\int_{\mathcal{U}(d)} \mathrm{H}(P_{\vartheta_U}) dU \geq h_d \ ,$$

where P_{ϑ_U} is the distribution obtained by measuring the state in basis $\vartheta_U \in \mathcal{S}_{\text{all}}$.

Proposition 4.25 *For any positive integer d,*

$$h_d = \left(\sum_{i=2}^{d} \frac{1}{i} \right) / \ln(2)$$

is the overall average entropic uncertainty bound in $\mathcal{H}_d$. It is attained for any pure state in $\mathcal{H}_d$.

The proposition follows immediately from Formula (14) in [JRW94] for a pure state, i.e. $(\lambda_1, \ldots, \lambda_n) = (1, 0, \ldots, 0)$. The result was originally shown by Sýkora [Sýk74] and by Jones [Jon91], another proof can be found in the appendix of an article by Jozsa, Robb, and Wootters [JRW94]. An elementary proof suggested by Harremoës based on recent results by Harremoës and Vignat [HV06] is given below.

Proof: Let $|\varphi\rangle$ be a pure state in $\mathcal{H}_d$. For the probability distribution $P_{\vartheta_U} = (p_1, \ldots, p_d)$ holds $p_i = |\langle\varphi|U|\omega_i\rangle|^2$. We want to compute the integral

$$\int_{\mathcal{U}(d)} -\sum_{i=1}^{d} p_i \log(p_i)\, dU = -\sum_{i=1}^{d} \int_{\mathcal{U}(d)} |\langle\varphi|U|\omega_i\rangle|^2 \log(|\langle\varphi|U|\omega_i\rangle|^2)\, dU.$$

Note that by the invariance of the Haar measure, all summands on the right-hand side are equal and it suffices to compute

$$-\, d \int_{\mathcal{U}(d)} |\langle\varphi|U|e_1\rangle|^2 \log(|\langle\varphi|U|e_1\rangle|^2)\, dU, \tag{4.10}$$

where $|e_1\rangle$ is the first vector in the computational basis, i.e. $|\langle\varphi|U|e_1\rangle|^2$ is the length of the projection onto the first coordinate of $U^*|\varphi\rangle$.

The Haar measure over $\mathcal{U}(d)$ is the uniform distribution over the d-dimensional complex sphere which can be seen as the uniform distribution over the $2d$-dimensional real sphere $S_{2d} = \{(X, Y) \in \mathbb{R}^{2d} | \sum_{i=1}^{2d} X_i^2 + Y_i^2 = 1\}$ where the complex coordinates are given by $(X_1 + iY_1, \ldots, X_d + iY_d)$. Setting $Z_i = X_i^2 + Y_i^2$

and $Z = (Z_1, \dots, Z_d)$ and using a result from [HV06] about the projection of the uniform distribution over S_{2d} to the first coordinate, we obtain that the density of Z_1 is $f(z) = (d-1)(1-z)^{d-2}dz$ for $z \in [0,1]$. Therefore, (4.10) equals

$$-d \int_0^1 z \log(z) \cdot (d-1)(1-z)^{d-2} dz = \left(\sum_{i=2}^{d} \frac{1}{i} \right) / \ln(2),$$

where the evaluation of this integral follows from standard calculus. By convexity of the Shannon entropy, the bound also holds for mixed states and the claim follows. □

The following table gives some numerical values of h_d for small values of d.

d	2	4	8	16
h_d	0.72	1.56	2.48	3.43
$\frac{h_d}{\log(d)}$	0.72	0.78	0.83	0.86

It is well-known that the harmonic series in Proposition 4.25 diverges in the same way as $\log(d)$ and therefore, $\frac{h_d}{\log(d)}$ goes to 1 for large dimensions d.

Chapter 5

Rabin OT in the Bounded-Quantum-Storage Model

In this chapter, we present an efficient protocol for Rabin Oblivious Transfer which is secure in the bounded-quantum-storage model. It first appeared in [DFSS05], a journal version of this paper is in preparation [DFSS08].

5.1 The Definition

A protocol for Rabin Oblivious Transfer (*Rabin OT*) between sender Alice and receiver Bob allows for 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

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

In this chapter, we are considering quantum protocols for *Rabin OT*. This means that while the inputs 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 quantum state.

Any such (two-party) protocol is specified by a family $\{(\mathsf{S}_n, \mathsf{R}_n)\}_{n>0}$ of pairs of interactive quantum circuits (i.e. interacting through a quantum channel). Each pair is indexed by a security parameter $n > 0$, where S_n and R_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 S's input bit b, and let A and Y denote the binary random variables describing R's two output bits, where the meaning is that A indicates whether the bit was received or not. Furthermore, for a dishonest sender $\tilde{\mathsf{S}}$, the final state of a fixed candidate protocol for *Rand 1-2 OT* can be described by the ccq-state $\rho_{AY\tilde{\mathsf{S}}}$ where (by slight abuse of notation) we also denote by $\tilde{\mathsf{S}}$ the quantum register that the sender outputs. Its state may depend on A and Y. Similarly, for a dishonest receiver $\tilde{\mathsf{R}}$, we have the cq-state $\rho_{B\tilde{\mathsf{R}}}$.

Definition 5.1 *A two-party (quantum) protocol* (S,R) *is a* ε-secure *Rabin OT if the following holds:*

ε-Correctness: *For honest* S *and* R*,*

$$P[B = Y|A = 1] \geq 1 - \varepsilon\,.$$

ε-Receiver-security: *For honest* R *and any dishonest* $\tilde{\mathsf{S}}$ *there exists*[1] *a binary random variable* B' *such that*

$$P[B' = Y|A = 1] \geq 1 - \varepsilon, \quad \text{and} \quad \delta\big(\rho_{AB'\tilde{\mathsf{S}}}, \mathbb{1} \otimes \rho_{B'\tilde{\mathsf{S}}}\big) \leq \varepsilon\,.$$

ε-Sender-security: *For any* $\tilde{\mathsf{R}}$ *there exists an event* $\mathcal{E}$ *with* $P[\mathcal{E}] \geq \frac{1}{2} - \varepsilon$ *such that*

$$\delta\big(\rho_{B\tilde{\mathsf{R}}|\mathcal{E}}, \rho_B \otimes \rho_{\tilde{\mathsf{R}}|\mathcal{E}}\big) \leq \varepsilon\,.$$

If any of the above holds for $\varepsilon = 0$*, then the corresponding property is said to hold* **perfectly**. *If one of the properties only holds with respect to a restricted class* $\mathfrak{S}$ *of* $\tilde{\mathsf{S}}$*'s respectively* $\mathfrak{R}$ *of* $\tilde{\mathsf{R}}$*'s, then this property is said to hold (and the protocol is said to be secure)* **against** $\mathfrak{S}$ *respectively* $\mathfrak{R}$.

Receiver-security requires that the joint quantum state is essentially the same as when the dishonest sender chooses a bit B' according to some distribution and a (possibly dependent) quantum state, and gives B' to an ideal functionality which passes it on to the receiver with probability $\frac{1}{2}$. Sender-security requires that the joint quantum state is essentially the same as when the dishonest receiver gets the sender's bit B with probability $\frac{1}{2}$ and prepares some state that may depend on B in case he receives it, and prepares some state that does not depend on B otherwise. In other words, security requires that the dishonest party cannot do more than when attacking an ideal functionality. From such a strong security guarantee we expect nice composition behavior, for instance like in [CSSW06].

Note that the original definition given in [DFSS05] does not guarantee that the distribution of the input bit is determined at the end the execution of *Rabin OT*. This is a strictly weaker definition and does not fully capture what is expected from a *Rabin OT*: it is easy to see that if the dishonest sender can still influence his input bit after the execution of the protocol, then known schemes based on *Rabin OT*, like bit commitments, are not secure anymore. The security definition given here is in the spirit of the security definition from [DFR+07] for 1-2 OT, described in the next Chapter 6.

[1] Recall from Section 2.3: Given a cq-state ρ_{XE}, by saying that there exists a random variable Y such that ρ_{XYE} satisfies some condition, we mean that ρ_{XE} can be understood as $\rho_{XE} = \mathrm{tr}_Y(\rho_{XYE})$ for a ccq-state ρ_{XYE} that satisfies the required condition.

5.2 The Protocol

We present a quantum protocol for *Rabin OT* that will be shown perfectly correct and perfectly receiver-secure (against any sender) and statistically sender-secure against any quantum-memory-bounded receiver. Our protocol exhibits some similarity with quantum conjugate coding introduced by Wiesner [Wie83].

QOT(b):

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

Figure 5.1: Quantum Protocol for *Rabin OT*

The protocol given in Figure 5.1 is very simple: S picks $x \in_R \{0,1\}^n$ and sends to R n qubits in state either $|x\rangle_+$ or $|x\rangle_\times$ each chosen with probability $\frac{1}{2}$. R then measures all received qubits either in the rectilinear or in the diagonal basis. With probability $\frac{1}{2}$, R picked the right basis and gets x, while any $\tilde{\mathsf{R}}$ 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 based on any two-universal class of hashing functions $\mathcal{F}_n$ is then used to eliminate partial information (as explained in Section 2.5). For simplicity, we focus on the case where the output size of the family $\mathcal{F}_n$ is just one bit, i.e. $\ell = 1$, but all results of this chapter can easily be extended to *Rabin OT*$^\ell$ of ℓ-bit strings, by using an output size $\ell > 1$ and adjusting the memory bounds accordingly, see Section 5.7.

In order to avoid aborting, we specify that if a dishonest $\tilde{\mathsf{S}}$ refuses to participate, or sends data in incorrect format, then R samples its output bits a and y both at random in $\{0,1\}$.

We first consider receiver-security.

Proposition 5.2 QOT *is perfectly receiver-secure.*

It is obvious that no information about whether R has received the bit is leaked to any sender $\tilde{\mathsf{S}}$, since R does not send anything. However, one needs to show the existence of a random variable B' as required by receiver-security.

Proof: Recall, the quantum state $\rho_{AY\tilde{\mathsf{S}}}$ is defined by the experiment where the dishonest sender $\tilde{\mathsf{S}}$ interacts with the honest memory-bounded R. Consider a modification of the experiment where we allow R to be *unbounded* in memory and where R waits to receive r and then measures all qubits in basis r. Let X' be the resulting string. Nevertheless, R picks $r' \in_R \{+, \times\}$ at random and outputs $(A, Y) = (0, 0)$ if $r' \neq r$ and $(A, Y) = (1, e \oplus f(X'))$ if $r' = r$. Since the only difference between the two experiments is *when* R measures the qubits and *in what basis* R measures them when $r \neq r'$, in which case his final output is independent of the measurement outcome, the two experiments result in the same $\rho_{AY\tilde{\mathsf{S}}}$. However, in the modified experiment we can choose B' to be $e \oplus f(X')$, such that by construction $B' = Y$ if $A = 1$ and A is uniformly distributed, independent of anything, and thus $\rho_{AB'\tilde{\mathsf{S}}} = \mathbb{1} \otimes \rho_{B'\tilde{\mathsf{S}}}$. □

As we shall see in Section 5.4, the security of the QOT protocol against receivers with bounded-size quantum memory holds as long as the bound applies before Step 3 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 5.2 is easier to prove secure. This technique was pioneered by Ekert [Eke91] in the scenario of quantum key distribution. A similar approach was taken in the Shor-Preskill proof of security for the BB84 quantum-key-distribution scheme [SP00].

EPR-QOT(b):

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

Figure 5.2: Protocol for EPR-based *Rabin OT*

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

Lemma 5.3 QOT *is ε-sender-secure if and only if* EPR-QOT *is.*

Proof: The proof follows easily after observing that S's choices of r and f, together with the measurements all commute with $\tilde{\mathsf{R}}$'s actions. Therefore, they can be performed right after Step 1 with no change for $\tilde{\mathsf{R}}$'s view. Modifying EPR-QOT that way results in QOT. □

Note that for a dishonest receiver it is not only irrelevant whether he tries to attack QOT or EPR-QOT, but in fact there is no difference in the two protocols from his point of view.

5.3 Modeling Dishonest Receivers

We model dishonest receivers in QOT, respectively 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 3 in (EPR-)QOT. Before (and after) 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 5.4 *The set $\mathfrak{R}_\gamma$ denotes all possible quantum dishonest receivers $\{\tilde{\mathsf{R}}_n\}_{n>0}$ in* QOT *or* EPR-QOT *where for each $n > 0$, $\tilde{\mathsf{R}}_n$ has quantum memory of size at most γn when Step 3 is reached.*

In general, the adversary $\tilde{\mathsf{R}}$ is allowed to perform any quantum computation compressing the n qubits received from S into a quantum register M of size at most γn when Step 3 is reached. More precisely, the compression function is implemented by some unitary transform T acting upon the quantum state received and an ancilla register of arbitrary size (initially in the state $|0\rangle$). The compression is performed by a measurement that we assume in the computational basis without loss of generality. Before starting Step 3, the adversary first applies a unitary transform T:

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

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 in its most general form when Step 3 in EPR-QOT is reached is thus of the form

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

where $\sum_x |\alpha_x|^2 = 1$. We will prove security for any such state $|\psi\rangle$ and thus conditioned on any value y that may be observed. It is therefore safe to leave the dependency on y implicit.

5.4 Security Against Dishonest Receivers

In this section, we use the uncertainty relation derived in Section 4.3 to 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 1.

Theorem 5.5 *For all $\gamma < \frac{1}{2}$,* QOT *is ε-secure for a negligible (in n) ε against $\mathfrak{R}_\gamma$.*

Proof: After Lemmas 5.3 and 5.2, it remains to show that EPR-QOT is ε-sender-secure against $\mathfrak{R}_\gamma$. Since $\gamma < \frac{1}{2}$, we can find $\kappa > 0$ with $\gamma + \kappa < \frac{1}{2}$. Consider a dishonest receiver $\tilde{\mathsf{R}}$ in EPR-QOT with quantum memory of size γn. Let R and X denote the random variables describing the basis r and the outcome x of S's measurement (in basis r) in Step 3 of EPR-QOT, respectively. We implicitly understand the distribution of X given R to be conditioned on the classical outcome y of the measurement $\tilde{\mathsf{R}}$ performed when the memory bound applies, as described in Section 5.3; the following analysis works no matter what y is. Corollary 4.17 with $\lambda = \gamma + \kappa$ implies the existence of ε negligible in n and an event $\mathcal{E}$ such that $P[\mathcal{E}] \geq \frac{1}{2} - \varepsilon$ and such that $\mathrm{H}_\infty(X|R{=}r, \mathcal{E}) \geq \gamma n + \kappa n$ for any relevant r. Note that by construction, the random variables X and R, and thus also the event $\mathcal{E}$, are independent of the sender's input bit B, and hence $\rho_{B|\mathcal{E}} = \rho_B$. It remains to show that $\delta\big(\rho_{B\tilde{\mathsf{R}}|\mathcal{E}}, \rho_{B|\mathcal{E}} \otimes \rho_{\tilde{\mathsf{R}}|\mathcal{E}}\big) \leq \varepsilon$. As the bit B is masked by the output of the two-universal hash function $F(X)$ in Step 4 of EPR-QOT (where the random variable F represents the random choice for f), it suffices to show that $F(X)$ is close to uniform and essentially independent from $\tilde{\mathsf{R}}$'s view, conditioned on $\mathcal{E}$. But this is guaranteed by the above bound on $\mathrm{H}_\infty(X|R{=}r, \mathcal{E})$ and by the privacy-amplification theorem (Corollary 2.25 with $\varepsilon := 0, \ell := 1, q := \gamma n$ and U constant). □

5.5 On the Necessity of Privacy Amplification

In this section, we show that randomized privacy amplification is needed for protocol QOT to be secure. For instance, it is tempting to believe that the sender could use the XOR $\bigoplus_i x_i$ in order to mask the bit b, rather than $f(x)$ for a randomly sampled $f \in \mathcal{F}_n$. This would reduce the communication complexity as well as the number of random coins needed. However, we argue in this section that this is not secure (against an adversary as we model it). Indeed, somewhat surprisingly, this variant can be broken by a dishonest receiver that has *no quantum memory at all* (but that can do coherent measurements on pairs of qubits) in the case n is even. For odd n, the dishonest receiver needs to store *a single qubit.*

Clearly, a dishonest receiver can break the modified scheme QOT and learn the bit b with probability 1 if he can compute $\bigoplus_i x_i$ with probability 1. Note that, using the equivalence between QOT and EPR-QOT, x_i can be understood as the outcome of the measurement in either the +- or the ×-basis, performed by the sender on one part of an EPR pair while the other is handed over to the receiver. The following proposition shows that indeed the receiver can learn $\bigoplus_i x_i$ by a suitable measurement of his parts of the EPR pairs. Concretely, he measures the qubits he receives pair-wise by a suitable measurement which allows him to learn the XOR of the two corresponding x_i's, no matter what the basis is (and he needs to store one single qubit in case n is odd). This obviously allows him to learn the XOR of all x_i's in all cases.

Proposition 5.6 *Consider two EPR pairs, i.e.,* $|\psi\rangle = \frac{1}{2}\sum_x |x\rangle^S |x\rangle^R$ *where* x *ranges over* $\{0,1\}^2$. *Let* $r \in \{+,\times\}$, *and let* x_1 *and* x_2 *be the result when measuring the two qubits in register* S *in basis* r. *There exists a fixed measurement for register* R *so that the outcome together with* r *uniquely determines* $x_1 \oplus x_2$.

Proof: The measurement that does the job is the *Bell measurement*, i.e., the measurement in the Bell basis $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$. Recall,

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle_+ + |11\rangle_+\big) = \frac{1}{\sqrt{2}}\big(|00\rangle_\times + |11\rangle_\times\big)\\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle_+ + |10\rangle_+\big) = \frac{1}{\sqrt{2}}\big(|00\rangle_\times - |11\rangle_\times\big)\\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}\big(|00\rangle_+ - |11\rangle_+\big) = \frac{1}{\sqrt{2}}\big(|01\rangle_\times + |10\rangle_\times\big)\\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}\big(|01\rangle_+ - |10\rangle_+\big) = \frac{1}{\sqrt{2}}\big(|10\rangle_\times - |01\rangle_\times\big)\,.
\end{aligned}$$

Due to the special form of the Bell basis, when register R is measured and, as a consequence, one of the four Bell states is observed, the state in register S collapses to that *same* Bell state. Indeed, when doing the basis transformation, all cross-products cancel each other out. It now follows by inspection that knowledge of the Bell state and the basis r allows to predict the XOR of the two bits observed when measuring the Bell state in basis r. For instance, for the Bell state $|\Psi^+\rangle$, the XOR is 1 if $r = +$ and it is 0 if $r = \times$. □

Note that from the proof above, one can see that the receiver's attack, respectively his measurement on each pair of qubits, can be understood as teleporting one of the two entangled qubits from the receiver to the sender using the other as EPR pair. However, the receiver does not send the outcome of his measurement to the sender, but keeps it in order to predict the XOR.

Clearly, the same strategy also works against any fixed linear function. Therefore, the only hope for doing deterministic privacy amplification is by using a non-linear function. However, it has been shown recently by Ballester, Wehner, and Winter [BWW06], that also this approach is doomed to fail in our scenario, because the outcome of *any fixed Boolean function* can be perfectly predicted by a dishonest receiver who can store a single qubit and later learns the correct basis $r \in \{+,\times\}$.

5.6 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. In addition, it also requires a perfect quantum source which on request produces *one and only 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 sender-security of QOT is vulnerable to imperfect sources that once in a while transmit more than one qubit in the same state: a malicious receiver $\tilde{\mathsf{R}}$ 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 parties.

In this section, we present such a protocol based on BB84 states [BB84], BB84-QOT (see Figure 5.3). The security proof follows essentially by adapting the security analysis of QOT in a rather straightforward way, as will be discussed later.

5.6.1 Weak Quantum Model

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*. By adjusting the parameters, this model can also cope with dark counts and empty pulses, see Section 9.1.1.

In order to deal with noisy quantum communication, we need to do error-correction without giving the adversary too much information. Techniques to solve this problem are known as *information reconciliation* (as introduced for instance by Brassard and Salvail [BS93]) or as *secure sketches* introduced by Dodis, Reyzin, Smith [DRS04]. Let $x \in \{0,1\}^\ell$ be an arbitrary string, and let $x' \in \{0,1\}^\ell$ be the result of flipping every bit in x (independently) with probability ϕ. It is well known that learning the syndrome $S(x)$ of x, with respect to a suitable efficiently-decodable linear error-correcting code C of length ℓ, allows to recover x from x', except with negligible probability in ℓ (see,e.g., [Mau91, Cré97, DRS04]). Furthermore, it is known from coding theory that, for large enough ℓ, such a code can be chosen with rate R arbitrarily close to but smaller than $1-h(\phi)$, i.e., such that the syndrome length s is bounded by $s < (h(\phi)+\varepsilon)\ell$ where $\varepsilon > 0$ (see e.g. [Cré97] or the full version of [DRS04] and the references therein).

Regarding the loss of information, we can use the privacy-amplification statement in form of Corollary 2.25 with $\varepsilon := 0$ and constant U in a similar way as before, just by appending the classical syndrome $S(x)$ (of length s) to the quantum register E, which results in

$$\delta\big(\rho_{F(X)FS(X)E}, \mathbb{1} \otimes \rho_{FS(X)E}\big) \leq \frac{1}{2} 2^{-\frac{1}{2}(\mathrm{H}_\infty(X)-q-s-1)}. \tag{5.1}$$

Consider the protocol BB84-QOT shown in Figure 5.3 in the (ϕ, η)-weak quantum model. The protocol uses an efficiently decodable linear code C_ℓ, parametrized in $\ell \in \mathbb{N}$, with codeword length ℓ, rate $R = 1-h(\phi)-\varepsilon$ for some small $\varepsilon > 0$, and being able to correct errors occurring with probability

ϕ (except with negligible probability). Let S_ℓ be the corresponding syndrome function. Like before, the memory bound in BB84-QOT applies before Step 3.

> BB84-QOT(b):
>
> 1. S picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$ and sends x_i in the corresponding bases $|x_1\rangle_{\theta_1}, \ldots, |x_n\rangle_{\theta_n}$ to R.
> 2. R picks $r' \in_R \{+,\times\}$ and measures all qubits in basis r'. Let $x' \in \{0,1\}^n$ be the result.
> 3. S picks $r \in_R \{+,\times\}$, sets $I := \{i : \theta_i = \{+,\times\}_{[r]}\}$ and $\ell := |I|$, and announces r, I, $syn := S_\ell(x|_I)$, $f \in_R \mathcal{F}_\ell$, and $e := b \oplus f(x|_I)$.
> 4. R recovers $x|_I$ from $x'|_I$ and syn, and outputs $a := 1$ and $b' := e \oplus f(x|_I)$ if $r' = r$ and else $a := 0$ and $b' := 0$.

Figure 5.3: Protocol for the BB84 version of *Rabin OT*

By the above mentioned properties of the code C_ℓ, it is obvious that R receives the correct bit b if $r' = r$, except with negligible probability. (The error probability is negligible in ℓ, but by Chernoff's inequality (Lemma 2.5), ℓ is linear in n except with negligible probability.) Also, since there is no communication from R to S, a dishonest sender $\tilde{\mathsf{S}}$ cannot learn whether R received the bit. In fact, BB84-QOT can be shown perfectly receiver-secure in the same way as in Proposition 5.2. Similar as for protocol QOT, in order to argue about sender-security we compare BB84-QOT with a purified version shown in Figure 5.4. 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 S in BB84-EPR-QOT so that there is no difference from R's point of view.

The security equivalence between BB84-QOT (in the (ϕ,η)-weak quantum model) and BB84-EPR-QOT (in the $(\phi, 0)$-weak quantum model) follows along the same lines as in Section 5.2.

Theorem 5.7 *In the (ϕ,η)-weak quantum model,* BB84-QOT *is ε-secure with ε negligible in n against $\mathfrak{R}_\gamma$ for any $\gamma < \frac{1-\eta}{4} - \frac{h(\phi)}{2}$ and n large enough.*

Proof Sketch: It remains to show that BB84-EPR-QOT is sender-secure against $\mathfrak{R}_\gamma$ (in the $(\phi, 0)$-weak quantum model). The reasoning goes analogous to the proof of Theorem 5.5, except that we restrict our attention to those i's which are in J. By Chernoff's inequality (Lemma 2.5), ℓ lies within $(1 \pm \varepsilon)n/2$ and $|J|$ within $(1 - \eta \pm \varepsilon)n/2$ except with negligible probability. In order to make the proof easier to read, we assume that $\ell = n/2$ and $|J| = (1-\eta)n/2$, and we also treat the ε occurring in the rate of the code C_ℓ as zero. For the full proof, we simply need to carry the ε's along, and then choose them small enough at the end of the proof.

Write $n' = |J| = (1-\eta)n/2$, and let γ' be such that $\gamma n = \gamma' n'$, i.e., $\gamma' = 2\gamma/(1-\eta)$. Assume $\kappa > 0$ such that $\gamma' + \kappa < \frac{1}{2}$, where we make sure

BB84-EPR-QOT(b):

1. S prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Additionally, S initializes $I'_+ := \emptyset$ and $I'_\times := \emptyset$. For every $i \in \{1, \ldots, n\}$, S does the following. With probability $1 - \eta$, S sends one half of the i-th pair to R and keeps the other half. While with probability η, S picks $\theta_i \in_R \{+, \times\}$, 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 R where $x_i \in_R \{0, 1\}$.
2. R picks $r' \in_R \{+, \times\}$ and measures all received qubits in basis r'. Let $x' \in \{0, 1\}^n$ be the result.
3. S picks a random index set $J \subset_R \{1, \ldots, n\} \setminus (I'_+ \cup I'_\times)$. Then, it picks $r \in_R \{+, \times\}$, sets $I := J \cup I'_r$ and $\ell := |I|$, and for each $i \in J$ it measures the corresponding qubit in basis r. Let x_i be the corresponding outcome, and let $x|_I$ be the collection of all x_i's with $i \in I$. S announces r, I, $syn = S_\ell(x|_I)$, $f \in_R \mathcal{F}_\ell$, and $e = b \oplus f(x|_I)$.
4. R recovers $x|_I$ from $x'|_I$ and syn, and outputs $a := 1$ and $b' := e \oplus f(x|_I)$, if $r' = r$ and else $a := 0$ and $b' := 0$.

Figure 5.4: Protocol for EPR-based *Rabin OT*, BB84 version

later that such κ exists. It then follows from Corollary 4.17 that there exists an event $\mathcal{E}$ such that $P[\mathcal{E}] \geq \frac{1}{2} - negl(n') = \frac{1}{2} - negl(n)$ and

$$\mathrm{H}_\infty\left(X|_J \middle| R{=}r, \mathcal{E}\right) \geq (\gamma' + \kappa)n' = \gamma n + \kappa(1 - \eta)n/2\,.$$

By Inequality (5.1), it remains to argue that this is larger than $q + s = \gamma n + h(\phi)n/2$, i.e.,

$$\kappa(1 - \eta) > h(\phi)\,,$$

where κ has to satisfy

$$\kappa < \frac{1}{2} - \gamma' = \frac{1}{2} - 2\gamma/(1 - \eta)\,.$$

This can obviously be achieved (by choosing κ appropriately) if and only if the claimed bound on γ holds. □

5.7 *Rabin OT* of Strings

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

Chapter 6

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

In the last chapter, we have shown how to construct *Rabin OT* securely in the bounded-quantum-storage model. Although other flavors of *OT* can be constructed from *Rabin OT* using standard reductions, a more direct approach gives a better ratio between storage-bound and communication-complexity.

In this chapter, we present an efficient protocol for *1-2* Oblivious Transfer secure in the bounded-quantum-storage model. The protocol is very close to Wiesner original "conjugate-coding" protocol [Wie83] from the early 70's. The uncertainty relation from Section 4.5 will be extensively used for proving the security.

The results of this section appeared in [DFR$^+$07].

6.1 The Definition

In *1-2* OT^ℓ, the sender Alice sends two ℓ-bit strings S_0, S_1 to the receiver Bob in such a way that Bob can choose which string he wants to receive, but does not learn anything about the other. Alice does not get to know which string Bob has chosen. As explained in Chapter 3, the common way to build *1-2* OT^ℓ is by constructing a protocol for (Sender-)Randomized *1-2* OT^ℓ, which then can easily be converted into an ordinary *1-2* OT^ℓ. *Rand 1-2* OT^ℓ essentially coincides with ordinary *1-2* OT^ℓ, except that the two strings S_0 and S_1 are not *input* by the sender but generated uniformly at random during the protocol and *output* to the sender.

For the formal definition of the security requirements for a quantum protocol for *Rand 1-2* OT^ℓ, we translate the classical Definition 3.1 to the quantum setting using a similar notation as for the definition of *Rabin OT* in Section 5.1: Let C denote the binary random variable describing receiver R's choice bit, let S_0, S_1 denote the ℓ-bit long random variables describing sender S's output strings, and let Y denote the ℓ-bit long random variable describing R's output string (supposed to be S_C). Furthermore, for a fixed candidate protocol for *Rand 1-2* OT^ℓ, and for a fixed input distribution for C, the overall quantum state in case of a dishonest sender $\tilde{\mathsf{S}}$ is given by the ccq-state $\rho_{CY\tilde{\mathsf{S}}}$. Analogously, in the case of a dishonest receiver $\tilde{\mathsf{R}}$, we have the ccq-state $\rho_{S_0S_1\tilde{\mathsf{R}}}$.

Definition 6.1 (*Rand 1-2* OT^ℓ) *An ε-secure Rand 1-2 OT^ℓ is a quantum protocol between* S *and* R*, with* R *having input* $C \in \{0,1\}$ *while* S *has no input, such that for any distribution of* C*, the following holds:*

ε-Correctness: *If* S *and* R *follow the protocol, then* S *gets output strings* $S_0, S_1 \in \{0,1\}^\ell$ *and* R *gets* $Y = S_C$ *except with probability* ε*.*

ε-Receiver-security: *If* R *is honest, then for any* $\tilde{\mathsf{S}}$*, there exist*[1] *random variables* S_0' *and* S_1' *such that* $\Pr\big[Y = S_C'\big] \geq 1 - \varepsilon$ *and*

$$\delta\big(\rho_{CS_0'S_1'\tilde{\mathsf{S}}}, \rho_C \otimes \rho_{S_0'S_1'\tilde{\mathsf{S}}}\big) \leq \varepsilon \,.$$

ε-Sender-security: *If* S *is honest, then for any* $\tilde{\mathsf{R}}$*, there exists a random variable* $D \in \{0,1\}$ *such that*

$$\delta\big(\rho_{S_{1-D}S_D D\tilde{\mathsf{R}}}, \mathbb{1} \otimes \rho_{S_D D\tilde{\mathsf{R}}}\big) \leq \varepsilon \,.$$

If any of the above holds for $\varepsilon = 0$*, then the corresponding property is said to hold* perfectly*. If one of the properties only holds with respect to a restricted class* $\mathfrak{S}$ *of* $\tilde{\mathsf{S}}$*'s respectively* $\mathfrak{R}$ *of* $\tilde{\mathsf{R}}$*'s, then this property is said to hold and the protocol is said to be secure* against $\mathfrak{S}$ *respectively* $\mathfrak{R}$*.*

Receiver-security, as defined here, implies that whatever a dishonest sender does is as good as the following: generate the ccq-state $\rho_{S_0'S_1'\tilde{\mathsf{S}}}$ independently of C, let R know S_C', and output $\rho_{\tilde{\mathsf{S}}}$. On the other hand, sender-security implies that whatever a dishonest receiver does is as good as the following: generate the ccq-state $\rho_{S_D D\tilde{\mathsf{R}}}$ arbitrarily, let S know S_D and an independent uniformly distributed S_{1-D}, and output $\rho_{\tilde{\mathsf{R}}}$. In other words, a protocol satisfying Definition 6.1 is a secure implementation of the natural *Rand 1-2* OT^ℓ ideal functionality, except that it allows a dishonest sender to influence the distribution of S_0 and S_1, and the dishonest receiver to influence the distribution of the string of his choice. This is in particular good enough for constructing a standard *1-2* OT^ℓ in the straightforward way.

We would like to point out the importance of requiring the existence of S_0' and S_1' in the formulation of receiver-security in a quantum setting: requiring only that the sender learns no information on C, as is sufficient in the classical setting (see e.g. [CSSW06]), does not prevent a dishonest sender from obtaining S_0, S_1 by a suitable measurement *after* the execution of the protocol in such a way that he can choose $S_0 \oplus S_1$ at will, and S_C is the string the receiver has obtained in the protocol. This would for instance make the straightforward construction of a bit commitment [2] based on *1-2 OT* insecure.

[1] Recall from Section 2.3: Given a cq-state ρ_{XE}, by saying that there exists a random variable Y such that ρ_{XYE} satisfies some condition, we mean that ρ_{XE} can be understood as $\rho_{XE} = \mathrm{tr}_Y(\rho_{XYE})$ for a ccq-state ρ_{XYE} that satisfies the required condition.

[2] The committer sends two random bits of parity equal to the bit he wants to commit to, the verifier chooses to receive at random one of those bits.

6.2 The Protocol

We present a quantum protocol for *Rand 1-2 OT*$^\ell$ that will be shown perfectly receiver-secure against any sender and statistically sender-secure against any quantum-memory-bounded receiver. The first two steps of the protocol are identical to Wiesner's "conjugate coding" protocol [Wie83] from circa 1970 for *"transmitting two messages either but not both of which may be received"*.

The simple protocol is described in Figure 6.1. The sender S sends random BB84 states to the receiver R, who measures all received qubits according to his choice bit C. S then picks randomly two functions from a fixed two-universal class of hash functions $\mathcal{F}_n$ from $\{0,1\}^n$ to $\{0,1\}^\ell$, where ℓ is to be determined later, and applies them to the bits encoded in the $+$-basis respectively the bits encoded in $\times$-basis to obtain the output strings S_0 and S_1. Note that we may apply a function $f \in \mathcal{F}_n$ to a n'-bit string with $n' < n$ by padding it with zeros[3] (which does not decrease its entropy). S announces the encoding bases and the hash functions to the receiver who then can compute S_C. Intuitively, a dishonest receiver who cannot store all the qubits until the right bases are announced will measure some qubits in the wrong basis and thus cannot learn both strings simultaneously.

RAND 1-2 QOT $^\ell$**:** Let c be R's choice bit.

1. S picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$ and sends $|x_1\rangle_{\theta_1}, |x_2\rangle_{\theta_2}, \ldots, |x_n\rangle_{\theta_n}$ to R.
2. R measures all qubits in basis $[+,\times]_c$. Let $x' \in \{0,1\}^n$ be the result.
3. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}_n$, announces θ and f_0, f_1 to R, and outputs $s_0 := f_0(x|^\circ_{I_0})$ and $s_1 := f_1(x|^\circ_{I_1})$ where $I_b := \{i : \theta_i = [+,\times]_b\}$.
4. R outputs $s_c = f_c(x'|^\circ_{I_c})$.

Figure 6.1: Quantum Protocol for *Rand 1-2 OT*$^{\boldsymbol{\ell}}$.

We would like to stress that although protocol description and analysis are designed for an ideal setting with perfect noiseless quantum communication and with perfect sources and detectors, all our results can easily be extended to a more realistic noisy setting along the same lines as in the previous Chapter 5.

It is clear by the non-interactivity of RAND 1-2 QOT $^\ell$ that a dishonest sender cannot learn anything about the receiver's choice bit. Below, we show RAND 1 -2 QOT $^\ell$ perfectly receiver-secure according to Definition 6.1.

Proposition 6.2 RAND 1-2 QOT $^\ell$ *is perfectly receiver-secure.*

Proof: Recall that the ccq-state $\rho_{CY\tilde{\mathsf{S}}}$ is defined by the experiment where $\tilde{\mathsf{S}}$ interacts with the honest memory-bounded R. We now define (in a new Hilbert

[3]Recall the notation for padding $x|^\circ_I$ introduced in Section 2.1.

space) the ccccq-state $\hat{\rho}_{\hat{C}\hat{Y}\hat{S}_0'\hat{S}_1'\tilde{\mathsf{S}}}$ by a slightly different experiment: We let $\tilde{\mathsf{S}}$ interact with a receiver with *unbounded* quantum memory, which waits to receive θ and then measures the i-th qubit in basis θ_i for $i = 1, \ldots, n$. Let X be the resulting string, and define $\hat{S}_0' = f_0(X|^{\circ}_{I_0})$ and $\hat{S}_1' = f_1(X|^{\circ}_{I_1})$. Finally, sample $\hat{C}$ according to P_C and set $\hat{Y} = \hat{S}_C'$. It follows by construction that $\Pr\big[\hat{Y} \neq \hat{S}_{\hat{C}}'\big] = 0$ and $\hat{\rho}_{\hat{C}}$ is independent of $\hat{\rho}_{\hat{S}_0'\hat{S}_1'\tilde{\mathsf{S}}}$. It remains to argue that $\hat{\rho}_{\hat{C}\hat{Y}\tilde{\mathsf{S}}} = \rho_{CY\tilde{\mathsf{S}}}$, so that corresponding S_0' and S_1' also exist in the original experiment. But this is obviously satisfied since the only difference between the two experiments is when and in what basis the qubits at position $i \in I_{1-C}$ are measured, which, once C is fixed, cannot influence $\rho_{Y\tilde{\mathsf{S}}}$ respectively $\hat{\rho}_{\hat{Y}\tilde{\mathsf{S}}}$. □

6.3 Security Against Dishonest Receivers

As in Section 5.3, we model dishonest receivers in RAND 1-2 QOT $^\ell$ under the assumption that the maximum size of their quantum storage is bounded. Such adversaries are only required to have bounded quantum storage when Step 3 in RAND 1-2 QOT $^\ell$ is reached. Before and after that, the adversary can store and carry out arbitrary 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 6.3 *The set $\mathfrak{R}_\gamma$ denotes all possible quantum dishonest receivers $\tilde{\mathsf{R}}$ in* RAND 1-2 QOT $^\ell$ *which have quantum memory of size at most γn when Step 3 is reached.*

First, we consider a purified version of RAND 1-2 QOT $^\ell$, EPR RAND 1-2 QOT $^\ell$ in Figure 6.2, where S prepares an EPR pair $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ instead of $|x_i\rangle_{\theta_i}$ and sends one part to the receiver while keeping the other. Only when Step 3 is reached and $\tilde{\mathsf{R}}$'s quantum memory is bound to γn qubits, S measures her qubits in basis $\theta \in_R \{+, \times\}^n$. It is easy to see that for any $\tilde{\mathsf{R}}$, EPR RAND 1-2 QOT $^\ell$ is equivalent to the original RAND 1-2 QOT $^\ell$, and it suffices to prove sender-security for the former. Indeed, S's choices of θ and f_0, f_1, together with the measurements all commute with R's actions. Therefore, they can be performed right after Step 1 with no change for R's view. Modifying EPR RAND 1-2 QOT $^\ell$ that way results in RAND 1-2 QOT $^\ell$.

Theorem 6.4 RAND 1-2 QOT $^\ell$ *is ε-secure against $\mathfrak{R}_\gamma$ for a negligible (in n) ε if there exists $\delta > 0$ such that $\gamma n \leq n/4 - 2\ell - \delta n$.*

The proof has the same structure as the security-proof for the reduction *OT2UOT* described at the end of Section 3.4.2. The uncertainty relation from Section 4.5 lower bounds the dishonest receiver's (smooth) min-entropy about the sender's X. Hence, we have an (imperfect) $(\infty, \frac{n}{2})$-$UOT(\{0,1\}^n)$ from which we get an ordinary *Rand 1-2 OT* $^\ell$ via the min-entropy splitting lemma and privacy amplification against quantum adversaries.

EPR Rand 1-2 QOT $^\ell$:

1. S prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one half of each pair to R and keeps the other halves.
2. R measures all qubits in basis $[+,\times]_c$. Let $x' \in \{0,1\}^n$ be the result.
3. S picks random $\theta \in_R \{+,\times\}^n$, and she measures the ith qubit in basis θ_i. Let $x \in \{0,1\}^n$ be the outcome. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}_n$, announces θ and f_0, f_1 to R and outputs $s_0 := f_0(x|^\circ_{I_0})$ and $s_1 := f_1(x|^\circ_{I_1})$ where $I_b := \{i : \theta_i = [+,\times]_b\}$.
4. R outputs $s_c = f_c(x'|^\circ_{I_c})$.

Figure 6.2: Protocol for EPR-based *Rand 1-2 OT$^{\boldsymbol{\ell}}$*.

Proof: Consider the ccq-state $\rho_{X\Theta\tilde{\mathsf{R}}}$ in EPR Rand 1-2 QOT $^\ell$ after $\tilde{\mathsf{R}}$ has measured all but γn of his qubits, where X describes the outcome of the sender measuring her part of the state in random basis Θ. Also, let F_0 and F_1 be the random variables that describe the random and independent choices of $f_0, f_1 \in \mathcal{F}_n$. Finally, let X_b be $X_b = X|^\circ_{\{i:\,\Theta_i=[+,\times]_b\}}$ (padded with zeros so it makes sense to apply F_b).

Choose λ, κ all positive, but small enough such that (for large enough n)

$$\gamma n \leq (1/4 - \lambda - \lambda' - \kappa)n - 1 - 2\ell.$$

From the uncertainty relation (Corollary 4.23), we know that $\mathrm{H}^\varepsilon_\infty(X_0X_1|\Theta) \geq (1/2 - 2\lambda)n$ for ε exponentially small in n. Therefore, by the Min-Entropy Splitting Lemma 2.15, there exists a binary random variable D such that

$$\mathrm{H}^\varepsilon_\infty(X_{1-D}D|\Theta) \geq (1/4 - \lambda)n.$$

We denote by the random variables F_0, F_1 Alice's choices of hash functions. It is clear that we can condition (for free) on the independent F_D. We write $S_D = F_D(X_D)$, set $\varepsilon' = 2^{-\lambda' n}$, and use the chain rule (Lemma 2.12) to condition on D, S_D as well.

$$\begin{aligned}
&\mathrm{H}^{\varepsilon+\varepsilon'}_\infty(X_{1-D}|\Theta F_D D S_D) \\
&\qquad \geq \mathrm{H}^\varepsilon_\infty(X_{1-D}DS_D|\Theta F_D) - \mathrm{H}_0(DS_D|\Theta F_D) - \lambda' n \\
&\qquad \geq (1/4 - \lambda - \lambda')n - 1 - \ell \\
&\qquad \geq \gamma n + \ell + \kappa n,
\end{aligned}$$

by the choice of $\lambda, \lambda', \kappa$.

We can now apply privacy amplification in form of Corollary 2.25 to obtain

$$\begin{aligned}
&\delta\big(\rho_{S_{1-D}F_{1-D}\Theta F_D D S_D \tilde{\mathsf{R}}}, \mathbb{1} \otimes \rho_{F_{1-D}\Theta F_D D S_D \tilde{\mathsf{R}}}\big) \\
&\quad \le \frac{1}{2} 2^{-\frac{1}{2}\left(\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X_{1-D}|\Theta S_D F_D D)-\gamma n-\ell\right)} + (\varepsilon+\varepsilon') \\
&\quad \le \frac{1}{2} 2^{-\frac{1}{2}\kappa n} + \varepsilon + \varepsilon',
\end{aligned}$$

which is negligible. This shows ε-sender-security according to Definition 6.1. □

6.4 Extensions

6.4.1 *1-2 OT*$^\ell$ with Longer Strings

It is possible to extend recent techniques by Wullschleger [Wul07] described in Section 3.4.3 to the quantum case and hence, the security of RAND 1-2 QOT$^\ell$ can be proven against $\mathfrak{R}_\gamma$ if there exists $\delta > 0$ such that $\gamma n \le n/4 - \ell - \delta n$.

6.4.2 Weakening the Assumptions

As described in Section 5.6 for *Rabin OT*, we can extend protocol RAND 1-2 QOT to work in the (ϕ, η)-weak quantum model. To enable the receiver to recover from errors in the transmission, the sender S additionally sends error-correcting information in Step 3. The players agree beforehand on an efficiently decodable error-correcting code of length $n/2$ with syndrome length s roughly $h(\phi)n/2$ as in Section 5.6. Then, S sends along the two syndromes of $S(x|_{I_0})$ and $S(x|_{I_1})$ (where the $x|_{I_b}$ are padded with 0s or truncated to length $n/2$). It can be argued as for *Rabin OT* that this will reduce the min-entropy by the length s of the syndrome and hence, we can show sender-security of this protocol against the class of receivers $\mathfrak{R}_\gamma$ with γ such that there exists $\delta > 0$ with

$$\gamma n \le \left(\frac{1-\eta}{4} - \frac{h(\phi)}{2}\right) n - 2\ell - \delta n\,.$$

6.4.3 Reversing the Quantum Communication

In order to illustrate the versatility of our security analysis, we show that the proofs carry easily over to a protocol where the direction of the quantum communication is reversed. In the protocol described in Figure 6.3, the receiver R of the *Rand 1-2 OT* sends n qubits, encoded in the basis determined by his choice bit. The sender of the *Rand 1-2 OT* S measures them in a random basis. The players then proceed as in RAND 1-2 QOT.

It is clear by construction that the protocol is perfectly correct. ε-Sender-security against dishonest receivers in $\mathfrak{R}_\gamma$ can be argued as in Theorem 6.4 above by observing that the uncertainty relation applies to any n-qubit state of the honest sender which is measured in a random basis and about which the dishonest receiver holds at most γn qubits of information.

For the security of an honest receiver against a dishonest sender, we can show the existence of the two input strings as in Proposition 6.2 above by

RAND 1-2 QOT $^\ell$**:** Let c be R's choice bit.

1. R picks $x' \in \{0,1\}^n$ at random and sends $|x'\rangle_{\theta'}$ to R where $\theta' = [+,\times]_c$.
2. S picks $\theta \in_R \{+,\times\}^n$ and measures the received qubits in basis θ. Let $x \in \{0,1\}^n$ be the result.
3. S picks two hash functions $f_0, f_1 \in_R \mathcal{F}_n$, announces θ and f_0, f_1 to R, and outputs $s_0 := f_0(x|^{\circ}_{I_0})$ and $s_1 := f_1(x|^{\circ}_{I_1})$ where $I_b := \{i : \theta_i = [+,\times]_b\}$.
4. R outputs $s_c = f_c(x'|^{\circ}_{I_c})$.

Figure 6.3: RAND 1-2 QOT $^\ell$ with Reversed Quantum Communication.

letting the sender interact with an unbounded receiver. In an error-free model, it further holds that the sender cannot infer the basis in which the qubits are encoded and therefore does not learn any information about the receiver's choice bit. However, in a more realistic setting with multi-pulse emissions, this coding scheme with reversed communication is highly insecure, as a malicious sender can determine the encoding basis from a multi-pulse qubit. The same problem occurred for the *Rabin OT*-protocol QOT from the last chapter.

Chapter 7

Quantum Bit Commitment

This chapter is about quantum Bit Commitment (*BC*) schemes. In *BC*, a committer C commits himself to a choice of a bit $b \in \{0,1\}$ 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 choose 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 the next 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. Therefore, there is no way for the verifier to get information about the committed bit, i.e. the scheme is perfectly hiding.

In Section 7.3, we define two notions of the binding property and show our scheme secure against quantum-memory-bounded committer in both of these senses. Similar techniques as in the two previous chapters for the analysis of the oblivious-transfer protocols are used.

The results in this chapter appeared in [DFSS05, DFR$^+$07].

7.1 The Protocol

The protocol is given in Figure 7.1. Intuitively, a commitment to a bit b is made by measuring random BB84-states in basis $\{+,\times\}_{[b]}$.

As for the oblivious-transfer protocols in the two previous chapters, we present an equivalent EPR-version of the protocol that is easier to analyze (see Figure 7.2).

Lemma 7.1 COMM *is secure against dishonest committers* $\tilde{\mathsf{C}}$ *if and only if* EPR-COMM *is.*

Proof: The proof uses similar reasoning as the one for Lemma 5.3. First, it clearly makes no difference, if we change Step 4 to the following:

4'. 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.

COMM(b):

1. V picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$ and sends x_i in the corresponding bases $|x_1\rangle_{\theta_1}, |x_2\rangle_{\theta_2}, \ldots, |x_n\rangle_{\theta_n}$ to C.
2. C commits to the bit b by measuring all qubits in basis $\{+,\times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
3. To open the commitment, C sends b and x' to V.
4. V verifies that $x_i = x'_i$ for those i where $\theta_i = \{+,\times\}_{[b]}$. V accepts if and only if this is the case.

Figure 7.1: Protocol for quantum bit commitment

EPR-COMM(b):

1. V prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. V sends one half of each pair to C and keeps the other halves.
2. C commits to the bit b by measuring all received qubits in basis $\{+,\times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
3. To open the commitment, C sends b and x' to V.
4. 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 7.2: Protocol for EPR-based quantum bit commitment

Finally, we can observe that the view of $\tilde{\mathsf{C}}$ 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 $\tilde{\mathsf{C}}$ 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 $\tilde{\mathsf{C}}$'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 7.2 EPR-COMM *is perfectly hiding.*

7.2 Modeling Dishonest Committers

A dishonest committer $\tilde{\mathsf{C}}$ with bounded memory of at most γn qubits in EPR-COMM can be modeled very similarly to the dishonest oblivious-transfer receivers $\tilde{\mathsf{R}}$ from Section 5.3 and 6.3: $\tilde{\mathsf{C}}$ 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 $\tilde{\mathsf{C}}$ 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 7.3 *We define $\mathfrak{C}_\gamma$ to be the class of all committers $\{\tilde{\mathsf{C}}_n\}_{n>0}$ in* COMM *or* EPR-COMM *that, at the start of the opening phase (i.e. at Step 3), have a quantum memory of size at most γn qubits.*

7.3 Defining the Binding Property

7.3.1 The "Standard" Binding Condition

In the context of unconditionally secure *quantum* bit commitment, it is widely accepted that "the right way" of defining the *binding property* is to require that the probability of opening a commitment successfully to 0 plus the probability of opening it successfully to 1 is essentially upper bounded by one, put forward by Dumais, Mayers, and Salvail [DMS00]. We call this notion *weakly binding*, as opposed to the new notion of *strongly binding* defined in the next section below.

Definition 7.4 *A (quantum) bit-commitment scheme is* weakly binding *against $\mathfrak{C}$ if for all $\{\tilde{\mathsf{C}}_n\}_{n>0} \in \mathfrak{C}$, the probability $p_b(n)$ that $\tilde{\mathsf{C}}_n$ opens $b \in \{0,1\}$ with success satisfies*

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

In the next Section 7.4, we show that EPR-COMM is weakly binding against $\mathfrak{C}_\gamma$ for any $\gamma < \frac{1}{2}$.

Note that the binding condition given here in Definition 7.4 is weaker than the classical one, where one would require that a bit b exists such that $p_b(n)$ is negligible. For a general quantum adversary though who can always commit to 0 and 1 in superposition, this is a too strong requirement; thus, it is typically argued that Definition 7.4 is the best one can hope for.

However, we argue now that this weaker notion is not really satisfactory, and we show that there exists a stronger notion, which still allows the committer to commit to a superposition and thus is not necessarily impossible to achieve in a quantum setting, but which is closer to the classical standard way of defining the binding property.

7.3.2 A Stronger Binding Condition

A shortcoming of Definition 7.4 is that committing bit by bit is not guaranteed to yield a secure string commitment—the argument that one is tempted to use requires independence of the p_b's between the different executions, which in general does not hold.

We now argue that this notion is *unnecessarily* weak, at least in some cases, and in particular in the case of commitments in the bounded-quantum-storage model where the dishonest committer is forced to do some partial measurement and where we assume honest parties to produce only classical output (by measuring their entire quantum state). Technically, this means that for any dishonest committer $\tilde{\mathsf{C}}$, the joint state of the honest verifier and of $\tilde{\mathsf{C}}$ after the commit phase is a ccq-state $\rho_{VZ\tilde{\mathsf{C}}} = \sum_{v,z} P_{VZ}(v,z)|v\rangle\langle v| \otimes |z\rangle\langle z| \otimes \rho_{\tilde{\mathsf{C}}}^{v,z}$, where the first register contains the verifier's (classical) output and the remaining two registers contain $\tilde{\mathsf{C}}$'s (partially classical) output. We propose the following definition.

Definition 7.5 *A commitment scheme in the bounded-quantum-storage model is called* ε-binding, *if for every (dishonest) committer* $\tilde{\mathsf{C}}$, *inducing a joint state* $\rho_{VZ\tilde{\mathsf{C}}}$ *after the commit phase, there exists a classical binary random variable* D, *given by its conditional distribution* $P_{D|VZ}$, *such that for* $b = 0$ *and* $b = 1$ *the state* $\rho^b_{VZ\tilde{\mathsf{C}}} = \sum_v P_{VZ|D}(v,z|b)|v\rangle\langle v| \otimes |z\rangle\langle z| \otimes \rho_{\tilde{\mathsf{C}}}^{v,z}$ *satisfies the following condition. When executing the opening phase on the state* $\rho^b_{V\tilde{\mathsf{C}}}$, *for any strategy of* $\tilde{\mathsf{C}}$, *the honest verifier accepts an opening to* $1-b$ *with probability at most* ε.

It is easy to see that the binding property as defined here implies the above discussed weak version, namely $p_b \leq P_D(b) + P_D(1-b)\varepsilon$ and thus $p_0 + p_1 \leq 1+\varepsilon$. Furthermore, it is straightforward to see that this stronger notion allows for a formal proof of the obvious reduction of a string to a bit commitment by committing bit-wise: the i-th execution of the bit commitment scheme guarantees a random variable D_i, defined by $P_{D_i|V_iZ}$, such that the committer cannot open the i-th bit commitment to $1-D_i$, and thus there exists a random variable S, namely $S = (D_1, \ldots, D_m)$ defined by $P_{D_1 \cdots D_m|V_1 \cdots V_m Z} = \prod_i P_{D_i|V_iZ}$, such that for any opening strategy, the committer cannot open the list of commitments to any other string than S.

In Section 7.5, we show that the bit commitment COMM from Figure 7.1 as a matter of fact satisfies this stronger and more useful notion of security. This turns out to be a rather straightforward consequence of the security of the *1-2 OT* scheme from Chapter 6.

7.4 Weak Binding of the Commitment Scheme

In this section, we use the techniques from the analysis of the *Rabin OT* protocol from Chapter 5 to prove our commitment scheme COMM (or rather its purified version EPR-COMM) weakly binding against quantum-memory-bounded adversarial committers.

Note that the first two steps of EPR-QOT (from Figure 5.2) and EPR-COMM (i.e. before the memory bound applies) are exactly the same! This allows us to reuse Corollary 4.17 and the analysis of Section 5.4 to prove the weakly binding property of EPR-COMM.

Theorem 7.6 *For any* $\gamma < \frac{1}{2}$, COMM *is perfectly hiding and weakly 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 weak binding property then follows immediately from Corollary 4.17. 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 the +-basis has 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 $\varepsilon, \delta > 0$ be such that $\gamma+2h(\delta)+2\varepsilon < 1/2$, where h is the binary entropy function. Recall that the number $\mathrm{B}^{\delta n}$ of n-bit strings of Hamming-distance at most δn from a fixed string is at most $2^{h(\delta)n}$. Let R be the basis, determined by the bit that $\tilde{\mathsf{C}}$ claims in Step 3, and in which V measures the quantum state in Step 4, and let X be the outcome. Corollary 4.17 implies the existence of an event $\mathcal{E}$ such that $P[\mathcal{E}|R{=}+]+P[\mathcal{E}|R{=}\times] \geq 1-negl(n)$ and $\mathrm{H}_\infty(X|R{=}r,\mathcal{E}) \geq (\gamma+2h(\delta)+2\varepsilon)n$. Applying Corollary 2.26 (with constant U and $\varepsilon = 0$), it follows that any guess $\hat{X}$ for X satisfies

$$P\big[\hat{X} \in \mathrm{B}^{\delta n}(X) \,|\, R{=}r, \mathcal{E}\big] \leq 2^{-\frac{1}{2}(\mathrm{H}_\infty(X|X\in S^+)-\gamma n-1)+\log(\mathrm{B}^{\delta n})} \leq 2^{-\varepsilon n+\frac{1}{2}}.$$

However, if $\hat{X} \notin \mathrm{B}^{\delta n}(X)$ then sampling a random subset of the positions will detect an error except with probability at most $2^{-\delta n}$. Hence, writing $q^+ := P[\mathcal{E}|R{=}+]$ and $q^\times := P[\mathcal{E}|R{=}\times]$,

$$p_0(n) \leq (1-q^+) + q^+ \cdot (2^{-\varepsilon n+\frac{1}{2}} + 2^{-\delta n}) \leq 1 - q^+ + negl(n)$$

and analogously $p_1(n) \leq 1 - q^\times + negl(n)$. We conclude that

$$p_0(n) + p_1(n) \leq 2 - q^+ - q^\times + negl(n) \leq 1 + negl(n)\,.$$

□

7.5 Strong Binding of the Commitment Scheme

In this section, we reuse the analysis of the *1-2 OT*-protocol from Chapter 6 to prove the strong binding condition.

Theorem 7.7 *The quantum bit-commitment scheme* COMM *is ε-binding according to Definition 7.5 against $\mathfrak{C}_\gamma$ for a negligible (in n) ε if $\gamma < \frac{1}{4}$.*

Intuitively, one can argue that X has (smooth) min-entropy about $n/2$ given Θ. The Min-Entropy Splitting Lemma implies that there exists D such that X_{1-D} has smooth min-entropy about $n/4$ given Θ and D. Privacy amplification implies that $F(X_{1-D})$ is close to random given Θ, D, F and $\tilde{\mathsf{C}}$'s quantum register of size γn, where F is a two-universal one-bit-output hash function, which in particular implies that $\tilde{\mathsf{C}}$ cannot guess X_{1-D}. The formal proof is given below.

Proof: It remains to show that EPR-COMM is strongly binding against $\mathfrak{C}_\gamma$. Let $\Theta \in \{+,\times\}^n$ be the random basis that would correspond to the choice of basis in the first step of COMM, i.e. $\theta_i = \{+,\times\}_{[b]}$ for $i \in I$ and $\theta_i = \{+,\times\}_{[1-b]}$ for

$i \notin I$. Let X be the measurement outcome when V measures his halves of the EPR-pairs in basis Θ.

Recall that $h(\cdot)$ denotes the binary Shannon entropy. Choose $\lambda, \lambda', \kappa$ and δ all positive, but small enough such that $\gamma \leq 1/4 - \lambda - \lambda' - 2h(\delta) - 2\kappa$, $h(\delta) \leq \lambda' - \kappa$, and $h(\delta) \leq \frac{\lambda^4}{32} - \kappa$. Before Step 3, the overall state is given by the ccq-state $\rho_{X\Theta\tilde{\mathsf{C}}}$ after $\tilde{\mathsf{C}}$ has measured all but γn of his qubits, where X describes the outcome of the verifier V measuring his part of the state in random basis Θ. From the uncertainty relation (Corollary 4.23), we know that $\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \geq (1/2 - 2\lambda)n$ for $\varepsilon = 2^{-\frac{\lambda^4}{32}n}$ exponentially small in n. Therefore, by Corollary 2.16, there exists a binary random variable $D \in \{0,1\}$ such that for $\varepsilon' = 2^{-\lambda' n}$, it holds that

$$\begin{aligned}\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X_{1-D} \mid \Theta D) &\geq (1/4 - \lambda - \lambda')n - 1\\ &\geq (1/4 - \lambda - \lambda')n - 1\\ &\geq \gamma n + 2h(\delta)n + 2\kappa n - 1\,.\end{aligned}$$

Recall that $\mathrm{B}^{\delta n} \leq 2^{h(\delta)n}$. Applying Corollary 2.26, it follows that any guess $\hat{X}$ for X_{1-D} satisfies

$$\begin{aligned}P\big[\hat{X} \in \mathrm{B}^{\delta n}(X_{1-D})\big] &\leq 2^{-\frac{1}{2}(\mathrm{H}_\infty^{\varepsilon+\varepsilon'}(X_{1-D}|\Theta D) - \gamma n - 1) + \log(\mathrm{B}^{\delta n})} + (2\varepsilon + 2\varepsilon')\mathrm{B}^{\delta n}\\ &\leq 2^{-\frac{1}{2}(2\kappa n - 2)} + 2 \cdot 2^{-\frac{\lambda^4}{32}n + h(\delta)n} + 2 \cdot 2^{-\lambda' n + h(\delta)n}\\ &\leq \frac{1}{2}2^{-\kappa n} + 2 \cdot 2^{-\kappa n} + 2 \cdot 2^{-\kappa n}\,,\end{aligned}$$

which is negligible by the choice of the parameters. □

7.6 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 5.6 (see also Section 9.1.1), with $\phi < \frac{1}{2}$ and $\eta < 1 - \phi$.

The protocol COMM' in Figure 7.3 is the same as COMM from Figure 7.1 except that in the last Step 4, 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 7.8 *In the (ϕ, η)-weak quantum model,* COMM' *is perfectly hiding and it is weakly binding against $\mathfrak{C}_\gamma$ for any γ satisfying $\gamma < \frac{1}{2}(1 - \eta) - 2h(\phi)$.*

Proof Sketch: Using Chernoff's inequality (Lemma 2.5), 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 7.2. And the binding property can be argued essentially along

COMM'(b, ϕ):

1. V picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$ and sends x_i in the corresponding bases $|x_1\rangle_{\theta_1}, |x_2\rangle_{\theta_2}, \ldots, |x_n\rangle_{\theta_n}$ to C.
2. C commits to the bit b by measuring all qubits in basis $\{+,\times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
3. To open the commitment, C sends b and x' to V.
4. V verifies that $x_i = x'_i$ for i where $\theta_i = \{+,\times\}_{[b]}$. V accepts if and only if this is the case *for all but a ϕ-fraction of these positions.*

Figure 7.3: Protocol for noise-tolerant quantum bit commitment

the lines of Theorem 7.6, 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 Chernoff's inequality (Lemma 2.5), 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 $\tilde{\mathsf{C}}$ 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. Using Corollary 2.26, we can show that for a correctly chosen $\delta > 0$, the probability of guessing $\hat{X}$ within Hamming distance δn to the real X is negligible. Therefore, $\tilde{\mathsf{C}}$ succeeds with only negligible probability if the fraction of allowed errors $\phi/(1-\eta)$ is smaller than δ, i.e.

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

Additionally, in order for the machinery from Theorem 7.6 to work, δ must be such that

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

δ can be chosen that way if

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

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 $\gamma + 2h(\phi) < \frac{1}{2}(1-\eta)$. □

Theorem 7.9 *In the (ϕ,η)-weak quantum model,* COMM' *is perfectly hiding and it is strongly binding against $\mathfrak{C}_\gamma$ for any γ satisfying $\gamma < \frac{1}{4}(1-\eta) - 3h(\phi) - \sqrt[4]{32\,h(\phi)}$.*

Proof Sketch: The proof goes like the proof of Theorem 7.8, but uses the techniques from Section 7.5. In order for those to work, we need to choose

λ, λ', and δ all positive and such that

$$\begin{aligned} \frac{\phi}{1-\eta} &< \delta, \\ \frac{\gamma}{1-\eta} + 2h(\delta) + \lambda' + \lambda &< 1/4\,, \\ h(\delta) &< \lambda'\,, \\ h(\delta) &< \frac{\lambda^4}{32}\,. \end{aligned} \tag{7.1}$$

We verify that the assumption $\gamma < \frac{1}{4}(1-\eta) - 3h(\phi) - \sqrt[4]{32\,h(\phi)}$ on γ allows for that. Rearranging the terms and using that $x < \sqrt[4]{x}$ for $0 < x < 1$ yields

$$\frac{\gamma}{1-\eta} + 3\frac{h(\phi)}{1-\eta} + \sqrt[4]{32\frac{h(\phi)}{1-\eta}} < 1/4\,.$$

Using as in the previous proof 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 $\nu p \leq 1$, we get that

$$\frac{\gamma}{1-\eta} + 3h\left(\frac{\phi}{1-\eta}\right) + \sqrt[4]{32\,h\left(\frac{\phi}{1-\eta}\right)} < 1/4.$$

That allows to choose $\delta > \frac{\phi}{1-\eta}$ such that

$$\frac{\gamma}{1-\eta} + 2h(\delta) + h(\delta) + \sqrt[4]{32\,h(\delta)} < 1/4,$$

and therefore, also λ and λ' can be chosen such that the conditions (7.1) are fulfilled. $\square$

Chapter 8

QKD Secure Against Quantum-Memory-Bounded Eavesdroppers

In this chapter, we present another application for the uncertainty relation derived in Section 4.5. This illustrates that these relations are useful in scenarios beyond the simple two-party setting.

In Quantum Key Distribution (*QKD*), two honest players Alice and Bob want to agree on a secure key, using only completely insecure quantum and authentic classical communication. The computationally unbounded eavesdropper Eve should not get any information about the key. A major difficulty when implementing *QKD* schemes is that they require a low-noise quantum channel. The tolerated noise level depends on the actual protocol and on the desired security of the key. Because the quality of the channel typically decreases with its length, the maximum tolerated noise level is an important parameter limiting the maximum distance between Alice and Bob.

We consider a model in which the adversary has a limited amount of quantum memory to store the information she intercepts during the protocol execution. In this model, we show that the maximum tolerated noise level is larger than in the standard scenario where the adversary has unlimited resources.

For simplicity, we restrict ourselves to *one-way QKD protocols* which are protocols where error-correction is performed non-interactively, i.e., a single classical message is sent from one party to the other.

The results in this chapter appeared in [DFR$^+$07].

8.1 Derivation of the Maximum Tolerated Noise Level

Let $\mathcal{S}$ be a set of orthonormal bases of a d-dimensional Hilbert space $\mathcal{H}_d$. For each basis $\vartheta \in \mathcal{S}$, we assume that the d basis vectors are parametrized by the elements of the fixed set $\mathcal{X}$ of size $|\mathcal{X}| = d$. We then consider *QKD* protocols consisting of the steps described in Figure 8.1.

Note that the quantum channel is only used in the preparation step. Afterwards, the communication between Alice and Bob is only classical (over an

One-Way *QKD*: let $N \in \mathbb{N}$ be arbitrary

1. *Preparation:* For $i = 1 \dots N$, Alice chooses at random a basis $\vartheta_i \in \mathcal{S}$ and a random element $X_i \in \mathcal{X}$. She encodes X_i into the state of a quantum system according to the basis ϑ_i and sends this system to Bob. Bob measures each of the states he receives according to a randomly chosen basis ϑ'_i and stores the outcome $Y_i \in \mathcal{X}$ of this measurement.
2. *Sifting:* Alice and Bob publicly announce their choices of bases and keep their data at position i only if $\vartheta_i = \vartheta'_i$. In the following, we denote by X and Y the concatenation of the remaining data X_i and Y_i, respectively. X and Y are sometimes called the *sifted raw key*.
3. *Error correction:* Alice computes some error correction information C depending on X and sends C to Bob. Bob computes a guess $\hat{X}$ for Alice's string X, using C and Y.
4. *Privacy amplification:* Alice chooses at random a function f from a two-universal family of hash functions and announces f to Bob. Alice and Bob then compute the final key by applying f to their strings X and $\hat{X}$, respectively.

Figure 8.1: General form for *one-way QKD* protocols.

authentic channel).

As shown in [Ren05, Lemma 6.4.1], the length ℓ of the secret key that can be generated by the protocol described above is given by[1]

$$\ell \approx \mathrm{H}^{\varepsilon}_{\min}(\rho_{XE} \mid E) - \mathrm{H}_0(C)\,,$$

where the cq-state ρ_{XE} is the state of the quantum system with the property that E contains all the information Eve has gained during the preparation step of the protocol and where $\mathrm{H}_0(C)$ is the number of error correction bits sent from Alice to Bob. Note that this formula can be seen as a generalization of the well-known expression by Csiszár and Körner for classical key agreement [CK78].

Let us now assume that Eve's system E can be decomposed into a classical part U and a purely quantum part E'. Then, by the same derivation as in the proof of Corollary 2.25, we find

$$\ell \approx \mathrm{H}^{\varepsilon}_{\min}(\rho_{XUE'} \mid UE') - \mathrm{H}_0(C) \geq \mathrm{H}^{\varepsilon}_{\infty}(X \mid U) - \mathrm{H}_{\max}(\rho_{E'}) - \mathrm{H}_0(C)\ .$$

As, during the preparation step, Eve does not know the encoding bases which are chosen at random from the set $\mathcal{S}$, we can apply our uncertainty relation (Theorem 4.22) to get a lower bound for the min-entropy of X conditioned on

[1] The approximation in this and the following equations holds up to some small additive value which depends logarithmically on the desired security ε of the final key.

Eve's classical information Θ, i.e.,

$$\mathrm{H}_\infty^\varepsilon(X \mid \Theta) \geq Mh,$$

where M denotes the length of the sifted raw key X and h is the average entropic uncertainty bound for $\mathcal{S}$. [write much more!] Let q be the bound on the size of Eve's quantum memory $\mathrm{H}_{\max}(\rho_{E'}) \leq q$. Moreover, let e be the average amount of error correction information that Alice has to send to Bob per symbol of the sifted raw key X. Then

$$\ell \gtrapprox M(h - e) - q \ .$$

Hence, if the memory bound only grows sublinearly in the length M of the sifted raw key, then the *key rate*, i.e., the number of key bits generated per bit of the sifted raw key, is lower bounded by

$$\text{rate} \geq h - e \ .$$

8.2 The Binary-Channel Setting

For a binary channel (with a two-dimensional Hilbert space $\mathcal{H}_2$), the average amount of error correction information e is given by the binary Shannon entropy[2] $h(p)$, where p is the bit-flip probability (for classical bits encoded according to some orthonormal basis as described above). The achievable key rate of a *QKD* protocol using a binary quantum channel is thus given by

$$\text{rate}_{\text{binary}} \geq h - h(p) \ .$$

Summing up, we have derived the following theorem.

Theorem 8.1 *Let $\mathcal{S}$ be a set of orthonormal bases of $\mathcal{H}_2$ with average entropic uncertainty bound h. Then, a* one-way *QKD protocol as in Figure 8.1 produces a secure key against eavesdroppers whose quantum-memory size is sublinear in the length of the raw key (i.e., sublinear in the number of qubits sent from Alice to Bob) at a positive rate as long as the bit-flip probability p fulfills*

$$h(p) < h \ . \tag{8.1}$$

For the BB84 protocol [BB84], we have $h = \frac{1}{2}$ (cf. Inequality (4.2)). Inequality (8.1) is thus satisfied as long as $p \leq 11\%$. This bound coincides with the known bound for one-way *QKD* in the standard model (with an unbounded eavesdropper). So, using our analysis here, the memory-bound does not give an advantage.

The situation is different for the six-state protocol where $h = \frac{2}{3}$. According to (8.1), security against memory-bounded adversaries is guaranteed (i.e. $h(p) < \frac{2}{3}$) as long as $p \leq 17\%$. If one requires security against an unbounded adversary, the threshold for the same protocol lies below 13% as

[2] This value of e is only achieved if an optimal error-correction scheme is used. In practical implementations, the value of e might be slightly larger.

shown by Lo [Lo01], and even the best known QKD protocol on binary channels with one-way classical post-processing can only tolerate noise up to roughly 14.1% [RGK05]. It has also been shown that, in the unbounded model, no such protocol can tolerate an error rate of more than 16.3%.

The performance of *QKD* protocols against quantum-memory bounded eavesdroppers can be improved further by making the choice of the encoding bases more random. For example, they might be chosen from the set of all possible orthonormal bases on a two-dimensional Hilbert space. As shown in Section 4.5.3, the overall average entropic uncertainty bound is then given by $h \approx 0.72$ and (8.1) is satisfied if $p \lessapprox 20\%$. For an unbounded adversary, the thresholds are the same as for the six-state protocol (i.e., 14.1% for the best known one-way protocol).

8.3 Possible Extensions

It is an interesting open problem to consider protocols using higher-dimensional quantum systems. The results described in Section 4.5.3 show that for high-dimensional systems, the average entropic uncertainty bound converges to its theoretical maximum. The maximal tolerated channel noise might thus be higher for such protocols (depending on the noise model for higher-dimensional quantum channels).

Another interesting problem is to derive completely one-way quantum-key-distribution schemes, i.e. to eliminate the interactive sifting phase from the protocol in Figure 8.1. The idea is to let the honest parties use a pre-shared secret key to determine the bases of the encoding. If a key of size linear in the number of qubits is used, the scheme has to guarantee that a big portion of the key can be reused several times in order to yield a reasonable amount of fresh key. Quantifying the amount of information an eavesdropper can learn about the pre-shared key by interfering in the preparation step and eavesdropping on the following classical communication is an open problem.

Another approach consists of expanding a pre-shared key of size only logarithmic in the number of qubits into a pseudo-random linear-size key to determine the bases of the encoding. It is an open question how to extend our uncertainty relation from Section 4.5 to the case of only pseudo-random bases.

Chapter 9

Conclusion

9.1 Towards Practice

In the following two sections, we elaborate on the question how close to practice our systems are. First, we argue that imperfections occurring in practice like *dark counts* and *empty pulses* are covered by our (ϕ, η)-weak quantum model used in Sections 5.6, 6.4.2, and 7.6. Second, we sketch how our techniques can be extended to the more realistic setting of *noisy quantum memory.*

9.1.1 More Imperfections

A natural approach for implementing two-party protocols like BB84-QOT, RAND 1-2 QOT $^{\ell}$, and COMM is to use the polarization of photons governed by the laws of quantum optics. Such systems are nowadays at the stage where they can be built in a optical physics lab. Besides the already modeled bit errors and multi-pulse emissions, more imperfections of the physical apparatus such as *empty pulses* and *dark counts* need to be taken into account.

The players have synchronized clocks and in every predefined time slot, the sender is supposed to send out a single qubit. In practice, weak coherent pulses are used to approximate single-photon sources by producing in average only a small fraction of one qubit per pulse. This means that most of the pulses are *empty*, but on the other hand, there is also a small probability for a multi-qubit pulse. The receiver reports to the sender in which time slots he received pulses.

Empty pulses also occur when the quantum channel lets a transmitted qubit escape or when it is absorbed. It is realistic that a good estimate on the rate at which empty pulses are produced (when no adversary is present) is known, e.g., from the hardware specifications and by measuring and calibrating the experimental setup. In this case, the adversary can only take advantage of empty pulses caused by absorption in the fiber. The best the adversary can do is to substitute the fiber for one that preserves all qubits sent and to report empty pulses when a single pulse has been received. The effect is to increase the rate at which multi-qubit pulses occur. This attack is known as *Photon-Number-Splitting attack* as first noted by Huttner, Imoto, Gisin, and Mor [HIGM95] and for instance explained in [BLMS00a, BLMS00b] in the setting of quantum key distribution. It follows that empty pulses can also be included in the (ϕ, η)-weak quantum model by an appropriate adjustment of parameter η.

Furthermore, thermal fluctuation in the detector hardware might result in detection even though no qubit was received. This is called a *dark count*. In this time slot, the receiver will report the reception of a qubit and as the outcome is random, it agrees with the actual bit sent with probability $\frac{1}{2}$.

Formally, assume that a practical implementation of BB84-QOT, RAND 1-2 QOT $^\ell$, or COMM takes place in a setting where ϕ_X is the probability for a bit error caused by the channel, ϕ_DC is the probability for a dark count in a specific time slot, η_MQ is the probability for a multi-qubit transmission in a non-empty pulse, and η_AB is the probability for an empty pulse caused by absorption of a non-empty pulse. In these terms, dark counts contribute $\frac{\phi_\mathrm{DC}}{2}$ to the bit-error rate ϕ_X. If the adversary is able to get perfect transmission, she can suppress single-qubit pulses up to a rate of η_AB, thereby increasing the rate η_MQ of multi-photon pulses by $\frac{1}{1-\eta_\mathrm{AB}}$. It follows that if BB84-QOT, COMM, and RAND 1-2 QOT $^\ell$ are secure in the $(\phi_\mathrm{X} + \frac{\phi_\mathrm{DC}}{2}, \frac{\eta_\mathrm{MQ}}{1-\eta_\mathrm{AB}})$-weak quantum model, then their implementation is also secure, provided it is accurately modeled by these four parameters.

Likewise, a variety of imperfections specific to particular implementations may be adapted to the weak quantum model.

9.1.2 Generalizing the Memory Model

The bounded-quantum-storage model limits the number of physical qubits the adversary's memory can contain. A more realistic model would rather address the noise process the adversary's memory undergoes. For instance, it is not hard to build a very large, but unreliable memory device containing a large number of qubits. It is reasonable to expect that our protocols remain secure also in a scenario where the adversary's memory is of arbitrary size, but where some quantum operation (modeling noise) applies to it. If we do not substitute $\mathrm{H}_{\max}(\rho_E)$ with the number of qubits q in Term (2.6) in the privacy-amplification Section 2.5, then our constructions can cope with slightly more general memory models. In particular, all our protocols that are secure against adversaries with memory of no more than γn qubits are also secure against any noise model that reduces the rank $\mathrm{H}_{\max}(\rho_E)$ of the mixed state ρ_E held by the adversary to at most $2^{\gamma n}$.

An example of a noise process resulting in a reduction of $\mathrm{H}_{\max}(\rho_E)$ is an erasure channel. Assuming the n initial qubits are each erased with probability larger than $1-\gamma$ when the memory bound applies, it holds except with negligible probability in n that $\mathrm{H}_{\max}(\rho_E) < \gamma n$. The same applies if the noise process is modeled by a depolarizing channel with error probability $p = 1 - \gamma$. Such a depolarizing channel replaces each qubit by a random one with probability p and does nothing with probability $1 - p$.

The technique we have developed does not allow to deal with depolarizing channels with $p < 1 - \gamma$ although one would expect that some $0 < p < 1 - \gamma$ should be sufficient to ensure security against such adversaries. The reason being that not knowing the positions where the errors occurred should make it more difficult for the adversary than when the noise process is modeled by an erasure channel. However, it seems that our uncertainty relations are not strong enough to address this case. Generalizing the bounded-quantum-storage model to more realistic noisy-memory models is an interesting open question.

9.2 Conclusion

The bounded-quantum-storage model presented in this thesis is an attractive model, in both the theoretical and practical sense. On the theoretical side, it allows for very simple protocols implementing basic two-party primitives such as oblivious transfer and bit commitment. New high-order entropic uncertainty relations have been established in order to show the security with the help of techniques such as purification and privacy amplification by two-universal hashing. These uncertainty relations can also be applied in different settings like quantum key distribution.

On the practical side, the protocols do not require any quantum memory for honest players and remain secure provided the adversary has a quantum memory of size bounded by a constant fraction of all transmitted qubits. Such a gap between the amount of storage required for honest players and adversaries is not achievable by classical means. The protocols can be adapted to tolerate various kinds of errors and in fact, they can be implemented with today's technology. A collaboration of people from the computer science and physics departments of the University of Aarhus is currently working on the implementation of these protocols[1].

In summary, one can say that the bounded-quantum-storage model has passed its first tests by proving its power (the possibility of oblivious transfer) and by inspiring beautiful theoretical results (quantum uncertainty relations). It is a good sign that the protocols for the basic primitives are simple in structure. In principle, enough instances of these protocols could be used to implement more involved cryptographic tasks like secure identification, which reduces essentially to securely checking whether two inputs are equal (without revealing more than this mere bit of information). However, it is a natural next step to find more efficient, direct protocols for those tasks, secure in the bounded-quantum-storage model. Such a direct approach gives a better ratio between storage-bound and communication-complexity and is the topic of a recent paper [DFSS07].

A major open problem is the optimality of the bounds on the adversary's quantum memory. The bit-commitment protocol COMM for instance appears to be secure against any adversary with memory less than n qubits, but our analysis requires the memory to be smaller than $n/2$ (or $n/4$ for strong binding). Also, finding protocols secure against adversaries in more general noisy-memory models, as discussed in the last Section 9.1.2, would certainly be a natural and interesting extension of this work to more practical settings [DSTW07]. Furthermore, there is still a lack of simple and intuitive security definitions for

[1] See `http://www.brics.dk/~salvail/qusep.html` for further information on the QUSEP project.

primitives like *1-2 OT* etc. with rigorous composability results (like universal composability) in the quantum setting. Very recent results in this direction have been established in [WW07].

Notation

General

log	binary logarithm
ln	natural logarithm
$\mathbb{N}$	natural numbers: $1, 2, 3, \ldots$
$\mathbb{R}$	real numbers
$[a, b]$	set of real numbers r such that $a \leq r \leq b$
$(a, b]$	set of real numbers r such that $a < r \leq b$
$x\|_I$	substring of x consisting of bit positions in index set I
$x\|_I^\circ$	as above, padded with 0s
$\mathrm{B}^{\delta n}(x)$	set of n-bit strings with Hamming distance at most δn from x $negl(n)$
$negl(n)$	any function in n smaller than the inverse of any polynomial for large enough n
$[+, \times]_b$	$+$ for $b = 0$ and $\times$ for $b = 1$
$\delta_{i,j}$	Kronecker delta

Classical Information Theory

$P_{X\|Y}$	conditional probability distribution of X given Y
$\mathbb{E}[R]$	expected value of the real random variable R
$\delta(P, Q)$	variational distance between distributions P and Q
$P \approx_\varepsilon Q$	P and Q are at variational distance at most ε
UNIF	independent and uniformly distributed binary random variable
UNIF^ℓ	ℓ copies of it
$\mathcal{E}$	event
$\mathbb{1}_\mathcal{E}$	indicator random variable of event $\mathcal{E}$
$X \leftrightarrow Z \leftrightarrow Y$	Markov chain

Quantum Information Theory

$\mathcal{H}_d$	Hilbert space of dimension d
$\mathcal{P}(\mathcal{H})$	set of density operators on $\mathcal{H}$
ρ	density operator: normalized, Hermitian, non-negative
$\mathrm{tr}(\rho)$	trace of ρ
$\mathbb{1}$	fully mixed state
$\delta(\rho, \sigma)$	trace distance between ρ and σ
$\|b\rangle_\theta$	classical bit b encoded in basis θ
ρ_{XE}	cq-state

Entropies	
$h(\cdot)$	binary Shannon entropy function
$\pi_\alpha(X\|Y)$	α-order sum of X given Y with joint distribution P_{XY}
$\mathrm{H}_\alpha(X\|Y)$	Rényi entropy of order α of X given Y
$\mathrm{H}_\infty(X\|Y)$	min-entropy of X given Y
$\mathrm{H}_2(X\|Y)$	collision entropy of X given Y
$\mathrm{H}(X\|Y)$	Shannon entropy of X given Y
$\mathrm{H}_0(X\|Y)$	max-entropy of X given Y
$\tilde{\mathrm{H}}_\alpha(X\|Y)$	average conditional Rényi entropy of order α
$\mathrm{H}^\varepsilon_\alpha(X\|Y)$	ε-smooth Rényi entropy of order α of X given Y
$\mathrm{H}^\varepsilon_\infty(X\|Y)$	ε-smooth min-entropy of X given Y
$\mathrm{H}^\varepsilon_0(X\|Y)$	ε-smooth max-entropy of X given Y
$\mathrm{H}_\alpha(\rho)$	Rényi entropy of order α of the state ρ
$\mathrm{H}_{\min}(\rho_{AB}\|\sigma_B)$	min-entropy of ρ_{AB} relative to σ_B
$\mathrm{H}_{\min}(\rho_{AB}\|B)$	min-entropy of ρ_{AB} given $\mathcal{H}_B$
$\mathrm{H}^\varepsilon_{\min}(\rho_{AB}\|\sigma_B)$	ε-smooth min-entropy of ρ_{AB} relative to σ_B
$\mathrm{H}^\varepsilon_{\min}(\rho_{AB}\|B)$	ε-smooth min-entropy of ρ_{AB} given $\mathcal{H}_B$

Bibliography

[ADR02] Yonatan Aumann, Yan Zong Ding, and Michael O. Rabin. Everlasting security in the bounded storage model. *IEEE Transactions on Information Theory*, 48(6):1668–1680, June 2002.

cited on page 4.

[AS00] Noga Alon and Joel Spencer. *The Probabilistic Method*. Series in Discrete Mathematics and Optimization. Wiley-Interscience, 2nd edition, 2000.

cited on pages 15 and 57.

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

cited on page 62.

[Azu67] Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tôhoku Mathematical Journal*, 19:357–367, 1967.

cited on page 57.

[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.

cited on pages 8, 80, and 101.

[BB06] I. Bialynicki-Birula. Formulation of the uncertainty relations in terms of the Rényi entropies. *Physical Review A*, 74:052101, 2006.

cited on page 62.

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

cited on pages 26 and 29.

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology—CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 1991.

cited on page 10.

[BBM75] I. Bialynicki-Birula and J. Mycielski. Uncertainty relations for information entropy. *Communications in Mathematical Physics*, 129(44), 1975.

cited on page 60.

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

cited on page 26.

[BC97] Gilles Brassard and Claude Crépeau. Oblivious transfers and privacy amplification. In *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*. Springer, 1997.

cited on pages 31, 32, 42, and 43.

[BCJL93] Gilles Brassard, Claude Crépeau, Richard Jozsa, and Denis Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *34th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 362–371, 1993.

cited on page 10.

[BCW03] Gilles Brassard, Claude Crépeau, and Stefan Wolf. Oblivious transfer and privacy amplification. *Journal of Cryptology*, 16(4), 2003.

cited on pages 31, 32, 36, 37, 42, 43, 44, 47, and 48.

[Bea95] Donald Beaver. Precomputing oblivious transfer. In *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 97–109. Springer, 1995.

cited on page 33.

[Bha97] Rajendra Bhatia. *Matrix Analysis.* Graduate Texts in Mathematics. Springer-Verlag, 1997.

cited on page 56.

[BLMS00a] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330–1333, August 2000.

cited on page 103.

[BLMS00b] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Security aspects of practical quantum cryptography. In *Advances in Cryptology—EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 289–299. Springer, 2000.

cited on page 103.

[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`.

cited on page 6.

[BS93] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology—EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer, 1993.

cited on page 80.

[BWW06] Manuel A. Ballester, Stephanie Wehner, and Andreas Winter. State discrimination with post-measurement information, 2006. `http://arxiv.org/abs/quant-ph/0608014`.

cited on page 79.

[Cac97] Christian Cachin. Smooth entropy and Rényi entropy. In *Advances in Cryptology—EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 193–208. Springer, 1997.

cited on page 20.

[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.

cited on pages 31, 32, 42, 44, and 45.

[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.

cited on pages 4 and 42.

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

cited on page 100.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions. In *29th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 42–53, 1988.

cited on pages 3 and 42.

[CM97] Christian Cachin and Ueli M. Maurer. Unconditional security against memory-bounded adversaries. In *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 292–306. Springer, 1997.

cited on page 4.

[CMW04] Claude Crépeau, 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.

cited on pages 3 and 42.

[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.

cited on pages 31 and 42.

[Cré94] Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2455 – 2466, 1994.

cited on page 10.

[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.

cited on page 80.

[CRE04] Matthias Christandl, Renato Renner, and Artur Ekert. A generic security proof for quantum key distribution. http://arxiv.org/abs/quant-ph/0402131, February 2004.

cited on page 26.

[CS06] Claude Crépeau and Georges Savvides. Optimal reductions between oblivious transfers using interactive hashing. In *Advances in Cryptology—EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 201–221. Springer, 2006.

cited on pages 31, 42, 43, and 47.

[CSSW06] Claude Crépeau, George Savvides, Christian Schaffner, and Jürg Wullschleger. Information-theoretic conditions for two-party secure function evaluation. In *Advances in Cryptology—EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 538–554. Springer, 2006.

cited on pages 5, 6, 32, 33, 34, 74, and 84.

[CT91] T.M. Cover and J.A. Thomas. *Elements of Information Theory*. Wiley, 1991.

cited on pages 13 and 22.

[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.

cited on page 27.

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

cited on page 60.

[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.

cited on pages 3 and 42.

[DFR+07] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2007.

cited on pages 4, 55, 74, 83, 91, and 99.

[DFSS05] 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.

cited on pages 4, 73, 74, and 91.

[DFSS06] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Oblivious transfer and linear functions. In *Advances in Cryptology—CRYPTO '06*, volume 4117 of *Lecture Notes in Computer Science*, pages 427–444. Springer, 2006.

cited on pages 4, 31, and 47.

[DFSS07] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer, 2007.

cited on page 105.

[DFSS08] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *special issue of SIAM Journal of Computing*, 2008. to appear.

cited on pages 4, 55, and 73.

[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.

cited on pages 4 and 42.

[Din01a] Yan Zong Ding. Oblivious transfer in the bounded storage model. In *Advances in Cryptology—CRYPTO '01*, volume 2139 of *Lecture Notes in Computer Science*, pages 155–170. Springer, 2001.

cited on page 4.

[Din01b] 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.

cited on page 42.

[Din05] Yan Zong Ding. Error correction in the bounded storage model. In *Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 578–599. Springer, 2005.

cited on page 4.

[DKS99] Ivan 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.

cited on pages 3 and 42.

[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.

cited on page 4.

[DMS00] Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *Advances in Cryptology—EUROCRYPT '00*, volume 1807 of *Lecture Notes in Computer Science*, pages 300–315. Springer, 2000.

cited on pages 6 and 93.

[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.

cited on page 62.

[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.

cited on page 80.

[DSTW07] David P. DiVincenzo, Christian Schaffner, Barbara M. Terhal, and Stephanie Wehner. Cryptography from noisy quantum storage. private communication, 2007.

cited on page 105.

[EGL82] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*. Plenum Press, 1982.

cited on pages 1 and 31.

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letter*, 67(6):661–663, August 1991.

cited on page 76.

[Eng03] B.-G. Englert. Mutually unbiased bases. Open Problems in Quantum Information Theory, 2003. `http://www.imaph.tu-bs.de/qi/problems`.

cited on page 60.

[FGG+97] Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chie-Sheng Niu, and Asher Peres. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Physical Review A*, 56:1163 – 1172, 1997.

cited on page 9.

[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.

cited on page 29.

[Gol95] Oded Goldreich. Three XOR-lemmas - an exposition. *Electronic Colloquium on Computational Complexity (ECCC)*, 2(56), 1995.

cited on page 36.

[Hei27] Werner Heisenberg. Schwankungserscheinungen und quantenmechanik. *Zeitschrift für Physik*, 40:501–506, 1927.

cited on page 60.

[HIGM95] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, Mar 1995.

cited on page 103.

[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.

cited on page 29.

[HR06] Thomas Holenstein and Renato Renner. On the randomness of independent experiments. `http://www.arxiv.org/cs.IT/0608007`, 2006.

cited on page 22.

[HU88] J. Hilgevood and J.B.M. Uffink. The mathematical expression of the uncertainty principle. In *Microphysical Reality and Quantum Description*. Kluwer Academic, 1988.

cited on page 60.

[HV06] Peter Harremoës and Christophe Vignat. Rényi entropies of marginal distributions. submitted to Elsevier Science, 2006.

cited on pages 70 and 71.

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *21st Annual ACM Symposium on Theory of Computing (STOC)*, pages 12–24, 1989.

cited on pages 20, 26, and 29.

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

cited on page 59.

[Jon91] K.R.W. Jones. Riemann-Liouville fractional integration and reduced distributions on hyperspheres. *Journal of Physics A: Mathematical and General*, 24:1237–1244, 1991.

cited on page 70.

[JRW94] Richard Jozsa, Daniel Robb, and William K. Wootters. Lower bound for accessible information in quantum mechanics. *Physical Review A*, 49(2):668–677, 1994.

cited on page 70.

[KGR05] Barbara Kraus, Nicolas Gisin, and Renato Renner. Lower and upper bounds on the secret key rate for qkd protocols using one-way classical communication. *Physical Review Letters*, 95(080501), August 2005. eprint archive: http://arxiv.org/abs/quant-ph/0410215.

cited on page 26.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 20–31, 1988.

cited on pages 1 and 31.

[Kit97] Fuad Kittaneh. Norm inequalities for certain operator sums. *Journal of Functional Analysis*, 143(FU962957):337–348, 1997.

cited on page 56.

[KMR05] Robert König, Ueli Maurer, and Renato Renner. On the power of quantum memory. *IEEE Transaction on Information Theory*, 51(7):2391–2401, July 2005. eprint archive: http://arxiv.org/abs/quant-ph/0305154.

cited on page 26.

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

cited on page 60.

[KT06] Robert König and Barbara M. Terhal. The bounded storage model in the presence of a quantum adversary. `http://arxiv.org/abs/quant-ph/0608101`, 2006.

cited on page 26.

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

cited on page 61.

[LBZ02] Jay Lawrence, Časlav Brukner, and Anton Zeilinger. Mutually unbiased binary observable sets on N qubits. *Physical Review A*, 65(3), February 2002.

cited on page 60.

[LC97] Hong-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, April 1997.

cited on pages 2 and 10.

[Lo97] Hong-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.

cited on page 10.

[Lo01] Hong-Kwong Lo. Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Information and Computation*, 1(2):81–94, 2001.

cited on page 102.

[Lu04] Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1):27–42, 2004.

cited on page 4.

[Lüt00] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61:052304, 2000.

cited on page 9.

[Mau90] Ueli M. Maurer. A provably-secure strongly-randomized cipher. In *Advances in Cryptology—EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 361–373. Springer, 1990.

cited on pages 3 and 118.

[Mau91] Ueli M. Maurer. Perfect cryptographic security from partially independent channels. In *23rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 561–572, 1991.

cited on page 80.

[Mau92] Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992. Preliminary version: [Mau90].

cited on page 4.

[May95] Dominic Mayers. On the security of the quantum oblivious transfer and key distribution protocols. In *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 124–135. Springer, 1995.

cited on page 10.

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

cited on pages 2 and 10.

[MN05] Tal Moran and Moni Naor. Basing cryptographic protocols on tamper-evident seals. In *32nd International Colloquium on Automata, Languages and Programming (ICALP)*, volume 3580 of *Lecture Notes in Computer Science*, pages 285–297. Springer, 2005.

cited on page 2.

[MP95] Rajeev Motwani and Raghavan Prabhakar. *Randomized Algorithms*. Cambridge University Press, 1995.

cited on pages 15 and 57.

[MS94] Dominic Mayers and Louis Salvail. Quantum oblivious transfer is secure against all individual measurements. In *Workshop on Physics and Computation, PhysComp '94*, pages 69–77, November 1994.

cited on page 10.

[MST04] 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.

cited on page 7.

[MU88] Hans Maassen and Jos B. M. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(12):1103–1106, March 1988.

cited on pages 8, 60, 63, and 69.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge university press, 2000.

cited on pages 13 and 16.

[Rab81] M. Rabin. How to exchange secrets by oblivious transfer. Technical report, Harvard Aiken Computation Lab, 1981.

cited on pages 2 and 31.

[Rén61] Alfréd Rényi. On measures of entropy and information. In *Proceedings of the 4th Berkeley Symposium Mathematical Statistics and Probability*, volume 1, pages 547–561. University of California Press, 1961.

cited on page 17.

[Ren05] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zürich (Switzerland), September 2005. `http://arxiv.org/abs/quant-ph/0512258`.

cited on pages 10, 16, 20, 24, 25, 26, 27, 29, and 100.

[RGK05] Renato Renner, Nicolas Gisin, and Barbara Kraus. An information-theoretic security proof for QKD protocols. *Phys. Rev. A*, 72(012332), July 2005.

cited on pages 9, 26, and 102.

[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.

cited on pages 17, 24, 26, and 27.

[Rus94] Mary Beth Ruskai. Beyond Strong Subadditivity? Improved Bounds on the Contraction of Generalized Relative Entropy. *Reviews in Mathematical Physics*, 6:1147–1161, 1994.

cited on page 16.

[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, pages 199–216. Springer, 2005.

cited on pages 20, 21, 22, 26, and 29.

[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.

cited on page 7.

[Sán93] Jorge Sánchez-Ruiz. Entropic uncertainty and certainty relations for complementary observables. *Physics Letters A*, 173(3):233–239, February 1993.

cited on page 69.

[Sán95] 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.

cited on page 61.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *Bell Telephone System Technical Publications*, 1948.

cited on page 18.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, July 2000.

cited on page 76.

[Sýk74] Stanislav Sýkora. Quantum theory and the Bayesian inference problems. *Journal of Statistical Physics*, 11(1):17–27, 1974.

cited on page 70.

[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`.

cited on page 6.

[Vad04] Salil P. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. *Journal of Cryptology*, 17(1):43–77, 2004.

cited on page 4.

[Vaz86] Umesh Virkumar Vazirani. *Randomness, adversaries and computation*. PhD thesis, University of California, Berkeley, 1986.

cited on page 36.

[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.

cited on page 27.

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

cited on page 59.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Original manuscript written circa 1970.

cited on pages 1, 10, 31, 59, 75, 83, and 85.

[Wol00] Stefan Wolf. Reducing oblivious string transfer to universal oblivious transfer. In *IEEE International Symposium on Information Theory (ISIT)*, 2000.

cited on pages 31, 32, and 42.

[Wul07] Jürg Wullschleger. Oblivious-Transfer amplification. In *Advances in Cryptology—EUROCRYPT '07*, Lecture Notes in Computer Science. Springer, 2007.

cited on pages 3, 23, 32, 42, 47, 48, and 88.

[WW07] Stephanie Wehner and Jürg Wullschleger. Security in the bounded-quantum-storage model. private communication, 2007.

cited on page 106.

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *27th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 67–75, 1995.

cited on page 10.

Index