Doctoral Thesis

Classical and Quantum Secure Two-Party Computation

Author(s):
Winkler, Severin

Publication Date:
2012

Permanent Link:
https://doi.org/10.3929/ethz-a-007339443

Rights / License:
In Copyright - Non-Commercial Use Permitted
Classical and Quantum Secure Two-Party Computation

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

SEVERIN WINKLER
MSc in Computer Science, ETH Zurich

born May 5, 1975
citizen of Adliswil, ZH, Switzerland

accepted on the recommendation of

Prof. Dr. Stefan Wolf, examiner
Prof. Dr. Ivan Damgård, co-examiner
Prof. Dr. Renato Renner, co-examiner

2012
The completion of this thesis would not have been possible without the assistance and support of many people.

I want to thank my supervisor Stefan Wolf for initiating and supporting my doctorate. I thank Ivan Damgård and Renato Renner for investing their time in studying my work and in serving on my Ph.D. committee as well as for their valuable comments and suggestions that helped to improve this dissertation.

Much of the research in this thesis was done in close collaboration with Jürg Wullschleger. It was always a pleasure to work with him and I thank him for many inspiring discussions and his support.

A special thank goes to Renato Renner for his encouragement, support, advice and guidance during the whole time of my doctorate and for many inspiring discussions and ideas.

I would also like to thank all my co-authors: It was a great pleasure to work with Dejan Dukaric, Manuel Forster, Stefan Hengl, Samuel Rane-llucci, Renato Renner, Alain Tapp, Marco Tomamichel, Stefan Wolf, and Jürg Wullschleger.

I always enjoyed to work in the Quantum Information Group: I thank all current and past members of the group, Dejan Dukaric, Matthias Fitzi, Manuel Forster, Viktor Galliard, Esther Hänggi, and Stefan Wolf for their constant support and providing a relaxed and motivating work environment. Furthermore, I thank the Complexity and Algorithms Group, Chandan Dubey, Jan Hazła, Thomas Holenstein, Trinh Huynh, and Robin Künzler for scientific discussions, for their company and for the friendly takeover of our research group.

I am grateful to all the members of the quantum information theory groups from the physics department for the joint research days and seminars. This includes Normand Beaudry, Mario Berta, Matthias Christandl, Oscar Dahlsten, Frédéric Dupuis, Philippe Faist, David Gross, Ste-
fan Hengl, Renato Renner, Lídia del Rio, Christian Schilling, Cyril Stark, Marco Tomamichel, Michael Walter and Johan Åberg.

I am very thankful to my office-mates Dejan Dukaric, Manuel Forster and Kfir Barhum for contributing to an enjoyable work environment and many scientific and non-scientific discussions.

Many thanks to Manuel Forster, Esther Hänggi and Robin Künzler for reading preliminary versions of this thesis and for their valuable comments. Many thanks go to Beate Bernhard-Temme and Denise Spicher for their great administrative support during my doctorate.

Finally, I want to express special thanks to my parents Brigitte and Peter and my sister Rebecca for their continuous support during my studies.

This work was supported by the Swiss National Science Foundation (SNF) and the ETH research commission.
Abstract

Given a classical communication channel only, it is impossible for two parties to perform an arbitrary joint computation on their respective inputs in such a way that a computationally unbounded player cannot learn more than what he can derive from his own input and the output of the computation. While quantum information is in general fundamentally different from classical information, it seems not more powerful in this context: Even if the parties can communicate over a quantum channel, this task cannot be solved without restricting the computational power of the parties. However, there is a solution once the two parties share a black-box which computes a certain function of the two inputs of the players and gives the outcome to one of them. A simple example of such a function, which allows the two parties to perform any joint computation securely, is oblivious transfer. In the first part of this thesis, we study the possibility and efficiency of such computations. In particular, we provide lower bounds on the number of invocations of oblivious transfer that are needed to securely compute a general function.

A bit commitment protocol consists of two phases, where after the first phase the sender is committed to a bit. The protocol is secure if the value of the bit is fixed and cannot be changed, while the receiver still has no information about the value of the bit. At a later time, the players may execute the second phase, where the bit is revealed to the receiver. It is known that there is no information-theoretically secure bit commitment protocol if the two parties can only use a communication channel - even if the communication is quantum. In the second part of this thesis, we study two-party protocols that implement bit commitments from trusted correlated randomness that is pre-distributed to the parties. We consider protocols that implement many bit commitments at the same time and show that the entropy and, therefore, also the number of the random bits that is needed per bit commitment grows linearly with the statistical secu-
rity parameter. This result is in contrast to known results for implementations of oblivious transfer that only use a constant number of instances of certain distributed correlations per instance if a large number of instances is realized at once.

While quantum communication allows two parties to establish a secret key that remains unknown to any computationally unbounded eavesdropper, neither bit commitment nor oblivious transfer can be realized from quantum communication. However, establishing a secret key is only possible if the two parties already share a short secret key initially. In the third part of this thesis, we ask whether similar quantum protocols could exist that extend commitments in the sense that a commitment to a large string can be securely realized from a smaller number of bit commitments. We answer this question in the negative. Next, we show that quantum protocols that implement oblivious transfer from trusted distributed randomness can violate our impossibility results for classical protocols. However, we prove lower bounds on the entropy of the distributed randomness that is needed by such protocols, which show in particular that also oblivious transfer cannot be extended by quantum protocols. Finally, we present a lower bound on the number of commitments which are necessary to implement oblivious transfer in the quantum setting and a protocol which is optimal with respect to this result.
Zusammenfassung

Es ist unmöglich für zwei Parteien, welche nur über einen klassischen Kommunikationskanal verfügen, eine beliebige gemeinsame Berechnung auf ihren jeweiligen Eingaben sicher auszuführen. Sicherheit bedeutet in diesem Kontext, dass ein Spieler mit unbegrenzten rechnerischen Ressourcen aus der Berechnung nicht mehr lernen kann als das, was er bereits aus seiner Eingabe und der Ausgabe der Berechnung ableiten kann. Während sich Quanteninformation im Allgemeinen grundlegend von klassischer Information unterscheidet, so scheint sie in diesem Zusammenhang nicht mächtiger: Auch wenn die Parteien über einen Quantenkanal kommunizieren können, kann diese Aufgabe nicht gelöst werden ohne die Rechenleistung der Parteien zu begrenzen. Es gibt jedoch eine Lösung, sobald die beiden Parteien eine Black-Box teilen, welche eine bestimmte Funktion der beiden Eingaben der Spieler berechnet und das Ergebnis an einen der Spieler ausgibt. Ein einfaches Beispiel einer solche Funktion, die den beiden Parteien erlaubt, jede beliebige gemeinsame Berechnung sicher durchzuführen, ist Oblivious Transfer. Im ersten Teil dieser Arbeit untersuchen wir die Möglichkeit und Effizienz solcher Berechnungen. Insbesondere zeigen wir untere Schranken für die Anzahl der Aufrufe von Oblivious Transfer, die benötigt werden, um eine allgemeine Funktion sicher zu berechnen.

Ein Bit Commitment Protokoll besteht aus zwei Phasen. In der der ersten Phase legt der Sender den Wert eines Bits fest. Das Protokoll ist sicher, wenn der Wert des Bits nicht mehr verändert werden kann, während der Empfänger noch keine Information über den Wert des Bits erhält. Zu einem späteren Zeitpunkt können die Spieler die zweite Phase ausführen, in welcher der Sender den Wert des Bits offenlegt. Es ist bekannt, dass keine informationstheoretisch sicheren Protokolle für Bit Commitment existieren, wenn die beiden Parteien nur einen Kommunikationskanal benutzen können - auch wenn der Kanal Quanteninformation überträgt. Im
zweiten Teil dieser Arbeit untersuchen wir Protokolle für zwei Parteien, die Bit Commitment aus korrelierten zufälligen Bits, welche im Voraus an die Parteien verteilt werden, implementieren. Wir betrachten Protokolle, die mehrere Instanzen von Bit Commitment gleichzeitig erzeugen und zeigen, dass die Entropie und damit auch die Anzahl der Zufallsbits, die pro Bit Commitment notwendig ist, linear mit dem statistischen Sicherheitsparameter zunimmt. Dieses Ergebnis steht im Gegensatz zu bekannten Protokollen, welche viele Instanzen von Oblivious Transfer gleichzeitig implementieren und nur eine konstante Anzahl Zufallsbits pro implementierter Instanz benötigen.

# Contents

1 Introduction .................................................. 1
   1.1 Secure Two- and Multi-Party Computation ............... 1
      1.1.1 Security .................................................. 2
      1.1.2 Commitments ................................................. 3
      1.1.3 (Two-Party) Secure Function Evaluation ............. 4
      1.1.4 Oblivious Transfer ......................................... 5
      1.1.5 Trusted (Pre-)Distributed Randomness ............... 6
   1.2 Outline and Main Results .................................. 6

2 Preliminaries ................................................... 9
   2.1 Information Theory ........................................... 10
   2.2 Sampling ....................................................... 13
   2.3 Classical Smooth Min- and Max-Entropies ................. 13
      2.3.1 Properties of Smooth Entropies ....................... 15
   2.4 Min-Entropy Sampling ......................................... 22
   2.5 Randomness Extraction and Privacy Amplification .... 23
   2.6 Interactive Hashing ............................................ 23
   2.7 Quantum Information .......................................... 24
      2.7.1 Quantum Entropies ...................................... 29
      2.7.2 Privacy Amplification against Quantum Adversaries 35
      2.7.3 Uncertainty Relation .................................... 36

3 Lower Bounds for Classical Secure Function Evaluation .... 39
   3.1 Introduction ................................................... 39
   3.2 Primitives and Randomized Primitives .................... 42
      3.2.1 Sufficient Statistics and Common Part ................ 44
   3.3 Protocols and Security in the Semi-Honest Model ...... 45
      3.3.1 Malicious OT implies Semi-honest OT ................ 46
3.4 Lower Bounds

3.4.1 Additional Bounds for Implementations of OT
3.4.2 Lower Bounds on Min-Entropy
3.4.3 Lower Bounds for Protocols implementing OT
3.4.4 Lower Bounds for Equality Function
3.4.5 Lower Bounds for Inner Product Function
3.4.6 Lower Bounds for Protocols implementing OLFE
3.4.7 Malicious OT

3.5 String OT from Universal OT

3.5.1 Protocol and Security Definition
3.5.2 Proof of Security
3.5.3 Repeated Universal OT

4 Efficiency of Commitments from Noisy Correlations

4.1 Introduction
4.2 Model and Security Definition
4.3 Lower Bound for Multiple Bit Commitments
4.4 Lower Bounds for Multiple String Commitments
4.5 Concluding Remarks

5 Quantum Commitment and Oblivious Transfer Reductions

5.1 Model
5.2 Impossibility of Extending Quantum Commitments
5.2.1 Security Definition
5.2.2 (Classical) Bit Commitments
5.2.3 Quantum Commitments
5.2.4 Noisy Correlations
5.3 Reversing String OT Efficiently
5.4 Impossibility Results for Quantum OT Reductions
5.4.1 Security Definition
5.4.2 Impossibility Results for Quantum OT Protocols
5.4.3 Reduction of OT to String Commitments
Chapter 1

Introduction

The security of almost all cryptographic systems that are in use today relies on unproven computational hardness assumptions and on the assumption that the adversary’s computational resources are bounded. The advantage of information-theoretic security is that it does not depend on any such possibly unjustified assumption. Its disadvantage is that many interesting cryptographic functionalities cannot be realized from scratch, i.e., if the involved parties only have access to a communication channel. Therefore, there is a lot of interest in information-theoretically secure reductions of cryptographic functionalities to simpler (or seemingly weaker) primitives. In this thesis we study the possibility and efficiency of information-theoretically secure reductions of cryptographic two-party functionalities, such as secure function evaluation or commitments, to different primitives, such as different variants of oblivious transfer or bit commitments - both in the classical and in the quantum setting.

1.1 Secure Two- and Multi-Party Computation

In secure multi-party computation, the goal is to devise protocols which allow a set of mutually distrustful players to perform a joint computation on their inputs in a secure way. Intuitively, security here means that the players compute the result of the computation correctly without learning more than what they can derive from their own input and the output of the computation. The concept of multi-party computation was introduced by Yao [Yao82], Goldreich, Micali, and Wigderson [GMW87], and, independently, Chaum, Damgård, and van de Graaf [CDvdG88] showed
that any function can be computed with computational security if less than half of the players deviate from the protocol. Later, Ben-Or, Goldwasser, and Wigderson [BGW88] and, independently, Chaum, Crépeau, and Damgård [CCD88] showed that in a model with only pairwise secure channels, multi-party computation among \( n \) players information-theoretically secure against an active adversary is achievable if and only if less than one third of the players are corrupted. Beaver [Bea89] and independently Rabin and Ben-Or [RB89] showed that this bound can be improved to a minority \( t < n/2 \) of dishonest players in the information-theoretic setting, assuming that global broadcast channels are available.

### 1.1.1 Security

Security for multi-party computation tasks is defined using the real/ideal model simulation paradigm, which considers a real world, where the parties execute a protocol, and an ideal world, where the parties communicate with a trusted party (or an ideal functionality) that performs the task on their behalf. A protocol securely realizes a functionality if any adversary that attacks an execution of the protocol in the real world cannot achieve more than an equally powerful adversary (or simulator) that attacks the ideal functionality. This means that any attack in the real model can be simulated in the restricted setting of the ideal model. This approach to show security of secure multi-party computation has first been used in the seminal work of Goldreich, Micali and Wigderson [GMW87] and can be traced back to the definitions of zero-knowledge proofs [GMR85] and semantic security [GM84]. Formal definitions for secure multi-party computation have been introduced by Micali and Rogaway [MR92] and by Beaver [Bea92]. Protocols that are secure according to this definition are sequentially composable: If a protocol that uses an ideal functionality is secure, then it remains secure if the ideal functionality is replaced by a secure implementation of the functionality. A comprehensive and simplified definition of standalone security together with a formal proof of sequential composability has been provided by Canetti [Can96, Can00] (see also [Gol04]). Similar results on sequential composability of protocols have been obtained in the quantum case for different variants of the quantum stand-alone model [WW08a, FS09]. However, all these security definitions only guarantee that a protocol is composable in a restricted way and it is known that attacks against concurrent executions of protocols are more powerful in general than attacks against sequential executions.
1.1. Secure Two- and Multi-Party Computation

In the classical setting, stronger security definitions that overcome this restriction have been proposed by Canetti [Can01] and by Backes, Pfitzmann and Waidner [PW02, BPW03]. In these models protocols are universally composable, i.e., protocols can be composed arbitrarily in any environment. Universal compositability has been adapted to the quantum setting by Ben-Or and Mayers [BOM04] and by Unruh [Unr04, Unr10].

Depending on the restrictions of the adversary and the simulator, we consider different notions of security: Semi-honest adversaries are restricted to follow the prescribed protocol, but try to gain additional information from the whole record of the computation. The corresponding simulator is restricted to semi-honest behavior as well, i.e., it is not allowed to substitute the provided inputs. Semi-honest security is achieved if for every semi-honest adversary in the real world there is a semi-honest simulator in the ideal world. In the malicious model the adversary in the real world and the simulator may behave arbitrarily. All the results in thesis hold in the information-theoretic setting, where the adversary is computationally unbounded. Furthermore, we distinguish between perfect security, where the execution in the real world and the simulation are perfectly indistinguishable, and statistical security, where a protocol is secure with an error \( \varepsilon \) if the execution in the real world can be distinguished from the simulation with probability at most \( \varepsilon \).

For all impossibility results in this thesis, we will consider (weakened) definitions of security against semi-honest or malicious adversaries in the standalone model. We will introduce the details of these definitions in the corresponding chapters.

1.1.2 Commitments

A primitive of fundamental importance in multi-party computation is commitment. An ideal commitment functionality takes a bit string \( x \) as input from the first party, the sender, and outputs the message committed to the second party, the receiver. Later, on input open from the sender, the functionality sends the message \((\text{open}, x)\) to the receiver. A commitment scheme is a pair of protocols that implement this functionality in two phases: the commit phase, where the sender has to decide on a value \( x \), and the open phase, where the bit \( x \) is revealed to the receiver. The scheme is called a bit commitment if \( x \) is only one bit, and it is called a string commitment if \( x \) is a longer bit string. Intuitively, such a scheme is

---

1While a scheme consists in general of multiple protocols, we use the terms protocol and scheme interchangeably in this thesis.
secure for the sender (or hiding) if the receiver has no information on the committed string before the commitment is opened by the sender. The scheme is secure for the receiver (binding) if after the commit phase there is only one string that the sender can successfully open.

Commitments [Blu83] are one of the basic building blocks of two-party computation [Yao82]. They can be used in coin-flipping [Blu83], zero-knowledge proofs [GMR85, GMW91], zero-knowledge arguments [BCC88] or as a tool in general two-party computation protocols to prevent malicious players from actively cheating (see, for example, [CvdGT95]). Furthermore, black-box bit commitments are sufficient to implement statistically secure oblivious transfer using quantum communication.

If the two players have access to a noiseless classical communication channel only, information-theoretically secure bit commitment is known to be impossible (see, for example, Chapter 4 for a proof). After the suggestion of several quantum schemes for information-theoretically secure secure bit commitment [BB84, BC90, BCJL93], quantum bit commitment was shown to be impossible in [May97, LC97] - even in the presence of superselection rules [KMP04], which limit the physically realizable quantum operations. Thus, we either need to assume that the adversary is limited in certain ways or give the players access to some additional resources in order to implement secure commitments. In the classical setting, bit commitment is possible against computationally bounded adversaries if one-way functions exist [Nao91, HILL99, HR07]. It is possible with information-theoretic security if the players have access to a (weak) noisy channel or noisy correlations [Cre97, DKS99, WNI03, Wul09]. Bit commitment can also be implemented if the players are given access to trusted non-local correlations [BCU06, WWW11]. In the quantum setting, bit commitment (and oblivious transfer) can be implemented with information-theoretic security if the adversary’s quantum memory is limited [DFSS06, DFR06, WW08a] or if his quantum storage is subject to noise [Weh08, STW09, KWW09, Sch10].

1.1.3 (Two-Party) Secure Function Evaluation

Most works that study secure two- and multi-party computation have focused on functionalities for secure function evaluation (SFE), which are also referred to as (deterministic) non-reactive functionalities. In this thesis, we focus on the case of two-party one-sided secure function evaluation, which is a special case of general two-party SFE where only one party gets an output. In the literature this functionality is often also called asym-
metric SFE. For a two-party function \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \), a functionality for one-sided secure function evaluation takes input \( x \in \mathcal{X} \) from the first party, Alice, and \( y \in \mathcal{Y} \) from the second party, Bob. After the functionality has received both inputs, it sends the output \( f(x, y) \) to Bob.

### 1.1.4 Oblivious Transfer

Oblivious transfer (OT) is a special case of one-sided secure function evaluation and a primitive of central importance in secure two-party computation. In particular, OT is sufficient to execute any two-party computation securely and (different variants of) OT can be precomputed offline, i.e., before the actual inputs to the computation are available, and converted into OTs later. The original form of OT \((\frac{1}{2})\)-RabinOT \(^1\) has been introduced by Rabin \([Rab81]\). It allows a sender to send a bit \( x \), which the receiver will get with probability one half. Another variant of OT, called one-out-of-two Bit OT \((\frac{2}{1})\)-OT \(^1\) was defined in \([EGL85]\) (see also \([Wie83]\)). Here, the sender has two input bits \( x_0 \) and \( x_1 \). The receiver gives as input a choice bit \( c \) and receives \( x_c \) without learning \( x_{1-c} \). The sender gets no information about the choice bit \( c \). Other important variants of OT are \((n_t)\)-OT \(^k\), where the inputs are strings of \( k \) bits each and the receiver can choose \( t < n \) out of \( n \) secrets, and \((p)\)-RabinOT \(^k\), where the inputs are strings of \( k \) bits and the erasure probability is \( p \in (0, 1) \).

If the two players have access to noiseless classical or quantum communication only, it is impossible to implement any of these variants of OT in an information-theoretic security. While oblivious transfer can be implemented against computationally bounded adversaries in the classical setting from dense trapdoor permutations \([Hai04]\) or based on various number-theoretic assumptions, it is not known how to implement OT from one-way functions and there cannot exist a black-box reduction of OT to one-way functions \([IR89]\). However, one-way functions are sufficient to implement a large number of OTs given an initial smaller number of OTs. This means that OT can be extended using one-way functions \([Bea96]\) in the computational setting.

\((p)\)-RabinOT \(^k\) and \((\frac{2}{1})\)-OT \(^1\) are equally powerful in the sense that one can be implemented from the other \([Cré88]\). Numerous reductions between different variants of \((\frac{n}{t})\)-OT \(^k\) are known as well: \((\frac{2}{1})\)-OT \(^k\) can be implemented from \((\frac{2}{1})\)-OT \(^1\) \([BBR88, CS91, BCS96b, BCW03]\), and \((n_t)\)-OT \(^k\) can be implemented from \((\frac{2}{1})\)-OT \(^k'\) \([BCR86, BCS96b, DM99, WW05a]\). There has also been a lot of interest in reductions of OT to weaker prim-
Chapter 1. Introduction

It is known that OT can be realized with information-theoretic security from noisy channels [CK88, CMW04, DFMS04, Wu09], noisy correlations [WW04, NW06], or weak variants of OT [CK88, Cac98, DKS99, BCW03, DFSS06, Wu07b].

In the quantum setting, information-theoretically secure OT can be implemented from black-box commitments [BBCS92, Yao95, DFL+09, Unr10]; this reduction is impossible in the classical setting.

1.1.5 Trusted (Pre-)Distributed Randomness

Trusted distributed randomness is a very simple but powerful two-party functionality that takes no input from the players, generates values \((u, v)\) according to a joint probability distribution \(P_{UV}\) and sends \(u\) to the first player and \(v\) to the second player. Such a functionality allows the two players to securely realize different variants of OT. In particular, the correlation that is generated by invoking OT with random inputs and storing the inputs and the output enables the two players to implement one instance of OT, and, therefore, OT can actually be precomputed and stored for later use [Bea95]. Thus, in a model where a trusted third party pre-distributes correlations to the two parties in an offline-stage [Bea97], any two-party computation can be executed with information-theoretic security. We also refer to trusted distributed randomness as noisy correlations.

1.2 Outline and Main Results

In Chapter 2, we introduce the notation and present concepts from information theory and the technical tools we will use in the following chapters. In Section 2.3, we introduce the formalism of classical smooth min- and max-entropies [RW05] and prove properties of these entropic measures. In Section 2.7, we present concepts from quantum information theory that we will use in Chapter 5. In particular, we introduce definitions and properties of the quantum smooth min- and max-entropy.

(Classical) Secure Function Evaluation

In the first part of this work, we provide bounds on the efficiency of secure one-sided two-party computation of arbitrary finite functions from distributed randomness with statistical security in the semi-honest model. From these results we derive bounds on the efficiency of such protocols.
that use (different variants of) OT as a black-box. When applied to implementations of OT, our impossibility results generalize known results for perfectly secure protocols to the case of statistical security. Our results hold in particular for transformations between finite numbers of primitives and for any error. The lower bounds for implementations of oblivious transfer also hold in the malicious model. Furthermore, we provide an improved analysis of a protocol from [CS06] for implementations of String OT from Universal OT, a variant of OT where the security of the sender is weakened in the sense that only an upper bound on the information (in terms of min-entropy) obtained by the receiver is known. Our analysis shows that the protocol can implement OT over strings of a length which is asymptotically optimal with respect to our statistical impossibility results.

Efficiency of Commitments from Noisy Correlations

While there exist information-theoretically secure implementations of oblivious transfer from noisy correlations or channels which achieve constant rates, no such constructions are known for bit commitment. In Chapter 4, we show that one needs at least $\Omega(kn)$ instances of a given resource such as oblivious transfer or a noisy channel to implement $n$ instances of bit commitment with an error of at most $2^{-k}$. More precisely, in Theorem 4.1 we show that if a commitment scheme implements $n$ bit commitments with a security of at least $2^{-k}$ from distributed randomness, then the mutual information between the sender’s and the receiver’s randomness must be essentially bounded by $kn$ from below. Our proof is built on the insight that any such protocol must reveal at least $k$ bits of information about the receiver’s randomness for each committed bit that is opened. This implies that we need at least $\Omega(kn)$ instances of oblivious transfer or noisy channels to implement $n$ bit commitments. Thus, executing for each bit commitment a protocol that uses $O(k)$ instances is optimal. In combination with the lower bound from [WNI03], this bound can be generalized to string commitments: any protocol that implements $n$ string commitments of length $\ell$ needs at least $\Omega(n(\ell + k))$ bits of distributed randomness.

Quantum Commitment and Oblivious Transfer Reductions

Information-theoretically secure commitments or oblivious transfer are impossible to achieve from quantum communication only [May97] [LC97].
However, the known impossibility results leave open the possibility that there exist protocols that implement a larger number of these primitives with information-theoretic security once some instances of the primitive are available, i.e., that quantum protocols can extend oblivious transfer or commitments. In Chapter 5, we provide several impossibility results, which in particular imply that neither of these primitives can be extended by statistically secure quantum protocols.

First, we provide bounds on the efficiency of reductions of commitments to black-box commitments and trusted distributed randomness. These results imply in particular that there is no statistically secure quantum protocol that extends commitments. Next, we present a lower bound on the entropy of the randomness that is needed to implement OT with quantum protocols from trusted distributed randomness. This result implies that oblivious transfer cannot be extended by quantum protocols. Furthermore, we present a lower bound on the number of individual commitments and on the number of committed bits which are needed to implement OT from commitments. Finally, we present a protocol that is essentially optimal with respect to these two bounds. Our construction is based on the protocol proposed in [BBCS92]. We use an uncertainty relation for smooth quantum entropies [TR11, Tom12] to prove the security for Alice of this protocol, used to prove the security of quantum key distribution schemes [TLGR12]. Our result shows that it is also a useful tool for tw
Chapter 2

Preliminaries

We use calligraphic letters to denote sets throughout this thesis. For an integer \( k \geq 1 \), we write \([k]\) to denote the set \( \{1, \ldots, k\} \). Given a tuple \( x = (x_1, \ldots, x_n) \in \mathcal{X}^n \) and \( \mathcal{T} := \{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\} \), we use the notation \( x_{\mathcal{T}} \) for \( (x_{i_1}, x_{i_2}, \ldots, x_{i_k}) \in \mathcal{X}^k \). If \( x, y \in \{0, 1\}^n \), then \( x \oplus y \) denotes the bitwise XOR of \( x \) and \( y \).

We denote the distribution of a random variable \( X \) over \( \mathcal{X} \) by \( P_X(x) \). We write \( P_{UNIF^k} \) for the uniform distribution over the \( k \)-bit strings. Given a distribution \( P_{XY} \) over \( \mathcal{X} \times \mathcal{Y} \), the marginal distribution is denoted by \( P_X(x) := \sum_{y \in \mathcal{Y}} P_{XY}(x, y) \). For every \( y \in \mathcal{Y} \) with \( P_Y(y) > 0 \), the conditional distribution \( P_{X|Y}(x, y) := P_{XY}(x, y) / P_Y(y) \) over \( \mathcal{X} \times \mathcal{Y} \) defines a distribution \( P_{X|Y = y} \) with \( P_{X|Y = y}(x) = P_{X|Y}(x, y) \) over \( \mathcal{X} \). \( P_{X|Y} \) can be seen as a randomized function that has input \( y \) and outputs \( x \) distributed according to \( P_{X|Y = y} \). We sometimes also refer to \( P_{X|Y} \) as a channel (with input \( y \) and output \( x \)).

The closeness of two distributions can be measured by the statistical distance.

**Definition 2.1.** The statistical distance between the distributions \( P_X \) and \( P'_{X} \) over the domain \( \mathcal{X} \) is defined as

\[
D(P_X, P'_X) := \sum_{x \in \mathcal{X}} |P_X(x) - P'_X(x)| .
\] (2.0.1)

The statistical distance can equivalently be defined as the maximum over all (inefficient) distinguishers \( \delta : \mathcal{X} \to \{0, 1\} \) of the distinguishing advantage

\[
D(P_X, P'_X) = \max_{\delta} | \Pr[\delta(X) = 1] - \Pr[\delta(X') = 1] | .
\]
If \( D(P_X, P_{X'}) \leq \varepsilon \), we may also say that \( P_X \) is \( \varepsilon \)-close to \( P_{X'} \). The support of a distribution \( P_X \) over \( \mathcal{X} \) is defined as

\[
\text{supp}(P_X) := \{ x \in \mathcal{X} : P_X(x) > 0 \}.
\]

If \( \Omega \) is a random variable over \( \{0, 1\} \), then we also call it an event. Given an event \( \Omega \) and random variables \( X \) and \( Y \) with a joint distribution \( P_{\Omega XY} \), we use the notation \( P_{X \Omega \mid Y = y} \) for the sub-normalized distribution with

\[
P_{X \Omega \mid Y = y}(x) := P_{\Omega XY}(1, x, y) / P_Y(y).
\]

We will also use the shorthand notation \( P_{\Omega \mid X = x} \) to denote the probability \( P_{\Omega \mid X = x}(1) \). We use the convention that \( P_{X \Omega \mid Y = y} = 0 \) if \( P_Y(y) = 0 \). We say that \( X \), \( Y \) and \( Z \) form a Markov-chain, denoted by \( X \leftrightarrow Y \leftrightarrow Z \), if \( X \) and \( Z \) are independent given \( Y \), which means that \( P_{X \mid Y = y} = P_{X \mid Y = y, Z = z} \) for all \( y, z \).

### 2.1 Information Theory

In the following we introduce tools from information theory that are used in our proofs. We refer to [CT91, HK01] for more details on this topic.

**Definition 2.2.** The conditional Shannon entropy of \( X \) given \( Y \) is defined as

\[
H(X \mid Y) := - \sum_{(x, y) \in \text{supp} (P_{XY})} P_{XY}(x, y) \log P_{X \mid Y}(x, y).
\]

We use the notation

\[
h(p) = -p \log(p) - (1 - p) \log(1 - p)
\]

for the binary entropy function, i.e., \( h(p) \) is the entropy of the Bernoulli distribution\(^1\) with parameter \( p \). Note that the function \( h(p) \) is concave and positive, which implies that for any \( 0 \leq p \leq 1 \) and \( 0 \leq c \leq 1 \), we have

\[
h(c \cdot p) \geq c \cdot h(p).
\]

The chain rule for conditional entropy is

\[
H(XY \mid Z) = H(X \mid Z) + H(Y \mid XZ).
\]

---

\(^1\)Throughout this thesis, all logarithms are binary.

\(^2\)The Bernoulli distribution with parameter \( p \in [0, 1] \) takes on the value 1 with probability \( p \) and 0 otherwise.
Definition 2.3. The conditional mutual information of \( X \) and \( Y \) given \( Z \) is defined as
\[
I(X; Y|Z) := H(X|Z) - H(X|YZ)
\]

Note that \( X \leftrightarrow Y \leftrightarrow Z \) if and only if \( I(X; Z|Y) = 0 \), i.e., \( X \) and \( Z \) are conditionally independent given \( Y \). Furthermore, the conditional entropy and the conditional mutual information have the following monotonicity properties
\[
H(XY|Z) \geq H(X|Z) \geq H(X|YZ), \quad (2.1.3)
\]
\[
I(WX; Y|Z) \geq I(X; Y|Z). \quad (2.1.4)
\]

The mutual information satisfies the chain rule
\[
I(X_1, \ldots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y|X_1, \ldots, X_{i-1}).
\]

Definition 2.4. The Kullback-Leibler divergence or relative entropy of two distributions \( P_X \) and \( Q_X \) on \( \mathcal{X} \) is defined as
\[
D_{KL}(P_X||Q_X) := \sum_{x \in \mathcal{X}} P_X(x) \log \frac{P_X(x)}{Q_X(x)}.
\]

The conditional divergence of two distributions \( P_{XY} \) and \( Q_{XY} \) on \( \mathcal{X} \times \mathcal{Y} \) is defined as
\[
D_{KL}(P_{Y|X}||Q_{Y|X}) := \sum_{x \in \mathcal{X}} P_X(x) D_{KL}(P_{Y|X=x}||Q_{Y|X=x}).
\]

The binary divergence of two probabilities \( p \) and \( q \) is defined as the divergence of the Bernoulli distributions with parameters \( p \) and \( q \), i.e.,
\[
d_{KL}(p||q) := p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}.
\]

The divergence (and hence also the conditional divergence) is always non-negative. Furthermore, we have the following chain rule
\[
D_{KL}(P_{XY}||Q_{XY}) = D_{KL}(P_X||Q_X) + D_{KL}(P_{Y|X}||Q_{Y|X}). \quad (2.1.5)
\]

---

\(^3\)We use the convention that \( P_X(x) \log P_X(x)/Q_X(x) \) is interpreted as 0 if \( P(x) = 0 \) and as \(+\infty\) if \( P(x) > 0 \) and \( Q(x) = 0 \).
This implies
\[ D_{KL}(P_X P_{Y|X} \| P_X Q_{Y|X}) = D_{KL}(P_{Y|X} \| Q_{Y|X}). \]  
(2.1.6)

Let \( Q_X \) and \( P_X \) be two distributions over the inputs to the same channel \( P_{Y|X} \). Then the divergence between the outputs \( P_Y = \sum_x P_X P_{Y|X} \) and \( Q_Y = \sum_x Q_X P_{Y|X} \) of the channel is not greater than the divergence between the inputs, i.e., the divergence satisfies the data processing inequality
\[ D_{KL}(P_{Y|X} \| Q_{Y|X}) \geq D_{KL}(P_X \| Q_X). \]  
(2.1.7)

Furthermore, for random variables \( X, Y \) and \( Z \) distributed according to \( P_{XYZ} \)
\[ I(X;Y|Z) = D_{KL}(P_{X|Y,Z} \| P_{X|Z}). \]  
(2.1.8)

If \( X, Y, Z \) form a Markov chain, \( X \leftrightarrow Y \leftrightarrow Z \), then
\[ H(X|Z) \geq H(X|YZ) = H(X|Y). \]  
(2.1.9)

It is easy to show that if \( W \leftrightarrow XZ \leftrightarrow Y \), then
\[ I(X;Y|ZW) \leq I(X;Y|Z) \quad \text{and} \quad I(W;Y|Z) \leq I(X;Y|Z). \]  
(2.1.10)

The following lemma shows that the difference between the conditional entropies of two random variables cannot be too large if their distributions are close in terms of the statistical distance.

**Lemma 2.1.** Let \( (X, Y) \), and \( (\hat{X}, \hat{Y}) \) be random variables distributed according to \( P_{XY} \) and \( P_{\hat{X}\hat{Y}} \), and let \( D(P_{XY}, P_{\hat{X}\hat{Y}}) \leq \epsilon \). Then
\[ H(\hat{X}|\hat{Y}) \geq H(X|Y) - \epsilon \log |\mathcal{X}| - h(\epsilon). \]

**Proof.** There exist random variables \( A, B \) such that \( P_{XY|A=0} = P_{\hat{X}\hat{Y}|B=0} \) and \( \Pr[A = 0] = \Pr[B = 0] = 1 - \epsilon \). Thus, using the monotonicity of the entropy and the fact that \( H(X) \leq \log(|\mathcal{X}|) \) we obtain
\[
H(\hat{X}|\hat{Y}) \geq (1 - \epsilon)H(\hat{X}|\hat{Y}A = 0) + \epsilon H(\hat{X}|\hat{Y}A = 1)
\geq (1 - \epsilon)H(X|YB = 0)
= H(X|YB) - \epsilon H(X|YB = 1)
= H(XB|Y) - H(B|Y) - \epsilon H(X|YB = 1)
\geq H(X|Y) - h(\epsilon) - \epsilon \log(|\mathcal{X}|).
\]

\[\square\]
Lemma (2.1) implies Fano’s inequality: For all $X, \hat{X} \in \mathcal{X}$ with $\Pr[X \neq \hat{X}] \leq \varepsilon$, we have
\[
H(X|\hat{X}) \leq \varepsilon \cdot \log |\mathcal{X}| + h(\varepsilon) .
\]

2.2 Sampling

The following bound by Hoeffding [Hoe63] shows that for independently distributed random variables $X_0, \ldots, X_{n-1}$ from $[0, 1]$ the sum of the random variables is close to the mean with high probability.

**Lemma 2.2 (Hoeffding’s bound).** Let $P_{X_0X_1 \ldots X_{n-1}} = P_{X_0}P_{X_1} \ldots P_{X_{n-1}}$ be the (product) distribution of random variables $X_i \in [0, 1]$. Let $\bar{X} = \frac{1}{n} \sum_{i=0}^{n-1} X_i$. Then, for any $\varepsilon > 0$,
\[
\Pr[\bar{X} \geq E[\bar{X}] + \varepsilon] \leq \exp(-2n\varepsilon^2) ,
\]
and
\[
\Pr[\bar{X} \leq E[\bar{X}] - \varepsilon] \leq \exp(-2n\varepsilon^2) .
\]

We will need the following sampling result, which follows from Lemma 5.5 in [BH05] and Lemma 2.2.

**Lemma 2.3.** Let $\alpha \in [0, \frac{1}{2}]$. Let $y = (y_1, \ldots, y_m)$ be a bit string of length $m := bk$ that we group into $k$ blocks of size $b$. Let $t$ be a random subset of $[k]$ of size $\alpha k$, $\mathcal{T}$ the corresponding set of bits in $[m]$ and $\bar{\mathcal{T}}$ the complement of $\mathcal{T}$. Let $\mathcal{T}'$ be a uniform random subset of $\mathcal{T}$. We have, for any $\delta > 0$,
\[
\Pr\left[\frac{1}{|\mathcal{T}'|} \sum_{i \in \mathcal{T}'} y_i \leq \frac{1}{(1 - \alpha)m} \sum_{i \in \mathcal{T}} y_i - \delta\right] \leq \varepsilon ,
\]
where $\varepsilon := 3 \exp(-(1/2 - \varepsilon)\alpha k \delta^2/8)$.

2.3 Classical Smooth Min- and Max-Entropies

Next, we introduce two variants of the smooth conditional min-entropy and a definition of smooth max-entropy in the classical case and prove properties of this entropic measures that we will use in the following
The min-entropy \( H_\infty(X) \) is defined as the negative logarithm of the probability of the most likely element, i.e.,

\[
H_\infty(X) := -\log \max_x P_X(x).
\]

The max-entropy \( H_0(X) \) is defined as the logarithm of the size of the support of \( X \), i.e.,

\[
H_0(X) := \log \text{supp}(P_X).
\]

There is no standard definition of the conditional min- or max-entropy. A natural definition of the min-entropy is the following:

\[
\tilde{H}_\infty(X|Y) := -\log \sum_y P_Y(y) \max_x P_{X|Y=y}(x) = -\log \sum_y \max_x P_{XY}(x, y).
\]

This min-entropy \( \tilde{H}_\infty(X|Y) \) can be interpreted as the negative logarithm of a guessing probability: \( 2^{-\tilde{H}_\infty(X|Y)} \) corresponds to the maximal probability to guess \( X \) from \( Y \). An alternative definition has been used in [RW05], where the conditional min-entropy has been defined as

\[
H_\infty(X|Y) := \min_{x,y} (-\log(P_{X|Y=y}(x))).
\]

In contrast to Shannon entropy, min- and max-entropies are not robust to small changes in the distribution. Therefore, one often considers smoothed versions of these measures, where the entropy is optimized over a set of distributions that are close in terms of some distance measure. While the concept of smoothed entropies has already been used in the literature on randomness extraction [NZ96], the term smooth entropy has been introduced in [RW05]. There it has been shown that the smoothed min- and max-entropy have similar properties as the Shannon entropy, i.e., they satisfy a chain rule, monotonicity and subadditivity.

**Definition 2.5.** For random variables \( X, Y \) and \( \varepsilon \in [0, 1) \), we define the smooth max-entropy as

\[
H_0^\varepsilon(X|Y) := \min_{\Omega : \Pr[\Omega] \geq 1-\varepsilon} \max_y \log |\text{supp}(P_{X\Omega|Y=y})|.
\]

---

4 This entropy corresponds to the Rényi entropy [Rén61] of order \( \infty \).

5 This entropy has been introduced by Hartley in [Har28] and corresponds to the Rényi entropy [Rén61] of order 0.
2.3. Classical Smooth Min- and Max-Entropies

Definition 2.6. For random variables \(X, Y\) and \(\varepsilon \in [0, 1)\), we define the smooth min-entropy as

\[
H^\varepsilon_\infty(X|Y) := \max_{\Omega: \Pr[\Omega] \geq 1 - \varepsilon} \min_{x, y} \left(- \log(P_{X\Omega|Y=y}(x))\right).
\]

Definition 2.7. For random variables \(X, Y\) and \(\varepsilon \in [0, 1)\), we define the smooth average min-entropy as

\[
\tilde{H}^\varepsilon_\infty(X|Y) := \max_{\Omega: \Pr[\Omega] \geq 1 - \varepsilon} -\log \sum_y \max_x P_{XY\Omega}(x, y).
\]

Note that the two notions of smooth conditional min-entropy are equivalent up to an additive term \(\log(1/\varepsilon)\) when smoothed, i.e., \(H^\varepsilon_\infty(X|Y) \geq \tilde{H}^\varepsilon_\infty(X|Y) - \log(1/\varepsilon')\), which follows from Markov’s inequality (see, for example, [DORS08]).

2.3.1 Properties of Smooth Entropies

In the following we prove different properties of the entropies \(H^\varepsilon_\infty(X|Y)\) and \(H^0_\infty(X|Y)\) that we will use in Chapter 3. Note that some of these properties (or special cases of them) have already been shown in [RW05].

We first introduce the following auxiliary quantities.

Definition 2.8. For random variables \(X, Y\) and \(\varepsilon \in [0, 1)\), we define

\[
r^\varepsilon_0(X|Y) := \min_{\Omega: \Pr[\Omega] \geq 1 - \varepsilon} \max_{y} \max_{x, z} \left|\text{supp}(P_{X\Omega|Y=y})\right|;
\]

\[
r^\varepsilon_\infty(X|Y) := \min_{\Omega: \Pr[\Omega] \geq 1 - \varepsilon} \max_{y} \max_{x} \left(P_{X\Omega|Y=y}(x)\right).
\]

Note that \(H^\varepsilon_\infty(X|Y) = -\log r^\varepsilon_\infty(X|Y)\) and \(H^0_\infty(X|Y) = \log r^0_\infty(X|Y)\).

The following lemma shows that the smooth conditional max-entropy is subadditive.

Lemma 2.4 (Subadditivity). Let \(X, Y, Z\) be random variables and \(\varepsilon, \varepsilon' \geq 0\) such that \(\varepsilon + \varepsilon' \in [0, 1)\). Then

\[
H_0^{\varepsilon+\varepsilon'}(XY|Z) \leq H^\varepsilon_0(X|Z) + H^\varepsilon'_0(Y|XZ).
\]

Proof. Let \(\Omega\) be an event with \(\Pr[\Omega] \geq 1 - \varepsilon\) and

\[
\max_{x, z} \left|\text{supp}(P_{Y\Omega|X=x, Z=z})\right| \leq r^\varepsilon_0(Y|XZ).
\]
Let $\Omega'$ be an event with $\Pr[\Omega'] \geq 1 - \varepsilon'$ and $\Omega' \leftrightarrow (X, Z) \leftrightarrow (Y, \Omega)$ such that

$$|\text{supp}(P_{X\Omega'|Z=z})| \leq r_{\text{max}}^\varepsilon(X|Z).$$

Then $\Pr[\Omega, \Omega'] \geq 1 - \varepsilon - \varepsilon'$ and

$$r_{\text{max}}^{\varepsilon+\varepsilon'}(XY|Z) \leq \max_z |\text{supp}(P_{XY\Omega'|Z=z})|.$$

We obtain

$$\max_z |\text{supp}(P_{XY\Omega'|Z=z})|$$

$$\leq \max_z (|\text{supp}(P_{X\Omega'|Z=z})| \cdot \max_x |\text{supp}(P_{Y\Omega|x=x,Z=z})|)$$

$$\leq \max |\text{supp}(P_{X\Omega'|Z=z})| \cdot \max_{x,z} |\text{supp}(P_{Y\Omega|x=x,Z=z})|.$$

The Shannon entropy satisfies the inequality $H(X|Z) - H(X|YZ) = I(X; Y|Z) \leq H(Y|Z)$. The next lemma shows that this property can be generalized to the smooth min- and max-entropy.

**Lemma 2.5.** Let $X, Y, Z$ be random variables and $\varepsilon, \varepsilon' \geq 0$ such that $\varepsilon + \varepsilon' \in [0, 1)$. Then

$$H_\infty^\varepsilon(X|Z) - H_0^{\varepsilon'}(X|YZ) \leq H_\infty^{\varepsilon+\varepsilon'}(Y|Z).$$

**Proof.** Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$ and

$$\max_{x,z} P_{X\Omega|Z=z}(x) \leq r_{\text{min}}^\varepsilon(X|Z).$$

Let $\Omega'$ be an event with $\Pr[\Omega'] \geq 1 - \varepsilon'$ and

$$\max_{y,z} |\text{supp}(P_{X\Omega'|Y=y,Z=z})| \leq r_{\text{max}}^\varepsilon(X|YZ).$$

Then $\Pr[\Omega, \Omega'] \geq 1 - \varepsilon - \varepsilon'$ and

$$r_{\text{min}}^{\varepsilon+\varepsilon'}(Y|Z) \leq \max_{y,z} P_{Y\Omega'|Z=z}(y).$$
We obtain
\[
\max_{y,z} P_{Y\Omega'|Z=z}(y) = \max_{y,z} \sum_x P_{XY\Omega'|Z=z}(x, y) \\
\leq \max_{y,z} \sum_{x'} \max_x P_{XY\Omega'|Z=z}(x', y) \\
\leq \max_{y,z} (|\text{supp}(P_{X\Omega'|Y=y,Z=z})| \max_x P_{XY\Omega'|Z=z}(x, y)) \\
\leq \max_{y,z} (\max_y |\text{supp}(P_{X\Omega'|Y=y,Z=z})| \max_x P_{XY\Omega'|Z=z}(x, y)) \\
\leq \max_{y,z} (\max_y |\text{supp}(P_{X\Omega'|Y=y,Z=z})| \max_x P_{X\Omega|Z=z}(x)) \\
\leq \max_{y,z} |\text{supp}(P_{X\Omega'|Y=y,Z=z})| \cdot \max_{x,z} P_{X\Omega|Z=z}(x) .
\]

Note that the proof also implies the stronger inequality
\[
H^\varepsilon_\infty(XY|Z) - H^{\varepsilon'}_\infty(X|YZ) \leq H^{\varepsilon'+\varepsilon}_\infty(Y|Z),
\]
which corresponds in a certain sense to the inequality
\[
H(X|Z) - H(X|YZ) \leq H(XY|Z)
\]
for the Shannon entropy.

Next, we show that conditioning on an additional random variable cannot reduce the conditional smooth entropies.

**Lemma 2.6 (Monotonicity).** Let $X, Y, Z$ be random variables and $\varepsilon \in [0, 1)$. Then
\[
H^\varepsilon_\infty(X|Z) \geq H^\varepsilon_\infty(X|YZ) .
\]

**Proof.** Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$. Then
\[
\max_{x,z} P_{X\Omega|Z=z}(x) = \max_{x,z} \sum_y P_{Y|Z=z}(y) P_{X\Omega|Y=y,Z=z}(x) \\
\leq \max_{x,z} \sum_y P_{Y|Z=z}(y) \max_{x,y',z} P_{X\Omega|Y=y',Z=z}(x) \\
\leq \max_{x,y,z} P_{X\Omega|Y=y,Z=z}(x) .
\]

The following lemma shows that the smooth min-entropy $H^\varepsilon_\infty(X|Y)$ satisfies a data processing inequality, i.e., it cannot be decreased by additionally processing $Y$.

**Lemma 2.7 (Data Processing).** Let $X, Y, Z$ be random variables with $X \leftrightarrow Y \leftrightarrow Z$ and $\varepsilon \in [0, 1)$. Then
\[
H^\varepsilon_\infty(X|Y) \leq H^\varepsilon_\infty(X|YZ) .
\]
Proof. Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$ and $\Omega \leftrightarrow XY \leftrightarrow Z$ such that
\[
r^\varepsilon_\infty (X|Y) = \max_{x,y} (P_{X\Omega|Y=y}(x)).
\]
Then
\[
r^\varepsilon_\infty (X|YZ) \leq \max_{x,y,z} P_{X\Omega|Y=y,Z=z}(x) \]
\[
= \max_{x,y,z} P_{X|Y=y,Z=z}(x) P_{\Omega|X=x,Y=y,Z=z} \]
\[
= \max_{x,y} P_{X|Y=y}(x) P_{\Omega|X=x,Y=y} \]
\[
= \max_{x,y} P_{X\Omega|Y=y}(x). \qedhere
\]

The smooth max-entropy $H^\varepsilon_0(X|Y)$ also satisfies a data processing inequality, i.e., it cannot be decreased by additionally processing $Y$.

**Lemma 2.8.** Let $X, Y, Z$ be random variables with $X \leftrightarrow Y \leftrightarrow Z$ and $\varepsilon \in [0, 1)$. Then
\[
H^\varepsilon_0(X|Y) \leq H^\varepsilon_0(X|YZ).
\]

**Proof.** Let $\Omega$ be an event such that
\[
r^\varepsilon_0(X|YZ) = \max_{y,z} |\text{supp} (P_{X\Omega|Y=y,Z=z})|.
\]
For all $y$, we define $\varepsilon_y := P_{\Omega|Y=y}$. Let $\Omega_y$ be an event such that
\[
r^\varepsilon_y(X|Z, Y = y) = \max_{z} |\text{supp} (P_{X\Omega_y|Y=y,Z=z})|.
\]
Let $\bar{z}_y$ be such that $P_{\Omega_y|Y=y,Z=\bar{z}_y}$ is maximal. We define $\bar{\Omega}$ with $P_{\bar{\Omega}|X=x,Y=y} := P_{\Omega_y|X=x,Y=y,Z=\bar{z}_y}$. Then, we have $P_{\bar{\Omega}|Y=y} \geq P_{\Omega_y|Y=y} \geq 1 - \varepsilon_y$ and $P_{X\bar{\Omega}|Y=y,Z=z} \geq P_{X\Omega_y|Y=y,Z=\bar{z}_y} = P_{X\Omega|Y=y}$ and, therefore,
\[
r^\varepsilon_y(X|Z, Y = y) \geq r^\varepsilon_0(X|Y = y).
\]
Thus, we get
\[
r^\varepsilon_0(X|YZ) = \max_{y,z} |\text{supp} (P_{X\Omega|Y=y,Z=z})| \]
\[
\geq \max_{y} r^\varepsilon_y(X|Z, Y = y) \]
\[
\geq \max_{y} r^\varepsilon_y(X|Y = y) \]
\[
\geq r^\varepsilon_0(X|Y). \qedhere
\]
The next lemma bounds the smooth conditional min-entropy of an additional random variable $Y$.

**Lemma 2.9.** Let $X, Y, Z$ be random variables and $\varepsilon \in [0, 1)$. Then

$$H^\varepsilon_\infty(X|Z) \geq H^\varepsilon_\infty(XY|Z) - H_0(Y).$$

**Proof.** Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$ and

$$\max_{x,y,z} P_{XY|Z=\omega}(x,y) = r^\varepsilon_\infty(XZ|Z).$$

Then, we have

$$\max_{x,y,z} P_{XY|Z=\omega}(x,y) \cdot |\text{supp}(P_Y)| \geq \max_{x,z} \sum_y P_{XY|Z=\omega}(x,y)$$

$$= \max_{x,z} P_{X|Z=\omega}(x)$$

$$\geq r^\varepsilon_\infty(X|Z). \qed$$

The smooth max-entropy satisfies the following monotonicity properties.

**Lemma 2.10.** Let $X, Y, Z$ be random variables and $\varepsilon \in [0, 1)$. Then

$$H^\varepsilon_0(XY|Z) \geq H^\varepsilon_0(X|Z) \geq H^\varepsilon_0(X|YZ).$$

**Proof.** Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$. Then the first inequality follows from

$$\max_z |\text{supp}(P_{XY|Z=\omega})| \geq \max_z |\text{supp}(P_{X|Z=\omega})|.$$ 

and the second inequality from

$$\max_{y,z} |\text{supp}(P_{X|Y=\omega, Z=\omega})| \leq \max_z |\text{supp}(P_{X|Z=\omega})|. \qed$$

Next, we show that Lemmas 2.5, 2.6, 2.7 and (a stronger variant of) Lemma 2.9 also hold for $\tilde{H}^\varepsilon_\infty(X|Y)$. We introduce the following auxiliary quantity.

**Definition 2.9.** For a distribution $P_{XY}$ and $\varepsilon \in [0, 1)$, we define

$$\tilde{r}^\varepsilon_\infty(X|Y) := \min_{\Omega: \Pr[\Omega] \geq 1 - \varepsilon} \sum_y P_Y(y) \max_x P_{XY|Y=\omega}(x).$$
Lemma 2.11. Let $X, Y, Z$ be random variables and $\varepsilon, \varepsilon' \geq 0$ such that $\varepsilon + \varepsilon' \in [0, 1)$. Then

$$\tilde{H}_\infty^\varepsilon (X|Z) - H_0^\varepsilon' (X|YZ) \leq \tilde{H}_\infty^{\varepsilon + \varepsilon'} (Y|Z).$$

Proof. Let $\Omega$ be an event with $\Pr[\Omega] \geq 1 - \varepsilon$ and

$$\sum_z \max_x P_{XZ\Omega}(x, z) \leq \tilde{r}_\infty^\varepsilon (X|Z).$$

Let $\Omega'$ be an event with $\Pr[\Omega'] \geq 1 - \varepsilon'$ such that

$$\max_{y, z} |\text{supp} (P_{X\Omega'|Y=y, Z=z})| \leq r_{\max}^\varepsilon (X|YZ).$$

Then $\Pr[\Omega, \Omega'] \geq 1 - \varepsilon - \varepsilon'$ and

$$\tilde{r}_{\infty}^{\varepsilon + \varepsilon'} (Y|Z) \leq \sum_z P_Z(z) \max_y P_{Y\Omega'|Z=z}(y).$$

We have for all $z$

$$\max_{x, y} P_{XY\Omega'|Z=z}(x, y) \leq \max_{x, y} P_{XY\Omega'|Z=z}(x, y) \leq \max_x P_{X\Omega|Z=z}(x).$$

Furthermore, it holds that

$$|\{x : P_{XY\Omega'|Z=z}(x, y)\} \leq |\text{supp} (P_{X\Omega'|Y=y, Z=z})|.\]

Together, we obtain

$$\sum_z P_Z(z) \max_y P_{Y\Omega'|Z=z}(y) = \sum_z P_Z(z) (\max_y \sum_x P_{XY\Omega'|Z=z}(x, y))$$

$$\leq \sum_z P_Z(z) (\max_{y, z} |\text{supp} (P_{X\Omega'|Y=y, Z=z})| \cdot \max_{x, y} P_{XY\Omega'|Z=z}(x, y))$$

$$\leq \max_{y, z} |\text{supp} (P_{X\Omega'|Y=y, Z=z})| \cdot \sum_z P_Z(z) \max_x P_{X\Omega|Z=z}(x)$$

$$\leq \tilde{r}_{\infty}^\varepsilon (X|Z) \cdot r_{\max}^\varepsilon (X|YZ).$$

Lemma 2.12. Let $X, Y, Z$ be random variables and $\varepsilon \in [0, 1)$. Then

$$\tilde{H}_\infty^\varepsilon (X|YZ) \geq \tilde{H}_\infty^\varepsilon (X|Y|Z) - H_0(Y).$$
2.3. Classical Smooth Min- and Max-Entropies

Proof. Let Ω be an event with \( \Pr[\Omega] \geq 1 - \varepsilon \) and

\[
\sum_z P_Z(z) \max_{x,y} P_{X Y \Omega \mid Z = z}(x, y) = \tilde{r}^\varepsilon_\infty(X Y \mid Z) .
\]

Then it holds that

\[
\sum_z P_Z(z) \max_{x,y} P_{X Y \Omega \mid Z = z}(x, y) \cdot |\text{supp}(P_Y)| \\
\geq \sum_z P_Z(z) \sum_y \max_x P_{X Y \Omega \mid Z = z}(x, y) \\
= \sum_{y, z} P_{YZ}(y, z) \max_x P_{X \Omega \mid Y = y, Z = z}(x) \\
\geq \tilde{r}^\varepsilon_\infty(X \mid Y Z). \quad \Box
\]

Lemma 2.13. Let \( X, Y, Z \) be random variables and \( \varepsilon \in [0, 1) \). Then

\[
\tilde{H}^\varepsilon_\infty(X \mid Z) \geq \tilde{H}^\varepsilon_\infty(X \mid Y Z).
\]

Proof. Let Ω be an event with \( \Pr[\Omega] \geq 1 - \varepsilon \). Then

\[
\sum_z P_Z(z) \max_x P_{X \Omega \mid Z = z}(x) \\
= \sum_z P_Z(z) \max_x \sum_y P_{Y \mid Z = z}(y) P_{X \Omega \mid Y = y, Z = z}(x) \\
\leq \sum_z P_Z(z) \max_{x, y} P_{X \Omega \mid Y = y, Z = z}(x). \quad \Box
\]

Lemma 2.14 (Data Processing). Let \( X, Y, Z \) be random variables with \( X \leftrightarrow Y \leftrightarrow Z \) and \( \varepsilon \in [0, 1) \). Then

\[
\tilde{H}^\varepsilon_\infty(X \mid Y) \leq \tilde{H}^\varepsilon_\infty(X \mid Y Z).
\]

Proof. Let Ω be an event with \( \Pr[\Omega] \geq 1 - \varepsilon \) and \( \Omega \leftrightarrow XY \leftrightarrow Z \) such that

\[
\tilde{r}^\varepsilon_\infty(X \mid Y) = \sum_y \max_x P_{X Y \Omega}(x, y).
\]

It holds that

\[
P_{X \Omega \mid Y = y, Z = z}(x) = P_{X \mid Y = y, Z = z}(x) P_{\Omega \mid X = x, Y = y, Z = z} \\
= P_{X \mid Y = y}(x) P_{\Omega \mid X = x, Y = y} \\
= P_{X \Omega \mid Y = y}(x). \]
Thus, we have
\[
\tilde{r}_\infty^\varepsilon(X|YZ) \leq \sum_{y,z} P_{YZ}(y, z) \max_x P_{X|Y=y,Z=z}(x) = \sum_y P_Y(y) \max_x P_{X|Y=y}(x).
\]

2.4 Min-Entropy Sampling

In the security proof for the reduction of String-OT from Universal-OT using the protocol from [CS06], we make use of a known result on min-entropy-sampling. First, we introduce averaging samplers.

**Definition 2.10.** An \((n, \xi, \varepsilon)-\)sampler is a probability distribution \(P_S\) over subsets \(S \subset [n]\) with the property that

\[
\Pr \left[ \frac{1}{|S|} \sum_{i \in S} \beta_i \leq \frac{1}{n} \sum_{i=1}^n \beta_i - \xi \right] \leq \varepsilon, \quad \text{for all } (\beta_1, \ldots, \beta_n) \in [0, 1]^n.
\]

The following lemma is a consequence of the Hoeffding-Azuma inequality.

**Lemma 2.15 ([BH05]).** Let \(r < n\) and let \(P_S\) be the uniform distribution over subsets \(S \subset [n]\) of size \(|S| = r\). This defines a \((n, \xi, e^{-r\xi^2/2})\) sampler for every \(r > 0\) and \(\xi \in [0, 1]\).

In [Vad03] it has been shown that randomly sampling bits from a weak random source preserves the min-entropy rate up to an arbitrarily small additive loss. This refines a result from [NZ96] and implies, together with Lemma 2.15, the following lemma.

**Lemma 2.16 ([Vad03]).** Let \(S\) be uniformly distributed over the subsets \(s \subset [n]\) of size \(|s| = r\). Let \(\tau > 0\). We define \(\theta := \tau / \log(\tau)\) and \(\gamma := 2^{-r\theta^2/2}\). Then there exists a constant \(c > 0\) such that for every \(X\) from \([0, 1]^n\) with \(H_\infty(X) \geq \delta n\) on \([0, 1]^n\) the random variable \((S, X_S)\) is \((\gamma + 2^{-ctn})\)-close to \((A, B)\) where \(A\) is uniform over the subsets \(S \subset [n]\) of size \(|S| = r\) and \(H_\infty(B|A) \geq (\delta - 3\tau)r\), i.e., \(B\) has min-entropy at least \((\delta - 3\tau)r\) conditioned on every \(a\).
2.5 Randomness Extraction and Privacy Amplification

The min-entropy characterizes the amount of uniform randomness that can be extracted from a random variable $X$ using two-universal hashing. A family of functions is called two-universal if the collision probability of $x \neq x'$ is the same as for a completely random function.

**Definition 2.11.** Let $\mathcal{F}$ be a family of functions from $\mathcal{X}$ to $\mathcal{Z}$. Then $\mathcal{F}$ is called *two-universal* if, for all $x \neq x' \in \mathcal{X}$,

$$\Pr[f(x) = f(x')] \leq \frac{1}{|\mathcal{Z}|},$$

where the probability is taken over $f$ chosen uniformly from $\mathcal{F}$.

The following theorem shows that two-universal hash functions are strong extractors, i.e., the output of the function is uniform with respect to the choice of the function.

**Lemma 2.17** (Leftover hash lemma \[BBR88, ILL89\]). Let $\mathcal{F}$ be a two-universal family of hash functions from $\mathcal{X}$ to $\{0, 1\}^\ell$ with $\ell > 0$. Let $X$ be a random variable over $\mathcal{X}$. Then

$$D(P_{F(X)\mathcal{F}}, P_{UNI\ell}P_F) \leq \frac{1}{2} \sqrt{2^\ell - H_\infty(X)},$$

for $F$ independent and uniform over $\mathcal{F}$.

It is important to stress that the extracted key $F(X)$ is secure even if the adversary is given $F$. Lemma 2.17 immediately gives rise to a procedure allowing parties sharing some random variable $X$ to extract a key secure against an adversary by public discussion. Indeed, one party can simply choose a function $f$ from the family $\mathcal{F}$ uniformly at random, and publicly distribute $f$. Since two-universal hash functions can be efficiently constructed (using, for example, linear functions \[CW79\]), this privacy amplification protocol \[BBR88, ILL89, BBCM95\] is efficient.

2.6 Interactive Hashing

In the protocol of Section 3.5 we make use of *interactive hashing* (IH), a tool that has been introduced in \[OVY91\] and used in \[CCM98, Din01\].
IH is a two-party primitive where Bob inputs a bit string $W \in \{0, 1\}^t$, and Alice has no input. The primitive then generates two strings $W_0, W_1 \in \{0, 1\}^t$, with the property that one of the two equals $W$. For a protocol implementing this primitive, security is intuitively specified by the following conditions: Alice does not learn which of the two strings is equal to $W$. Conversely, Bob should not have too much control over the strings created by the protocol. In particular, he should not be able to force both outputs to be from a small set.

Lemma 2.18 (Interactive Hashing [OVY91, CCM98, Din01, Sav07]). There exists a protocol called interactive hashing between two players, Alice and Bob, where Alice has no input, Bob has input $W \in \{0, 1\}^t$ and both players output $(W_0, W_1) \in \{0, 1\}^t \times \{0, 1\}^t$, satisfying the following:

1. Correctness: If both players are honest, then $W_0 \neq W_1$ and there exists a $D \in \{0, 1\}$ such that $W_D = W$. Furthermore, the distribution of $W_{1-D}$ is uniform on $\{0, 1\}^t \setminus \{W\}$.

2. Security for Bob: If Bob is honest, then $W_0 \neq W_1$ and there exists a $D \in \{0, 1\}$ such that $W_D = W$. If Bob chooses $W$ uniformly at random, then $D$ is uniform and independent of Alice’s view.

3. Security for Alice: If Alice is honest, then, for all $S \subseteq \{0, 1\}^t$,

$$\Pr[W_0 \in S \text{ and } W_1 \in S] \leq 16 \cdot \frac{|S|}{2^t}.$$

2.7 Quantum Information

In this section, we introduce the notation we use to describe quantum systems and present some concepts from quantum information theory. We refer to [NC00] and [Wat08] for a detailed introduction to quantum information theory.

In this thesis, we restrict our attention to finite-dimensional quantum systems and use the density operator formalism on finite dimensional Hilbert spaces. We use capital letters $A, B, C$ to denote quantum systems or quantum registers, and use the notation $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$ for the Hilbert spaces associated with these systems. We use the notation $|A|$ for the dimension of a system $A$.

We use $\mathcal{P}(\mathcal{H})$ to denote the set of positive semi-definite operators on $\mathcal{H}$. We call a positive semi-definite operator $\rho_A \in \mathcal{P}(\mathcal{H})$ pure if it has rank one. A pure operator $\rho_A$ can be represented as a ket $|\psi\rangle_A$, i.e., $\rho_A = |\psi\rangle_A \langle \psi|_A$. 
An operator that is not pure is called \textit{mixed}. We define the set of quantum states by 
\[ S_\otimes(\mathcal{H}) := \{ \rho \in \mathcal{P}(\mathcal{H}) : \text{tr} \rho = 1 \}. \]
For technical reasons, we also consider the set of sub-normalized states that is defined by 
\[ S_{\leq}(\mathcal{H}) := \{ \rho \in \mathcal{P}(\mathcal{H}) : 0 < \text{tr} \rho \leq 1 \}. \]
Given a quantum state \( \rho_{AB} \in S_\otimes(\mathcal{H}_A \otimes \mathcal{H}_B) \) we denote by \( \rho_A \) and \( \rho_B \) its marginal states \( \rho_A = \text{tr}_B(\rho_{AB}) \) and \( \rho_B = \text{tr}_A(\rho_{AB}) \). We also use indices to denote multipartite Hilbert spaces, i.e., 
\( \mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B \). We use the symbol \( \mathbb{I}_A \) to denote either the identity operator on \( \mathcal{H}_A \) or the identity operator on \( \mathcal{P}(\mathcal{H}_A) \); it should be clear from the context which one is meant.

Given a finite set \( \mathcal{X} \) and an orthonormal basis \( \{ |x\rangle | x \in \mathcal{X} \} \) of a Hilbert space \( \mathcal{H}_X \cong (\mathbb{C}^{|\mathcal{X}|}) \) we can encode a classical probability distribution \( P_X \) as a quantum state

\[ \rho_X = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle \langle x| \quad . \]

Thus, we can represent any discrete probability distribution as a state of a quantum system. We usually denote these classical systems by letters \( X, Y, Z \). We define the state corresponding to the uniform distribution on \( \mathcal{X} \) as 
\[ \pi_{\mathcal{X}} := \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} |x\rangle \langle x| \; . \]

A state \( \rho_{XB} \in S_\otimes(\mathcal{H}_X \otimes \mathcal{H}_B) \) is a \textit{classical-quantum} state (cq-state) if the state of the system \( B \) depends on the random variable \( X \), i.e., it is of the form

\[ \rho_{XB} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle \langle x| \otimes \rho_x^B \; . \] (2.7.1)

This notion can be generalized in a natural way to states that depend on several random variables, for example to ccq-states \( \rho_{XYB} \) which are classical on \( X \) and \( Y \). For a cq-state \( \rho_{XB} \), \( X \) is independent of \( B \) if and only if \( \rho_{XB} = \rho_X \otimes \rho_B \). For a cq-state \( \rho_{XB} \) and an event \( \mathcal{A} \) defined by a conditional distribution \( P_{\mathcal{A}|X} \), the state conditioned on the event \( \mathcal{A} \) is defined as 
\[ \rho_{XB|\mathcal{A}} := \sum_x P_{\mathcal{A}|X}(x) |x\rangle \langle x| \otimes \rho_x^B \; . \]

Any transformation of a quantum system can be represented by a trace-preserving completely positive map (TP-CPM). Any such transformations can be simulated by adding an ancillary system, applying a unitary on the composite system, and then tracing out part of the remaining system. More precisely, for any TP-CPM \( E \) from \( S_\otimes(\mathcal{H}_A) \) to \( S_\otimes(\mathcal{H}_B) \), there
exists a Hilbert space $\mathcal{H}_R$, a unitary $U$ acting on $\mathcal{H}_{ABR}$ and a pure state $\sigma_{BR} \in \mathcal{S}_-(\mathcal{H}_{BR})$ such that

$$\mathcal{E}(\rho_A) = \text{tr}_{AR}(U(\rho_A \otimes \sigma_{BR})U^\dagger). \quad (2.7.2)$$

This is known as the Stinespring dilation \cite{Sti55} of $\mathcal{E}$.

A measurement can be seen as a completely positive trace preserving map that takes a quantum state on $A$ and maps it to a classical register $X$, which contains the measurement result, and a system $A'$, which contains the post-measurement state. Such a measurement map is of the form

$$\mathcal{M}(\rho_A) = \sum \langle x | x \rangle_X \otimes M_x \rho_A M_x^\dagger,$$

where all $| x \rangle$ are from an orthonormal basis of $\mathcal{H}_X$ and the $M_x$ are such that $\mathcal{M}$ is a TP-CPM. Then, the probability that we measure $x$ is given by $\text{tr}(M_x \rho_A M_x^\dagger)$. Furthermore, the state of $A'$ is $M_x \rho_A M_x^\dagger / \text{tr}(M_x \rho_A M_x^\dagger)$ if the outcome of the measurement is $x$. A projective measurement is a special case of a quantum measurement where all measurement operators $M_x$ are projectors. If the post-measurement state is not important and we are only interested in the classical result, the measurement can be fully described by the set of operators $\{ M_x M_x^\dagger \}$. Such a set is then called a positive operator valued measure (POVM).

According to \eqref{eq:2.7.2}, any measurement has a Stinespring dilation, i.e., there exists a Hilbert space $\mathcal{H}_R$, a unitary $U$ acting on $\mathcal{H}_{AXA'R}$ and a pure state $\sigma_{XA'BR} \in \mathcal{S}_-(\mathcal{H}_{XA'RR})$ with $\mathcal{M}(\rho_A) = \text{tr}_{AR}(U(\rho_A \otimes \sigma_{XA'BR})U^\dagger)$.

The Hadamard transform is the unitary described by the matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ in the computational basis $\{|0\rangle, |1\rangle\}$. For $x, \theta \in \{0,1\}^n$, we write $H^\theta | x \rangle$ for the state $H^\theta | x \rangle = H^\theta_1 | x_1 \rangle \ldots H^\theta_n | x_n \rangle$. We also call states of this form BB84-states. When speaking of the basis $\theta \in \{0,1\}^n$ we mean the basis $\{ H^\theta | x \rangle : x \in \{0,1\}^n \}$. For a given basis $\{| x_1 \rangle, \ldots, | x_d \rangle \}$ we say that we measure in basis $B$ to indicate that we perform a projective measurement given by the operators $P_k = | x_k \rangle \langle x_k |$ for all $k \in [d]$.

For any quantum state $\rho_A$, there exists a pure quantum state $| \psi \rangle_{AA'} \in \mathcal{H}_{AA'}$ with $\mathcal{H}_A \simeq \mathcal{H}_{A'}$ such that $\rho_A = \text{tr}_A(| \psi \rangle \langle \psi |_{AA'})$. The state $| \psi \rangle_{AA'}$ is called a purification of $\rho_A$. For a cq-state $\rho_{XB} = \sum_{x \in \mathcal{X}} P_X(x) | x \rangle \langle x | \otimes \rho_B^x$, we can choose the purification to be of the form

$$| \psi \rangle_{XX'B'B'} = \sum_{x \in \mathcal{X}} | x \rangle_X \otimes | x \rangle_{X'} \otimes | \psi^x \rangle_{BB'},$$

where $| \psi^x \rangle_{BB'}$ is a purification of $\rho_B^x$ on $BB'$.  

2.7. Quantum Information

Distance Measures

Definition 2.12. For $\rho, \tau \in S_\oplus(H_\Lambda)$, we define the trace distance between $\rho$ and $\tau$ as

$$D(\rho, \tau) := \frac{1}{2} \|\rho - \tau\|_1 ,$$

where the Schatten 1-norm is defined as $\|X\|_1 := \text{tr} |X| = \text{tr} \sqrt{X^\dagger X}$.

The trace distance between two quantum states $\rho$ and $\tau$ can also be defined as

$$D(\rho, \tau) := \max_E D(E(\rho), E(\tau)) ,$$

where the maximum is over all POVMs and $E(\rho)$ is the probability distribution of the measurement outcomes. For $b \in \{0, 1\}$, let

$$\rho_{XB}^b = \sum_x |x\rangle\langle x| \otimes \rho_{x,b}^\Lambda$$

be cq-states. Then, we have

$$\|\rho_{XB}^0 - \rho_{XB}^1\|_1 = \sum_{x \in X} \|\rho_{x,0}^\Lambda - \rho_{x,1}^\Lambda\|_1 . \quad (2.7.3)$$

Definition 2.13. For $\rho_{AB} \in S_\oplus(H_{\Lambda^B})$ we define the distance from uniform of $A$ conditioned on $B$ as

$$\Delta(A|B)_\rho := \min_{\sigma_B} D(\rho_{AB}, \pi_A \otimes \sigma_B) ,$$

where the minimum is taken over all $\sigma_B \in S_\oplus(H_B)$.

Lemma 2.19. Let $\rho_{XB} = \sum_{x \in \{0,1\}} \frac{1}{2} |x\rangle\langle x| \otimes \rho_{x,B}^\Lambda$ be a cq-state and $\Delta(X|B)_\rho \leq \varepsilon$. Then

$$D(\rho_{X,B}^0, \rho_{X,B}^1) \leq 2\varepsilon .$$

Proof. $D(\rho_{X,B}, \pi_{\{0,1\}} \otimes \sigma_B) \leq \varepsilon$ implies

$$\|\rho_{B}^0 - \rho_{B}^1\|_1 \leq \|\rho_{B}^0 - \sigma_B\|_1 + \|\rho_{B}^1 - \sigma_B\|_1 \leq 4\varepsilon ,$$

where we used (2.7.3) and, therefore, we have $D(\rho_{B}^0, \rho_{B}^1) \leq 2\varepsilon$.

Another measure of distance is the fidelity between two quantum states.
Definition 2.14. The fidelity between two operators \( \rho, \tau \in \mathcal{P}(\mathcal{H}) \) is defined as

\[
F(\rho, \tau) := \|\sqrt{\rho}\sqrt{\tau}\|_1.
\]

The fidelity can be related to the trace distance by the inequalities [FvdG99]

\[
1 - D(\rho, \tau) \leq F(\rho, \tau) \leq \sqrt{1 - D(\rho, \tau)}
\]

(2.7.4)

for any two quantum states \( \rho \) and \( \tau \).

To prove our impossibility results in Sections 5.2 and 5.4, we will make use of the following well-known technical lemma which is also used in [May97, LC97, Lo97]. Let \( |\phi\rangle^0_{AB} \) and \( |\phi\rangle^1_{AB} \) be two pure states. If the marginal state of \( |\phi\rangle^0_{AB} \) and \( |\phi\rangle^1_{AB} \) on system \( B \) is (almost) the same, then there exists a unitary \( U_A \) on system \( A \) that (approximately) transforms \( |\phi\rangle^0_{AB} \) into \( |\phi\rangle^1_{AB} \), i.e., \( (U_A \otimes 1_B)|\phi^0_{AB} \approx |\phi^1_{AB} \).

Lemma 2.20. Let \( |\psi^0_{AB} \rangle \) and \( |\psi^1_{AB} \rangle \) be states with \( D(\rho_B^0, \rho_B^1) \leq \epsilon \) where \( \rho_B^x = \text{tr}_A(|\psi^x\rangle\langle\psi^x|_{AB}) \). Then there exists a unitary \( U_A \) such that

\[
D(|\phi^1_{AB} \rangle\langle\phi^1_{AB}|, |\psi^1_{AB} \rangle\langle\psi^1_{AB}|) \leq \sqrt{2\epsilon}
\]

with \( |\phi^1_{AB} \rangle = (U_A \otimes 1_B)|\psi^0_{AB} \rangle \).

Proof. \( D(\rho_B^0, \rho_B^1) \leq \epsilon \) implies \( F(\rho_B^0, \rho_B^1) \geq 1 - \epsilon \). From Uhlmann’s theorem [Uhl76] we know that there exists a unitary \( U_A \) such that

\[
F(|\phi^1_{AB} \rangle\langle\phi^1_{AB}|, |\psi^1_{AB} \rangle\langle\psi^1_{AB}|) \geq 1 - \epsilon
\]

where \( |\phi^1_{AB} \rangle = (U_A \otimes 1_B)|\psi^0_{AB} \rangle \). It follows from (2.7.4) that \( D(\rho, \tau) \leq \sqrt{1 - F(\rho, \tau)^2} \). Thus, we have \( \sqrt{1 - D(|\phi^1_{AB} \rangle\langle\phi^1_{AB}|, |\psi^1_{AB} \rangle\langle\psi^1_{AB}|)^2} \geq 1 - \epsilon \). Hence,

\[
D(|\phi^1_{AB} \rangle\langle\phi^1_{AB}|, |\psi^1_{AB} \rangle\langle\psi^1_{AB}|) \leq \sqrt{1 - (1 - \epsilon)^2} \leq \sqrt{2\epsilon}.
\]

Lemma 2.20 can be generalized to states which are pure conditioned on all classical information available to both \( A \) and \( B \) in the following way.

Lemma 2.21. For \( b \in \{0, 1\} \), let

\[
\rho^b_{XX'AB} = \sum_x P_b(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes |\psi^{x,b}_{AB} \rangle\langle\psi^{x,b}_{AB}|_{AB}
\]
with $D(\rho^0_{X'B}, \rho^1_{X'B}) \leq \varepsilon$. Then there exists a unitary $U_{XA}$ such that

$$D(\rho^1_{XX'AB}, \rho^1_{XX'AB}) \leq \sqrt{2\varepsilon}$$

where $\rho^1_{XX'AB} = (U_{XA} \otimes \mathbb{1}_{X'B}) \rho^0_{XX'AB} (U_{XA} \otimes \mathbb{1}_{X'B})^\dagger$. 

**Proof.** Define $|\psi^b_{XX'X''AB}\rangle := \sum_x \sqrt{p_b(x)} |x\rangle_X \otimes |x\rangle_{X'} \otimes |x\rangle_{X''} \otimes |\psi^{x,b}_{XX'}\rangle_{AB}$ and let

$$\rho^b_{XX'X''B} = \text{tr}_{X''}(|\psi^b_{XX'X''AB}\rangle \langle \psi^b_{XX'X''AB}|).$$

Then

$$D(\rho^0_{XX'B}, \rho^1_{XX'B}) = D(\rho^0_{XX'B}, \rho^1_{XX'B}) \leq \varepsilon.$$ 

Thus, Lemma 2.20 implies the existence of a unitary $U_{XA}$ such that

$$D(|\phi^1_{XX'X''AB}\rangle \langle \phi^1_{XX'X''AB}|, |\psi^1_{XX'X''AB}\rangle \langle \psi^1_{XX'X''AB}|) \leq \sqrt{2\varepsilon}$$

with $|\phi^1_{XX'X''AB}\rangle = (U_{XA} \otimes \mathbb{1}_{X'B}) |\psi^0_{XX'X''AB}\rangle$. The statement then follows from the fact that taking the partial trace over $X''$ cannot increase the trace distance and commutes with the unitary $U_{XA}$ as follow: Omitting the identity operators on $X'B$ and $X'X''B$, we have

$$D(\rho^1_{XX'AB}, \rho^1_{XX'AB}) = D((U_{XA}) \text{tr}_{X''}(\rho^0_{XX'X''AB})(U_{XA})^\dagger, \text{tr}_{X''}(\rho^1_{XX'X''AB})) = D(\text{tr}_{X''}((U_{XA}) \rho^0_{XX'X''AB}(U_{XA})^\dagger, \text{tr}_{X''}(\rho^1_{XX'X''AB})) \leq D((U_{XA}) \rho^0_{XX'X''AB}(U_{XA})^\dagger, \rho^1_{XX'X''AB}) \leq \sqrt{2\varepsilon}.$$

\[\square\]

### 2.7.1 Quantum Entropies

In the following, we will introduce different entropic quantities for quantum systems and present some of their properties. First, we introduce the (conditional) von Neumann entropy.

**Von Neumann Entropy**

**Definition 2.15.** The von Neumann entropy is defined as

$$H(A|B)_\rho := H(\rho_{AB}) - H(\rho_B),$$

where $H(\rho) := \text{tr}(-\rho \log(\rho))$. 

The Alicki-Fannes inequality \[AF04\] implies that, for any state $\rho_{AB} \in \mathcal{H}_{AB}$ with $D(\rho_{AB}, \tau_A \otimes \rho_B) \leq \varepsilon$, we have

$$H(A|B)_\rho \geq (1 - 4\varepsilon) \cdot \log |A| - 2h(\varepsilon). \tag{2.7.5}$$

Let $X \in \{0, 1\}^k$. If there exists a measurement on $B$ with outcome $X'$ such that $\Pr[X' \neq X] \leq \varepsilon$, then

$$H(X|B)_\rho \leq H(X|X') \leq h(\varepsilon) + \varepsilon \cdot k. \tag{2.7.6}$$

Let $\rho_{ABC}$ be a tripartite state. Subadditivity and the triangle inequality \[AL70\] imply that

$$H(A|BC)_\rho \geq H(A|B)_\rho - 2H(C)_\rho. \tag{2.7.7}$$

The conditional entropy $H(A|B)_\rho$ can decrease by at most $\log |Z|$ when conditioning on an additional classical system $Z$, i.e., for any tripartite state $\rho_{ABZ}$ that is classical on $Z$ with respect to some orthonormal basis $\{|z\rangle\}_z$, we have

$$H(A|BZ)_\rho \geq H(A|B)_\rho - \log |Z|. \tag{2.7.8}$$

Relative Entropy

**Definition 2.16.** The *relative entropy* for two quantum states $\rho$ and $\sigma$ is defined as

$$S(\rho||\sigma) := \text{tr}(\rho \log \rho) - \text{tr}(\rho \log \sigma).$$

If $\rho_X = \sum_x P_X(x)|x\rangle\langle x|$ and $\sigma_X = \sum_x Q_X(x)|x\rangle\langle x|$, i.e., both states are classical, then

$$S(\rho||\sigma) = D_{KL}(P_X||Q_X). \tag{2.7.9}$$

The quantum relative entropy cannot increase under quantum operations \[Lin75, Uhl77\], i.e., we have

$$S(\rho||\sigma) \geq S(\mathcal{E}(\rho)||\mathcal{E}(\sigma)). \tag{2.7.10}$$

for any TP-CPM $\mathcal{E}$. 
Smooth Min- and Max-Entropy

Quantum versions of the (smooth) min- and max-entropy have first been considered in [Ren05, RK05] in the context of quantum cryptography. The smooth entropy formalism has been developed further and found a wide range of applications since then. The relevance of these entropic measures comes from the fact that they have operational meanings, i.e., they quantitatively characterize certain tasks in information theory. The min-entropy $H_{\min}^\varepsilon(X|B)$ characterizes the uniform randomness that can be extracted from $X$ against quantum side information $B$ [Ren05] (cf. Section 2.7.2). The max-entropy $H_{\max}^\varepsilon(X|B)$ characterizes source compression with quantum side information $B$ [RR10]. Moreover, the max-entropy $H_{\max}^\varepsilon(X|B)$ characterizes the amount of entanglement needed in single-shot state merging [Ber08]. For a detailed introduction to the smooth entropy framework we refer to [Tom12].

First, we define the non-smooth min-entropy.

**Definition 2.17.** Let $\rho_{AB} \in S_{\leq}(\mathcal{H}_{AB})$, then the min-entropy of $A$ given $B$ is defined as

$$H_{\min}(A|B)_\rho := \max_{\sigma_B \in S_{=}(\mathcal{H}_B)} \sup \{ \lambda \in \mathbb{R} : 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \geq \rho_{AB} \} .$$

For a classical state $\rho_{XY} = \sum_{x,y} P_{XY}(x,y) |x\rangle \langle x| \otimes |y\rangle \langle y|$, the min-entropy evaluates to $H_{\min}(X|Y)_\rho = -\log \sum_y \max_x P_{XY}(x,y)$, which corresponds to the classical (average) conditional min-entropy $\tilde{H}_\infty(X|Y)$ (Definition 2.7). The classical entropy $\tilde{H}_\infty(X|Y)$ can be interpreted as the logarithm of the probability that an observer that holds $Y$ can guess $X$. In [KRS09] it has been shown that this interpretation can be extended to any cq-state $\rho_{XB}$: the maximum probability that an observer who has access to the quantum system $B$ guesses $X$ correctly is then also given by $2^{-H_{\min}(X|B)_\rho}$. This means the conditional min-entropy can be written as

$$H_{\min}(X|B)_\rho = -\log P_{\text{guess}}(X|B)_\rho ,$$

where

$$P_{\text{guess}}(X|B)_\rho := \max_{\mathcal{M}} \sum_{x \in \mathcal{X}} P_X(x) \text{tr}(M_x \rho_x)$$

The maximum is taken over all POVMs $\mathcal{M} = \{M_x\}_{x \in \mathcal{X}}$ on $B$. For any two cq-states $\rho_{XA}$ and $\sigma_{XA}$, $D(\rho_{XA}, \sigma_{XA}) \leq \varepsilon$ implies that

$$|P_{\text{guess}}(X|A)_\rho - P_{\text{guess}}(X|A)_\sigma| \leq \varepsilon .$$

(2.7.12)
If we choose $\sigma_{XA} := \pi_{\{0,1\}} \otimes \sigma_A$, this implies that
\[ \Pr[P_{\text{guess}}(X|A)_\rho] \leq \frac{1}{2} + \varepsilon. \] (2.7.13)

We use the following definition of the quantum max-entropy.

**Definition 2.18.** Let $\rho_{AB} \in S_\leq(\mathcal{H}_{AB})$, then the max-entropy of $A$ conditioned on $B$ of the state $\rho_{AB}$ is
\[ H_{\text{max}}(A|B)_\rho := \max_{\sigma_B} 2 \log F(\rho_{AB}, 1_A \otimes \sigma_B), \] (2.7.14)
where the maximum is over $\sigma_B \in S_\leq(\mathcal{H}_B)$.

For a classical state $\rho_{XY} = \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y|$, the max-entropy evaluates to
\[ H_{\text{max}}(X|Y)_\rho = \log \left( \sum_y \left( \sum_x \sqrt{P_{XY}(x,y)} \right)^2 \right) = \log \sum_y P_Y(y) 2^{H_{\frac{1}{2}}(X)_{P_X|Y=y}}, \]
where $H_{\frac{1}{2}}(X)_{P_X|Y=y} = 2 \log \sum_x \sqrt{P_{X|Y=y}(x)}$ is the Rényi entropy of order 1/2. The entropy $H_{\frac{1}{2}}(X)_{P_X|Y=y}$ is bounded from above by $H_0(X) = \sup_{\sigma} (P_X|Y=y)$.

For any state $\rho_{ABZ} = \sum_z P_Z(z) \rho_{AB}^z \otimes |z\rangle\langle z|$, we have
\[ H_{\text{max}}(A|BZ)_\rho = \log \sum_z P_Z(z) 2^{H_{\text{max}}(X|B)_{\rho^z}}. \] (2.7.15)

We define the smoothed versions of the min-entropy and max-entropy of a state $\rho$ as an optimization of the non-smooth entropy over a set of states that are close to $\rho$. As a distance measure between two states we use the purified distance, which corresponds to the minimum trace distance between purifications of these states [TCR10].

**Definition 2.19.** For $\rho, \tau \in S_\leq(\mathcal{H})$, we define the purified distance between $\rho$ and $\tau$ as
\[ P(\rho, \tau) := \sqrt{1 - \bar{F}(\rho, \tau)^2} \]
where $\bar{F}(\rho, \tau) = F(\rho, \tau) + \sqrt{(1 - \text{tr} \rho)(1 - \text{tr} \tau)}$ is the generalized fidelity. Note that $\bar{F}(\rho, \tau) = F(\rho, \tau)$ if at least one of the states is normalized.
The purified distance of two states can be bounded from above in terms of the trace distance. For any two quantum state \(\rho, \tau \in S(\mathcal{H})\), we have

\[
P(\rho, \tau) \leq \sqrt{2D(\rho, \tau)}.
\]

(2.7.16)

Let \(\varepsilon \geq 0\) and \(\rho \in S(\mathcal{H})\) with \(\sqrt{\text{tr} \rho} > \varepsilon\). Then, we define an \(\varepsilon\)-ball around \(\rho\) as

\[
\mathcal{B}^\varepsilon(\mathcal{H}; \rho) := \{\tau \in S(\mathcal{H}) : P(\tau, \rho) \leq \varepsilon\}.
\]

In the following, we will assume that \(\varepsilon\) is sufficiently small such that \(\sqrt{\text{tr} \rho} > \varepsilon\) always satisfied.

The smoothed version of the min-entropy is defined as follows.

**Definition 2.20.** Let \(\varepsilon \geq 0\) and \(\rho_{AB} \in S(\mathcal{H}_{AB})\), then the \(\varepsilon\)-smooth min-entropy of A conditioned on B of \(\rho_{AB}\) is defined as

\[
H^\varepsilon_{\min}(A|B)_\rho := \max_{\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}.
\]

The smooth min-entropy \(H^\varepsilon_{\min}(A|B)\) cannot increase when a quantum operation is applied to the system B.

**Lemma 2.22.** Let \(\varepsilon > 0\) and let \(\mathcal{E} : \mathcal{P}(\mathcal{H}_B) \rightarrow \mathcal{P}(\mathcal{H}_{B'})\) be a quantum operation (TP-CPM). Then we have, for any quantum state \(\rho_{AB}\) on \(\mathcal{H}_{AB}\),

\[
H^\varepsilon_{\min}(A|B)_\rho \leq H^\varepsilon_{\min}(A|B')_{\tau}
\]

where \(\tau_{AB'} := (\mathbb{I}_A \otimes \mathcal{E})(\rho_{AB})\).

The smoothed version of the max-entropy is defined as follows.

**Definition 2.21.** Let \(\varepsilon \geq 0\) and \(\rho_{AB} \in S(\mathcal{H}_{AB})\), then the \(\varepsilon\)-smooth max-entropy of A conditioned on B of \(\rho_{AB}\) is defined as

\[
H^\varepsilon_{\max}(A|B)_\rho := \min_{\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}.
\]

For a probability distribution \(P_{XY}\) over \(\mathcal{X} \times \mathcal{Y}\) we write \(H^\varepsilon_{\max}(X|Y)_P\) for the entropy \(H^\varepsilon_{\max}(X|Y)_\rho\), where \(\rho_{XY} := \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y|\).

For any state \(\rho_{XAB} \in S(\mathcal{H}_{XAB})\), which is classical on \(X\), it holds that

\[
H^\varepsilon_{\max}(A|B)_\rho \leq H^\varepsilon_{\max}(X A|B)_\rho.
\]

(2.7.17)

Furthermore, conditioning on an additional system can only decrease the smooth max-entropy, i.e., for any state \(\rho_{ABC} \in S(\mathcal{H}_{ABC})\) we have

\[
H^\varepsilon_{\max}(A|BC)_\rho \leq H^\varepsilon_{\max}(A|B)_\rho.
\]

(2.7.18)
Let $\rho_{XYT}$ be a classical state, where $X$ is an $n$-bit string and $T$ is a subset of $[n]$. Then, we obtain the following lemma from (2.7.18) and (2.7.17).

**Lemma 2.23.**

\[
H^e_{\max}(X_T|YT)_{\rho} \leq H^e_{\max}(X|YT)_{\rho}. \tag{2.7.19}
\]

**Proof.** Let $\bar{\rho}_{XYT} = \sum_t P_T(t) |t\rangle_T \otimes \rho_X^t$ be a cq-state such that

\[
H^e_{\max}(X|YT)_{\rho} = H^e_{\max}(X|YT)_{\bar{\rho}}.
\]

Such a state which is classical on the same subsystems as $\rho$ always exists according to [Tom12]. By (2.7.17) and (2.7.18), we can conclude that

\[
H^e_{\max}(X|YT)_{\rho} = \log \sum_t P_T(t) 2^{H^e_{\max}(X|Y)_{\rho^t}}
\]

\[
\geq \log \sum_t P_T(t) 2^{H^e_{\max}(X_t|Y)_{\rho^t}}
\]

\[
= H^e_{\max}(X_T|YT)_{\bar{\rho}}.
\]

Since TP-CPMs cannot increase the purified distance [TCR10], it holds that $H^e_{\max}(X_T|YT)_{\bar{\rho}} \geq H^e_{\max}(X_T|YT)_{\rho}$. This implies the statement. $\Box$

In the following lemma we show that the conditional min-entropy $H^e_{\min}(A|B)_{\rho}$ can decrease by at most $\log |Z|$ when conditioning on an additional classical system $Z$.

**Lemma 2.24 ([RR10]).** Let $\varepsilon > 0$ and let $\rho_{ABZ}$ be a tripartite state that is classical on $Z$ with respect to some orthonormal basis $\{|z\rangle\}_z$. Then

\[
H^e_{\min}(A|BZ)_{\rho} \geq H^e_{\min}(A|B)_{\rho} - \log |Z|.
\]

The following lemma from [WTHR11] shows that the min-entropy $H^e_{\min}(A|BC)_{\rho}$ cannot increase too much when a projective measurement is applied to the system $C$.

**Lemma 2.25 ([WTHR11]).** Let $\varepsilon \geq 0$ and let $\rho_{ABC}$ be a tripartite state. Furthermore, let $\mathcal{M}$ be a projective measurement in the basis $\{|z\rangle\}_z$ on $C$ and $\rho_{ABZ} := (\mathbb{1}_{AB} \otimes \mathcal{M})(\rho_{ABC})$, where $\mathbb{1}_{AB}$ is the identity operation on $A$ and $B$. Then,

\[
H^e_{\min}(A|BC)_{\rho} \geq H^e_{\min}(A|BZ)_{\rho} - \log |Z|.
\]
2.7. Quantum Information

Using the asymptotic equipartition property \cite{TCD09}, one can obtain from Lemma 2.25 the corresponding lemma for the von Neumann entropy.

**Lemma 2.26.** Let $\rho_{ABC}$ be a tripartite state. Furthermore, let $\mathcal{M}$ be a projective measurement in the basis $\{|z\rangle\}_{z \in Z}$ on $C$ and $\rho_{ABZ} := (1_{AB} \otimes \mathcal{M})(\rho_{ABC})$. Then

$$H(A|BC)_\rho \geq H(A|BZ)_\rho - \log |Z|.$$

Lemmas 2.24 and 2.25 imply that conditioning on an additional quantum system $C$ cannot decrease the conditional smooth min-entropy by more than $2 \log |C|$.

**Lemma 2.27.** $H^{\epsilon}_{\text{min}}(A|BC)_\rho \geq H^{\epsilon}_{\text{min}}(A|B)_\rho - 2 \log |C|$.

### 2.7.2 Privacy Amplification against Quantum Adversaries

The following lemma \cite{RK05, Ren05} is a generalization of Lemma 2.17 and shows that two-universal hashing can be used to extract randomness relative to quantum side information. More precisely, two-universal hash functions are strong extractors against quantum side information, i.e., the output of the function is uniform with respect to the side information and the choice of the function.

**Lemma 2.28 (Leftover Hash Lemma).** Let $F$ be a two-universal family of hash functions from $\mathcal{X}$ to $\{0,1\}^\ell$. Let $\rho_{XB} = \sum_x P(x) |x\rangle\langle x|_X \otimes \rho^x_B$ be a cq-state and $\rho_{FZB} = \frac{1}{|F|} \sum_f \sum_z |f\rangle\langle f|_F \otimes |z\rangle\langle z|_Z \otimes \rho^f_{B,z}$ with $z \in \{0,1\}^\ell$ and $\rho^f_{B,z} = \sum_{x \in f^{-1}(z)} P(x) \rho^x_B$. Then

$$D(\rho_{ZBF}, \pi_{\{0,1\}^\ell} \otimes \rho_{BF}) \leq \epsilon + \frac{1}{2} \sqrt{2^{\ell - H^{\epsilon}_{\text{min}}(X|B)_\rho}}.$$

The quantum version of the Leftover Hash Lemma implies the following technical lemma that we will use to prove the impossibility of extending commitments with quantum protocols in Section 5.2.

**Lemma 2.29.** Let $\rho_{XB} = \frac{1}{2^k} \sum_{x \in \{0,1\}^k} |x\rangle\langle x|_X \otimes \rho^x_B$ be a cq-state. Then there exists a function $f : \{0,1\}^k \rightarrow \{0,1\}$ such that

$$D(\rho_{B,z}^{f,0}, \rho_{B,z}^{f,1}) \leq 2 \left( \epsilon + \frac{1}{2} \sqrt{2^{1 - H^{\epsilon}_{\text{min}}(X|B)_\rho}} \right),$$

where $\rho_{B,z}^{f,z} = \frac{1}{|f^{-1}(z)|} \sum_{x \in f^{-1}(z)} \rho^x_B$. 

Proof. Let \( \mathcal{F} \) be a family of two-universal hash functions \( f : \{0,1\}^k \rightarrow \{0,1\} \) such that every \( f \) is balanced, i.e., \( |\{ x \in \{0,1\}^k : f(x) = 0 \}| = 2^{k-1} \). From Lemma 2.28 we know that

\[
\Delta(Z|BF)_\rho \leq \delta ,
\]

where \( \delta := \varepsilon + \frac{1}{2} \sqrt{2^{1-H_{\min}^\varepsilon(X|B)_\rho}} \) and \( Z := f(X) \). Thus, there must exist a function \( f \in \mathcal{F} \) such that \( \Delta(Z|B)_{\rho[f]} \leq \delta \). For \( z \in \{0,1\} \), we define

\[
\rho_{f,z}^B := \frac{1}{2^{k-1}} \sum_{x \in f^{-1}(z)} \rho_x^B .
\]

We can use Lemma 2.19 to obtain that \( D(\rho_{f,0}^B, \rho_{f,1}^B) \leq 2\delta \). \( \square \)

### 2.7.3 Uncertainty Relation

The uncertainty relation for smooth entropies in [TR11] provides an upper bound in terms of smooth entropies on the accuracy with which the outcome of two incompatible measurements can be predicted. This result will allow us to give a proof that there is an unconditionally secure reduction of oblivious transfer to ideal string commitments using a quantum protocol (see Section 5.4.3). We consider a tripartite state \( \rho_{ABC} \) and two POVMs with elements \( \mathcal{X} = \{ M_x \} \) and \( \mathcal{Y} = \{ N_y \} \) acting on system \( A \). When measuring system \( A \) using these two POVMs, storing the measurement result in classical registers \( X \) and \( Y \) and disregarding the post-measurement state on \( A \), we obtain the two states \( \rho_{XBC} \) and \( \rho_{YBC} \). The uncertainty relation then bounds the sum of the min- and max-entropy of these states using the overlap \( c \) of the two measurements

\[
H_{\min}^\varepsilon(X|B)_\rho + H_{\max}^\varepsilon(Y|C)_\rho \geq \log \frac{1}{c} ,
\]

In [Tom12] the following, more general lower bound on the uncertainty of two incompatible measurement, \( X \) and \( Y \), conditioned on quantum side-information and the result of an additional projective measurement that is applied before \( X \) and \( Y \) has been proved.

**Lemma 2.30 (Uncertainty Relation).** [TR11] Let \( \varepsilon \geq 0 \). Let \( \rho_{ABC} \in S_{\leq}(\mathcal{H}_{ABC}) \) be a tripartite state. Let \( \mathcal{X} = \{ M_x \} \) and \( \mathcal{Y} = \{ N_y \} \) be POVMs on \( \mathcal{H}_A \) and \( \mathcal{K} = \{ P^k \} \) a projective measurement on \( \mathcal{H}_A \). Then, the post-measurements
2.7. Quantum Information

states

\[ \rho_{XKB} = \sum_{x,k} |x\rangle\langle x| \otimes |k\rangle\langle k| \otimes \text{tr}_{AC}(\sqrt{M_x} P^k \rho_{ABC} \sqrt{M_x}) \quad \text{and} \quad (2.7.20) \]

\[ \rho_{YKC} = \sum_{y,k} |y\rangle\langle y| \otimes |k\rangle\langle k| \otimes \text{tr}_{AB}(\sqrt{N_y} P^k \rho_{ABC} \sqrt{N_y}) \quad (2.7.21) \]

satisfy

\[ H^\epsilon_{\min}(X|KB)_\rho + H^\epsilon_{\max}(Y|KC)_\rho \geq \log \frac{1}{c_K}, \]

where the $K$-overlap, $c_K$, is given as

\[ c_K := \max_{k,x,y} \| \sqrt{M_x} P^k \sqrt{N_y} \|_\infty \]

where the infinity norm, $\| \cdot \|_\infty$, is defined as $\| S \|_\infty := \sup_{\phi} \| S|\phi\rangle \|$, where the supremum is over all $|\phi\rangle$ with $\|\phi\|_\infty \leq 1$. 

Chapter 3

Lower Bounds for Classical Secure Function Evaluation

3.1 Introduction

Secure computation of functions between two mutually distrustful parties is a cryptographic task of great importance. While most functions cannot be computed with information-theoretic security from scratch, it is known that all functions can be computed once the players have access to a complete function as a black-box. It is an interesting question how efficient such information-theoretically secure reductions can be in principle, i.e., how many instances of a given complete primitive are needed to implement a certain function. In the case of perfectly secure computation of OT (and also of some other functions), good lower bounds are known. However, in practice one is usually willing to tolerate a small probability of error and it is known that these statistical reductions can in general be much more efficient. Thus, the known bounds have only limited application. In this chapter, we explore the efficiency of secure one-sided two-party computation of arbitrary finite functions from primitives such as different variants of OT and general noisy correlations in the statistical case.

Previous Results  Several lower bounds for OT reductions are known. The earliest impossibility result for information-theoretically secure reductions of OT \cite{Bea96} shows that the number of $\binom{2}{1}$-OT cannot be ex-
tended, i.e., there does not exist a protocol using \( n \) instances of \((2^1)\text{-OT}\) that perfectly implements \( m > n \) instances. Lower bounds for the number of instances of OT needed to perfectly implement other variants of OT have been presented in [DM99] (see also [Mau99]) and generalized in [WW05a, WW08b]. These bounds apply to both the semi-honest (where dishonest players follow the protocol) and the malicious (where dishonest players behave arbitrarily) model. If we restrict ourselves to the malicious model these bounds can be improved, as shown in [KKK08]. Lower bounds on the number of ANDs needed to implement general functions have been presented in [BM04].

All these results only consider perfect protocols and do not give much insight into the case of statistical implementations. As pointed out in [KKK08], their result only applies to the perfect case, because there is a statistical protocol that is more efficient [CS06]. There can be a large gap between the efficiency of perfect and statistical protocols, as shown in [BM04]: The number of OTs needed to compute the equality function is exponentially bigger in the perfect case than in the statistical case. Therefore, a bound in the perfect case does in general not imply a similar bound in the statistical case.

So far very little is known about statistically secure protocols. In [AC07] a proof sketch of a lower bound for statistical implementations of \((2^1)\text{-OT}^k\) has been presented. However, this result only holds in the asymptotic case, where the number \( n \) of resource primitives goes to infinity and the error goes to zero as \( n \) goes to infinity. In [BM04] a non-asymptotic lower bound on the number of ANDs needed for one-sided secure computation of arbitrary functions with Boolean output has been shown. This result directly implies lower bounds for protocols that use \((n^1)\text{-OT}^k\) as a black-box. However, besides being restricted to Boolean-valued functions this result is not strong enough to show optimality of several known reductions and it does not provide bounds for reductions to randomized primitives such as \((1/2)\text{-RabinOT}\).

Contributions In Section 3.4 we consider statistically secure protocols that compute a function between two parties from trusted randomness distributed to the players. We provide two bounds on the efficiency of such reductions - in terms of the conditional Shannon entropy and the mutual information of the randomness - that allow us in particular to derive bounds on the minimal number of \((n^1)\text{-OT}^k\) or \((p)\text{-RabinOT}^k\) needed

\[1\]Note that in the computational setting, OT can be extended, see [Bea96, IKNP03].
to compute a general function securely. Our results hold in the non-asymptotic regime, i.e., we consider a finite number of resource primitives and our results hold for any error.

We will use the formalism of smooth entropies introduced in Section 2.3 to show that one of these two bounds can be generalized to a bound in terms of the conditional min-entropy. This leads to tighter bounds in many cases and to arbitrarily better bounds for some reductions.

In Section 3.4.3 we provide an additional bound for the special case of statistical implementations of \( (n_1) - \text{OT}^k \) in the semi-honest model\(^2\). The bounds for implementations of \( (n_1) - \text{OT}^k \) (Theorem 3.4) imply the following corollary that gives a general bound on the conversion rate between different variants of OT.

**Corollary 3.1.** For any reduction that implements \( M \) instances of \( (N_1) - \text{OT}^K \) from \( m \) instances of \( (n_1) - \text{OT}^k \) in the semi-honest model with an error of at most \( \varepsilon \), we have

\[
\frac{m}{M} \geq \max\left( \frac{(N-1)K}{(n-1)k}, \frac{K}{k}, \frac{\log N}{\log n} \right) - 7N K \cdot (\varepsilon + h(\varepsilon)) .
\]

Corollary 3.1 generalizes the lower bounds for perfect implementations from [DM99, WW05a, WW08b] to the statistical case and is strictly stronger than the impossibility bounds from [AC07]. If we let \( M = m + 1 \), \( N = n = 2 \) and \( K = k = 1 \), we obtain a stronger version of Theorem 3 in [Bea96], which states that OT cannot be extended.

Our lower bounds show that the following protocols are (close to) optimal in the sense that they use the minimal number of instances of the given primitive.

- The protocol in [BCS96a, DM99] which uses \( \frac{N-1}{n-1} \) instances of \( (n_1) - \text{OT}^k \) to implement \( (N_1) - \text{OT}^K \) is optimal.

- The protocol in [WW05a] which uses \( t \) instances of \( (n_1) - \text{OT}^{kn_t-1} \) to implement \( (n_t) - \text{OT}^k \) is optimal.

- The trivial protocol that implements \( (2_1) - \text{OT}^k \) from \( k \) instances of \( (2_1) - \text{OT}^1 \) in the semi-honest model is optimal. In the malicious case, the protocol in [CS06] uses asymptotically (as \( k \) goes to infinity) the same amount of instances and is, therefore, asymptotically optimal.

\(^2\)Bounds on OT in the semi-honest model imply similar bounds in the malicious model, see Section 3.3.1 and Section 3.4.7
• The protocol in $[\text{Sav07}]$ that implements $(\frac{1}{4})$-OT$^k$ from $(\frac{1}{2})$-RabinOT$^1$ in the malicious model is asymptotically optimal.

• The protocol from $[\text{CS06}]$ that implements OT from Universal OT (UOT) is optimal.

Finally, we present an improved security analysis of the protocol in $[\text{CS06}]$ that implements OT from UOT. Our proof of security uses a known result on min-entropy-sampling (cf. Section 2.4). Combined with our impossibility results, this allows us to give a tight bound on the asymptotic rate of this reduction. This answers an open question in $[\text{CS06}]$.

The two impossibility results in Theorems 3.1 and 3.2 can be generalized to statistically secure implementations of $(p)$-RabinOT$^k$ using the same proof technique. This has been shown in the full version of $[\text{WW10}]$.

Most results in Section 3.4 are joint work with Jürg Wullschleger and some of these results have previously been published in $[\text{WW10}]$.

### 3.2 Primitives and Randomized Primitives

In the following we consider two-party primitives that take inputs $x$ from Alice and $y$ from Bob and output $\bar{x}$ to Alice and $\bar{y}$ to Bob, where $(\bar{x}, \bar{y})$ is distributed according to $P_{\bar{X}\bar{Y}|X\bar{Y}}$. For simplicity, we identify such a primitive with $P_{\bar{X}\bar{Y}|X\bar{Y}}$. If the primitive has no input and outputs values $(u,v)$ distributed according to $P_{UV}$, we may simply write $P_{UV}$. If the primitive is deterministic and only Bob receives an output, i.e., if there exists a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ such that $P_{\bar{X}\bar{Y}|X=x,Y=y}(\bot, f(x, y)) = 1$ for all $x,y$, then we identify the primitive with the function $f$.

Examples of such primitives are $(\binom{n}{t})$-OT$^k$, $(p)$-RabinOT$^k$, $(p)$-BNC, EQ$^n$ and IP$^n$:

- $(\binom{n}{t})$-OT$^k$ is the primitive where Alice has an input $x = (x_0, \ldots, x_{n-1})$ from $\{0, 1\}^{k \cdot n}$, and Bob has an input $I_c \subseteq \{0, \ldots, n-1\}$ with $|I_c| = t$. Bob receives $y = x_{I_c} \in \{0, 1\}^t$. If $t = 1$, we represent Bob’s input $c$ by an element from $[n]$.

- $(p)$-RabinOT$^k$ is the primitive where Alice has an input $x \in \{0, 1\}^k$. Bob receives $y$ which is equal to $x$ with probability $p$ and $\Delta$ otherwise.

- $(p)$-BNC is a primitive where Alice has an input $x \in \{0, 1\}$. Bob receives $y$ which is equal to $x$ with probability $p$ and $1-x$ otherwise.
3.2. Primitives and Randomized Primitives

- The equality function \( \text{EQ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\} \) is defined as
  \[
  \text{EQ}_n(x,y) = \begin{cases} 
  1, & \text{if } x = y, \\
  0, & \text{otherwise}.
  \end{cases}
  \]

- The inner-product-modulo-two function \( \text{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \) is defined as \( \text{IP}_n(x,y) = \oplus_{i=1}^n x_i y_i \).

We often allow a protocol to use a primitive \( P_{UV} \) that does not have any input. This is sufficient to model reductions to \((\binom{n}{i})\)-OT\(^k\) and \((p)\)-RabinOT\(^k\), since these primitives are equivalent to distributed randomness \( P_{UV} \), i.e., there exist two protocols that are secure in the semi-honest model and in the malicious model: one that generates the distributed randomness using one instance of the primitive, and one that implements one instance of the primitive using the distributed randomness as input to the two parties. The fact that \((\binom{2}{1})\)-OT\(^1\) is equivalent to distributed randomness has been shown in [BBCS92, Bea95]. The generalization to \((\binom{n}{i})\)-OT\(^k\) is straightforward. The randomized primitives are obtained by simply choosing all inputs uniformly at random. The corresponding primitive \( P_{UV} \), which is also known as an oblivious key, is given by the distribution

\[
P_{UV}((x_0, \ldots, x_{n-1}), (c, y)) = \begin{cases} 
  \frac{1}{n^{2^{nk}}}, & \text{if } y = x_c \\
  0, & \text{otherwise}
  \end{cases},
\]

where \((x_0, \ldots, x_{n-1}) \in (\{0,1\}^k)^n\) and \((c, y) \in \{0, \ldots, n-1\} \times \{0,1\}^k\).

For a formal proof of the security of these reductions we refer to the full version of [CSSW06] and to [Wul07a]. For \((p)\)-RabinOT\(^k\) and \((p)\)-BNC the randomized primitives are also obtained by choosing the input at random and the implementations from the randomized primitives are straightforward. Therefore, any protocol that uses some instances of \((\binom{n}{i})\)-OT\(^k\), \((p)\)-RabinOT\(^k\) or \((p)\)-BNC can be converted into a protocol with the same security that only uses a primitive \( P_{UV} \) without any input.

**Universal OT**

An universal oblivious transfer with parameter \( \alpha \) over bit strings of length \( n \) (\( \alpha \)-UOT\(^n\)) is the following two-party primitive: Alice has input \( x = (x_0, x_1) \in \{0,1\}^{2n} \). If Bob is honest, he has input \( c \in \{0,1\}^n \) and gets output \( y = (x_{c_1}, \ldots, x_{c_n}) \). A malicious Bob can choose a channel \( P_{Y|X} \) such that \( H_\infty(X|Y) \geq \alpha n \) for a uniformly random input \( X \in \{0,1\}^{2n} \) and gets the output of the channel \( P_{Y|X} \) on input \( X = (X_0, X_1) \).
3.2.1 Sufficient Statistics and Common Part

The common part and the sufficient statistics\(^3\) are useful to quantify the cryptographic potential of a pair of correlated random variables [WW08b]. More precisely, one can define three information-theoretic quantities for such pairs \((U,V)\) of random variables, which are monotones for perfectly secure realizations of a primitive \(P_{U'V'}\). This means that no two-party protocol can increase these quantities and each of them must be at least as large for \((U,V)\) as for \((U',V')\) if \(P_{U'V'}\) can be implemented from \(P_{UV}\) with perfect security. The common part and the sufficient statistics will allow us in the following to strengthen our impossibility results for secure implementations of two-party functions from a primitive \(P_{UV}\).

Intuitively speaking, the sufficient statistics of \(X\) with respect to \(Y\), denoted \(X \uparrow Y\), is the part of \(X\) that is correlated with \(Y\).

**Definition 3.1.** Let \(X\) and \(Y\) be random variables, and let \(f(x) := P_{Y|X=x}\). The sufficient statistics of \(X\) with respect to \(Y\) is defined as \(X \uparrow Y := f(X)\).

It is easy to show (see for example [FWW04]) that for any \(P_{XY}\), we have \(X \leftrightarrow X \uparrow Y \leftrightarrow Y\). This immediately implies that any protocol with access to a primitive \(P_{UV}\) can be transformed into a protocol with access to \(P_{U \uparrow V, V \uparrow U}\) (without compromising the security) because the players can compute \(P_{UV}\) from \(P_{U \uparrow V, V \uparrow U}\) privately. Thus, in the following we only consider primitives \(P_{UV}\) where \(U = U \uparrow V\) and \(V = V \uparrow U\).

The common part was first introduced in [GK73]. In a cryptographic context, it was used in [WW04]. Roughly speaking, the common part \(X \land Y\) of \(X\) and \(Y\) is the maximal element of the set of all random variables (i.e., the finest random variable) that can be generated both from \(X\) and from \(Y\) without any error. For example, if \(X = (X_0, X_1) \in \{0, 1\}^2\) and \(Y = (Y_0, Y_1) \in \{0, 1\}^2\), and we have \(X_0 = Y_0\) and \(\Pr[X_1 = Y_1] = \varepsilon > 0\), then the common part of \(X\) and \(Y\) is equivalent to \(X_0\).

**Definition 3.2.** Let \(X\) and \(Y\) be random variables with distribution \(P_{XY}\). Let \(\mathcal{X} := \text{supp}(P_X)\) and \(\mathcal{Y} := \text{supp}(P_Y)\). Then \(\mathcal{X} \land \mathcal{Y}\), the common part of \(X\) and \(Y\), is constructed in the following way:

- Consider the bipartite graph \(G\) with vertex set \(\mathcal{X} \cup \mathcal{Y}\), and where two vertices \(x \in \mathcal{X}\) and \(y \in \mathcal{Y}\) are connected by an edge if \(P_{XY}(x,y) > 0\) holds.

\(^3\)In [FWW04], sufficient statistics is called dependent part.
3.3 Protocols and Security in the Semi-Honest Model

We will consider the following model: The two parties use a primitive $P_{UV}$ that has no input and outputs values $(u, v)$ distributed according to $P_{UV}$ to the players. Alice and Bob receive inputs $x$ and $y$. Then, the players exchange messages in several rounds, where we assume that Alice sends the first message. If $i$ is odd, then Alice computes the $i$-th message as a randomized function of all previous messages, her input $x$ and $u$. If $i$ is even, then Bob computes the $i$-th message as a randomized function of all previous messages, his input $y$ and $v$. We assume that the number of rounds is bounded by a constant $t$ from above. By padding the protocol with empty rounds, we can thus assume without loss of generality that the protocol uses $t$ rounds in every execution. After $t$ rounds, Alice computes her output $\tilde{x}$ as a randomized function of $(M, U, x)$ and Bob computes his output $\tilde{y}$ as a randomized function of $(M, V, y)$, where $M = (M_1, \ldots, M_t)$ is the sequence of all messages exchanged. It is easy to check that inequalities (2.1.10) and (2.1.11) imply that, for every distribution of the inputs $X$ and $Y$, we have $I(\tilde{Z}; XU|YM) = 0$, $I(\tilde{Z}Y; X|VM) = 0$ and $I(\tilde{Z}YV; X|UM) = 0$.

We will consider the semi-honest model, where both players behave honestly, but may save all the information they get during the protocol to obtain extra information about the other player’s input or output. A protocol securely implements $P_{XY|XY}$ with an error of $\varepsilon$, if the entire view of each player can be simulated with an error of at most $\varepsilon$ in an ideal setting, where the players only have black-box access to the primitive $P_{XY|XY}$. Note that this simulation is allowed to change neither the input nor the output. This definition of security follows Definition 7.2.1 from [Gol04], but is adapted to the case of computationally unbounded adversaries and statistical indistinguishability.

**Definition 3.3.** Let $\Pi$ be a protocol with black-box access to a primitive $P_{UV}$ that implements a primitive $P_{XY|XY}$. The random variables $\text{View}_{A}^{\Pi}(x, y)$
and $\text{View}_B^\Pi(x, y)$ denote the views of Alice and Bob on input $(x, y)$ defined as $(x, u, m_1, \ldots, m_t, r_A)$ and $(x, v, m_1, \ldots, m_t, r_B)$, respectively, where $r_A$ ($r_B$) is the private randomness of Alice (Bob), $m_i$ represents the $i$-th message and $u, v$ is the output from $P_{UV}$. $\text{Output}_A^\Pi(x, y)$ and $\text{Output}_B^\Pi(x, y)$ denote the outputs (which are implicit in the views) of Alice and Bob respectively on input $(x, y)$. The protocol is secure in the semi-honest model with an error of at most $\varepsilon$, if there exist two randomized functions $S_A$ and $S_B$, called the simulators\footnote{We do not require the simulator to be efficient.} such that for all $x$ and $y$:  
\[
D((\text{View}_A^\Pi(x, y), \text{Output}_B^\Pi(x, y)), ((\bar{x}, S_A(x, \bar{x})), \bar{y})) \leq \varepsilon, \\
D((\bar{x}, (\bar{y}, S_B(y, \bar{y}))), (\text{Output}_A^\Pi(x, y), \text{View}_B^\Pi(x, y))) \leq \varepsilon,
\]

where $\bar{x}, \bar{y}$ are distributed according to $P_{XY|X=x,Y=y}$.

Note that security in the semi-honest model does not directly imply security in the malicious model, as the simulator is allowed to change the input/output in the malicious model, while he is not allowed to do so in the semi-honest model. We will, therefore, also consider security in the weak semi-honest model, which is implied both by security in the semi-honest model and by security in the malicious model. Here, the simulator is allowed to change the input to the ideal primitive and change the output from the ideal primitive. Thus, in order to show impossibility of certain protocols in the malicious and in the semi-honest model, it is sufficient to show impossibility in the weak semi-honest model.

### 3.3.1 Malicious OT implies Semi-honest OT

In the malicious model the adversary is not required to follow the protocol. Therefore, a protocol that is secure in the malicious model protects against a much bigger set of adversaries. On the other hand, the security definition in the malicious model only implies that for any (also semi-honest) adversary there exists a malicious simulator for the ideal primitive, i.e., the simulator is allowed to change his input or output from the ideal primitive. Since this is not allowed in the semi-honest model, security in the malicious model does not imply security in the semi-honest model in general. For implementations of OT\footnote{And any other so-called deviation revealing functionality.} however, it has been shown in \cite{PR08} that this implication does hold, because a simulator can only change the input with small probability if the adversary is semi-honest.
3.4. Lower Bounds

Otherwise, he is not able to correctly simulate the input or the output of
the protocol. Therefore, any impossibility result for OT in the semi-honest
model also implies impossibility in the malicious model.

We will state this result for \( (\binom{n}{1})^k \)-OT with explicit bounds on the errors.

**Lemma 3.1.** If a protocol implementing \( (\binom{n}{1})^k \)-OT is secure in the malicious
model with an error of at most \( \varepsilon \), then it is also secure in the semi-honest model
with an error of at most \( (2n + 1)\varepsilon \).

**Proof.** From the security of the protocol we know that there exists a (ma-
licious) simulator that simulates the view of honest Alice. If two hon-
est players execute the protocol on input \( (x_0, \ldots, x_{n-1}) \) and \( c \), then with probability \( 1 - \varepsilon \) the receiver gets \( y = x_c \). Thus, the simulator can change
the input \( x_i \) with probability at most \( 2\varepsilon \) for all \( 0 \leq i \leq n - 1 \). We construct a new simulator that executes the malicious simulator but never changes
the input. This simulation is \( (2n + 1)\varepsilon \)-close to the distribution of the pro-
tocol. From the security of the protocol we also know that there exists a (malicious) simulator that simulates the view of honest Bob. If two hon-
est players execute the protocol with uniform input \( (X_0, \ldots, X_{n-1}) \) and choice bit \( c \), then with probability \( 1 - \varepsilon \) the receiver gets \( y = x_c \). If the simulator changes the choice bit \( c \), he does not learn \( x_c \) and the simulated \( y \) is not equal to \( x_c \) with probability at least \( 1/2 \). Therefore, the simula-
tor can change \( c \) or the output with probability at most \( 4\varepsilon \). As above we can construct a simulator for the semi-honest model with an error of at
most \( 5\varepsilon \).

\( \square \)

### 3.4 Lower Bounds

Let a protocol be an \( \varepsilon \)-secure implementation of a primitive \( P_{XY|XY} \) in the
semi-honest model. Let \( P_{XY} \) be the input distribution and let \( P_{XY|XY} \) be the corresponding output distribution of the ideal primitive, i.e., \( P_{XY|XY} := P_{XY} P_{XY|XY} \), and let \( M \) be the whole communication during the execu-
tion of the protocol. Then the security of the protocol implies the follow-
ing lemma that we will use in our proofs.

**Lemma 3.2.**

\[
H(X|VM) \geq H(X|Y\bar{Y}) - \varepsilon \log |\mathcal{X}| - h(\varepsilon).
\]

**Proof.** The security of the protocol implies that there exists a randomized
function \( S_B \) such that \( D(P_{XY\bar{Y}S_B(Y,\bar{Y})}, P_{XY\bar{Y}VM}) \leq \varepsilon \). Using Lemma 2.1
and (2.1.9), we obtain

\[
H(X|VM) \geq H(X|SB(Y, \bar{Y})) - \varepsilon \log |X| - h(\varepsilon) \\
\geq H(X|Y\bar{Y}) - \varepsilon \log |X| - h(\varepsilon) .
\]

We will now give lower bounds for information-theoretically secure implementations of functions \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \) from a primitive \( P_{UV} \) in the semi-honest model. Let \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \) be a function such that

\[
\forall x \neq x' \in \mathcal{X} \exists y \in \mathcal{Y} : f(x, y) \neq f(x', y) . \tag{3.4.1}
\]

This means that, for any \( x \), it is possible to compute \( x \) from the set \( \{(f(x, y), y) : y \in \mathcal{Y}\} \). In any secure implementation of \( f \), Alice does not learn which \( y \) Bob has chosen, but has to make sure that Bob can compute \( f(x, y) \) for any \( y \). This implies that she cannot hold back any information about \( x \). The statement of Lemma 3.3 formally captures this intuition.

Unless otherwise specified, we assume that Alice and Bob choose their inputs \( X \) and \( Y \) uniformly at random in the following.

**Lemma 3.3.** For any protocol that is an \( \varepsilon \)-secure implementation of a function \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \) that satisfies (3.4.1) in the semi-honest model, it holds for any \( y \in \mathcal{Y} \) that

\[
H(X|UM, Y = y) \leq (3|\mathcal{Y}| - 2)(\varepsilon \log |\mathcal{Z}| + h(\varepsilon))
\]

**Proof.** There exists a randomized function \( S_A \) such that

\[
D(P_{XMU|Y=y}, P_{XSA(X)}) \leq \varepsilon
\]

for all \( y \in \mathcal{Y} \). Therefore, the triangle inequality implies that for any \( y, y' \)

\[
D(P_{XMU|Y=y}, P_{XMU|Y=y'}) \leq 2\varepsilon . \tag{3.4.2}
\]

It holds that \( I(X; Z|UM, Y = y) = 0 \). Furthermore, we have \( \Pr[Z \neq f(X, Y) | Y = y] \leq \varepsilon \). Thus, it follows from (2.1.9) and (2.1.12) that

\[
H(f(X, y)|UM, Y = y) \leq H(f(X, y)|Z, Y = y) \\
\leq \varepsilon \cdot \log |Z| + h(\varepsilon) . \tag{3.4.3}
\]

Together with (3.4.2) and Lemma 2.1 this implies that for any \( y, y' \)

\[
H(f(X, y)|UM, Y = y') \leq 3\varepsilon \log |Z| + h(\varepsilon) + h(2\varepsilon) \\
\leq 3(\varepsilon \log |Z| + h(\varepsilon)) ,
\]
3.4. Lower Bounds

where the second inequality follows from (2.1.1). Since \( X \) can be computed from the values \( f(X, y_1), \ldots, f(X, y_{|Y|}) \), we obtain

\[
H(X|UM, Y = y) 
\leq H(f(X, y_1), \ldots f(X, y_{|Y|})|UM, Y = y) 
\leq \sum_{y' \in \mathcal{Y}} H(f(X, y')|UM, Y = y) 
\leq (3|\mathcal{Y}| - 2)(\varepsilon \log |Z| + h(\varepsilon)) .
\]

where we used (2.1.3) in the first and (2.1.2) and (2.1.3) in the second inequality.

\[\]

**Theorem 3.1.** Let \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \) be a function that satisfies (3.4.1). If there exists a protocol that implements \( f \) from a primitive \( P_{UV} \) with an error \( \varepsilon \) in the semi-honest model, then

\[
H(U|V) \geq \max_y H(X|f(X, y)) - (3|\mathcal{Y}| - 1)(\varepsilon \log |Z| + h(\varepsilon)) - \varepsilon \log |\mathcal{X}| .
\]

**Proof.** Let \( y \in \mathcal{Y} \). It follows from Lemma 3.3 and (2.1.3) that

\[
H(X|UM, Y = y) \leq H(X|UM, Y = y) 
\leq (3|\mathcal{Y}| - 2)(\varepsilon \log |Z| + h(\varepsilon)) .
\]

We can use (2.1.3), (2.1.2) and Lemma 2.1 to obtain

\[
H(X|VM, Y = y) = H(U|VM, Y = y) + H(X|VM, Y = y) 
- H(U|XVM, Y = y) 
\leq H(U|VM, Y = y) + (3|\mathcal{Y}| - 2)(\varepsilon \log |Z| + h(\varepsilon)) 
\leq H(U|V) + (3|\mathcal{Y}| - 2)(\varepsilon \log |Z| + h(\varepsilon)) .
\]

By Lemma 3.2 we know that

\[
H(X|f(X, y)) - \varepsilon \log |\mathcal{X}| - h(\varepsilon) \leq H(X|VM, Y = y) .
\]

The statement follows by maximizing over all \( y \). \( \square \)

Note that in (3.4.3) the term \( \log |Z| \) could be replaced by

\[
d_f := \log \max_y |\{ f(x, y) : x \in \mathcal{X} \}| \leq \log \min(|Z|, |\mathcal{X}|) .
\]
The resulting bound,
\[ H(U|V) \geq \max_y H(X|f(X,y)) - (3|\mathcal{Y}| - 1)(\varepsilon \cdot d_f + h(\varepsilon)) - \varepsilon \log |\mathcal{X}|, \]
is stronger in general, but does not lead to improved results for the examples considered here.

If the domain $|\mathcal{Y}|$ of a function is large, Theorem 3.1 may only imply a rather weak bound. A simple way to improve this bound is to restrict the domain of $f$, i.e., to consider a function $f'(x,y) : \mathcal{X}' \times \mathcal{Y}' \rightarrow \mathcal{Z}$ where $\mathcal{X}' \subset \mathcal{X}$ and $\mathcal{Y}' \subset \mathcal{Y}$ with $f'(x,y) = f(x,y)$ that still satisfies condition (3.4.1). Clearly, if $f$ can be computed from a primitive $P_{UV}$ with an error $\varepsilon$ in the semi-honest model, then $f'$ can be computed with the same error. Thus, any lower bound for $f'$ implies a lower bound for $f$.

The following corollary for implementations of \binom{n}{t} OT $^k$ follows immediately from Theorem 3.1.

**Corollary 3.2.** For any implementation of $m$ independent instances of \binom{n}{t} OT $^k$ from a primitive $P_{UV}$ that is $\varepsilon$-secure in the semi-honest model, the following lower bound must hold:
\[ H(U|V) \geq ((1-\varepsilon)n - t)km - (3[\frac{n}{t}] - 1)(\varepsilon mtk + h(\varepsilon)). \]

**Proof.** We can choose subsets $C_i \subseteq \{0, \ldots, n - 1\}$, with $1 \leq i \leq \lceil \frac{n}{t} \rceil$, of size $t$ such that $\bigcup_{i=1}^{\lceil \frac{n}{t} \rceil} C_i = \{1, \ldots, n\}$, and restrict Bob to choose one of these sets as input for every instance of OT. It is easy to check that condition (3.4.1) is satisfied. The statement follows from Theorem 3.1.

For our next lower-bound, the function $f$ must satisfy the following property. Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a function such that there exist $y_1 \in \mathcal{Y}$ such that
\[ \forall x \neq x' \in \mathcal{X} : f(x,y_1) \neq f(x',y_1), \] (3.4.4)
and $y_2 \in \mathcal{Y}$ such that
\[ \forall x, x' \in \mathcal{X} : f(x,y_2) = f(x',y_2). \] (3.4.5)
Thus, Bob will receive Alice’s whole input if his input is $y_1$, and will get no information about Alice’s input if his input is $y_2$. This property can for example be satisfied by restricting Alice’s input in \binom{n}{t} OT $^k$, as we will see in Corollary 3.3.
3.4. Lower Bounds

Let Alice’s input $X$ be uniformly distributed. Loosely speaking, the security of the protocol implies that the communication gives (almost) no information about Alice’s input $X$ if Bob’s input is $y_2$. But the communication must be (almost) independent of Bob’s input, otherwise Alice could learn Bob’s input. Thus, Alice’s input $X$ is uniform with respect to the whole communication even when Bob’s input is $y_1$. Let now Bob’s input be fixed to $y_1$ and let $M$ be the whole communication. The following lower bound can be proved using the given intuition.

**Lemma 3.4.**

\[
\mathrm{H}(f(X, y_1)|M, U \land V, Y = y_1) \geq \log |X| - 6(\varepsilon \log |X| + h(\varepsilon)) .
\]

**Proof.** Let $g_U, g_V$ be the functions that compute the common part of $P_{UV}$. As in inequality (3.4.2) in the proof of Lemma 3.3, we obtain that

\[
D(P_{XMU|Y=y, P_{XMU|Y=y'}) \leq 2\varepsilon ,
\]

for all $y \neq y' \in \mathcal{Y}$. This implies that

\[
D(P_{Xg_U(U)|Y=y, P_{Xg_U(U)|Y=y'}) \leq 2\varepsilon , \tag{3.4.6}
\]

and

\[
D(P_XP_{Mg_U(U)|Y=y, P_XP_{Mg_U(U)|Y=y'}) \leq 2\varepsilon . \tag{3.4.7}
\]

Because the protocol is secure, there exists a simulator $S_B$ such that

\[
D(P_{XMV|Y=y_2, P_XS_B(y_2, f(X,y_2))}) \leq \varepsilon .
\]

From the property (3.4.5), we can conclude that

\[
D(P_{XMV|Y=y_2, P_XP_{S_B(y_2, f(X,y_2))}}) \leq \varepsilon .
\]

Therefore, we can use the triangle inequality to derive the following upper bound on the distance from uniform of $X$ with respect to $Mg_U(U)$ conditioned on $y_2$:

\[
D(P_{XMg_U(U)|Y=y_2, P_XP_{Mg_U(U)|Y=y_2}})
\]

\[
\leq D(P_{XMV|Y=y_2, P_XP_{MV|Y=y_2}})
\]

\[
\leq D(P_{XMV|Y=y_2, P_XP_{S_B(y_2, f(X,y_2))}})
\]

\[
+ D(P_XP_{S_B(y_2, f(X,y_2))}, P_XP_{MV|Y=y_2})
\]

\[
\leq 2\varepsilon . \tag{3.4.8}
\]
This implies that a weaker upper bound also holds conditioned on $y_1$ as follows: We can use the triangle inequality again to conclude from (3.4.6), (3.4.7) and (3.4.8) that

$$
D(P_{XMg_U(U)}|Y=y_1, P_X P_{Mg_U(U)}|Y=y_1) \\
\leq D(P_{XMg_U(U)}|Y=y_1, P_{XMg_U(U)}|Y=y_2) \\
+ D(P_{XMg_U(U)}|Y=y_2, P_X P_{Mg_U(U)}|Y=y_2) \\
+ D(P_{X P_{Mg_U(U)}|Y=y_2, P_X P_{Mg_U(U)}|Y=y_1}) \\
\leq 6\varepsilon.
$$

Therefore, we obtain

$$
H(f(X, y_1)|M, U \wedge V, Y = y_1) = H(X|M, U \wedge V, Y = y_1) \\
\geq \log |X| - 6\varepsilon \log |X| - h(6\varepsilon) \\
\geq \log |X| - 6\varepsilon \log |X| - 6h(\varepsilon),
$$

where we used Lemma 2.1 in the first inequality.

We use Lemma 3.4 to prove the following lower bound on the mutual information of the distributed randomness for implementations of a two-party function $f$ from a primitive $P_{UV}$ in the semi-honest model.

**Theorem 3.2.** Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a function that satisfies (3.4.4) and (3.4.5). Then for any protocol that implements $f$ with an error of at most $\varepsilon$ in the semi-honest model from a primitive $P_{UV}$

$$
I(U; V) \geq I(U; V|U \wedge V) \\
\geq \log |\mathcal{X}| - 7(\varepsilon \log |\mathcal{X}| + h(\varepsilon)).
$$

**Proof.** Let Alice’s input $X$ be uniformly distributed and Bob’s input be fixed to $y_1$. Let $Z$ be Bob’s output and $M$ the whole communication. Then Lemma 3.4 implies that

$$
H(f(X, y_1)|M, U \wedge V) \geq \log |\mathcal{X}| - 6\varepsilon \log |\mathcal{X}| - 6h(\varepsilon).
$$

Since $\Pr[Z \neq f(X, y_1)] \leq \varepsilon$ and $X \leftrightarrow VM \leftrightarrow Z$, it follows from (2.1.9) and (2.1.12) that

$$
H(f(X, y_1)|VM) \leq H(f(X, y_1)|Z) \leq \varepsilon \log |\mathcal{X}| + h(\varepsilon).
$$
Let $M^i := (M_1, \ldots, M_i)$, i.e., the sequence of all messages sent until the $i$-th round. Without loss of generality, let us assume that Alice sends the message of the $(i+1)$-th round. Since we have $M^{i+1} \leftrightarrow M^i U \leftrightarrow V$, it follows from (2.1.10) that

$$I(U; V|M^{i+1}, U \land V) \leq I(U; V|M^i, U \land V).$$

By induction over all rounds, it holds that

$$I(U; V|M, U \land V) \leq I(U; V|U \land V).$$

The statement follows.

The next corollary provides a lower bound on the mutual information for implementations of $(\binom{n}{t})$-OT$^k$ from a primitive $P_{UV}$. It follows immediately from Theorem 3.2.

**Corollary 3.3.** If there exists a protocol that implements $m$ independent instances of $(\binom{n}{t})$-OT$^k$ from a primitive $P_{UV}$ with an error of at most $\varepsilon$ in the semi-honest model, then the following lower bounds must hold: If $t \leq \lfloor n/2 \rfloor$, then

$$I(U; V|U \land V) \geq mt_k - 7(\varepsilon mt_k + h(\varepsilon)).$$

If $t > \lfloor n/2 \rfloor$, then

$$I(U; V|U \land V) \geq m(n-t)k - 7(\varepsilon m(n-t)k + h(\varepsilon)).$$

**Proof.** In the first case, consider the function that is obtained by setting the first $n-t$ inputs to a fixed value and choosing the remaining $t$ inputs from $\{0, 1\}^k$ for every instance of OT. In the second case, we use the fact that $(\binom{2n-2t}{n-t})$-OT$^k$ can be obtained from $(\binom{n}{t})$-OT$^k$ by fixing $2t - n$ inputs. Thus, both bounds follow from Theorem 3.2.
In order to generalize Theorem 3.2, we define the following relation on the rows of a matrix $M_f$, which has been introduced in [Kus89] to characterize privately computable functions.

**Definition 3.4 ([Kus89]).** The relation $\sim$ on the rows of a matrix $M_f$ is defined as follows: $x, x' \in \mathcal{X}$ satisfy $x \sim x'$ if there exists $y \in \mathcal{Y}$ such that $M_f(x, y) = M_f(x', y)$. The equivalence relation $\equiv$ on the rows of $M_f$ is defined as the transitive closure of $\sim$, i.e., $x, x' \in \mathcal{X}$ satisfy $x \equiv x'$ if there exist $x_1, \ldots, x_\ell$ such that $x \sim x_1 \sim \cdots \sim x_\ell \sim x'$. Furthermore, we say that $x, x' \in \mathcal{X}$ are $c$-equivalent with respect to $\equiv$ with $c \in \mathbb{N}$, if if there exist $x_1, \ldots, x_\ell$ such that $x \sim x_1 \sim \cdots \sim x_\ell \sim x'$ and $\ell \leq c$.

**Lemma 3.5.** Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a function such that all rows of $M_f$ are $c$-equivalent with respect to $\equiv$. Let $X$ and $Y$ be chosen uniformly at random. Then for all $x, x' \in \mathcal{X}$ and all $y \in \mathcal{Y}$

$$D(P_{M|X=x,Y=y}, P_{M|X=x',Y=y}) \leq 2(1 + 2(c + 1))\varepsilon = (6 + 4c)\varepsilon.$$  

*Proof.* As in the proof of Lemma 3.3 one can show that

$$D(P_{M|X=x,Y=y}, P_{M|X=x',Y=y'}) \leq 2\varepsilon,$$

for all $y \neq y' \in \mathcal{Y}$. From the security of the protocol there exists a simulator $S_B$ such that for all $x, y$

$$D(P_{M|X=x,Y=y}, P_{S_B(y,f(x,y))}) \leq \varepsilon.$$

Thus, for all $x, x', y$ with $f(x, y) = f(x', y)$, we have

$$D(P_{M|X=x,Y=y}, P_{M|X=x',Y=y}) \leq 2\varepsilon.$$

Since all all rows of $M_f$ are $c$-equivalent with respect to $\equiv$, we can conclude that

$$D(P_{M|X=x,Y=y}, P_{M|X=x',Y=y}) \leq 2(1 + 2(c + 1))\varepsilon = (6 + 4c)\varepsilon.$$

$$\square$$

Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a function such that there exists $\bar{y} \in \mathcal{Y}$ with $|\{f(x, \bar{y}) : x \in \mathcal{X}\}| \geq t$ and all rows of $M_f$ are $c$-equivalent with respect to $\equiv$. There exists $\mathcal{X}' \subseteq \mathcal{X}$ with $|\mathcal{X}'| = t$ and $f(x, \bar{y}) \neq f(x', \bar{y})$ for all $x \neq x' \in \mathcal{X}'$. Let Alice’s input $X$ be uniformly distributed over $\mathcal{X}'$. Let Bob’s input be fixed to $\bar{y}$. Let $M$ be the whole communication. Then the following lemma holds for any $\varepsilon$-secure implementation of $f$. 

Lemma 3.6.

\[ H(f(X, \bar{y}) | M) \geq \log(t) - (6 + 4c)(\varepsilon \log(t) + h(\varepsilon)) . \]

Proof. By Lemma 3.5, we know that

\[ D(P_{M|X=x}, P_{M|X=x'}) \leq 2(1 + 2(c + 1))\varepsilon = (6 + 4c)\varepsilon . \]

This immediately implies that

\[ D(P_{XM}, P_XP_M) \leq (6 + 4c)\varepsilon . \]

We can use Lemma 2.1 to obtain that

\[ H(f(X, \bar{y}) | M) = H(X | M) \geq \log(t) - (6 + 4c)(\varepsilon \log(t) + h(\varepsilon)) . \]

\[ \square \]

Now, we can use the proof of Theorem 3.2 together with Lemma 3.6 to generalize the statement of Theorem 3.2.

**Theorem 3.3.** Let \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \) be a function such that all rows of \( M_f \) are \( c \)-equivalent with respect to \( \equiv_r \) and such that there exists \( \bar{y} \in \mathcal{Y} \) with \( |\{f(x, \bar{y}) : x \in \mathcal{X}\}| \geq t \). Then for any protocol that implements \( f \) with an error of at most \( \varepsilon \) in the semi-honest model from a primitive \( P_{UV} \)

\[ I(U; V) \geq \log(t) - (7 + 4c)(\varepsilon \log(t) + h(\varepsilon)) . \]

In the case of perfect implementations the weaker bound \( H(U) \geq \log |\mathcal{X}| \) follows from Theorems 3.1 and 3.3. From this bound, we obtain that any perfectly secure protocol needs at least \( \log |\mathcal{X}| \) instances of \( (\frac{2}{1})\text{-OT}^1 \) to implement a function \( f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z} \). Since a secure AND can be implemented from one instance of \( (\frac{2}{1})\text{-OT}^1 \), this implies Theorem 4.11 from [BM04].

### 3.4.1 Additional Bounds for Implementations of OT

An instance of \( (\frac{2}{1})\text{-OT}^1 \) can be implemented from one instance of \( (\frac{2}{1})\text{-OT}^1 \) in the opposite direction [WW06]. Therefore, it follows immediately from Theorem 3.1 that

\[ H(V|U) \geq 1 - 5(\varepsilon + h(\varepsilon)) - 2\varepsilon , \]
since any violation of this bound would contradict the bound of Corollary 3.2. We will show that a generalization of this bound also holds for \( m \) independent copies of \( (n_i)\text{-OT}^k \) for any \( n \geq 2 \). Note that we can assume that \( k = 1 \). The resulting bound then also implies a bound for \( k > 1 \) because one instance of \( (n_1)\text{-OT}^1 \) can be implemented from one instance of \( (n_1)\text{-OT}^k \).

**Lemma 3.7.** Let a protocol having access to \( P_{UV} \) be an \( \varepsilon \)-secure implementation of \( m \) independent copies of \( (n)\text{-OT}^1 \) in the semi-honest model. Then

\[
H(V|U) \geq m \log n - m(4 \log n + 7)(\varepsilon + h(\varepsilon)) .
\]

**Proof.** Let Alice and Bob choose their inputs \( X = (X^1, \ldots, X^m) \in \{0, 1\}^{mn} \), where \( X^i = (X^i_0, \ldots, X^i_{n-1}) \), and \( C = (C^1, \ldots, C^m) \in \{0, \ldots, n-1\}^m \) uniformly at random. Let \( Y = (Y^1, \ldots, Y^m) \) be the output of Bob at the end of the protocol. Let \( j \in \{1, \ldots, m\} \). First, we consider the \( j \)th instance of \( (n)\text{-OT}^1 \). Let \( A_i := X^i_0 \oplus X^j_i \), for \( i \in \{1, \ldots, n-1\} \). From the security of the protocol follows that there exists a randomized function \( S_B(c, x_c) \) such that for all \( a = (a_1, \ldots, a_{n-1}) \in \{0, 1\}^{n-1} \),

\[
D(P_{Y^j\text{CV}M|A=a}, P_{X^j\text{CS}_B(C, x_C)}) \leq \varepsilon .
\]

Hence, the triangle inequality implies that

\[
D(P_{Y^j\text{CV}M|A=a}, P_{Y^j\text{CV}M|A=a'}) \leq D(P_{Y^j\text{CV}M|A=a}, P_{Y^j\text{CV}M|A=a'}) \\
\leq 2\varepsilon \tag{3.4.11}
\]

holds for all \( a, a' \). We have \( \Pr[Y^j \neq X^j_C | A = a] \leq \varepsilon \) for all \( a \). If \( A = (0, \ldots, 0) \), we have \( X^j_C = X^j_0 \). Since \( X^j \leftrightarrow VM \leftrightarrow Y^j \), it follows from (2.1.3) and (2.1.12) that

\[
H(Y^j|VM, A = (0, \ldots, 0)) \leq H(Y^j|X^j, A = (0, \ldots, 0)) \\
\leq H(Y^j|X^j_0, A = (0, \ldots, 0)) \\
\leq \varepsilon + h(\varepsilon) . \tag{3.4.12}
\]

Now, we map \( C^j \) to a bit string of size \( \lceil \log n \rceil \). Let \( C_b \) be the \( b \)-th bit of that bit string, where \( b \in \{0, \ldots, \lceil \log n \rceil - 1\} \). Let \( a^b = (a^b_1, \ldots, a^b_{n-1}) \), where \( a^b_i = 1 \) if and only if the \( b \)-th bit of \( i \) is 1. Conditioned on \( A = a^b \), we have \( X^j_C = X^j_0 \oplus C_b \). It follows from \( X^j \leftrightarrow VM \leftrightarrow Y^j C^j \), (2.1.3) and (2.1.12) that

\[
H(Y^j \oplus C_b|VM, A = a^b) \leq H(Y^j \oplus C_b|X^j_0, A = a^b) \\
\leq \varepsilon + h(\varepsilon) . \tag{3.4.13}
\]
By Lemma 2.1 (3.4.11) and (3.4.12), we obtain
\[ H(Y_j|VMA) \leq \varepsilon + h(\varepsilon) + 2\varepsilon + h(2\varepsilon) \leq 3\varepsilon + 3h(\varepsilon). \]

It follows from Lemma 2.1, (3.4.11) and (3.4.13) that for all \( b \)
\[ H(Y_j \oplus C_b|VMA) \leq 3\varepsilon + 3h(\varepsilon). \]

Since \((C_j, Y_j)\) can be calculated from \((Y_j, Y_j \oplus C_0, \ldots, Y_j \oplus C_{\lceil \log n \rceil - 1})\), this implies that
\[ H(C_j|VMA) \leq 3(\lceil \log n \rceil + 1)(\varepsilon + h(\varepsilon)). \]

The Markov chain \( A \leftrightarrow VM \leftrightarrow C_jY_j \), \([\log n] \leq \log n + 1\) and inequality (2.1.3) imply that
\[ H(C_j|VM) \leq 3(\log n + 2)(\varepsilon + h(\varepsilon)). \]

Thus, we obtain that
\[ H(C|VM) \leq \sum_{j=1}^{n} H(C_j|VM) \leq 3m(\log n + 2)(\varepsilon + h(\varepsilon)). \]

We can use (2.1.3), (2.1.2) and Lemmas 2.1 and 3.2 to obtain
\[ m(\log n - \varepsilon \log n) - h(\varepsilon) \leq H(C|UM) = H(V|UM) + H(C|UVM) - H(V|CUM) \leq H(V|UM) + 3m(\log n + 2)(\varepsilon + h(\varepsilon)) \leq H(V|U) + 3m(\log n + 2)(\varepsilon + h(\varepsilon)). \]

\[ \square \]

Altogether, Corollary 3.2, Corollary 3.3 and Lemma 3.7 prove the following theorem.

**Theorem 3.4.** Let a protocol having access to \( P_{UV} \) be an \( \varepsilon \)-secure implementation of \( m \) instances of \( \binom{n}{2} \)-\( OT^k \) in the semi-honest model. Then
\[ H(U|V) \geq m(n - 1)k - (4n - 1)(\varepsilon mk + h(\varepsilon)), \]
\[ H(V|U) \geq m \log n - m(4 \log n + 7)(\varepsilon + h(\varepsilon)), \]
\[ I(U; V|U \wedge V) \geq mk - 7\varepsilon mk - 7h(\varepsilon). \]
Since \( m \) instances of \( (\binom{n}{k}) \cdot \text{OT}^k \) are equivalent to a primitive \( P_{UV} \) with \( H(U|V) = m(n-1)k \), \( I(U;V) = mk \) and \( H(V|U) = m \log n \), any protocol that implements \( M \) instances of \( (\binom{n}{k}) \cdot \text{OT}^k \) from \( m \) instances of \( (\binom{n}{k}) \cdot \text{OT}^k \) with an error of at most \( \varepsilon \) needs to satisfy the following inequalities:

\[
\begin{align*}
    m(n-1)k & \geq M(N-1)K - (4N-1)(\varepsilon MK + h(\varepsilon)) , \\
    mk & \geq MK - 7\varepsilon MK - 7h(\varepsilon) , \\
    m \log n & \geq M \log N - M(4 \log N + 7)(\varepsilon + h(\varepsilon)) .
\end{align*}
\]

Thus, we get Corollary 3.1.

### 3.4.2 Lower Bounds on Min-Entropy

We will now use the proof of Theorem 3.1 and the smooth entropy formalism to derive a lower bound on the conditional min-entropy for information-theoretically secure implementations of functions \( f : X \times Y \rightarrow Z \) from a primitive \( P_{UV} \) in the semi-honest model. Let \( f : X \times Y \rightarrow Z \) be a function that satisfies (3.4.1). Let Alice and Bob choose their inputs \( X \) and \( Y \) uniformly at random and let \( M \) be the whole communication during the protocol. For the rest of this section, we assume that all parameters are sufficiently small such that the smoothing parameters of the smooth entropies are always in \([0, 1)\).

**Lemma 3.8.** If there exists an \( \varepsilon \)-secure implementation of \( f : X \times Y \rightarrow Z \) from a primitive \( P_{UV} \) in the (weak) semi-honest model, then

\[
H^3_{\varepsilon}(X|UM,Y = y) = 0 .
\]

**Proof.** Since the protocol is secure for Bob, there exists a randomized function \( S_A \) such that

\[
D(P_{XMU|Y=y}, P_{XSA(X)}) \leq \varepsilon
\]

for all \( y \in Y \). Therefore, for any \( y, y' \)

\[
D(P_{XMU|Y=y}, P_{XMU|Y=y'}) \leq 2\varepsilon . \tag{3.4.14}
\]

It holds that \( I(X; Z|UM,Y = y) = 0 \). Furthermore, we have \( \Pr[Z \neq f(X,Y) | Y = y] \leq \varepsilon \). Thus, we obtain

\[
H^\varepsilon(f(X,y)|UM,Y = y) \leq H^\varepsilon(f(X,y)|Z,Y = y) = 0 . \tag{3.4.15}
\]

Together with (3.4.14), this implies that for any \( y, y' \)

\[
H^\varepsilon(f(X,y)|UM,Y = y') = 0 .
\]
Since $X$ can be computed from the values $f(X, y_1), \ldots, f(X, y_{|Y|})$, we obtain

$$H_0^{3|Y|\varepsilon}(X | UM, Y = y) \leq H_0^{3|Y|\varepsilon}(f(X, y_1), \ldots, f(X, y_{|Y|}) | UM, Y = y) \leq \sum_{y' \in Y} H_0^{3\varepsilon}(f(X, y') | UM, Y = y) = 0,$$

where we used Lemma 2.10 and the subadditivity of the max-entropy (Lemma 2.4).

Let $P_{XY}$ be the input distribution to the ideal primitive. Then the security of the protocol implies the following lemma.

**Lemma 3.9.** For any protocol that is an $\varepsilon$-secure implementation of $f : X \times Y \rightarrow Z$ from a primitive $P_{UV}$ in the semi-honest model,

$$\tilde{H}^{\varepsilon + \varepsilon'}_\infty (X | VM) \geq \tilde{H}^{\varepsilon'}_\infty (X | Y f(X, Y)),$$

for any $\varepsilon' \geq 0$.

**Proof.** The security of the protocol implies that there exists a randomized function $S_B$, such that $D(P_{XY} S_B(Y, f(X, Y)), P_{XYVM}) \leq \varepsilon$. Therefore, we obtain

$$\tilde{H}^{\varepsilon + \varepsilon'}_\infty (X | VM) \geq \tilde{H}^{\varepsilon'}_\infty (X | S_B(Y, f(X, Y))) \geq \tilde{H}^{\varepsilon'}_\infty (X | Y f(X, Y)),$$

where we used Lemma 2.14 in the second inequality. \hfill \Box

**Theorem 3.5.** Let $f : X \times Y \rightarrow Z$ be a function that satisfies (3.4.1). If there exists a protocol having access to a primitive $P_{UV}$ that implements $f$ with an error of at most $\varepsilon$ in the semi-honest model, then

$$\tilde{H}^{(3|Y|+1)\varepsilon + \varepsilon'}_\infty (U | V) \geq \max_y \tilde{H}^{\varepsilon'}_\infty (X | f(X, y)),$$

for any $\varepsilon' \geq 0$.

**Proof.** Let $y \in Y$. It follows from Lemmas 2.13 and 3.8 that

$$H_0^{3|Y|\varepsilon}(X | VM, Y = y) \leq H_0^{3|Y|\varepsilon}(X | UM, Y = y) = 0.$$
Therefore, Lemmas 2.11 and 2.13 imply that
\[
\tilde{H}_{\infty}^{\varepsilon+\varepsilon'}(X|VM, Y = y) - H_0^{3|Y|\varepsilon}(X|VM, Y = y) \\
\leq \tilde{H}_{\infty}^{(3|Y|+1)\varepsilon+\varepsilon'}(U|VM, Y = y) \\
\leq \tilde{H}_{\infty}^{(3|Y|+1)\varepsilon+\varepsilon'}(U|V).
\]

We can use Lemma 3.9 to obtain
\[
\tilde{H}_{\infty}^{\varepsilon'}(X|f(X, y)) \leq \tilde{H}_{\infty}^{\varepsilon+\varepsilon'}(X|VM, Y = y).
\]
The statement follows by maximizing over all \( y \).

Note that the proof holds for any definition of the smooth conditional min-entropy such that the properties in Lemmas 2.11, 2.13 and 2.14 hold. Thus, Lemmas 2.5, 2.6 and 2.7 imply the following corollary.

**Corollary 3.4.** Let \( f : X \times Y \to Z \) be a function that satisfies (3.4.1). If there exists a protocol having access to a primitive \( P_{UV} \) that implements \( f \) with an error of at most \( \varepsilon \) in the semi-honest model, then
\[
H_{\infty}^{(3|Y|+1)\varepsilon+\varepsilon'}(U|V) \geq \max_y H_{\infty}^{\varepsilon'}(X|f(X, y))
\]
for any \( \varepsilon' \geq 0 \).

### 3.4.3 Lower Bounds for Protocols implementing OT

**Corollary 3.5.** Any protocol that implements \( M \) instances of \( (N\choose 1) \cdot \text{OT}^K \) from \( m \) instances of \( (n\choose 1) \cdot \text{OT}^k \) with an error of at most \( 0 \leq \varepsilon \leq 1/(6n + 2) \) in the semi-honest model must satisfy
\[
m(n-1)k \geq M(N-1)K - (6n+2)\varepsilon.
\]

**Proof.** From Theorem 3.5 follows that
\[
\tilde{H}_{\infty}^{(3n+1)\varepsilon}(U|V) \geq M(N-1)K.
\]

For the distribution \( P_{UV} \) of randomized OTs, the entropy \( \tilde{H}_{\infty}^{\varepsilon}(U|V) \) with \( 0 \leq \bar{\varepsilon} < 1 \) is maximized by the event \( \Omega \) with \( P_{\Omega|U=u, V=v} = 1 - \bar{\varepsilon} \) for all \( u, v \) in the support of \( P_{UV} \). Therefore, we have
\[
\tilde{H}_{\infty}^{(3n+1)\varepsilon}(U|V) \leq -\log(2^{-m(n-1)k}(1 - (3n + 1)\varepsilon)) \\
= m(n-1)k - \log(1 - (3n + 1)\varepsilon).
\]
The statement follows from the fact that \( \log(1/\varepsilon) \leq 2(1-\varepsilon) \) for any \( \varepsilon \) with \( 1/2 \leq \varepsilon \leq 1 \). \(\square\)
This corollary implies that there is no protocol that extends \((\frac{2}{1})\)-OT\(^1\) in the semi-honest model.

**Corollary 3.6.** Any protocol that implements \(m + 1\) instances of \((\frac{2}{1})\)-OT\(^1\) in the semi-honest model using \(m\) instances of \((\frac{2}{1})\)-OT\(^1\) must have an error \(\varepsilon \geq 1/14\).

Consider an \(\varepsilon\)-secure implementation of \((\frac{2}{1})\)-OT\(^K\) from \((1/2)\)-RabinOT\(^k\). Then, Corollary 3.2 provides a lower bound on \(k\) that is smaller than or equal to \(2K\). Corollary 3.5 however, shows that there is no such implementation if \(K \geq 2\) and \(0 \leq \varepsilon < 1/4\) (independently of \(k\)). For \(\varepsilon < 2^{-m}\), we have \(H^{\varepsilon}_\infty(U|V) = 0\) if \((U,V)\) corresponds to \(m\) randomized instances of \((1/2)\)-RabinOT\(^k\) (independently of \(k\)).

### 3.4.4 Lower Bounds for Equality Function

**Corollary 3.7.** Let a protocol having access to a \(P_{UV}\) be an \(\varepsilon\)-secure implementation of \(E_{Q_n}\) in the semi-honest model. Then

\[
H(U|V) \geq (1 - \varepsilon)k - (3 \cdot 2^k - 1)(\varepsilon + h(\varepsilon)) - 1 ,
\]

and

\[
H^{(3 \cdot 2^k + 1)\varepsilon}_\infty(U|V) \geq k - 1 ,
\]

for all \(0 \leq k \leq n\). If \(0 \leq \varepsilon \leq 1/(6 \cdot 2^k + 2)\) and \(P_{UV}\) is equivalent to \(m\) instances of \((\frac{2}{1})\)-OT\(^1\), then

\[
m \geq k - 1 - (6 \cdot 2^k + 2)\varepsilon ,
\]

for all \(0 \leq k \leq n\).

**Proof.** We can restrict the input domains of both players to the same subsets of size \(2^k\). Condition [3.4.1] will still be satisfied. Thus, the corollary follows immediately from Theorems 3.1 and 3.5.

There exists a secure reduction of \(E_{Q_n}\) to \(E_{Q_k}\) ([BM04]): Alice and Bob compare \(k\) inner products of their inputs with random strings using \(E_{Q_k}\). This protocol is secure in the semi-honest model with an error of at most \(2^{-k}\). Since there exists a circuit to implement \(E_{Q_k}\) with \(k\) XOR and \(k\) AND gates, it follows from [GV88] that \(E_{Q_k}\) can be securely implemented using \(k\) instances of \((\frac{3}{1})\)-OT\(^1\) or \(3k\) instances of \((\frac{2}{1})\)-OT\(^1\) in the semi-honest model. Since \(m\) instances of \((\frac{2}{1})\)-OT\(^1\) are equivalent to a primitive \(P_{UV}\) with \(H(U|V) = m\), the bound of Corollary 3.7 is optimal.
up to a factor of 3. Since the non-local AND can be computed using two
PR-Boxes [BBL+06] and a PR-Box can be simulated from one instance of
\((\frac{3}{2})\cdot\text{OT}^1\) [WW05b] one can actually show that EQ\(_k\) can be securely im-
plemented using at most 2\(k\) instances of \((\frac{3}{2})\cdot\text{OT}^1\) as follows: To compute
additive shares of \((x_1 \oplus y_1) \land (x_2 \oplus y_2)\) using two instances of
\((\frac{3}{2})\cdot\text{OT}^1\),

Alice chooses two random bits \(r_1, r_2\) and inputs \(r_1, r_1 \oplus x_1\) to the first and
\(r_2, r_2 \oplus x_2\) to the second instance. Bob uses \(y_2\) as the choice bit for the first
and \(y_1\) as the choice bit for the second instance of OT. Bob receives two
outputs \(z_1 = r_1 \oplus x_1 y_2\) and \(z_2 = r_2 \oplus x_2 y_1\). Setting \(a = r_1 \oplus r_2 \oplus x_1 x_2\)
and \(b = z_1 \oplus z_2 \oplus y_1 y_2\), we have \(a \oplus b = x_1 x_2 \oplus y_1 y_2 \oplus x_1 y_2 \oplus x_2 y_1 =
(x_1 \oplus y_1) \land (x_2 \oplus y_2)\). Thus, we can compute EQ\(_k\) with 2\((k - 1)\) instances
of \((\frac{3}{2})\cdot\text{OT}^1\).

### 3.4.5 Lower Bounds for Inner Product Function

**Corollary 3.8.** Let a protocol having access to a primitive \(P_{UV}\) be an \(\varepsilon\)-secure
implementation of the inner product function IP\(_n\) in the semi-honest model. Then it holds that

\[H(U|V) \geq n - 1 - 4n(\varepsilon + h(\varepsilon))\]

and

\[\tilde{H}_{\infty}^{(3k+1)\varepsilon}(U|V) \geq n - 1.\]

If \(P_{UV}\) is equivalent to \(m\) instances of \((\frac{3}{2})\cdot\text{OT}^1\) and \(0 \leq \varepsilon < 1/(6n + 2)\), then

\[m \geq n - 1 - (6n + 2)\varepsilon.\]

**Proof.** Let \(e_i \in \{0, 1\}^n\) be the string that has a one at the \(i\)-th position and
is zero otherwise. Let \(S := \{e_i : 1 \leq i \leq n\}\). Then the protocol is an \(\varepsilon\)-
secure implementation of the restriction of the inner-product function to
inputs from \(\{0, 1\}^n \times S\). Since this restricted function satisfies condition
(3.4.1), the statement follows from Theorem 3.1.

If \(\varepsilon < 1/(8n)\), then it immediately follows from Corollary 3.8 that we
need at least \(n - 2\) calls to \((\frac{3}{2})\cdot\text{OT}^1\) to compute IP\(_n\) with an error of at
most \(\varepsilon\). Consider the following protocol from [BM04] that is adapted to
\((\frac{3}{2})\cdot\text{OT}^1\): Alice chooses \(r = (r_1, \ldots, r_{n-1})\) uniformly at random and sets
\(r_n := \oplus_{i=1}^{n-1} r_i\). Then, for each \(i\), Alice inputs \(a_{i,0} := r_i\) and \(a_{i,1} := x_i \oplus r_i\)
to the OT and Bob inputs $y_i$. Bob receives $z_i$ from the OTs and outputs $\bigoplus_{i=1}^{n} z_i$. Since $\bigoplus_{i=1}^{n} z_i = \bigoplus_{i=1}^{n} (x_i y_i \oplus r_i) = (\bigoplus_{i=1}^{n} x_i y_i) \oplus (\bigoplus_{i=1}^{n} r_i) = \bigoplus_{i=1}^{n} x_i y_i = \text{IP}_n(x, y)$, the protocol is correct. The security for Alice follows from the fact that $z_1, \ldots, z_n$ is a uniformly random string subject to $\bigoplus_{i=1}^{n} z_i = \text{IP}_n(x, y)$. Thus, there exists a perfectly secure protocol that computes $\text{IP}_n$ from $n$ instances of $(2_1^1)$-OT\textsuperscript{1}. Hence, Corollary 3.8 is almost tight.

### 3.4.6 Lower Bounds for Protocols implementing OLFE

We will now show that Theorems 3.1 and 3.2 also imply bounds for oblivious linear function evaluation ($(q)$-OLFE), which is defined as follows:

- For any finite field $GF(q)$ of size $q$, $(q)$-OLFE is the primitive where Alice has an input $a, b \in GF(q)$ and Bob has an input $c \in GF(q)$. Bob receives $d = a + b \cdot c \in GF(q)$.

**Corollary 3.9.** Let a protocol having access to $P_{UV}$ be an $\epsilon$-secure implementation of $m$ instances of $(q)$-OLFE in the semi-honest model. Then

$$H(U|V) \geq m \log q - 5(\epsilon m \log q + h(\epsilon)), \quad (3.4.18)$$

$$H(V|U) \geq m \log q - 5(\epsilon m \log q + h(\epsilon)), \quad (3.4.19)$$

$$I(U; V|U \land V) \geq m \log q - 7(\epsilon m \log q + h(\epsilon)). \quad (3.4.20)$$

**Proof.** Inequalities (3.4.18) and (3.4.20) follow from Theorem 3.1 and Theorem 3.2. Furthermore, it has been shown in [WW06] that $(q)$-OLFE is symmetric. Hence, a violation of (3.4.19) would imply a violation of the lower bound in (3.4.18). \qed

### 3.4.7 Malicious OT

Lemma 3.1 shows that lower bounds for implementations of OT in the semi-honest model imply almost the same bounds in the malicious model. In the following, we generalize these results by allowing a dishonest Bob to additionally receive randomness $V'$. This generalizes the result of Section 3.3.1 where a dishonest Bob only gets $V$. Moreover, it provides a stronger impossibility result, in the case when $V'$ is trivial, than the one that follows from the combination of Lemma 3.1 and Theorem 3.5.

**Corollary 3.10.** Let a protocol be an $\epsilon$-secure implementation of $(2_1^1)$-OT\textsuperscript{k} in the malicious model from randomness $(U, VV')$. Then

$$\tilde{H}_\infty^{7\epsilon}(U|VV') \geq k.$$
Proof. We consider only honest players, but allow the simulator to change the inputs to the ideal OT and the outputs from the ideal OT. Lemma 3.8 holds in the weak semi-honest model and, therefore, also in the malicious model. Thus, we have

\[ H_0^{6\varepsilon}(X|UM, Y = y) = 0. \]

The security of the protocol implies that there exists a randomized function \( S_B \) such that

\[ D(P_{XS_B(C,X_{\tilde{C}})}, P_{XVV'M}) \leq \varepsilon, \]

where \( \tilde{C} \) is the input to the ideal OT by the simulator. Therefore, we obtain

\[ \tilde{H}^{\varepsilon}(X|VV'M, C = c) \geq \tilde{H}(X|S_B(c, X_{\tilde{C}})) \geq \tilde{H}(X|X_{\tilde{C}}) \geq k. \] (3.4.21)

As in the proof of Theorem 3.5 this implies

\[ k \leq \tilde{H}^{\varepsilon}(X|VV'M, C = c) \leq \tilde{H}^{7\varepsilon}(U|VV'). \]

In the same way, we can show that the impossibility result for implementations of \( (\frac{2}{1})'-\text{OT}^k \) that follows from Theorem 3.1 also holds in the malicious model.

Corollary 3.11. Let a protocol be an \( \varepsilon \)-secure implementation of \( (\frac{2}{1})'-\text{OT}^k \) in the malicious model from randomness \( (U, VV') \). Then

\[ H(U|VV') \geq k - 6(k\varepsilon + h(\varepsilon)). \]

Proof. Lemma 3.3 also holds in the malicious model. Thus, we can use (2.1.3) to obtain

\[ H(X|UVV'M, C = c) \leq H(X|UM, C = c) \leq 4(k\varepsilon + h(\varepsilon)). \]

The security of the protocol implies that there exists a randomized function \( S_B \) such that

\[ D(P_{XS_B(C,X_{\tilde{C}})}, P_{XVV'M}) \leq \varepsilon, \]
where $\tilde{C}$ is the input to the ideal OT by the simulator. Therefore, we can use inequality (2.1) to obtain

\[
H(X|VV'M, C = c) \geq H(X|S_B(c, X_{\tilde{C}})) - \varepsilon \cdot 2k - h(\varepsilon) \\
\geq H(X|X_{\tilde{C}}) - \varepsilon \cdot 2k - h(\varepsilon) \\
\geq k - \varepsilon \cdot 2k - h(\varepsilon). \tag{3.4.22}
\]

As in the proof of Theorem 3.1, this implies

\[
H(U|VV') \geq k - 6(k\varepsilon + h(\varepsilon)). \tag{3.4.23}
\]

\[\square\]

An instance of $\alpha$-UOT$^n$ can be implemented from distributed randomness $(U, VV')$ such that \(U = (X_0, X_1)\) and \((V, V') = ((C, X_C), Y)\) where \((X_0, X_1, C, X_C)\) are random variables with the distribution of $n$ randomized instances of \((\frac{2}{1})\)-OT$^l$. \(V'\) is equal to the first $n - \lceil \alpha n \rceil$ bits of $X_{1-C}$. Then

\[
H_{\min}(U|VV') = \lceil \alpha n \rceil \geq \alpha n.
\]

Thus, we can use Corollary 3.10 to obtain the following impossibility result for implementations of \((\frac{2}{1})\)-OT$^k$ from $\alpha$-UOT$^n$.

**Lemma 3.10.** Let $0 < \alpha \leq 1$. If there exists an $\varepsilon$-secure implementation of \((\frac{2}{1})\)-OT$^k$ from an $\alpha n$-UniversalOT, where $\varepsilon \leq 1/14$, then

\[
\alpha n \geq k - 1 - 14\varepsilon.
\]

**Proof.** Corollary 3.10 implies that

\[
H_{\infty}^{7\varepsilon}(U | VV') \geq k.
\]

The statement then follows from

\[
\tilde{H}_{\infty}^{7\varepsilon}(U|VV') \leq -\log(2^{-\lceil \alpha n \rceil} - 7\varepsilon / 2^\lceil \alpha n \rceil) \\
= -\log(2^{-\lceil \alpha n \rceil}(1 - 7\varepsilon)) \\
= \lceil \alpha n \rceil - \log(1 - 7\varepsilon) \\
\leq \alpha n + 1 - \log(1 - 7\varepsilon).
\]

\[\square\]
### 3.5 String OT from Universal OT

#### 3.5.1 Protocol and Security Definition

**Protocol 1: \((\binom{2}{1})^{\text{ROT}}^k\) from \(\alpha\text{-UOT}^n\)**

Parameters: \(0 < \alpha \leq 1\). A positive integer \(n\) and \(x > 0\) such that \(xn, 2x^2n\) and \(k := (\alpha - 33x)n - 1\) are positive integers. Inputs: Bob receives input \(c\). Outputs: \((z_0, z_1) \in \{0, 1\}^{2k}\) to Alice, and \(y \in \{0, 1\}^k\) to Bob.

1: Alice chooses two random strings \(x_0 = (x_{00}, \ldots, x_{0n}), x_1 = (x_{10}, \ldots, x_{1n}) \in \{0, 1\}^n\). Bob selects \(w \in \{0, 1\}^t\) uniformly at random and decodes \(w\) into a subset \(s \subset [n]\) of cardinality \(xn\).

2: Alice transmits \(x_0\) and \(x_1\) to Bob using \(\alpha\text{-UOT}^n\). Bob inputs \(\tilde{c} = (\tilde{c}_1, \ldots, \tilde{c}_n)\), with \(\tilde{c}_i = c\) if \(i \in s\) and \(\tilde{c}_i = 1 - c\) otherwise.

3: Bob sends \(w\) to Alice using interactive hashing. Alice and Bob compute the two output strings, labeled \(w_0, w_1\) according to lexicographic order. Bob computes \(b \in \{0, 1\}\) such that \(w_b = w\).

4: Alice checks if \(|\text{enc}(w_0) \cap \text{enc}(w_1)| \leq 2x^2n\). Otherwise, she outputs two uniform strings \(z_0, z_1 \in \{0, 1\}^k\) and terminates the protocol.

5: Both parties compute \(s_0 := \text{enc}(w_0) \setminus (\text{enc}(w_0) \cap \text{enc}(w_1))\) and \(s_1 := \text{enc}(w_1) \setminus (\text{enc}(w_0) \cap \text{enc}(w_1))\).

6: Bob announces \(a = b \oplus c, (x_0)_{s_1-a}\) and \((x_1)_{s_a}\).

7: Alice checks that the strings announced by Bob are consistent with \(a\) and contain no errors. Otherwise, she outputs two uniform strings \(z_0, z_1 \in \{0, 1\}^k\) and terminates the protocol.

8: Alice and Bob discard the bits at positions \(\text{enc}(w_0) \cup \text{enc}(w_1)\) and keep the remaining positions in \(\mathcal{R} = [n] \setminus (\text{enc}(w_0) \cup \text{enc}(w_1))\). Let \(j = |\mathcal{R}|\) and \(r_0 = (x_0)_{\mathcal{R}}, r_1 = (x_1)_{\mathcal{R}}\).

9: Alice chooses two functions \(f_0, f_1\) randomly and independently from a two-universal family \(\mathcal{F}\) of hash functions from \(\{0, 1\}^j\) to \(\{0, 1\}^k\). She sends \(f_0, f_1\) to Bob and sets \(z_0 = f_0(r_0)\) and \(z_1 = f_1(r_1)\).

10: Bob sets \(y = f_c(r_c)\).
In the following, we consider the protocol (Protocol 1 above) from [CS06], which uses an instance of universal oblivious transfer to implement a sender-randomized OT over strings of length $k$. This functionality, denoted by $\binom{2}{1}$-ROT$^k$, takes a bit $C$ as input from Bob and outputs random $(Z_0, Z_1) \in \{0, 1\}^k \times \{0, 1\}^k$ to Alice and $Z_C$ to Bob. An instance of $\binom{2}{1}$-ROT$^k$ can be used to securely implement an instance of $\binom{2}{1}$-OT$^k$ (a proof of security for this reduction can be found, for example, in the full version of [CSSW06]). We will show that the protocol implements $\binom{2}{1}$-ROT$^k$ from an instance of $\alpha$-UOT$^n$ with an asymptotic rate $k/n$ of $\alpha$. This is optimal according to Lemma 3.10.

We use a security definition from [Sch07], which is a slightly simplified version of the security definition in [CSSW06].

**Definition 3.5.** An $\varepsilon$-secure sender-randomized oblivious transfer scheme over strings of length $k$ is a protocol between Alice and Bob, where Bob has input $C \in \{0, 1\}$, Alice has no input, Alice gets outputs $(Z_0, Z_1) \in \{0, 1\}^k \times \{0, 1\}^k$ and Bob gets output $Y \in \{0, 1\}^k$, satisfying the following properties.

1. **Correctness:** If both players are honest, then $Y = Z_C$ except with probability $\varepsilon$.

2. **Security for Alice:** If Alice is honest, then for any dishonest Bob with output $B'$ there exists a binary random variable $C'$ such that

$$D(P_{Z_0 Z_1 B'C'}, P_{UNIF^k} P_{Z_C B'C'}) \leq \varepsilon .$$

3. **Security for Bob:** If Bob is honest, then for any dishonest Alice with output $A'$, we have

$$D(P_{C A'}, P_C P_{A'}) \leq \varepsilon .$$

Since we consider security in the malicious model, a dishonest player may abort the protocol by not sending any message. A possibility to handle this would be to include a special output aborted to the definition of the ideal functionality. Here, we take the following, different approach, which is also used, for example, in [KWW09]: Whenever a player does not send a (well-formed) message, the other player assumes that a particular valid message has been sent. This approach only works if there is an
upper bound on the delivery time of a message, i.e., if we assume that the communication is synchronous. Since a dishonest player could have sent this message himself, not sending a message gives him no advantage.

Protocol 1 uses interactive hashing in conjunction with subsets. Thus, the protocol needs an encoding of subsets $\text{enc} : \{0, 1\}^t \rightarrow \mathcal{S}$, where $\mathcal{S}$ is the set of all subsets of $[n]$ of size $xn$. Here we choose $t$ such that $2^t \leq (\frac{n}{nx}) \leq 2 \cdot 2^t$. We use an injective encoding $\text{enc} : \{0, 1\}^t \rightarrow \mathcal{S}$. This means that not all possible subsets are encoded, but at least half of them. We refer to [CCM98, Sav07] for details on how to obtain such an encoding.

### 3.5.2 Proof of Security

The following lemma shows that we can split the min-entropy $H_\infty(X_0X_1)$ in a randomized sense such that either $X_0$ or $X_1$ have almost maximal entropy or, otherwise, both $X_0$ and $X_1$ have at least some entropy. The proof is similar to the proof of Theorem 5.1 in [Wul07a].

**Lemma 3.11 (Min-Entropy Splitting Lemma).** Let $X_0, X_1$ be random variables with a distribution $P_{X_0X_1}$ such that $H_\infty(X_0X_1) \geq \alpha n$. Then there exists a random variable $C \in \{0, 1, 2\}$ such that

$$H_\infty^{e}(X_1-c|X_c, C = c) \geq \alpha n - \delta n - 1,$$

for $c \in \{0, 1\}$ with $P_C(c) > 0$, and

$$H_\infty(X_0|C = 2) \geq \delta n - \log(1/\varepsilon),$$

$$H_\infty(X_1|C = 2) \geq \delta n - \log(1/\varepsilon),$$

if $P_C(2) > 0$.

**Proof.** We define the following function $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1, 2\}$:

$$f(x_0, x_1) := \begin{cases} 
0 & \text{if } P_{X_0}(x_0) > 2^{-\delta n} \text{ and } P_{X_1}(x_1) \leq 2^{-\delta n}, \\
1 & \text{if } P_{X_0}(x_0) \leq 2^{-\delta n} \text{ and } P_{X_1}(x_1) > 2^{-\delta n}, \\
2 & \text{if } P_{X_0}(x_0) \leq 2^{-\delta n} \text{ and } P_{X_1}(x_1) \leq 2^{-\delta n}, \\
u \in_R \{0, 1\} & \text{else.}
\end{cases}$$

where $u$ is a uniform random bit. Let $C := f(X_0, X_1)$. We define the sets $S_i := \{x \in \mathcal{X} : P_{X_i}(x) \leq 2^{-\delta n}\}$. Let $c \in \{0, 1\}$ such that $P_C(c) > 0$. We
consider \( x_c \notin S_c \). We can bound the probability \( P_{X_cC}(x_c, c) \) as follows:

\[
P_{X_cC}(x_c, c) = \sum_{x_{1-c} \in S_{1-c}} P_{X_{1-c}X_c}(x_{1-c}, x_c) + \sum_{x_{1-c} \notin S_{1-c}} \frac{P_{X_{1-c}X_c}(x_{1-c}, x_c)}{2}
\]

\[
\geq \frac{1}{2} \cdot P_{X_c}(x_c)
\]

\[
\geq 2^{-\delta n - 1}.
\]

We can use this lower bound to obtain

\[
P_{X_{1-c}|X_c=x_c,C=c}(x_{1-c}) = \frac{P_{X_{1-c}X_cC}(x_{1-c}, x_c, c)}{P_{X_cC}(x_c, c)}
\]

\[
\leq \frac{2^{-\alpha n}}{2^{-\delta n - 1}}
\]

\[
\leq 2^{-\alpha n + \delta n + 1}.
\]

This implies the desired lower bound on the conditional min-entropy:

\[
H_\infty(X_{1-c}|X_c, C = c) \geq (\alpha - \delta)n - 1.
\]

Next, we assume \( P_C(2) \geq \varepsilon \). Then, for \( i \in \{0, 1\} \), it holds that \( P_{X_iC}(x_i, 2) \leq 2^{-\delta n} \) and, therefore, \( P_{X_i|C=2}(x_i) \leq 2^{-\delta n}/\varepsilon \). This implies

\[
H_\infty(X_0|C = 2) \geq \delta n - \log(1/\varepsilon),
\]

\[
H_\infty(X_1|C = 2) \geq \delta n - \log(1/\varepsilon).
\]

If \( 0 < P_C(2) < \varepsilon \), then we consider the distribution \( P_{X_0X_1|C \neq 2} \). We define the random variable \( C' \), which is equal to \( C \) if \( C < 2 \), and zero otherwise. Then, we can conclude that

\[
H_\infty(X_{1-c'}|X_{c'}, C' = c') \geq H_\infty(X_{1-c}|X_c, C = c) \geq (\alpha - \delta)n - 1.
\]

From the proof in [CS06], we know that Protocol 1 is correct with a negligible error: The probability that the check in Step 4 fails is upper bounded by \( 2 \cdot \Pr[B(xn, \frac{x}{1-x}) \geq 2x^2n] \), where \( B(n, p) \) is the binomial distribution with parameters \( n \) and \( p \). We can use the Chernoff bound [Che52] to show that this probability is at most

\[
2 \exp \left( -\frac{(1 - 2x)^2x^2}{3(1 - x)}n \right).
\]
Furthermore, the protocol is perfectly secure for Bob.

Next, we will apply Lemma 3.11 to show that the protocol is secure for Alice. Intuitively speaking, the security for Alice follows from the fact the either the min-entropy of one of the two outputs given Bob’s information is almost maximal or otherwise Bob has some uncertainty about both outputs. In the first case, the security for Alice follows from privacy amplification. In the latter case, min-entropy sampling guarantees that the set of substrings of length $\delta xn$ of $X_0$ and $X_1$ that are bad, in the sense that Bob can guess them with good probability, must be small. The properties of interactive hashing imply that Bob is not able to generate two strings such that the corresponding substrings are from this bad set except with small probability.

Let $\tau := 4x/3$, $\theta := \tau/\log(\tau)$ and $\gamma := e^{-\theta^2xn/2}$. Let $\nu := (\gamma + 2^{-c\tau n})$, where $c$ is the constant from the statement of Lemma 2.16. Let $S$ be the set of all subsets $s \subset [n]$ with cardinality $|s| = xn$.

**Lemma 3.12.** Let $H_\infty(X) \geq 8xn$. Then the fraction of subsets $s \in S$ with $H_\infty'(X_s) < 4x^2n$ is less than $\sqrt{\nu}$.

*Proof.* Let $S$ be uniformly distributed over $S$. Then $P_{SX}$ is $\nu$-close to a distribution $P_{AB}$ where $A$ is uniform over the subsets of size $xn$ and $H_\infty(B|A) \geq (8x - 3\tau)xn = 4x^2n$ according to Lemmas 2.15 and 2.16. Let

$$\tilde{B} := \{s \in S : D(P_{X_s}, P_{X_s'}) \geq \sqrt{\nu} \text{ for all } P_{X_s'} \text{ with } H_\infty(X_s') \geq 4x^2n\}.$$

Then, it is easy to see that the probability that $s$ is in $\tilde{B}$ must be smaller or equal to $\sqrt{\nu}$, since otherwise the distance between the two distributions would be greater than $\nu$. Therefore, at most a $\sqrt{\nu}$-fraction of all subsets $s \in S$ satisfy $H_\infty'(X_s) < 4x^2n$. 

**Lemma 3.13.** Protocol 1 is secure for Alice with an error that is negligible in $n$, i.e., there exists a random variable $C'$ such that

$$D(P_{Z_0Z_1BC'}, P_{UNI kPZ_{C'}BC'}) \leq 65\sqrt{\nu} + 2^{-2x^2n}$$

where $B$ is the whole view of Bob.

*Proof.* Let $P_{Y|X}$ be the channel chosen by Bob and let $Y$ be the output of the UOT on input $X = (X_0, X_1)$. We define $\varepsilon := 2^{-8xn}$. We know from the properties of UOT that $H_\infty(X_0X_1|Y = y) \geq \alpha$ for all $y$. According to Lemma 3.11 it is sufficient to consider the following two cases:
1. There exists a $c'$ such that $H^ε_∞(X_{1−c'}|X_{c'}Y = y) \geq (α − 16x)n − 1$. Let $(F_0, F_1, B')$ be the whole view of Bob at the end of the protocol. According to Lemmas 2.6 and 2.7, we have

\begin{align*}
H^ε_∞(X_{1−c'}|Z_{c'}F_0F_1B', Y = y) &\geq H^ε_∞(X_{1−c'}|X_{c'}F_{c'}B', Y = y) \\
&\geq H^ε_∞(X_{1−c'}|X_{c'}B', Y = y) \\
&\geq (α − 16x)n − 1.
\end{align*}

Since Alice and Bob discard $xn$ bits, the min-entropy of the remaining string must be at least $(α − 17x)n − 1$ according to Lemma 2.9. Using privacy amplification (Lemma 2.17), we obtain that extracting

\[(α − 17x)n − 1 − 2\log(1/ε) = (α − 33x)n − 1 = k\]

bits from $X_{1−c'}$ results in a string that is $2ε$-close to uniform with respect to Bob’s view, i.e., we have

\[D(P_{X_{1−c'}X_{c'}F_0F_1B'|Y = y}, P_{X_{1−c'}X_{c'}F_0B'|Y = y}) \leq 2ε.\]

2. We have

\[\min(H_∞(X_0|Y = y), H_∞(X_1|Y = y)) \geq 16xn − \log(1/ε) \geq 8xn.\]

For $i \in \{0, 1\}$, we define the two sets

\[B^i := \left\{ s \in S : H^ε_∞((X_i)_s|Y = y) < 4x^2n \right\}.\]

According to Lemma 3.12, the fraction of subsets that is either in $B^0$ or in $B^1$ is at most $2\sqrt{ν}$. Using the properties of interactive hashing, we know that Bob can get strings $w_0$ and $w_1$ encoding subsets that are both either in $B^0$ or in $B^1$ with probability at most $ε' := 2 \cdot 16 \cdot 2\sqrt{ν}$. Thus, with probability at least $1 − ε'$ there is a bit $d$ such that

\[H^ε_∞(\langle X_0 \rangle_{enc(w_d)}|Y = y) \geq 4x^2n\]

and

\[H^ε_∞(\langle X_1 \rangle_{enc(w_d)}|Y = y) \geq 4x^2n.\]
If the check in Step 7 passes, then the intersection between the two sets \( \text{enc}(w_0) \) and \( \text{enc}(w_1) \) is at most of cardinality \( 2x^2n \). Therefore, we can use Lemma 2.9 to obtain
\[
H_\infty^\nu((X_0)_{s_d}|Y = y) \geq 2x^2n,
\]
\[
H_\infty^\nu((X_1)_{s_d}|Y = y) \geq 2x^2n.
\]
In this case the probability that Bob passes the test in Step 7 of the protocol is at most \( \sqrt{\nu} + 2^{-2x^2n} \). Thus, the distance from uniform in this case is at most
\[
\varepsilon' + \sqrt{\nu} + 2^{-2x^2n} = 65\sqrt{\nu} + 2^{-2x^2}.
\]
Since \( 2\varepsilon \leq 65\sqrt{\nu} + 2^{-2x^2} \), this implies that there exists a random variable \( C' \) such that
\[
D(P_{Z_0Z_1B}, P_{UNIF^k} P_{Z_{C'}B}) \leq 65\sqrt{\nu} + 2^{-2x^2n},
\]
where \( B \) is the whole view of Bob.

Thus, the following theorem is a consequence of the perfect security for Bob, of the correctness (3.5.1) and of Lemma 3.13.

**Theorem 3.6.** There exists a protocol that implements \((\frac{2}{1})\)-\(\text{OT}^k\) from \(\alpha\)-\(\text{UOT}^n\) with a rate of \(k/n\) that asymptotically reaches \(\alpha\) and has an error that is exponentially small in \(n\).

According to Lemma 3.10 this is asymptotically optimal.

### 3.5.3 Repeated Universal OT

Next, we consider implementations of OT from repeated Universal OT over pairs of bits as proposed in [BC97]. There the following variant of Universal OT over bits, which we call \(\alpha\)-\(\text{UOT}_H\), is considered: Bob can choose a channel \(P_{Y|X}\) such that \(H(X_0X_1|Y) \geq \alpha\), where \((X_0, X_1) \in \{0, 1\} \times \{0, 1\}\) are uniform and \(Y\) is the output of the channel \(P_{Y|X}\), and learns \(Y\). In [CS06] it has been proven that the above protocol can securely implement \((\frac{2}{1})\)-\(\text{OT}^k\) from \(n\) instances of \(\alpha\)-\(\text{UOT}_H\) with a rate \(k/n\) of \(2\rho(\alpha)\) where \(\rho(\alpha)\) is the unique solution to \(h(x) = \alpha\) for \(x \in [0, \frac{1}{2}]\). We can prove that the protocol actually achieves a rate \(k/n\) of \(\alpha\). The result follows from the fact that there is a trivial implementation of \((\alpha - \lambda)n\)-\(\text{UOT}\)
from $n$ instances of $\alpha$-UOT$_H$ over bits, where honest Bob uses the same choice bit for all instances. This protocol has an error that is negligible in $n$ for any $\lambda > 0$ as follows from the following lemma, which is implied by a straightforward generalization of the proof of Theorem 3.1 in [DFR+06].

**Lemma 3.14.** Consider random variables $Z_1, \ldots, Z_n$ over an alphabet $Z$, random variables $Y_1, \ldots, Y_n$ over an alphabet $Y$ and $\alpha > 0$ such that

$$H(Z_{i+1}|Z_1, \ldots, Z_i, Y_1, \ldots, Y_n) \geq \alpha$$

for all $i \in [n]$ and $(z_1, \ldots, z_{i-1}) \in Z^{i-1}$. Then, for any $0 < \lambda < \frac{1}{2}$,

$$H_{\infty}(Z_1, \ldots, Z_n|Y_1, \ldots, Y_n) \geq (\alpha - 2\lambda)n \quad (3.5.2)$$

with $\varepsilon = \exp\left(-\frac{\lambda^2 n}{32(\log(|Z|/\lambda)^2}\right)$.

**Proof.** Let $Z^i = (Z_1, \ldots, Z^i)$ and $Y^i = (Y_1, \ldots, Y_i)$ for all $i \in [n]$. We define random variables $S_i := \log P_{Z_i|Z^{i-1}Y^n}(Z_i|Z^{i-1}Y^n)$ for all $i \in [n]$. We can follow the proof of Theorem 3.1 in [DFR+06] to obtain

$$\Pr\left[\sum_{i=1}^{n}(S_i + \alpha - \lambda) \geq \lambda n\right] \leq \exp\left(\frac{\lambda^2 n}{2c^2}\right)$$

with $c^2 \leq 16 \log(|Z|/\lambda)^2$. Thus, we know that

$$\Pr\left[\sum_{i=1}^{n}(\log P_{Z_i|Z^{i-1}Y^n}(Z_i|Z^{i-1}Y^n) + \alpha - \lambda) \geq \lambda n\right] \leq \varepsilon \, . \quad (3.5.3)$$

For all $y^n \in Y^n$, we define the set $S_{y^n} \subseteq Y^n$ of all $z^n$ such that

$$-\log(P_{Z^n|Y^n}(z^n, y^n)) \geq (\alpha - 2\lambda)n.$$

We define the event $\Omega$ with

$$P_{\Omega|Z^n=z^n,Y^n=y^n} = \begin{cases} 1, & \text{if } z^n \in S_{y^n} , \\ 0, & \text{otherwise} . \end{cases}$$

By the inequality (3.5.3), we know that $\Pr[\Omega] \geq 1 - \varepsilon$. Thus, the definition of the smooth min-entropy implies that

$$H_{\infty}(Z^n|Y^n) \geq -\log \max_{z^n, y^n} P_{Z^n\Omega|Y^n=y^n}(z^n) \geq (\alpha - 2\lambda)n \, . \quad (3.5.4)$$
The rate of this implementation is essentially optimal according to Corollary 3.11. Bob can choose, for each instance of $\alpha$-UOT$_H$, the channel that outputs both inputs with probability $1 - \alpha$ and one of the inputs $X_c$ with probability $\alpha$. This primitive can be implemented from randomness $(U, VV') = ((X_0, X_1), (C, X_C, V'))$, where $(U, V)$ corresponds to a randomized $\binom{2}{1}$-OT$_1$ and $V' = X_{1-C}$ with probability $1 - \alpha$ and $V' = \bot$ otherwise. Then, we have $H(U|VV') \leq \alpha$. This solves an open question posed in [CS06].
Chapter 4

Efficiency of Commitments from Noisy Correlations

4.1 Introduction

Oblivious transfer can be implemented from noisy channels [Cré88, CK88, Cré97, CMW04], cryptogates [Kl00] and weak variants of noisy channels [DKS99, DFMS04, Wu07b, Wu09]. While all these protocols require \( \Omega(\kappa) \) instances of a given primitive to implement a single OT with a security of \( 2^{-\kappa} \), it has been shown in [HIKN08, IPS08, IKOS09, IKO+11] that there are more efficient protocols if many OTs are implemented at once. In the semi-honest model and in some cases also in the malicious model, it is possible to implement OT at a constant rate, which means that \( n \) instances of OT can be implemented from just \( O(n) \) instances of the given primitive if \( n \) is big enough compared to the security parameter. It is, therefore, possible to achieve the lower bounds for such reductions [DM99, BM04, WW05a, WW10] up to a constant factor. In this chapter we address the question whether such efficient protocols also exist in the case of bit commitment.

Related Work  Bit commitments can be implemented from a wide variety of information-theoretic primitives [Cré97, DKS99, WNI03, Wu09]. There are protocols which implement a single string commitment from noisy channels at a constant rate, meaning that the size of the string grows linearly with the number of instances of noisy channels used, which is essentially optimal [WNI03]. Protocols which implement individual bit
commitments at a constant rate, however, are not known. In [NOIMQ03] it has been shown that in any perfectly correct and perfectly hiding non-interactive bit commitment scheme from distributed randomness with a security of $2^{-\kappa}$, the size of the randomness given to the players must be at least $\Omega(\kappa)$.

**Contributions** We show that, in contrast to implementations of OT, no constant rate bit commitment scheme can exist. More precisely, we show that if a protocol implements $n$ bit commitments with a security of at least $2^{-\kappa}$ from distributed randomness, then the mutual information between the sender’s and the receiver’s randomness is essentially bounded by $\kappa n$ from below (Theorem 4.1). This implies that we need at least $\Omega(\kappa n)$ instances of oblivious transfer or noisy channels to implement $n$ bit commitments, and hence executing for each bit commitment a protocol that uses $O(\kappa)$ instances is optimal. In combination with the lower bound from [WNI03], this impossibility result can be generalized to string commitments: any protocol that implements $n$ string commitments of length $\ell$ needs at least $\Omega(n(\kappa + \ell))$ bits of distributed randomness. Most results in this chapter are joint work with Jürg Wullschleger and have been published in [RTWW11].

### 4.2 Model and Security Definition

We will consider the following model: The two parties use a primitive $P_{UV}$ that has no input and outputs values $(u,v)$ distributed according to $P_{UV}$ to the players (cf. Section 3.2). The sender receives an input bit $x \in \{0,1\}^\ell$. In the commit phase, the players exchange messages in several rounds. Let all the messages exchanged be $M$, which is a randomized function of $(U,V,x)$. In the open phase, the sender sends $x$ together with a value $D_1$ to the receiver. The receiver then sends a message $E_1$ to the receiver, who replies with a message $D_2$ and so on. Let $N := (D_1,E_1,D_2,E_2,\ldots,E_{t-1},D_t)$ be the total communication in the open phase. We assume that the number of rounds in the open phase is upper bounded by a constant $t$. By padding the protocol with empty rounds, we can thus assume without loss of generality that the protocol uses $t$ rounds in every execution. Finally, the receiver accepts or rejects, which we model by a randomized function $F(x,V,M,N)$ that outputs 1 for accept and 0 for reject. Let the distribution in the honest setting be $P_{UVMN|X=x}$. We define three parameters that quantify the security for
the sender and the receiver, respectively, and the correctness of the protocol.

**Definition 4.1.** An $\ell$-bit string commitment scheme using a primitive $P_{UV}$ is $\gamma$-binding, $\beta$-correct and $\varepsilon$-hiding if it satisfies the following conditions:

- **$\beta$-correct:** $\Pr[F(x, V, M, N) = 1] \geq 1 - \beta$.
- **$\varepsilon$-hiding:** $D(P_{VM|X=x}, P_{VM|X=x'}) \leq \varepsilon$ for all $x, x' \in \{0, 1\}^\ell$.
- **$\gamma$-binding:** For any $x \in \{0, 1\}^\ell$ and for any malicious sender that is honest in the commit phase on input $x$ and tries to open $x' \neq x$, we have $\Pr[F(x', V, M, N') = 1] \leq \gamma$, where $N'$ is the communication between the malicious sender and the honest receiver in the open phase.

Note that the above security conditions are not sufficient to prove the security of a protocol [1] but any sensible security definition for commitments implies these conditions. Since we only use the definition to prove the non-existence of certain protocols, this makes our result stronger.

## 4.3 Lower Bound for Multiple Bit Commitments

In the following we prove a lower bound on the mutual information between the randomness of the sender and the randomness of the receiver in any bit commitment protocol. First, we show the following technical lemma.

**Lemma 4.1.** If a protocol that implements bit commitment from distributed randomness $(U, V)$ is $\gamma$-binding, $\beta$-correct and $\varepsilon$-hiding, then for $x \in \{0, 1\}$

$$d_{KL}(1 - \beta || \gamma + \varepsilon) \leq \sum_{i=1}^{t} I(D_i; V | M D^{i-1} E^{i-1}, X = x). \quad (4.3.1)$$

**Proof.** Let $x \in \{0, 1\}$ and $\bar{x} := 1 - x$. Assume that the sender in the commit phase honestly commits to $x$. If she honestly opens $x$ in the open phase, the communication can be modeled by a conditional distribution $P_{DE|VM}$ (that may depend on $x$) and the resulting distribution is

$$P_{DEV M|X=x} = P_{DE|VM} P_{VM|X=x},$$

---

1To prove the security of a protocol one had to consider for example a malicious sender in the commit phase.
We have omitted $U$ as it is not needed in the following arguments. The correctness property implies that an honest receiver accepts values drawn from this distribution with probability at least $1 - \beta$. Let the sender commit to $\bar{x}$ and then try to open $x$ by sampling her messages according to the distributions $P_{D_1|M}$ and $P_{D_i|MD_{i-1}E_{i-1}}$ for $2 \leq i \leq t$. (Note that the sender does not know $V$ and, therefore, chooses her messages independently of $V$.) The communication in the opening phase can be modeled by a conditional distribution

$$Q_{DE|VM} := P_{D_1|M}P_{E_1|VM}D_1 \cdots P_{D_t|MD_{t-1}E_{t-1}}.$$  

The binding property implies that the receiver accepts values distributed according to $P_{VM|X=\bar{x}}Q_{DE|VM}$ with probability at most $\gamma$. The hiding property, $D(P_{VM|X=x}, P_{VM|X=\bar{x}}) \leq \varepsilon$, implies that

$$D(P_{VM|X=x}Q_{DE|VM}, P_{VM|X=\bar{x}}Q_{DE|VM}) \leq \varepsilon,$$

and hence values drawn from the distribution $P_{VM|X=x}Q_{DE|VM}$ are accepted with probability at most $\gamma + \varepsilon$. Note that the bit indicating acceptance can also be modeled by a conditional distribution $P_{F|DEVM}$. Thus, we can apply the data-processing inequality (2.1.7) to bound $d_{KL}(1 - \beta | \gamma + \beta)$. Using the chain rule (2.1.5) and the non-negativity of the relative entropy, we have (we omit conditioning on $X = x$ in the following)

$$d_{KL}(1 - \beta | \gamma + \varepsilon) \leq D_{KL}(P_{VM}P_{DE|VM} || P_{VM}Q_{DE|VM})$$

$$= D_{KL}(P_{DE|VM} || Q_{DE|VM})$$

$$= \sum_{i=1}^{t} D_{KL}(P_{D_i|VMD_{i-1}E_{i-1}} || P_{D_i|MD_{i-1}E_{i-1}})$$

$$+ \sum_{i=1}^{t-1} D_{KL}(P_{E_i|VMD_{i}E_{i-1}} || P_{E_i|VMD_{i}E_{i-1}})$$

$$= \sum_{i=1}^{t} D_{KL}(P_{D_i|VMD_{i-1}E_{i-1}} || P_{D_i|MD_{i-1}E_{i-1}})$$

$$= \sum_{i=1}^{t} I(D_i; V|MD_{i-1}E_{i-1}).$$

The next lemma, which we will use to bound the right-hand side of the inequality in (4.3.1), is an implication of Theorem 2.1 in [OW05].
Lemma 4.2. Let $\varepsilon = \beta = \gamma = 2^{-\kappa}$. Then, for $\kappa \geq 3$, we have

$$d_{KL}(1 - \beta || \gamma + \varepsilon) \geq (\kappa - 2) \cdot \frac{2^{\kappa - 2} - 2}{2^{\kappa - 2} - 1}.$$ 

Proof. Theorem 2.1 in [OW05] implies, for all $a, b$,

$$d_{KL}(a || b) \geq \frac{(a - b)^2}{1 - 2b} \log \frac{1 - b}{b}. \quad (4.3.2)$$

Then, for $\kappa \geq 3$, we have

$$d_{KL}(1 - \beta || \gamma + \varepsilon) = \frac{(1 - 3 \cdot 2^{-\kappa})^2}{1 - 2^{-\kappa + 2}} \log(2^{\kappa - 1} - 1)$$

$$\geq (\kappa - 2) \cdot \frac{1 - 2^{-\kappa + 3}}{1 - 2^{-\kappa + 2}}$$

$$\geq (\kappa - 2) \cdot \frac{2^{\kappa - 2} - 2}{2^{\kappa - 2} - 1}.$$ 

The following lemma generalizes the lower bounds on the size of the randomness from [NOIMQ03], which have only been shown for perfectly correct and perfectly hiding non-interactive schemes, to arbitrary protocols. Additionally, it also provides a more powerful result, namely a lower bound on the information that the communication in the open phase must reveal about the receiver’s randomness $V$ for any protocol that implements bit commitment from a shared distribution $P_{UV}$. The lower bound is essentially $\kappa$ if the error of the protocol is at most $2^{-\kappa}$. This stronger statement will allow us in the following to prove that there exist no constant rate reductions of bit commitment to distributed randomness, which is the main result of this section.

Lemma 4.3. Let $\kappa \geq 3$. Then any $2^{-\kappa}$-secure bit commitment must satisfy for $x \in \{0, 1\}$

$$I(N; V|M, X = x) - I(N; V|UM, X = x)$$

$$= I(U; V|M, X = x) - I(U; V|MN, X = x) \geq (\kappa - 2) \cdot \frac{2^{\kappa - 2} - 2}{2^{\kappa - 2} - 1}.$$ 

Proof. Again, we omit conditioning on $X = x$ in the following. Consider a protocol over $t$ rounds in the open phase, i.e., the whole communication
is $N = (D, E) = (D_1, E_1, \ldots, D_t)$. Since $D_i \leftrightarrow U M D^{i-1} E^{i-1} \leftrightarrow V$, we have $I(D_i; V|U M D^{i-1} E^{i-1}) = 0$. Hence,

$$I(NU; V|M) = I(U; V|M) + \sum_{i=1}^{t-1} I(E_i; V|U M D^i E^{i-1}) .$$

Furthermore, from $E_i \leftrightarrow V M D^i E^{i-1} \leftrightarrow U$ and inequality (2.1.10) follows that for all $i$

$$I(E_i; V|MD^i E^{i-1}) \geq I(E_i; V|UM D^i E^{i-1}) .$$

Hence, we have

$$I(N; V|M) = \sum_i I(E_i; V|MD^i E^{i-1}) + \sum_i I(D_i; V|MD^{i-1} E^{i-1})$$

$$\geq \sum_i I(E_i; V|UM D^i E^{i-1}) + \sum_i I(D_i; V|MD^{i-1} E^{i-1})$$

and

$$I(U; V|MN) = I(NU; V|M) - I(N; V|M)$$

$$= I(U; V|M) + \sum_i I(E_i; V|UM D^i E^{i-1}) - I(N; V|M)$$

$$\leq I(U; V|M) - \sum_i I(D_i; V|MD^{i-1} E^{i-1}) .$$

The statement now follows from Lemma 4.1 and Lemma 4.2.

Next, we consider implementations of $n$ individual bit commitments. The sender gets input $x^n = (x_1, \ldots, x_n)$ and commits to all bits at the same time, which results in the overall distribution

$$P_{UVM|X^n=x^n} = P_{UV} P_{M|UV, X^n=x^n} .$$

after the commit phase. To reveal the $i$-th bit, the sender and the receiver interact resulting in the transcript $N_i$. The following theorem says that the mutual information between the sender’s randomness $U$ and the receiver’s randomness $V$ must be almost $\kappa n$ to implement $n$ bit commitments with an error of at most $2^{-\kappa}$. The proof uses Lemma 4.3 to show a lower bound on the information that the sender must reveal about $V$ for every bit that he opens.
Theorem 4.1. Let $\kappa \geq 3$. Then any $2^{-\kappa}$-secure protocol that implements $n$ bit commitments from randomness $(U, V)$ must satisfy, for all $x^n \in \{0,1\}^n$,

$$I(U; V) \geq I(U; V| M, X^n = x^n) \geq n(\kappa - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1}.$$

for all $x^n \in \{0,1\}^n$.

Proof. Let $i \in [n]$. We first construct a commitment to a single bit, which will allow us to apply the bound from Lemma 4.3. This bit commitment scheme is defined as follows: If additiono commit to the bit $x$, the players execute the commit phase on input $x^n$, which is equal to the input bit $x$ on position $i$ and equal to the constant $\hat{x}^n \in \{0,1\}^n$ on all other positions. Additionally - still as part of the commit phase - the sender opens the first $i - 1$ commitments, which means that the messages $N^{i-1}$ get exchanged. To open the commitment, the sender opens bit $i$. This bit commitment scheme has at least the same security as the original commitment. Thus, Lemma 4.3 implies that (we omit conditioning on $X^n = \hat{x}^n$ in the following)

$$I(U; V| MN^i) \leq I(U; V| MN^{i-1}) - (\kappa - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1}. \quad (4.3.3)$$

Since this holds for all $i$, we can apply (4.3.3) repeatedly to get

$$
0 \leq I(U; V| MN^n) \\
\leq I(U; V| MN^{n-1}) - (\kappa - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1} \\
\leq I(U; V| M) - n(\kappa - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1}.
$$

By induction over all rounds of the commit protocol using (2.1.10) (see, for example, [WW10] for a detailed proof) it follows that

$$I(U; V | M) \leq I(U; V).$$

From Section 3.2 we know that it is possible to securely implement $(\frac{2}{1})$-OT$^1$ from randomness distributed according to $P_{UV}$ with $I(U; V) = 1$ and a binary symmetric noisy channel ($(p)$-BNC) with crossover probability $p$ can be implemented from randomness distributed according to $P_{UV}$. 

\[\square\]
with $I(U; V) = 1 - h(p)$. Together with these reductions, Theorem 4.1 implies that (almost) $\kappa n$ instances of $(\frac{2}{1})$-OT$^1$ or $\kappa n/(1 - h(p))$ instances of a $(p)$-BNC are needed to implement $n$ bit commitments with an error of at most $2^{-\kappa}$.

There exists a universally composable protocol\(^2\) that implements bit commitment from $2\kappa$ instances of $(\frac{2}{1})$-OT$^1$ with an error of at most $2^{-\kappa}$. Thus, $n$ bit commitments can be implemented from $2n(\kappa + \log(n))$ instances of $(\frac{2}{1})$-OT$^1$ with an error of at most $n \cdot 2^{-(\kappa + \log(n))} = 2^{-\kappa}$ using $n$ instances of this protocol in parallel. Theorem 4.1 shows that this is optimal up to a factor of 4 if $\kappa \geq \log(n)$. If one directly implements a multi-session functionality for $n$ bit commitments, it is easy to show that one can implement $n$ bit commitments from $2n\kappa$ instances of $(\frac{2}{1})$-OT$^\kappa$ with an error of at most $2^{-\kappa}$. This is optimal up to a factor 2 with respect to Theorem 4.1. Note that the factor 2 is due to the fact that we only consider honest senders. Given $n$ instances of $(\frac{2}{1})$-OT$^\kappa$, there is a protocol that implements $n$ bit commitments with an error of $2^{-\kappa}$ (see for example [WW08a, BFSK11]), where the receiver in the commitment protocol takes the role of Alice in all instances of $(\frac{2}{1})$-OT$^\kappa$. This is optimal according to Theorem 4.1. There is a protocol that implements a perfectly correct, perfectly hiding and $\frac{1}{q}$-binding commitment from one instance of (fully randomized) $(q)$-OLFE [Riv99]. The construction can easily be shown to be universally composable and can be used to implement $n$ bit commitments from $n$ instances of $(q)$-OLFE with an error of at most $\frac{1}{q}$. This is optimal according to Theorem 4.1.

### 4.4 Lower Bounds for Multiple String Commitments

In [WN103] a lower bound on the conditional entropy of the sender’s randomness $U$ given the receiver’s randomness $V$ for any string commitment protocol from randomness $(U, V)$ has been shown. This bound essentially says that $H(U|V)$ must be greater than or equal to $\ell$ to implement a string commitment of length $\ell$. The following lemma provides a similar bound for the security definition considered here.

**Lemma 4.4.** If any protocol implements an $\ell$-bit string commitment from ran-

---

\(^2\)See for example Claim 33 in the full version of [Can01].
**4.4. Lower Bounds for Multiple String Commitments**

Domness \((U, V)\) is \(\beta\)-correct, \(\varepsilon\)-hiding and \(\gamma\)-binding, then

\[
H(U|V) \geq (1 - \varepsilon - \beta - \gamma)\ell - h(\varepsilon) - h(\beta + \gamma).
\]

**Proof.** Let the sender commit to a uniform string \(X\). The hiding property implies that \(X\) is \(\beta\)-close to uniform with respect to the receiver’s view and, therefore, we can apply Lemma 2.1 to obtain

\[
H(X|VM) \geq (1 - \varepsilon)\ell - h(\varepsilon),
\]

where \(M\) is the whole communication in the commit phase. We consider the following cheating attempt by the sender: She chooses a string \(X\) uniformly at random and honestly commits to \(X\). After the commit phase, she chooses \(\hat{X}\) which maximizes the probability conditioned on \(U = u\) and \(M = m\) that the receiver accepts in the open phase and tries to open \(\hat{X}\). (Note that \(\hat{X}\) is a function of \(U\) and \(M\).) Then \(\hat{X}\) is accepted with probability at least \(1 - \varepsilon\), because \(X\) is accepted with probability at least \(1 - \varepsilon\). Since the protocol is \(\gamma\)-binding, it follows that \(\hat{X}\) must be equal to \(X\) with probability at least \(1 - \gamma - \varepsilon\) (otherwise the sender could find a \(X'\) that is always different from \(X\) and still accepted with probability strictly larger than \(\gamma\)). Together with Lemma 2.1 this implies

\[
H(X|UMV) \leq H(X|UM) \leq (\beta + \gamma)\ell - h(\beta + \gamma).
\]

(4.4.2)

Using monotonicity, the chain rule and inequalities (4.4.1) and (4.4.2), we get

\[
H(U|V) \geq H(U|VM) \\
\geq H(X|VM) - H(X|UVM) \\
\geq (1 - \varepsilon - \beta - \gamma)\ell - h(\varepsilon) - h(\beta + \gamma).
\]

(4.4.3)

Using a very similar proof, we obtain a lower bound on the smooth conditional min-entropy of the distributed randomness.

**Lemma 4.5.** If any protocol implements an \(\ell\)-bit string commitment from randomness \((U, V)\) is \(\beta\)-correct, \(\varepsilon\)-hiding and \(\gamma\)-binding, then

\[
H^\varepsilon+\delta+\gamma(U|V) \geq \ell.
\]
Proof. Using the proof of Lemma 4.4, the hiding property implies that
\[ H_{\infty}^{\beta}(X|VM) \geq \ell, \]
and, using Lemma 2.6, the binding property implies that
\[ H_{0}^{\beta+\gamma}(X|UMV) \leq H_{0}^{\beta+\gamma}(X|UM) \leq 0. \]
Using Lemma 2.5, the statement follows. 

Together with the bound of Theorem 4.1, we obtain the following lower bound on the randomness of the sender in any bit commitment protocol.

**Corollary 4.1.** Let \( \kappa \geq 3 \). For any protocol that implements \( n \) individual \( \ell \)-bit string commitments from randomness \((U, V)\) with an error of at most \( 2^{-\kappa} \)
\[ H(U) \geq n(\kappa + \ell - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1} - 3 \cdot 2^{-\kappa} \cdot n\ell - 3h(2^{-\kappa}). \]

**Proof.** Using Lemma 4.4 and Theorem 4.1 we get
\[ H(U) = I(U; V) + H(U|V) \]
\[ \geq n(\kappa - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1} + (1 - 3 \cdot 2^{-\kappa})n\ell - h(2^{-\kappa}) - h(2^{-\kappa + 1}) \]
\[ \geq n(\kappa + \ell - 2) \cdot \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1} - 3 \cdot 2^{-\kappa} \cdot n\ell - 3h(2^{-\kappa}). \]

In [BMSW02] it has been shown that any non-interactive perfectly hiding and perfectly correct bit commitment protocol from distributed randomness \( P_{UV} \) is at most \( (2^{-H(V|U)}) \)-binding. This result implies stronger bounds than Theorem 4.1 and Lemma 4.4 for certain reductions. The following lemma provides a lower bound on the uncertainty of the sender about the receiver’s randomness for any bit commitment protocol. This lower bound is essentially equal to \( \kappa \) if the protocol is \( 2^{-\kappa} \)-secure and implies, in particular, the result from [BMSW02].

**Lemma 4.6.** If a protocol that implements bit commitment from randomness \((U, V)\) is \( \gamma \)-binding, \( \beta \)-correct and \( \varepsilon \)-hiding, then
\[ d_{KL}(1 - \beta - \varepsilon||\gamma) \leq H(V|UM) \leq H(V|U). \]
where $M$ is the whole communication in the commit phase. If $\beta = \gamma = \varepsilon = 2^{-\kappa}$, then

$$H(V|U) \geq (\kappa - 1) \cdot \frac{2^{\kappa - 1} - 4}{2^{\kappa - 1} - 1}. \quad (4.4.3)$$

Proof. We have $D(P_{V \mid X=x}, P_{V \mid X=x}) \leq \beta$. This implies that the distribution $P_{U \mid V \mid X=x} P_{V \mid X=x}$ is $\beta$-close to $P_{UV \mid X=x}$. Thus, when the sender honestly opens $\bar{x}$ starting from values distributed according to $P_{U \mid V \mid X=x} P_{V \mid X=x}$, the receiver accepts the resulting values with probability at least $1 - \beta - \varepsilon$. We consider the following attack: the sender honestly commits to $x$, generates $v'$ by applying $P_{V \mid U \mid X=x}$ and then generates $u$ by applying the channel $P_{U \mid V \mid X=x}$ to $(v', m)$. When the sender now tries to open $\bar{x}$, the binding property guarantees that the receiver accepts the resulting values with probability at most $\gamma$. Thus, we can apply the data-processing inequality (2.1.7) to bound $d_{KL}(1 - \beta - \varepsilon || \gamma)$. Let $V'$ be a copy of $V$, i.e., a random variable with distribution $P_{V' \mid V}(v, v) = P_{V}(v)$. Using the chain rule (2.1.6), we have (we omit conditioning on $X = x$ in the following)

$$d_{KL}(1 - \beta - \varepsilon || \gamma) \leq D_{KL}(P_{VV' \mid UM} P_{UM} || P_{V \mid UM} P_{V \mid UM} P_{UM})$$
$$\leq D_{KL}(P_{VV' \mid UM} || P_{V \mid UM} P_{V \mid UM})$$
$$= H(V|UM)$$
$$\leq H(V|U).$$

If $\beta = \gamma = \varepsilon = 2^{-\kappa}$, then we use (4.3.2) to obtain

$$d_{KL}(1 - \beta - \varepsilon || \gamma) \geq \frac{(1 - 3 \cdot 2^{-\kappa})^2}{1 - 2^{-\kappa + 1}} \log(2\kappa - 1)$$
$$\geq (\kappa - 1) \frac{1 - 6 \cdot 2^{-\kappa}}{1 - 2^{-\kappa + 1}}$$
$$\geq (\kappa - 1) \frac{2^{\kappa - 1} - 4}{2^{\kappa - 1} - 1}. \quad \Box$$

Consider a protocol that implements $n$ bit commitment with security of $2^{-\kappa}$ from $n'$ instances of $\binom{2}{1}$-OT$^k$. Since $\binom{2}{1}$-OT$^k$ can be reduced to a primitive $P_{UV}$ with $H(V|U) = 1$ (cf. Section 3.2), Lemma 4.6 implies that $n' \geq (\kappa - 1) \cdot \frac{2^{\kappa - 1} - 4}{2^{\kappa - 1} - 1}$. This means that almost $\kappa$ instances of $\binom{2}{1}$-OT$^k$ are needed, independently of $k$. 
Together with Theorem 4.1 and Lemma 4.5, this implies the following lower bound on the number of instances of OT needed to implement multiple string commitments, which demonstrates that all three lower bounds can be meaningful in this scenario.

**Corollary 4.2.** Let $\kappa \geq 3$. For any protocol that implements $n$ individual $\ell$-bit string commitments with an error of at most $2^{-\kappa}$ from $n'$ instances of $\binom{n}{1}$-OT$^k$

$$n' \geq \max \left( \frac{\ell n - 6 \cdot 2^{-\kappa}}{k}, \frac{\kappa - 2}{k}, \frac{2^{\kappa-2} - 2}{2^{\kappa-2} - 1}, \frac{2^\kappa - 1 - 4}{2^\kappa - 1 - 1} \right).$$

In Section 5.2.4, we will show that Lemma 4.6 also applies to quantum protocols.

### 4.5 Concluding Remarks

In this chapter, we have shown a strong lower bound for reductions of multiple bit commitments to other information theoretic primitives, such as oblivious transfer or noisy channels. Our bound shows that every single bit commitment needs at least $\Omega(\kappa)$ instances of the underlying primitive if the error is at most $2^{-\kappa}$. This makes bit commitments often much more costly to implement than oblivious transfer. It would be interesting to see whether a similar result can be shown for quantum protocols that can use oblivious transfer, noisy correlations or a noisy channel.
Chapter 5

Quantum Commitment and Oblivious Transfer Reductions

In quantum key distribution [BB84, Eke91], two honest parties try to expand a shared secret key using insecure quantum communication. It is often neglected that an initial secret key is a necessary precondition for this to be possible. However, it is easy to see that without such a key, which can be used to authenticate the communication, it is impossible for Alice to distinguish between Bob and an eavesdropper pretending to be Bob. Even though it is thus impossible to share an initial secret key using insecure quantum communication, such a key can be expanded arbitrarily using the same resource (see, for example, [MQR09]). Similarly, there is no information-theoretically secure two-party protocol that generates a fair random coin which cannot be biased by a dishonest player [Blu83]. If the players have access to a certain number of ideal coin tosses to start with, however, there are protocols implementing a larger number of coin tosses which are secure in the standalone model [HMQU06]. In this chapter, we consider the task of extending commitments and oblivious transfer using quantum communication. More generally, we study the efficiency of quantum protocols that try to implement a string commitment or a $\binom{2}{1}$-OT$^k$ from a certain number of black-box commitments or from trusted distributed randomness. The latter scenario allows us in particular to consider quantum protocols that can use a certain number of OTs as black-boxes.
Chapter 5. Quantum Commitment and OT Reductions

Previous Results

In the quantum setting almost all known negative results show that a certain primitive is impossible to implement from scratch. Commitment has been shown to be impossible in the quantum setting in [May97, LC97] (see also [DKSW06]). Using a similar proof, it has been shown in [Lo97] that general one-sided two-party computation and, in particular, oblivious transfer are also impossible to implement securely in the quantum setting. These results have been generalized in [Col06, Col07, KMQR, SSS09]. Conversely, it has been shown that secure commitments can be implemented in relativistic settings, which involve multiple sites [Ken11]. Bounds on the quality of commitments, which are only partially secure, [SR01] for bit commitments and in [BCH+08] for string commitments. Non-trivial protocols for string commitment are possible for weak security definitions [BCH+08].

Contributions

In this chapter, we will first show that commitments cannot be extended using quantum protocols, i.e., there is no statistically secure quantum protocol that uses a certain number of ideal bit commitments and implements a commitment to a larger string (Theorem 5.1). Furthermore, we present a generalization of this impossibility result for a functionality that allows to commit to qubits (Theorem 5.2) and bounds for implementations of commitments from noisy correlations (Theorems 5.3 and 5.4). Then we present a statistically secure protocol that violates the known impossibility results for perfectly secure implementations of $\binom{2}{1} \cdot \text{OT}^k$ from trusted distributed randomness (Theorem 5.5). This implies that, in contrast to the classical case, the impossibility results for perfectly secure implementations of $\binom{2}{1} \cdot \text{OT}^k$ cannot be extended to the statistical case. We then present a weaker lower bound that does hold in the statistical quantum setting (Theorem 5.7). We use this bound to show that even quantum protocols cannot extend OT. Furthermore, we provide lower bounds on the number of instances of commitments and on the total number of committed bits that are needed to securely realize OT with quantum protocols (Theorems 5.6 and 5.8). Finally, we present a protocol that implements OT from string commitments (Theorem 5.9) and is essentially optimal with respect to the lower bounds of Theorems 5.6 and 5.8.

The results in Sections 5.2.2 and 5.2.3 are joint work with Stefan Hengl, Marco Tomamichel and Renato Renner and have previously been pub-
lished in [WTHR11]. The results in Sections 5.3 and 5.4 are based on joint work with Jürg Wullschleger and have partly been published in [WW10].

5.1 Model

We assume that the two parties, Alice (who holds system $A$) and Bob ($B$), have access to a noiseless quantum and a noiseless classical channel. The protocol proceeds in rounds, where in any round the parties may perform an arbitrary quantum operation on the system in their possession. This operation can be conditioned on the available classical information and generates the inputs to the communication channels. The quantum channel transfers a part of one party’s system to the other party. The classical channel measures the input in a canonical basis and sends the outcome of the measurement to other party. We assume that the total number of rounds of the protocol is bounded by a finite number. Since we can always introduce empty rounds, this corresponds to the assumption that the number of rounds is equal in every execution of the protocol. All quantum operations of both parties can be purified by introducing an additional memory space (cf. Section 2.7). Thus, we can assume that the parties apply in every round of the protocol a unitary to their system conditioned on the information shared over the classical channel. In particular, we can assume that the system remains in a pure state conditioned on the information shared over the classical channel if the initial state of the protocol is pure.

5.2 Impossibility of Extending Quantum Commitments

5.2.1 Security Definition

The main result of this section will be a quantitative statement on the impossibility of growing string commitments. To formulate this statement, we introduce two definitions that capture the cheating probability of Alice and the information gain of Bob, respectively. We emphasize that the properties required in these definitions are only necessary, but would not be sufficient for the security of a protocol. In particular, one would have to consider arbitrary malicious strategies of dishonest parties to prove the

\[^1\text{This assumption is not justified in the relativistic setting considered in [Ken11].}\]
Chapter 5. Quantum Commitment and OT Reductions

security of a protocol (see, for example, [DFR+06, KWW09] for complete security definitions for quantum commitment protocols). Therefore, we call the definitions weak. Since we are interested in the impossibility of certain protocols, this only strengthens our results.

Using a commitment protocol, a (quantum) Alice can always commit to a superposition of strings [May97, DMS] as follows: she prepares a state \( \frac{1}{\sqrt{|X|}} \sum_{x \in X} |x \rangle_X \otimes |x \rangle_X \otimes |x \rangle_X', \) where \( X \) is a subset of the \( \ell \)-bit strings. Then she honestly executes the commit protocol using system \( X \) as her input and keeps the system \( X' \). We denote the resulting joint state of Alice, Bob and the additional resource system by \( \rho_{X,A'BC} \), where \( A' \) stands for \( XX' \). Later, Alice can measure \( X' \) and execute the opening phase of the protocol with the resulting string \( x \). Thus, even for a perfectly binding commitment scheme, we cannot require that Alice is committed to a fixed value \( x \) after the commit phase. Rather, we can only demand that \( \sum_{x \in \{0,1\}^n} p_x \leq 1 \) where \( p_x \) is the probability that Alice successfully reveals some \( x \) in the opening phase.

In order to quantify the degree of bindingness of a protocol, we consider the following attack by Alice. First, she commits to a superposition of strings from a set \( X_0 \subseteq \{0,1\}^\ell \) as before. Then, she tries to map (by a local transformation \( \mathcal{E}_{A'} \) on her system) the resulting state \( \rho_{X_0,A'BC} \) to \( \rho_{X_1,A'BC} \), corresponding to the commitment to a set \( X_1 \subseteq \{0,1\}^\ell \) which is disjoint from \( X_0 \). Such an attack is successful with probability at least \( \Delta \) if the transformed state \( (\mathcal{E}_{A'} \otimes 1_{BC})(\rho_{X_0,A'BC}) \) is \( (1 - \Delta) \)-close to the target state \( \rho_{X_1,A'BC} \). This means that there is no protocol that can detect the transformation with probability more than \( 1 - \Delta \).

**Definition 5.1 (Weakly \( \Delta \)-binding).** We call a commitment scheme weakly \( \Delta \)-binding if

\[
\min_{X_0, X_1} \min_{\mathcal{E}_{A'}} D \left( (\mathcal{E}_{A'} \otimes 1_{BC})(\rho_{X_0,A'BC}), \rho_{X_1,A'BC} \right) \geq 1 - \Delta ,
\]

where \( X_0 \) and \( X_1 \) are disjoint sets of strings from \( \{0,1\}^\ell \) and \( \mathcal{E}_{A'} \) is a completely positive, trace preserving map acting on Alice’s system.

To define the hiding property, we consider the joint state \( \rho_{A'BC} \) of Alice’s and Bob’s systems that results from an execution of the protocol where both parties are honest and Alice commits to \( x \). For a commitment scheme to be \( \varepsilon \)-hiding, we require that \( D(\rho_{A'B}, \rho_{A'B}') \leq \varepsilon \) for any \( x, x' \). This immediately implies the following (necessary) security condition.
5.2. Impossibility of Extending Quantum Commitments

**Definition 5.2** (Weakly $\varepsilon$-hiding). A commitment scheme is weakly $\varepsilon$-hiding for uniform $X \in \{0, 1\}^\ell$ if the marginal state $\rho_{XB}$ after the commit phase is $\varepsilon$-close to a state where $X$ is uniform with respect to $B$, i.e.,

$$
\min_{\sigma_B} D(\rho_{XB} : \pi_{\{0,1\}^\ell} \otimes \sigma_B) \leq \varepsilon ,
$$

(5.2.1)

where the minimum is taken over all $\sigma_B \in \mathcal{S} = (\mathcal{H}_B)$.

5.2.2 (Classical) Bit Commitments

One can trivially implement a string commitment of length $n$ from $n$ bit commitments. Furthermore, it is easy to see that, using a functionality which allows the players to commit to $n$ qubits, one can implement $n$ individual commitments to two bits each using superdense coding [BW92], and, therefore, also a string commitment of length $2n$. In the following we present two different impossibility results for implementations of string commitments, which are essentially optimal in these two cases.

First, we consider implementations of string commitments that use $n$ black-box bit commitments. We show that the length of the implemented string commitment is essentially bounded by $n$ if the protocol has to be arbitrarily binding and hiding.

**Theorem 5.1.** Every quantum protocol which uses $n_A$ bit commitments from Alice to Bob and $n_B$ bit commitments from Bob to Alice (as a black-box), where $n = n_A + n_B$, and implements an $\varepsilon$-hiding and $\Delta$-binding string commitment of length $\ell$ must satisfy

$$
\ell \leq n - 2 \log \left( \frac{(1 - \Delta)^2}{4} - \sqrt{2\varepsilon} \right) - 1 .
$$

In particular, if $\Delta = \varepsilon \leq 0.01$, then $\ell < n + 6$.

**Proof.** Let $|x\rangle\langle x| \otimes \rho_{AB}^x$ be the state resulting from the execution of an $\varepsilon$-hiding commitment protocol when the input of Alice is $x$. Then $\rho_{XABC} = \sum_x \frac{1}{2^\ell} |x\rangle\langle x| \otimes \rho_{AB}^x$ is the state resulting from an execution where the committed string $X$ is uniformly distributed. Let $\varepsilon := \sqrt{2\varepsilon}$. Since $\rho_{XB}$ is $\varepsilon$-close to uniform, i.e., there exists a $\sigma_B$ such that

$$
D(\rho_{XB} : \pi_{\{0,1\}^\ell} \otimes \sigma_B) \leq \varepsilon ,
$$

we can use (2.7.16) to bound the purified distance

$$
P(\rho_{XB} : \pi_{\{0,1\}^\ell} \otimes \sigma_B) \leq \tilde{\varepsilon} .
$$
The definition of the smooth min-entropy then implies that
\[ H_{\min}^\varepsilon(X|B)_\rho \geq \log |X| = \ell. \] (5.2.2)

In the following, we consider a modified protocol that does not use the given bit commitment functionality. In this modified protocol Alice, instead of using the bit commitment functionality, measures the bits to be committed, stores a copy of each and sends them to Bob, who stores them in a classical register \( C_A \). When one of these commitments is opened, he moves the corresponding bit to his register \( B \). Bob simulates the action of his commitments locally as follows: instead of measuring a register, \( Y \), and sending the outcome to the commitment functionality, he applies the isometry \( U : |y\rangle_Y \mapsto |yy\rangle_{YY} \), purifying the measurement of the committed bit and stores \( Y' \) in register \( C_B \). When Bob has to open the commitment, he measures \( Y' \) and sends the outcome to Alice over the classical channel. Note that we make Bob more powerful in this modified protocol because he can simulate the original protocol locally. Thus, any successful attack of Alice against the modified protocol implies a successful attack against the original protocol. Since we only make use of the modified protocol to construct an attack against Bob, the modified protocol does not have to be hiding. Furthermore, the state conditioned on the classical communication is again pure.

Let \( \rho_{XABC} = \sum_x \frac{1}{2^\ell} |x\rangle\langle x| \otimes \rho_{xABC} \), where \( C \) stands for \( C_A, C_B \), be the state resulting from the execution of the modified protocol when the input \( X \) of Alice is uniformly distributed. Its marginal state, \( \rho_{XAB} \), is the corresponding state at the end of the commit phase of the original commitment protocol. Lemma 2.29 guarantees that there exists a function \( f : \{0, 1\}^\ell \to \{0, 1\} \) such that
\[ D(\rho_{B0C}, \rho_{B1C}) \leq 2\delta, \]
where \( \rho_{B0C} = \frac{1}{2^\ell-1} \sum_{x \in f^{-1}(0)} \rho_{BC} \) and \( \delta := \varepsilon + \frac{1}{2} \sqrt{2^{1-H_{\min}^\varepsilon(X|BC)_\rho}} \). Let \( z \in \{0, 1\} \). We let Alice prepare the state
\[ \sum_{x \in f^{-1}(z)} \frac{1}{\sqrt{2^{\ell-1}}} |x\rangle_X \otimes |x\rangle_{X'}, \]
and honestly execute the commit protocol using the first half of this state as her input. We consider the resulting state, \( \rho_{\hat{A}BCAC_B} = \rho_{XX'ABCAC_B} \), at the end of the commit phase. Since this state is pure conditioned on all
5.2. Impossibility of Extending Quantum Commitments

the shared classical information, Lemma 2.21 guarantees the existence of a unitary $U_A$ such that

$$D(\tilde{\rho}_{X_1 \cdots z}^{A'BC_A C_B}, \rho_{X_1 \cdots z}^{A'BC_A C_B}) \leq 2\sqrt{\delta},$$  \hspace{1cm} (5.2.3)$$

where $\tilde{\rho}_{A'BC_A C_B}^{X_1 \cdots z} = (U_{A'} \otimes 1_B)\rho_{A'BC_A C_B}^{X_1 \cdots z}(U_{A'} \otimes 1_B)$. We can apply Lemmas 2.24 and 2.25 to derive the following lower bound on the smooth min-entropy:

$$H_{\tilde{\epsilon}}^{\min}(X|BC A C) \rho \geq H_{\epsilon}^{\min}(X|BC) \rho - n_A$$

$$\geq H_{\epsilon}^{\min}(X|B) \rho - n$$

$$\geq \ell - n.$$  \hspace{1cm} (5.2.4)

Thus, we obtain

$$1 - \Delta \leq 2\sqrt{\delta} = 2\sqrt{\tilde{\epsilon} + \frac{1}{2}\sqrt{2^{1 - H_{\min}(X|BC A C_B) \rho}}}$$

$$\leq 2\sqrt{\tilde{\epsilon} + \frac{1}{2}\sqrt{2^{1 - \ell + n}}}$$

$$\leq 2\sqrt{\sqrt{2\tilde{\epsilon} + 2^{-\frac{1}{2}(\ell-n+1)}},}$$

where we used the definition of weakly $\Delta$-binding and inequalities (5.2.3) and (5.2.4).

The upper bound on the length of the implemented string commitment is equal to $n + 3$ for perfect implementations (with $\epsilon = \Delta = 0$), i.e., we cannot exclude protocols that extend commitments by 3 bits. However, if we assume that the protocol is composable, we can apply the protocol iteratively as follows: Given a composable protocol that implements a string commitment of length $n + 1$ from $n$ bit commitments with $\epsilon = \Delta$, we can apply the protocol 6 times to implement a string commitment of length $n + 6$ from $n$ bit commitments with an error $\epsilon' = \Delta' = 6\epsilon$. Theorem 5.1 then implies that $\epsilon' = \Delta' \geq 0.01$. Thus, we obtain the lower bound $\epsilon = \Delta \geq 1/600$.

5.2.3 Quantum Commitments

Next, we consider implementations of string commitments from a quantum commitment functionality. A quantum commitment functionality takes a qubit state $\rho$ and the message commit from the first party, the
sender, and sends the message committed to the other party, the receiver. When the sender gives the input open to the functionality, it transfers the state $\rho$ to the receiver. The following theorem shows that it is impossible to implement an arbitrarily hiding and binding string commitment of length larger than $2n$ from such a quantum commitment functionality that allows to commit to $n$ qubits.

**Theorem 5.2.** Every quantum protocol that has only access to a functionality that allows the players to commit to (and later reveal) $n$ qubit states and implements an $\varepsilon$-hiding and $\Delta$-binding string commitment of length $\ell$, must satisfy

$$\ell \leq 2n - 2\log \left( \frac{(1 - \Delta)^2}{4} - \sqrt{2\varepsilon} \right) - 1.$$  

(5.2.5)

In particular, if $\Delta = \varepsilon \leq 0.01$, then $\ell < 2n + 6$.

**Proof.** Let $|x\rangle \langle x| \otimes \rho^x_{ABC}$ be the state resulting from the execution of an $\varepsilon$-hiding commitment protocol when the input of Alice is $x$. Then $\rho^x_{ABC} = \sum_x \frac{1}{2^n} |x\rangle \langle x| \otimes \rho^x_{ABC}$ is the state resulting from an execution where the committed string $X$ is uniformly distributed. Let $\tilde{\varepsilon} := \sqrt{2\varepsilon}$. From the security definition, we know that $\rho_{XB}$ is $\varepsilon$-close to uniform. As in the proof of Theorem (5.1), the definition of the smooth min-entropy and inequality (2.7.16) imply

$$H^\tilde{\varepsilon}_{\text{min}}(X|B) \geq \log |X| = \ell.$$  

We consider again a modified protocol, where Bob simulates the quantum commitment functionality as follows: Alice, instead of using the commitment functionality, sends the committed qubits to Bob who stores them in a register $C$. Bob keeps all the qubits that he would send to the commitment functionality in the original protocol in register $C$. By Lemma 2.27, we obtain the following lower bound:

$$H^\tilde{\varepsilon}_{\text{min}}(X|BC) \geq H^\tilde{\varepsilon}_{\text{min}}(X|B) - 2 \log |C|.$$  

(5.2.6)

Lemma 2.29 guarantees that there exists a function $f : \{0, 1\}^\ell \to \{0, 1\}$ such that

$$D(\rho^0_{BC}, \rho^1_{BC}) \leq 2\delta ,$$

where $\rho^z_{BC} = \frac{1}{2^n} \sum_{x \in f^{-1}(z)} \rho^x_{BC}$ and $\delta := \tilde{\varepsilon} + \frac{1}{2} 2^{1 - H^\tilde{\varepsilon}_{\text{min}}(X|BC)}$. Let $z \in \{0, 1\}$. We let Alice prepare the state

$$\frac{1}{\sqrt{2^{\ell-1}}} \sum_{x \in f^{-1}(z)} |x\rangle X \otimes |x\rangle X'.$$
and honestly execute the commit protocol using the first half of this state as her input. Let \( \rho_{A'BC} = \rho_{X'ABC} \) be the resulting state. Since this state is pure conditioned on all the shared classical information, Lemma 2.21 implies that there exists a unitary \( U_{A'} \) such that

\[
D(\tilde{\rho}_{X'1-\mathcal{Z}_{A'BC}}, \rho_{X1-\mathcal{Z}_{A'BC}}) \leq 2\sqrt{\delta},
\]

where \( \tilde{\rho}_{X'1-\mathcal{Z}_{A'BC}} = (U_{A'} \otimes 1_{BC})\rho_{X'ABC}(U_{A'} \otimes 1_{BC})^\dagger \). In the same way as in the proof of Theorem (5.1), we can use the definition of weakly \( \Delta \)-binding and inequalities (5.2.6) and (5.2.7) to obtain the following upper bound on \( (1 - \Delta) \):

\[
1 - \Delta \leq 2\sqrt{\delta} \leq 2\sqrt{2\varepsilon + 2^{-\frac{1}{2}(\ell-2n+1)}}.
\]

This upper bound then immediately implies the statement of the theorem. \( \square \)

Note that the proof of Theorem 5.2 only uses the fact that the quantum commitment functionality could be simulated by Bob such that the resulting state at the end of the commit phase is pure conditioned on all the classical communication and the simulated functionality uses an additional memory of size at most \( \log |C| \). Thus, inequality (5.2.5) holds for an arbitrary functionality which can be simulated using an additional register of size \( \log |C| \leq n \). A simple example would be a functionality that generates a tripartite pure state \( |\psi\rangle_{ABC} \) and gives system \( A \) to Alice and \( B \) to Bob and keeps the system \( C \). In the following subsection we consider a special case of this example, where the systems \( A \) and \( B \) correspond to a classical correlation.

### 5.2.4 Noisy Correlations

Next, we consider Protocols that implement a string commitment from trusted distributed randomness \( P_{UV} \) (cf. Section 3.2). This classical primitive \( P_{UV} \) can be modeled by the quantum primitive

\[
|\psi\rangle_{UV E} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_{UV} \otimes |u,v\rangle_{E}
\]

that distributes the values \( u \) and \( v \) to the two players and keeps the system \( E \).
Theorem 5.3. Every quantum protocol that uses a primitive
\[ |\psi\rangle_{UVE} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_{UV} \otimes |u,v\rangle_{E} \]
and implements an \( \varepsilon \)-hiding and \( \Delta \)-binding string commitment of length \( \ell \) must satisfy
\[ \ell \leq n - 2 \log \left( \frac{(1 - \Delta)^2}{4} - \sqrt{2\varepsilon} \right) - 1. \] (5.2.8)
where \( n := H_0(U|V) + H_0(V|U) \). In particular, if \( \Delta = \varepsilon \leq 0.01 \), then it holds that \( \ell < n + 6 \).

Proof. Let \( \rho_{XABE} \) be the state resulting from the execution of an \( \varepsilon \)-hiding commitment protocol where the committed string \( X \) is uniformly distributed. As in the proof of Theorem (5.1), the definition of the smooth min-entropy and (2.7.16) imply that
\[ H_{\min}^{\varepsilon}(X|B)_{\rho} \geq \log |X| = \ell, \]
where \( \varepsilon = \sqrt{2\varepsilon} \). Consider a modified protocol that starts from a state
\[ |\psi\rangle_{UVB^{'}} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_{UV} \otimes |u,v\rangle_{B^{'}}, \]
where the systems \( V \) and \( B' \) belong to Bob. Since Bob can simulate the original protocol from the modified protocol, any successful attack of Alice against the modified protocol does obviously imply a successful attack against the original protocol. Let \( \rho_{XABB'} \) be the state at the end of the modified protocol. Its marginal state, \( \rho_{XAB} \), is the corresponding state at the end of the commit phase of the original commitment protocol. Then, we can use Lemmas 2.24 and 2.25 to obtain the following lower bound
\[ H_{\min}^{\varepsilon}(X|BB')_{\rho} \geq H_{\min}^{\varepsilon}(X|B)_{\rho} - \max_v \log |\text{supp}(P_{U|V=v})| \]
\[ - \max_u \log |\text{supp}(P_{V|U=u})| \]
\[ \geq \ell - \max_v \log |\text{supp}(P_{U|V=v})| - \max_u \log |\text{supp}(P_{V|U=u})| \]
\[ = \ell - H_0(U|V) + H_0(V|U) \]
\[ = \ell - n, \] (5.2.9)
5.2. Impossibility of Extending Quantum Commitments

where we used Lemmas \[2.27\] and \[2.25\]. From Lemma \[2.29\] we know that there exists a function \( f : \{0, 1\}^\ell \to \{0, 1\} \) such that

\[ D(\rho_{BB'}^X_0, \rho_{BB'}^X_1) \leq 2\delta \]

where \( \rho_{BB'}^X_z = \frac{1}{2^{\ell-1}} \sum x \in f^{-1}(z) \rho_{BB'}^x \) and \( \delta := \bar{\varepsilon} + \frac{1}{2} \sqrt{2^{1-H_{\min}(X|BB')^\rho}} \). Let \( z \in \{0, 1\} \) and let Alice prepare the state

\[ \frac{1}{\sqrt{2^{\ell-1}}} \sum_{x \in f^{-1}(z)} |x\rangle_X \otimes |x\rangle_X' \]

and honestly execute the commit protocol with the first half of this state as her input. Let \( \rho_{A'BB'}^{X_1-z} = \rho_{XX'ABB'}^{X_1-z} \) be the resulting state. Since this state is pure conditioned on all the shared classical information, Lemma \[2.21\] implies that there exists a unitary \( U_{A'} \) such that

\[ D(\rho_{A'BB'}^X_{1-z}, \rho_{A'BB'}^X_{1-z}) \leq 2\sqrt{\delta} , \] \hfill (5.2.10)

where \( \rho_{A'BB'}^{X_1-z} = (U_{A'} \otimes \mathbb{1}_{BB'}) \rho_{A'BB'}^{X_1-z} (U_{A'} \otimes \mathbb{1}_{BB'})^\dagger \). In the same way as in the proof of Theorem (5.1), we can use the definition of weakly \( \Delta \)-binding and inequalities (5.2.6) and (5.2.7) to obtain the following upper bound on \( 1 - \Delta \):

\[ 1 - \Delta \leq 2\sqrt{\delta} \leq 2 \sqrt{\left( \sqrt{2\bar{\varepsilon}} + 2^{-\frac{1}{2}(\ell-n+1)} \right)} . \]

This upper bound then directly implies the statement of the theorem. \( \square \)

Using the fact that \( \binom{2}{1} \)-OT\(^k\) can be securely implemented from distributed randomness \( P_{UV} \) (cf. Section \[3.2\]), this allows us to derive an upper bound on the length of a string commitment that can be implemented from a certain number of OTs. If \( P_{UV} \) is the randomized primitive corresponding to \( n \) instances of \( \binom{2}{1} \)-OT\(^1\), then it holds that

\[ H_0(U|V) + H_0(V|U) = 2n \]

for all \( u, v \). Thus, the length of the implemented string commitment is essentially bounded from above by \( 2n \). Note that this result is tight up to a factor of two \[WN103\] (cf. Section \[5.3\]).
Chapter 5. Quantum Commitment and OT Reductions

Bit Commitment

Next, we show that the impossibility result of Lemma 4.6 in Chapter 4 also holds for quantum protocols. First, we generalize the weakened security definition for bit commitment in Section 4.2 to quantum protocols (see, for example, [DFR+06, KWW09] for strong security definitions for quantum commitment protocols). We consider protocols that implement bit commitment from trusted distributed randomness $P_{UV}$, i.e., the initial state of the protocol is

$$\sigma_{UV} = \sum_{u,v} P_{UV}(u,v) |u⟩⟨u| \otimes |v⟩⟨v|.$$  

When Alice commits to the bit $x \in \{0, 1\}$, the resulting state at the end of the commit protocol is

$$\rho_{AUBV}^x = \sum_{u,v} P_{UV}(u,v) |u⟩⟨u| \otimes |v⟩⟨v| \otimes \rho_{AB}^{x,u,v}.$$  

(5.2.11)

If both parties are honest, the open protocol corresponds to a TP-CPM $O_{AUBV}$ which generates the output state $\tau_{\tilde{X}F} = O_{AUBV}(\rho_{AUBV}^x)$ of Bob, where $\tilde{X}$ is a bit and $F \in \{\text{accept, reject}\}$. As in Definition 4.1 in Section 4.2, we define three parameters that quantify the security of Alice and Bob, respectively, and the correctness of the protocol.

**Definition 5.3.** A quantum bit commitment scheme using a primitive $P_{UV}$ is $(\beta, \varepsilon, \gamma)$-secure if satisfies the following conditions:

- **$\beta$-correct:** When both players are honest and Alice commits to $x$, then Bob accepts $x$ except with probability $\beta$, i.e., Bob’s output state is $\beta$-close to $|x⟩⟨x| \otimes |\text{accept}⟩⟨\text{accept}|$.

- **$\varepsilon$-hiding:** It holds that $D(\rho_{BV}^0, \rho_{BV}^1) \leq \varepsilon$.

- **$\gamma$-binding:** Let $x \in \{0, 1\}$. For any TP-CPM $O'_{AUBV}$, which corresponds to a dishonest strategy of Alice in the opening phase and defines a resulting output state

$$\tau_{\tilde{X}F} = \sum_{x,f} P_{\tilde{X}F}(x,f) |x⟩⟨x| \otimes |f⟩⟨f| = O'_{AUBV}(\rho_{AUBV}^{1-x})$$

of Bob, Bob accepts $x$ with probability at most $\gamma$, i.e., we have

$$P_{\tilde{X}F}(x, \text{accept}) \leq \gamma.$$
5.2. Impossibility of Extending Quantum Commitments

The next lemma shows that for every quantum bit commitment protocol that can use trusted distributed randomness \( P_{UV} \) the size of the conditional entropy \( H(V|U) \) is essentially bounded by the security parameter \( \kappa \) from below.

**Theorem 5.4.** Every quantum bit commitment protocol using a primitive \( \sigma_{UV} = \sum_{u,v} P_{UV}(u,v)|u,v\rangle_{UV} \) which is \((\beta, \varepsilon, \gamma)\)-secure according to Definition 5.3 must satisfy

\[
d_{KL}(1 - \sqrt{2\delta} - \varepsilon || \gamma) \leq H(V|U) .
\]

If \( \beta = \varepsilon = \gamma = 2^{-\kappa} \) with \( \kappa \geq 9 \), then \( H(V|U) \geq 0.9(\kappa - 1) \).

**Proof.** For \( x \in \{0, 1\} \), we consider the joint state at the end of the commit phase, \( \rho_x^{AUBV} \), as defined in equation 5.2.11. We define the state

\[
\rho_{AUV',BV}^x := \sum_{u,v} P_{UV}(u,v)|u,v\rangle_{UV'} \otimes |v\rangle_{V} \otimes \rho_{ABV}^x ,
\]

where Alice has additionally access to a copy of \( v \). From the hiding property, we have

\[
D(\rho_0^{BV}, \rho_1^{BV}) \leq \varepsilon .
\]

Since the state \( \rho_{AUV',BV}^x \) is pure conditioned on all classical communication, \( u \) and \( v \), Lemma 2.21 guarantees that there exists a unitary \( U_{AUV'} \) on Alice’s system such that

\[
D(\rho_{AUV',BV}^1, \rho_{AUV',BV}^0) \leq \sqrt{2\varepsilon} ,
\]

where \( \rho_{AUV',BV}^1 = (U_{AUV'} \otimes 1_{BV})\rho_{AUV',BV}^0 (U_{AUV'} \otimes 1_{BV})^\dagger \). Thus, if the state at the end of the commit phase is \( \rho_{AUV',BV}^0 \) and Alice applies the unitary \( U_{AUV'} \) before opening 1, then Bob accepts with probability at least \( 1 - \sqrt{2\varepsilon} - \beta \). We consider the following attack by Alice: She commits to 0. Then, she generates a copy of \( v \) from \( u \) according to the conditional distribution \( P_{V|U} \). This results in the state

\[
\rho_{AUV',BV}^0 = \sum_{u,v,v'} P_{V|u=v'} P_{UV}(u,v)|u,v'\rangle_{UV'} \otimes |v\rangle_{V} \otimes \rho_{ABV}^{0,u,v} .
\]

Then, she applies \( U_{AUV'} \) before opening 1. Bob accepts with probability at most \( \gamma \) because the protocol is \( \gamma \)-binding. By (2.7.9) and the data processing inequality for the relative entropy (2.7.10), we obtain the desired
lower bound on the conditional entropy:
\[
d_{KL}(1 - \sqrt{2\varepsilon} - \beta||\gamma) \leq S(\rho^0_{AUV\cdot BV}||\rho^0_{AUV\cdot BV}) \\
\leq D_{KL}(P_{UVV}||P_{UV}P_{V|U}) \\
= H(V|U).
\]

If $\beta = \varepsilon = \gamma = 2^{-\kappa}$ with $\kappa \geq 9$, then (4.3.2) implies that
\[
d_{KL}(1 - \sqrt{2\varepsilon} - \beta||\gamma) \geq 0.9(\kappa - 1).
\]

\]

## 5.3 Reversing String OT Efficiently

The impossibility results of Chapter 3 generalize the known lower bounds for perfect implementations of OT \cite{DM99,BM04,WW08b} to the statistical case. Thus, it seems natural to ask whether similar lower bounds also hold for quantum protocols, i.e., whether the lower bounds for perfectly secure protocols presented in \cite{SSS09} can be generalized to the case of statistically secure protocols. We give a negative answer to this question by presenting a statistically secure quantum protocol that violates these bounds.

We introduce an ideal two-party functionality $\mathcal{F}_{MCOM}^{A\rightarrow B,k}$ that allows Alice to commit to a $k$-bit string $b$ and later reveal an arbitrary substring of $b$.

**Definition 5.4** (Multi-Commitment). The functionality $\mathcal{F}_{MCOM}^{A\rightarrow B,k}$ behaves as follows: Upon (the first) input $(\text{commit}, b)$ with $b \in \{0,1\}^k$ from Alice, send committed to Bob. Upon input $(\text{open}, T)$ with $T \subseteq [k]$ from Alice send $(\text{open}, b_T)$ to Bob. All communication/input/output is classical. We also call Alice the sender and Bob the receiver.

This functionality can be implemented from $\binom{n}{1}$-OT$^k$ with statistical and universally composable security. The Universal Composability (UC) Framework has been introduced in \cite{Can01} as a model to analyze the security of protocols in arbitrary environments. The details of this model are beyond the scope of this thesis and are not needed to understand the following proof, and we refer to the full version of \cite{Can01}. Informally, we say that a protocol is a statistically secure and universally composable realization of an ideal functionality $\mathcal{F}$ with an error of at most $\varepsilon$ if
for any adversary there exists a simulator such that any environment can distinguish an execution of the adversary and the protocol (real model) from an execution of the simulator and the functionality (ideal model) with probability at most $\varepsilon$. As shown in [Can01], this security definition implies a very strong composition theorem: If a protocol $\pi$ securely realizes a functionality $F$, then the functionality $F$ can be replaced by the protocol $\pi$ without affecting the security in any universally composable protocol that has access to $F$ as a black-box.

There is a protocol that implements $(\frac{2}{1})$-OT$^k$ from $2m = O(k + \kappa)$ bit commitments with an error of $2^{-\Omega(\kappa)}$ [BBCS92, Yao95, DFL+09]. In this protocol, Alice sends $m$ BB84-states to Bob who measures them either in the computational or in the Hadamard basis. In order to force Bob to measure all the qubits, he has to commit to the basis and the measurement outcome for all the qubits he has received. Alice then asks Bob to open a small subset of these pairs of commitments. OT can then be implemented using further classical processing (see Section 5.4.3 for a complete description of the protocol).

This protocol implements oblivious transfer that is statistically secure in the quantum universal composability model [Unr10]. Obviously, the construction remains secure if we replace the commitment scheme with the functionality $F_{\text{MCOM}}^{A \rightarrow B,2m}$. We show that $F_{\text{MCOM}}^{A \rightarrow B,k}$ can be implemented from the oblivious transfer functionality $F_{\text{OT}}^{A \rightarrow B,k}$ (see [Unr10] for a definition of $F_{\text{OT}}^{A \rightarrow B,k}$) using the protocol below.
Chapter 5. Quantum Commitment and OT Reductions

Protocol 1: $F_{\text{MCOM}}^{A \rightarrow B, k}$ from $\binom{k}{2}$-OT

Parameters: Inputs: Alice has an input $b = (b_1, \ldots, b_k) \in \{0, 1\}^k$ in Commit. Bob has an input $T \subseteq [k]$ in Open.

1: Commit($b$):

1. Alice and Bob invoke $F_{\text{OT}}^{A \rightarrow B, k}$ with random inputs $x_{0,i}^i, x_{1,i}^i \in \{0, 1\}^k$ and $c_i \in \{0, 1\}$.
2. Bob receives $y_i = x_{c_i}^i$ from $F_{\text{OT}}^{A \rightarrow B, k}$.
3. Alice sends $m_i := x_{0,i}^i \oplus x_{1,i}^i \oplus b$ to Bob.

2: Open($T$):

1. Alice sends $b_T, T$ and $(x_{0,i}^i)_T, (x_{1,i}^i)_T$ for all $1 \leq i \leq \kappa$ to Bob.
2. If $(m_i)_T = (x_{0,i}^i)_T \oplus (x_{1,i}^i)_T \oplus (b)_T$ and $(y_i)_T = (x_{c_i}^i)_T$ for all $1 \leq i \leq \kappa$, Bob accepts and outputs $b_T$, otherwise he rejects.

As it is done in the proofs of [Unr10], we assume that all communication between the players is over secure channels and we only consider static adversaries.

Lemma 5.1. There exists a protocol that is statistically secure and universally composable that realizes $F_{\text{MCOM}}^{A \rightarrow B, k}$ with an error of $2^{-\kappa/2}$ using $\kappa$ instances of $F_{\text{OT}}^{A \rightarrow B, k}$.

Proof. The statement is obviously true in the case of no corrupted parties and in the case when both the sender and the receiver are corrupted. We construct for any adversary $A$ a simulator $S$ that runs a copy of $A$ as a black-box. In the case where the sender is corrupted, the simulator $S$ can extract the commitment $b$ from the input to $F_{\text{OT}}^{A \rightarrow B, k}$ and the messages except with probability $2^{-\kappa/2}$ as follows: We define the extracted commitment as $b_i := \text{maj}(m_1^i \oplus x_{0,i}^1 \oplus x_{1,i}^1, \ldots, m_k^i \oplus x_{0,i}^k \oplus x_{1,i}^k)$ for all $1 \leq i \leq \kappa$ where maj denotes the majority function. Let $T$ be a (non-empty) subset of $[k]$ and let $\tilde{b} \in \{0, 1\}^k$ such that $\tilde{b}_T \neq b_T$. An honest receiver accepts $\tilde{b}_T$ together with $T$ in Open with probability at most $2^{-\kappa/2}$ as follows: There must exist $j \in T$ such that $b_j \neq \tilde{b}_j$. Then the sender needs to change either $x_{0,j}^i$ or $x_{1,j}^i$ for at least $\kappa/2$ instances $i$. Thus, the simulator extracts the bit $b$ in the commit phase as specified before and gives $(\text{commit}, b)$ to $F_{\text{MCOM}}^{A \rightarrow B, k}$. Upon getting $(\tilde{b}, T)$ from the adversary, the simulator gives $(\text{open}, T)$ to $F_{\text{MCOM}}^{A \rightarrow B, k}$, if $b_T = b_T$, otherwise it stops. Therefore, any en-
vironment can distinguish the simulation and the real execution with an advantage of at most $2^{-\kappa/2}$. In the case where the receiver is corrupted, the simulator $S$, upon getting the message committed from $F_{\text{MCOM}}^{A\rightarrow B,k}$ and the choice bit $c^i$, chooses the output $y^i$ from $F_{\text{OT}}^{A\rightarrow B,k}$ and the message $m^i$ uniformly and independently at random for all $i$. In the open phase the simulator $S$ gets $(T,b_T)$ and simulates the messages of an honest sender by setting $(x^i_{1-c^i})_T := (m^i)_T \oplus (y^i)_T \oplus b_T$ and $(x^i_{c^i})_T := (y^i)_T$ for all $i$. This simulation is perfectly indistinguishable from the real execution.

Any protocol that is statistically secure in the classical universal composability model \cite{Can01} is also secure in the quantum universal composability model \cite{Unr10}. Together with the proofs from \cite{DFL+09,Unr10}, we, therefore, obtain the following theorem.

**Theorem 5.5.** There exists a protocol that implements $(\frac{2}{1})^k$-OT with an error $\varepsilon$ from $\kappa = O(\log 1/\varepsilon)$ instances of $(\frac{2}{1})^k$-OT in the opposite direction where $k' = \Omega(k)$ if $k = \Omega(\kappa)$.

Since we can choose $k \gg \kappa$, this immediately implies that the bound of Corollary 3.2 does not hold for quantum protocols. Similar violations can be shown for the other two lower bounds (given in Corollary 3.1). For example, statistically secure and universally composable\footnote{Stand-alone statistically secure commitments based on stateless two-party primitives are universally composable \cite{DvdGMQN08}.} commitments can be implemented from shared randomness $P_{UV}$ that is distributed according to $(p)$-RabinOT at a rate of $H(U|V) = 1 - p$ \cite{WNI03}. Using Theorem 5.9, one can implement $F_{\text{OT}}^{B\rightarrow A,k}$ with $k \in \Omega(n(1-p))$ from $n$ copies of $F_{UV}$. Since it holds that $I(U;V) = p$, quantum protocols can also violate the bound of Corollary 3.3.

It has been an open question whether noiseless quantum communication can increase the commitment capacity \cite{WNI03}. Our example implies a positive answer to this question.

### 5.4 Impossibility Results for Quantum Oblivious Transfer Reductions

#### 5.4.1 Security Definition

A protocol is an $\varepsilon$-secure implementation of $(\frac{2}{1})^k$-OT in the malicious model if for any adversary $A$ attacking the protocol (real model), there ex-
ists a simulator \(S\) using the ideal OT (ideal model) such that for all inputs of the honest players the real and the ideal setting can be distinguished with an advantage of at most \(\varepsilon\). This definition (see also \[FS09\] and Section 5.4.3) implies the following three conditions.

- **Correctness:** If both players are honest, Alice has random inputs \((X_0, X_1) \in \{0, 1\}^k \times \{0, 1\}^k\) and Bob has input \(c \in \{0, 1\}\), then Bob always receives \(X_c\) in the ideal setting. This implies that in an \(\varepsilon\)-secure protocol, Bob must output a value \(Y\), where
  \[
  \Pr[Y \neq X_c] \leq \varepsilon. 
  \]  
  (5.4.1)

- **Security for Alice:** Let Alice be honest and Bob malicious, and let Alice’s input be chosen uniformly at random. In the ideal setting, the simulator must provide the ideal OT with a classical input \(C' \in \{0, 1\}\). He receives the output \(Y\) and then outputs a quantum state \(\sigma_B\) that may depend on \(C'\) and \(Y\). The output of the simulator together with classical values \(X_0, X_1\) and \(C'\) now defines the state \(\sigma_{X_0 X_1 B C'}\). Since \(X_1 - C'\) is random and independent of \(C'\) and \(Y\), we must have
  \[
  \sigma_{X_1 - C', X_{C'}, BC'} = \pi_{\{0, 1\}^k} \otimes \sigma_{X_{C'}, BC'} 
  \]  
  (5.4.2)
  and
  \[
  D(\sigma_{X_0 X_1 B}, \rho_{X_0 X_1 B}) \leq \varepsilon, 
  \]  
  (5.4.3)
  where \(\rho_{X_0 X_1 B}\) is the resulting state of the protocol\(^3\)

- **Security for Bob:** If Bob is honest and Alice malicious, the simulator outputs a quantum state \(\sigma_A\) that is independent of Bob’s input \(c\). Let \(\rho_A^c\) be the state that Alice has at the end of the protocol if Bob’s input is \(c\). The security definition now requires that \(D(\sigma_A, \rho_A^c) \leq \varepsilon\) for \(c \in \{0, 1\}\). By the triangle inequality, we get
  \[
  D(\rho_A^0, \rho_A^1) \leq 2\varepsilon. 
  \]  
  (5.4.4)

Note that the Conditions (5.4.1), (5.4.2), (5.4.3) and (5.4.4) are only necessary for the security of a protocol, they do not imply that a protocol is secure.

\(^3\)The standard security definition of OT considered here requires Bob’s choice bit to be fixed at the end of the protocol. To show that a protocol is insecure, it suffices, therefore, to show that Bob can still choose after the termination of the protocol whether he wants to receive \(x_0\) or \(x_1\). Lo in \[Lo97\] shows impossibility of OT in a stronger sense, namely that Bob can learn all of Alice’s inputs.
5.4.2 Impossibility Results for Quantum OT Protocols

First, we prove the following technical lemma, which we will use in our impossibility proofs.

**Lemma 5.2.** Let $\rho_{X_0X_1B}$ satisfy conditions (5.4.2) and (5.4.3). If there exists a measurement $G$ on system $B$ such that $\Pr[G(\rho_B) = X_1] \geq 1 - \varepsilon$, then

$$D(\rho_{X_0X_1B}, \pi_{X_0} \otimes \rho_{X_1B}) \leq 5\varepsilon.$$  

**Proof.** Let $\sigma_{X_0X_1BC'}$ be the state in conditions (5.4.2) and (5.4.3). Then inequality (2.7.13) implies that

$$\Pr[G(\sigma_B) = X_1] \geq \Pr[G(\rho_B) = X_1] - \varepsilon \geq 1 - 2\varepsilon.$$  

In the state $\sigma_{X_0X_1BC'}$, we can guess the first bit of $X_1-C'$ if we output the first bit of $G(\sigma_B)$ whenever $C' = 0$ and a random bit otherwise. We succeed with a probability $p_{\text{guess}}$ which is at least

$$p_{\text{guess}} \geq \frac{1}{2} \cdot \Pr[C' = 1] + \Pr[G(\sigma_B) = X_1 \land C' = 0]$$

$$= \frac{1}{2} \cdot (1 - \Pr[C' = 0]) + \Pr[C' = 0]$$

$$- \Pr[G(\sigma_B) \neq X_1 \land C' = 0]$$

$$\geq \frac{1}{2} \cdot (1 - \Pr[C' = 0]) + \Pr[C' = 0] - 2\varepsilon$$

$$= \frac{1}{2} + \frac{\Pr[C' = 0]}{2} - 2\varepsilon.$$  

Since $X_1-C'$ is uniform with respect to $\sigma_{X_0BC'}$, we have $p_{\text{guess}} \leq \frac{1}{2}$ and, therefore, $\Pr[C' = 0] \leq 4\varepsilon$. We define $\hat{\sigma}_{X_0X_1BC'} := \pi_{X_0} \otimes \sigma_{X_1B} \otimes |1\rangle\langle 1|$. Then, we obtain

$$D(\sigma_{X_1-C'X_0X_1BC'}, \hat{\sigma}_{X_1-C'X_0X_1BC'}) \leq 4\varepsilon$$

and, hence,

$$D(\rho_{X_0X_1B}, \pi_{X_0} \otimes \rho_{X_1B}) \leq D(\rho_{X_0X_1B}, \sigma_{X_0X_1B})$$

$$+ D(\sigma_{X_0X_1B}, \hat{\sigma}_{X_0X_1B})$$

$$\leq 5\varepsilon. \square$$
Next, we present two impossibility results for quantum protocols which can use a commitment functionality or trusted distributed randomness and implement \((\frac{2}{1})\)-OT\(^k\). The first result shows that any quantum protocol which implements an information-theoretically secure oblivious transfer over strings of length \(k\) from black-box bit commitments must use essentially \(k\) bit commitments.

**Theorem 5.6.** Any protocol that implements a \((\frac{2}{1})\)-OT\(^k\) with an error of at most \(\varepsilon\), where \(0 \leq \varepsilon \leq 0.002\), from black-box bit commitments, has to use at least \((1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon})\) bit commitments.

**Proof.** Let \(n\) be the number of commitments used in the protocol. We assume that Alice chooses her inputs \(X_0\) and \(X_1\) uniformly at random. Let the final state of the protocol on Alice’s and Bob’s system be \(\rho_{cAB}\) when both players are honest and Bob has input \(c \in \{0, 1\}\). If Bob is executing the protocol honestly using input \(c = 1\), he can compute \(X_1\) with an error of at most \(1 - \varepsilon\) according to correctness condition. Since the protocol is secure for Alice, we can use Lemma 5.2 to conclude that \(D(\rho_{X_0B}^1, \pi_{X_0} \otimes \rho_B^1) \leq 5\varepsilon\). Equation (2.7.5) implies that

\[
H(X_0|B)_{\rho^1} \geq (1 - 20\varepsilon) \cdot k - 2h(5\varepsilon) \geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon) .
\]

Now, we use the same approach as in the proof of Theorem 5.1. We consider a modified protocol that does not use the bit commitment functionality. In the modified protocol, Alice, instead of using the bit commitment functionality, measures the bits to be committed, stores a copy of each and sends them to Bob, who stores them in a classical register, \(C_A\). When one of these commitments is opened, he moves the corresponding bit to his register \(B\). Bob simulates the action of the commitment functionality locally as follows: Instead of measuring a register, \(Y\), and sending the outcome to the commitment functionality, he applies the isometry \(U : |y\rangle_Y \mapsto |yy\rangle_{YY'}\), purifying the measurement of the committed bit and stores \(Y'\) in another register, \(C_B\). When Bob has to open the commitment, he measures \(Y'\) and sends the outcome to Alice over the classical channel. This protocol is obviously still secure for Bob. Furthermore, the state conditioned on the classical communication is again pure. Let \(\rho_{ABC}^c\), where \(C\) stands for \(C_AC_B\), be the final state of this protocol. Note that its marginal state \(\rho_{AB}^c\) is the corresponding state at the end of the original protocol. Since the protocol is \(\varepsilon\)-secure for Bob, we have \(D(\rho_A^0, \rho_A^1) \leq 2\varepsilon\). From Lemma [2.21] follows that there exists a unitary \(U_{BC}\) such that Bob can transform the state \(\rho^1\) into the state \(\tilde{\rho}\) with \(D(\rho_{ABC}^0, \tilde{\rho}_{ABC}) \leq 2\sqrt{\varepsilon}\).
5.4. Impossibility Results for Quantum OT Reductions

Since given the state $\rho^0_{X_0B}$, $X_0$ can be guessed from $\rho^0_B$ with probability $1 - \varepsilon$, it follows from (2.7.12) that $X_0$ can be guessed from $\rho^1_{BC}$ with a probability of at least $1 - \varepsilon - 2\sqrt{\varepsilon}$. By inequality (2.7.6), we obtain

$$H(X_0|B)_{\rho^1} \leq h(\varepsilon) + h(2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k.$$ 

We can use Lemma 2.25 and (2.7.8) to conclude that

$$H(X_0|BCACB)_{\rho^1} \geq H(X_0|B)_{\rho^1} - n.$$ 

For $\varepsilon \leq 0.002$, we have $h(\sqrt{\varepsilon}) > 11h(\varepsilon)$ and $21\varepsilon < \sqrt{\varepsilon}$. This implies the statement.

Next, we consider protocols where the two players have access to distributed randomness $P_{UV}$, which we can again model as a quantum primitive $|\psi\rangle_{UE} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_U \otimes |u,v\rangle_E$. The following theorem provides two upper bounds on $k$ for quantum protocols which implement $(\frac{1}{2})$-OT$^k$ from such a primitive in terms of the Shannon entropy and in terms of the entropies $H_0(U|V)$ and $H_0(V|U)$.

**Theorem 5.7.** To implement $(\frac{1}{2})$-OT$^k$ with an error of at most $\varepsilon$, where $0 \leq \varepsilon \leq 0.002$, from a primitive $P_{UV}$, we need

$$H_0(U|V) + H_0(V|U) \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) ,$$

and

$$2H(UV) \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) .$$

**Proof.** As in the proof of the previous theorem we have

$$H(X_0|B)_{\rho^1} \geq (1 - 20\varepsilon) \cdot k - 2h(5\varepsilon) \geq (1 - 20\varepsilon) \cdot k - 10h(\varepsilon) .$$

Consider a modified protocol that starts from a state

$$|\psi\rangle_{ABB'} = \sum_{u,v} \sqrt{P_{UV}(u,v)} \cdot |u,v\rangle_A \otimes |u,v\rangle_{B'} ,$$

where the systems $B$ and $B'$ belong to Bob. Note that any successful attack of Alice against the modified protocol does obviously imply a successful attack against the original protocol. As in the proof of the previous theorem we, therefore, have

$$H(X_0|BB')_{\rho^1} \leq h(\varepsilon) + h(2\sqrt{\varepsilon}) + (\varepsilon + 2\sqrt{\varepsilon}) \cdot k .$$
By Lemma 2.25 and (2.7.8), we know that
\[ H(X_0|BB')_{\rho^1} \geq H(X_0|B)_{\rho^1} - \max_v \log |\text{supp}(P_{U|V=v})| \]
\[ - \max_u \log |\text{supp}(P_{V|U=u})|. \]

This implies the first statement. The second statement follows from the inequality
\[ H(X_0|BB')_{\rho^1} \geq H(X_0|B)_{\rho^1} - 2H(B'), \quad (5.4.5) \]
which is implied by (2.7.7). \(\square\)

Since \((\frac{2}{1})\)-OT\(^\ell\) can be securely implemented from distributed randomness \(P_{UV}\) (see Section 3.2) with
\[ H_0(U|V) = H_0(V|U) = k \]
for all \(u, v\), Theorem 5.7 immediately implies the following corollary.

**Corollary 5.1.** Any quantum protocol that implements \((\frac{2}{1})\)-OT\(^k\) with an error of at most \(\varepsilon\), where \(0 \leq \varepsilon \leq 0.002\), from \(n\) instances of \((\frac{2}{1})\)-OT\(^1\) (in either direction), has to use at least
\[ 2n \geq (1 - 3\sqrt{\varepsilon}) \cdot k - 3h(\sqrt{\varepsilon}) \]
instances of \((\frac{2}{1})\)-OT\(^1\).

Furthermore, Theorem 5.7 implies that \((\frac{2}{1})\)-OT\(^1\) cannot be extended by quantum protocols in the following sense: Given a protocol that implements \(m + 1\) instances of \((\frac{2}{1})\)-OT\(^1\) from \(m\) instances of \((\frac{2}{1})\)-OT\(^1\) with an error \(\varepsilon\), we can apply this protocol iteratively and implement \((\frac{2}{1})\)-OT\(^{4m}\) from \(m\) instances with an error of \(\varepsilon' := 3m\varepsilon\). By Corollary 5.1, we know that \(12\sqrt{\varepsilon'} + 3h(\sqrt{\varepsilon'})/m \geq 2\) if \(\varepsilon' \leq 0.002\). We conclude that \(\varepsilon' \geq 0.002\) and, therefore, \(\varepsilon \geq 1/(1500m)\). Thus, any quantum protocol that implements \(m + 1\) instances of \((\frac{2}{1})\)-OT\(^1\) from \(m\) instances of \((\frac{2}{1})\)-OT\(^1\) must have an error of at least \(1/(1500m)\).

Next, we give an additional lower bound for reductions of OT to commitments that shows that the number of commitments (of arbitrary size) used in any \(\varepsilon\)-secure protocol must be at least \(\Omega(\log(1/\varepsilon))\). We model the commitments as before, i.e., the functionality applies the isometry \(U : |y\rangle_Y \mapsto |yy\rangle_{YY'}\) and stores \(YY'\) in separate registers \(E_A\) and \(E_B\) for Alice and Bob.
5.4. Impossibility Results for Quantum OT Reductions

The proof considers the following attack: We let the adversary guess a subset \( T \) of commitments which he has to open during the protocol. He honestly uses all commitments in \( T \) as required by the protocol, but he commits to a default value when he has to use a commitment not in \( T \). If the adversary guesses \( T \) right, he can now attack the protocol in the same way as any protocol that does not use any commitments.

**Theorem 5.8.** Any quantum protocol that implements \((\binom{2}{1})\text{-OT}^k\) using \( \kappa \) commitments (of arbitrary length) must have an error of at least \( 2^{-\kappa/36} \).

**Proof.** We define \( \epsilon := 2^{-\kappa/36} \). Let \( \rho^{c}_{ABEAE} \) be the final state of an \( \epsilon \)-secure protocol, when both players are honest and Bob has input \( c \in \{0, 1\} \). We distinguish two cases. In the first case, we assume that

\[
D(\rho^{0}_{AE}, \rho^{1}_{AE}) \geq \epsilon' := 1/18.
\]

We let Bob be honest and let Alice apply the following strategy: She chooses a random subset \( T \) of \( [k] \). She executes all commitments in \( T \) honestly, but for all commitments not in \( T \) she sends \( |0\rangle \) to \( E_A \) and simulates the action of the commitment functionality in her quantum register. Otherwise, she follows the whole protocol honestly.

During the protocol, Bob may ask Alice to open a certain set of commitments, \( T' \). If \( T' = T \), which happens with probability \( 2^{-\kappa} \) independently of everything else, then at the end of the protocol the global state is \( \rho^c \), but \( E_A \) is now part of Alice’s system. Thus, the states of Alice’s system for \( c = 0 \) and \( c = 1 \), have distance at least \( \epsilon' \cdot 2^{-\kappa} > 2\epsilon \), which contradicts condition (5.4.4).

In the second case, we assume that \( D(\rho^{0}_{AE}, \rho^{1}_{AE}) < \epsilon' \). From condition (5.4.1) follows that honest Bob can guess \( X_1 \) with probability \( 1 - \epsilon \) if \( c = 1 \). According to Lemma 5.2, \( X_0 \) should be \( 5\epsilon \)-close to uniform with respect to \( \rho^1_B \). To obtain a contradiction to the security condition (5.4.3), it is according to equation (2.7.13) sufficient to show that Bob can guess the first bit of \( X_0 \) with a probability greater than \( 1/2 + 5\epsilon \).

Again, if Bob guesses the set \( T \) right, then \( E_B \) is part of Bob’s system. Then Lemma 2.21 guarantees the existence of a unitary \( U_{BE} \) such Bob can transform the state \( \rho^1 \) into a state \( \tilde{\rho}^1 \) with

\[
D(\rho^{0}_{ABEAE}, \tilde{\rho}^{1}_{ABEAE}) \leq \sqrt{2\epsilon'}.
\]

Thus, Bob can guess \( X_0 \) with an error of at most \( \sqrt{2\epsilon'} + \epsilon \) given \( \tilde{\rho}^1 \). If he fails to guess \( T \), he simply outputs a random bit as his guess for the first
bit of $X_0$. Since the probability that he guesses the subset $T$ correctly is exactly $2^{-\kappa}$, he can guess the first bit of $X_0$ with probability

$$(1 - 2^{-\kappa}) \cdot \frac{1}{2} + 2^{-\kappa} \cdot (1 - \varepsilon - \sqrt{2\varepsilon'})$$

$$= \frac{1}{2} + 2^{-\kappa} \cdot \left( \frac{1}{2} - \varepsilon - \sqrt{2\varepsilon'} \right)$$

$$> \frac{1}{2} + 2^{-\kappa} \cdot \left( \frac{1}{2} - \varepsilon'/2 - \sqrt{2\varepsilon'} \right)$$

$$= \frac{1}{2} + 2^{-\kappa} \cdot \frac{5}{36}$$

$$= \frac{1}{2} + 5\varepsilon .$$

\[\Box\]
5.4.3 Reduction of OT to String Commitments

We will now show how to construct a protocol that is optimal with respect to the lower bounds of Theorems 5.6 and 5.8. We modify the protocol from [BBCS92] by grouping the $m$ pairs of values into $\kappa$ blocks of size $b := m/\kappa$. We let Bob commit to the blocks of $b$ pairs of values at once. The subset $T$ is now of size $\alpha \kappa$, and defines the blocks to be opened by Bob. If Bob is able to open all commitments in $T$ consistently, then the state of the protocol must be close in a certain sense to the state that would result from correctly measuring all qubits.

We use the security definition from [FS09], which guarantees that the protocol is sequentially composable when used as subprotocol in a classical outer protocol.

**Definition 5.5.** [FS09] An $(\epsilon, k)$-randomized oblivious transfer scheme is a protocol between Alice and Bob, where Bob has input $C \in \{0, 1\}$, Alice has no input, Alice gets outputs $(Z_0, Z_1) \in \{0, 1\}^k \times \{0, 1\}^k$ and Bob gets output $Y \in \{0, 1\}^k$, satisfying the following properties:

1. **Correctness:** If both parties are honest, then, for any distribution of Bob’s input $C$, $Z_0$ and $Z_1$ are $\epsilon$-close to random and independent of $C$, and $Y = Z_C$ except with probability $\epsilon$.

2. **Security for Alice:** If Alice is honest, then, for any dishonest Bob, the resulting output state $\rho_{Z_0 Z_1 B'}$ can be extended by a classical binary $C$ such that $\rho_{Z_1 - C Z_C B' C}$ is $\epsilon$-close to $\pi_{\{0, 1\}^k} \otimes \rho_{Z_C B' C}$.

3. **Security for Bob:** If Bob is honest, then for any dishonest Alice and for any distribution of $C$, the resulting common output state $\rho_{A' CY}$ can be extended by classical values $Z_0, Z_1$ such that $\Pr[Y = Z_C] \geq 1 - \epsilon$ and $\rho_{Z_0 Z_1 A' C} \approx_{\epsilon} \rho_{Z_0 Z_1 A'} \otimes \rho_C$.

Note that our protocol (Protocol 2) is different from the protocols analyzed [DFL+09] [BF09]. Besides replacing the bit commitments by string commitments, we let, as in Section 3.5, the honest players never abort the protocol, i.e., the honest player chooses the messages himself if the dishonest player refuses to send (well-formed) messages. Furthermore, in our protocol, in contrast to the protocols in [DFL+09] [BF09], Alice outputs two random strings if she detects any inconsistencies in the tested subset or if Bob aborts in the commitment or in the check step. This allows us to implement an ideal OT functionality that does not have a special output aborted. Thus, we don’t have to handle abort events separately in
the proofs and we can directly use the security definition for randomized oblivious transfer from \[\text{FS09}\] (Definition 5.5).

**Protocol 2: OT from String Commitments**

Parameters: $0 < \alpha \leq 1/2$. Positive integers $m, b$ and $\kappa$ with $m = \kappa \cdot b$. A two-universal family $\mathcal{F}$ of hash functions from $\{0, 1\}^{(1-\alpha)m}$ to $\{0, 1\}^k$, where $f(x) := f(x||0^{(1-\alpha)m-m'})$ for $x \in \{0, 1\}^{m'}$ with $m' < (1-\alpha)m$.

Inputs: $c \in \{0, 1\}$ from Bob. Outputs: $(z_0, z_1) \in \{0, 1\}^k \times \{0, 1\}^k$ to Alice, and $y \in \{0, 1\}^k$ to Bob.

1: (State Preparation) Alice chooses $x, \theta \in \{0, 1\}^m$ and sends $H^\theta|x\rangle$ to Bob.

2: (Commitment) Bob chooses $\hat{\theta} \in \{0, 1\}^m$ and measures the received qubits in basis $\hat{\theta}$ resulting in a string $\hat{x}$ of measurement outcomes. Bob commits in blocks of size $b$ to $\hat{\theta}$ and $\hat{x}$.

3: (Check) Alice samples a random subset $t \subseteq \kappa$ of cardinality $\alpha \kappa$ and asks Bob to open the commitments to the corresponding blocks of values $(\hat{\theta}_i, \hat{x}_i)$. Let $\mathcal{T} \subseteq [m]$ be the set of bits corresponding to $t$. Alice measures her qubits indexed by $\mathcal{T}$ in Bob’s basis $\hat{\theta}_t$ to obtain $x_t$ and verifies that $x_i = \hat{x}_i$ whenever $\theta_i = \hat{\theta}_i$. If Bob does not commit to all values as required or does not open all commitments or if Alice detects an inconsistency, then she outputs two random $k$-bit strings $z_0, z_1$ and terminates the protocol.

4: (Set partitioning) Alice sends $\theta$ to Bob. Bob partitions $\mathcal{T} := [m] \setminus \mathcal{T}$ into the subsets $I_c = \{i \in \mathcal{T} : \theta_i = \hat{\theta}_i\}$ and $I_{1-c} = \{i \in \mathcal{T} : \theta_i \neq \hat{\theta}_i\}$ and sends $(I_0, I_1)$ to Alice.

5: (Key extraction) Alice uniformly chooses hash functions $f_0, f_1 \in \mathcal{F}$ and sends them to Bob. She computes $z_0 := f_0(x_{I_0})$ and $z_1 := f_1(x_{I_1})$. Bob computes $y = f(\hat{x}_{I_0})$.

For the analysis of the security for Alice, we introduce a modified version of Protocol 2: Alice, instead of sending BB84-states to Bob, prepares EPR-pairs and sends one qubit of each pair to Bob and measures the other qubits later in the protocol. In the modified protocol Alice measures the qubits in the tested subset not in her basis, but in the basis defined by the commitments opened by Bob. Since this positions are discarded in
the protocol anyway, this does not affect the security for Alice of the protocol. Since operations on different subsystems commute, the modified protocol is equivalent in the sense that the security of the modified protocol implies the security for Alice of Protocol 2.

**Protocol 2': OT from String Commitments**

Parameters: $0 < \alpha \leq 1/2$. Positive integers $m$, $b$ and $\kappa$ with $m = \kappa \cdot b$. A two-universal family $\mathcal{F}$ of hash functions from $\{0, 1\}^{(1-\alpha)m}$ to $\{0, 1\}^k$, where $f(x) := f(x||0^{(1-\alpha)m-m'})$ for $x \in \{0, 1\}^{m'}$ with $m' < (1-\alpha)m$.

Inputs: $c \in \{0, 1\}$ from Bob. Outputs: $(z_0, z_1) \in \{0, 1\}^k \times \{0, 1\}^k$ to Alice, and $y \in \{0, 1\}^k$ to Bob.

1: (State Preparation) Alice prepares $m$ EPR pairs $(|00\rangle + |11\rangle)/\sqrt{2}$ and sends one qubit of each pair to Bob. Alice chooses a basis $\theta \in \{0, 1\}^m$ at random (but does not measure her qubits yet).

2: (Commitment) Bob selects $\hat{\theta} \in \{+, \times\}^m$ at random and measures the received qubits in basis $\hat{\theta}$, obtaining $\hat{x} \in \{0, 1\}^m$. Bob commits in blocks of size $b$ to $\hat{\theta}$ and $\hat{x}$.

3: (Check) Alice samples a random subset $t \subseteq [\kappa]$ of cardinality $\alpha \kappa$. Let $\mathcal{T} \subseteq [m]$ be the set of bits corresponding to $t$. Alice measures her qubits indexed by $\mathcal{T}$ in Bob’s basis $\hat{\theta}_i$ to obtain $x_i$. Then, she asks Bob to open the commitments to the corresponding blocks of values $(\hat{\theta}_i, \hat{x}_i)$. She verifies that $x_i = \hat{x}_i$ whenever $\theta_i = \hat{\theta}_i$. If Bob does not commit to all values as required or does not open all commitments or Alice detects an inconsistency, then she outputs two random $k$-bit strings $z_0, z_1$ and terminates the protocol.

4: (Set partitioning) Alice sends $\theta$ to Bob. Bob partitions $\bar{\mathcal{T}} := [m] \setminus \mathcal{T}$ into the subsets $I_c = \{i \in \bar{\mathcal{T}} : \theta_i = \hat{\theta}_i\}$ and $I_{1-c} = \{i \in \bar{\mathcal{T}} : \theta_i \neq \hat{\theta}_i\}$ and sends $(I_0, I_1)$ to Alice.

5: (Key extraction) Alice measures her qubits in basis $\theta$ to obtain $x$. Alice uniformly chooses hash functions $f_0, f_1 \in \mathcal{F}$ and sends them to Bob. She computes $z_0 := f_0(x_{I_0})$ and $z_1 := f_1(x_{I_1})$. Bob computes $y = f(\hat{x}_{I_0})$.

The idea of the following proof of security for Alice is that the max-entropy of Alice’s measurement results in the $\hat{\theta}$ basis is small conditioned
Chapter 5. Quantum Commitment and OT Reductions

on Bob’s commitments. This implies that the min-entropy of the measurement results is high in the opposite basis. Since Alice will measure about half of her qubits in the opposite basis, the protocol is secure for Alice, i.e., there exists a bit $C$ such that $Z_{1-C}$ is close to uniform with respect to Bob’s system and $Z_C$.

**Lemma 5.3** (Security for Alice). Let $Z_0$ and $Z_1$ from $\{0, 1\}^k$ be the outputs of Alice. Then there exists a binary $C$ such that for any $\varepsilon, \delta > 0$ the following upper bound on the distance from uniform of $Z_{1-C}$ with respect to $Z_C$ and Bob’s system holds:

$$D(\rho_{Z_{1-C}Z_CBC}, \pi_{\{0,1\}^k \otimes \rho_{Z_CBC}}) \leq 2^{-\frac{1}{2}(\frac{1}{4} - \frac{\varepsilon}{2} - h(\delta))(1-\alpha)m - k) - 1 + 2 \exp(-2\varepsilon(1-\alpha)m) + \sqrt{3} \exp(-\alpha' \kappa \delta^2 / 16),$$

(5.4.6)

where $\alpha' := (1/2 - \delta)\alpha$ and $B$ is the quantum state which Bob outputs.

**Proof.** We consider an arbitrary basis $\hat{\theta} \in \{0, 1\}^m$. Let $\hat{Z} = (\hat{Z}_1, \ldots, \hat{Z}_m)$ be the measurement outcomes when Alice measures all her qubits in the basis $\hat{\theta}$ and let $\hat{X} = (\hat{X}_1, \ldots, \hat{X}_m)$ be the measurement outcomes which Bob has committed to. Since we want to prove an upper bound on (5.4.6), we can assume that Bob always opens all commitments as required in the protocol. Otherwise the distance from uniform can only decrease.

We closely follow the proofs of Theorem 2 and Lemma 3 in [TLGR12] in order to derive a lower bound on the min-entropy of the measurement outcomes in the basis $\theta$. We introduce the event, $\Omega_{\text{pass}}$, that Alice detects no inconsistencies, which means that $x_i$ is equal to $\hat{x}_i$ for all positions checked. We define the probability $p_{\text{pass}} := \Pr[\Omega_{\text{pass}}]$. Let $T \subseteq [m]$ be the subset of size $\alpha m$ that Alice checks and define $\Lambda := |\hat{Z}_T \oplus \hat{X}_T|/(\alpha m)$, i.e., $\Lambda$ is the relative hamming distance between $\hat{Z}$ and $\hat{X}$ on the tested subset. Let $\Lambda_{\hat{T}} := |\hat{Z}_{\hat{T}} \oplus \hat{X}_{\hat{T}}|/(1-\alpha)m$ be the relative hamming distance on the remainder of the strings. By Lemma 2.3, we know that

$$\Pr[\Lambda_{\hat{T}} \geq \Lambda + \mu] \leq 3 \exp(-\alpha' \kappa \mu^2 / 8),$$

where $\alpha' := (1/2 - \varepsilon)\alpha$. We set $\varepsilon := \sqrt{3} \exp(-\alpha' \kappa \mu^2 / 16)$. Then, we have

$$\Pr[\Lambda_{\hat{T}} \geq \Lambda + \mu | \Omega_{\text{pass}}] \leq \Pr[\Lambda_{\hat{T}} \geq \Lambda + \mu] / p_{\text{pass}} \leq \varepsilon^2 / p_{\text{pass}}.$$

To simplify the notation, we define the random variables $\hat{Z} := \hat{Z}_{\hat{T}}$ and $\hat{X} := \hat{X}_{\hat{T}}$. We will evaluate the entropy for the probability distribution
conditioned on the event that Alice’s test is passed. We define the distribution

$$P_{\tilde{Z}\tilde{X}}(\tilde{z}, \tilde{x}) := \Pr[\tilde{Z} = \tilde{z} \land \tilde{X} = \tilde{x} | \Omega_{\text{pass}}].$$

According to the proof of Lemma 3 from [TLGR12] this implies that there exists a distribution $Q_{\tilde{Z}\tilde{X}}$, which is $(\varepsilon/\sqrt{p_{\text{pass}}})$-close to $P$ in terms of the purified distance and which satisfies $|\tilde{z} \oplus \tilde{x}| \leq n\mu$ for all $(\tilde{z}, \tilde{x})$ in the support of $Q$. The entropy $H_{\text{max}}(\tilde{Z}|\tilde{X})_Q$ is bounded by $H_0(\tilde{Z}|\tilde{X})$ from above, i.e., by the maximum support of $Q_{\tilde{Z}|\tilde{X}=\tilde{x}}$ for any $\tilde{x}$. Thus, we can conclude that

$$H_{\text{max}}^{\varepsilon'}(\tilde{Z}|\tilde{X})_P \leq H_{\text{max}}^{\varepsilon'}(\tilde{Z}|\tilde{X})_Q \leq H_0(\tilde{Z}|\tilde{X}) \leq \sum_{i=0}^{\mu} \binom{n}{i} \leq nh(\mu),$$

where $n := (1 - \alpha)m$, $\varepsilon' := \frac{\varepsilon}{\sqrt{p_{\text{pass}}}}$ and $\mu = \sqrt{\frac{16}{\alpha'} \ln \frac{\sqrt{3}}{\varepsilon}}$. Since Alice chooses the basis $\theta$ uniformly, Hoeffding’s bound (Lemma 2.2) implies that the Hamming weight of $w := |\theta_T \oplus \tilde{\theta}_T|$ is at least $(1/2 - \tilde{\varepsilon})(1 - \alpha)m$ except with probability at most

$$2 \exp(-2\tilde{\varepsilon}^2(1 - \alpha)m).$$

If this lower bound holds, then for any partition $(I_0, I_1)$ of Bob there must be a bit $C$ such that the Hamming weight of $w$ restricted to $I_{1-C}$ is lower bounded by $(1/4 - \tilde{\varepsilon}/2)(1 - \alpha)m$. Let $A_T$ be the system that contains the $(1 - \alpha)m$ qubits of Alice that are not in $T$ and let $B$ denote the whole system of Bob. We introduce the state, $\tilde{\rho}_{\tilde{X}I_{01}\tilde{C}}$, conditioned on the event that this lower bound on the hamming weight holds. In the following we consider the post-measurement states that result from measuring the qubits in $A_T$. We denote the register containing the measurement outcome by $\hat{Z}_i (X_i)$ when measuring the $i$-th qubit in basis $\tilde{\theta}_i (\theta_i)$. This means that $\tilde{\rho}_{X_{I_{1-C}}A_{I_{1-C}}}X_{I_{01}\theta BC}$, for example, is the state obtained from $\tilde{\rho}_{A_T X_{I_{01}}\theta BC}$ by measuring all qubits in $A_{I_{1-C}}$ in basis $\theta_{I_{1-C}}$ and storing the measurement outcome in $X_{I_{1-C}}$. By inequality (2.7.18), we obtain that

$$H_{\text{max}}^{\varepsilon'}(\hat{Z}|\hat{X}I_0I_1)_{\tilde{\rho}} \leq H_{\text{max}}^{\varepsilon'}(\hat{Z}|\hat{X})_{\tilde{\rho}}.$$

By Lemma 2.23, this implies that

$$H_{\text{max}}^{\varepsilon'}(\hat{Z}_{I_{1-C}}|\hat{X}I_0I_1)_{\tilde{\rho}} \leq H_{\text{max}}^{\varepsilon'}(\hat{Z}|\hat{X})_{\tilde{\rho}} \leq (1 - \alpha)mh(\mu).$$
We can apply Lemma 2.30, the uncertainty relation for smooth entropies, to obtain the following lower bound on the min-entropy

\[ H_{\min}^{\tilde{\epsilon}'}(X_{I_1-C}|A_{I_C}B)_{\rho} \geq (1/4 - \tilde{\epsilon}/2) (1 - \alpha) m - H_{\max}^{\tilde{\epsilon}'}(\hat{Z}_{I_1-C}|\hat{X}_{I_0}I_1C)_{\rho} \]

\[ \geq (1/4 - \tilde{\epsilon}/2) (1 - \alpha) m - (1 - \alpha) mh(\mu) \]

The data processing inequality for smooth entropies (Lemma 2.22) implies that

\[ H_{\min}^{\tilde{\epsilon}'}(X_{I_1-C}|Z_{C}B)_{\rho} \geq H_{\min}^{\tilde{\epsilon}'}(X_{I_1-C}|X_{I_C}B)_{\rho} \geq H_{\min}^{\tilde{\epsilon}'}(X_{I_1-C}|A_{I_C}B)_{\rho} \]

Since we extract \( k \) bits, we can apply the leftover hash lemma (Lemma 2.28) to obtain that, conditioned on the event \( \Omega_{pass} \), the distance from uniform of \( Z_{1-C} \) with respect to \( Z_{C}B \) is bounded from above by

\[ \Delta := 2^{-((1/4 - \tilde{\epsilon}/2 - h(\mu(\epsilon)))(1-\alpha)m-k)/2-1} + \tilde{\epsilon}' + 2 \exp(-2\tilde{\epsilon}^2(1 - \alpha)m) \]

Thus, the total distance from uniform is bounded from above by \( p_{pass} \cdot \Delta \), and, therefore, is at most

\[ 2^{-((1/4 - \tilde{\epsilon}/2 - h(\mu(\epsilon)))(1-\alpha)m-k)/2-1} + \epsilon + 2 \exp(-2\tilde{\epsilon}^2(1 - \alpha)m) \]

Since this holds for any basis \( \hat{\theta} \in \{0, 1\}^m \), we obtain that there must exist a binary \( C \) such that the total distance from uniform of \( Z_{1-C} \) with respect to \( Z_{C}B \) is bounded from above by

\[ D(\rho_{Z_{1-C}Z_{C}B}, \pi_{\{0,1\}^k} \otimes \rho_{Z_{C}B}) \leq 2^{-((1/4 - \tilde{\epsilon}/2 - h(\mu(\epsilon)))(1-\alpha)m-k)/2-1} + \epsilon + 2 \exp(-2\tilde{\epsilon}^2(1 - \alpha)m) \]

\[ \leq 2^{-((1/4 - \tilde{\epsilon}/2 - h(\delta))(1-\alpha)m-k)/2-1} + \sqrt{3} \exp(-\alpha'\kappa\delta^2/16) \]

\[ + 2 \exp(-2\tilde{\epsilon}^2(1 - \alpha)m) \]

where \( \rho_{Z_{1-C}Z_{C}B} \) is the state at the end of the protocol.

Interestingly, the same security bound can also be shown using the sampling technique introduced in [BF09] (see also [DFL+09, Feh10]) as follows: We consider the state shared between Alice and Bob after Bob has committed to the bases \( \hat{\theta} \) and the measurement outcomes \( \hat{x} \), where we can without lost of generality assume that \( \hat{\theta} = \hat{x} = (0, \ldots, 0) \). Since
we want to prove an upper bound on \((5.4.6)\), we can assume that Bob always opens all commitments as required in the protocol. Otherwise the distance from uniform can only decrease. We consider the joint state of Alice and Bob and assume that the state is pure conditioned on the commitments. Alice now chooses a subset \(T\) to be opened by Bob. According to Theorem 3 in [BF09], Lemma 2.3 implies that the joint state is \(\sqrt{3}\exp(-\alpha'\kappa^2/16)\)-close to an ideal state that is for every choice of \(T\) and \(S\) in a superposition of states with relative Hamming weight in a \(\delta\)-neighborhood of \(\beta\) within \(A_T\), where \(\beta\) is the number of inconsistencies that Alice detects and \(S\) is the subset of \(T\) that Alice checks. We assume that the state equals this ideal state and add the error later.

Then, we can follow the proof of Theorem 4 in [BF09] for \(\beta = 0\) and obtain that the distance from uniform of one of the outputs, \(Z_{1-C}\), with respect to Bob’s system and the other output, \(Z_C\), is upper bounded by

\[
2^{-\frac{1}{2}((1/4-\varepsilon/2-h(\delta))(1-\alpha)m-k)-1} + 2 \exp(-2\varepsilon^2(1-\alpha)m). 
\]

In the proof of Theorem 4 in [BF09] (and in the corresponding part of the proof in [DFL+09]), it is actually neglected that Bob can generate the partitions \((I_0, I_1)\) using his quantum state. However, one can assume that the state conditioned on the choice of the partition and the basis \(\theta\) is again pure. This new state is then still in a superposition of states with relative Hamming weight at most \(\delta\) within \(A_T\) as required.

If \(\beta > 0\), the distance from uniform is zero. Thus, the statement of Lemma 5.3 follows by adding the distance of the ideal state to the real state.

**Lemma 5.4 (Security for Bob).** The protocol is perfectly secure for Bob.

**Proof.** Let \(\rho_{A'YC}\) be the state created by the protocol if Bob is honest. We consider a hypothetical protocol where Bob does not use any commitments. He stores all the qubits received from Alice. After Alice sends the set \(T\), he chooses a basis \(\hat{\theta}\) and measures his qubits corresponding to \(T\) in basis \(\hat{\theta}\) to obtain \(\hat{x}_T\), but does not yet measure the other qubits. Then he sends \(\hat{x}_T\) and \(\hat{\theta}_T\) to Alice. After he has received the basis \(\theta\) from Alice he measures all his remaining qubits in Alice’s basis \(\theta\) to obtain \(\hat{x}_T\). Next, he chooses his input \(C \in \{0, 1\}\) and constructs the sets \(I_0\) and \(I_1\) using \(\theta\) and \(\hat{\theta}\) as in the protocol. After receiving \(f_0, f_1 \in \mathcal{F}\) from Alice, he computes \(z_0 = f_0(\hat{x}_{I_0})\) and \(z_1 = f_1(\hat{x}_{I_1})\). This results in a state \(\sigma_{A'Z_0Z_1C}\), where \(Z_0\) and \(Z_1\) are the values computed by Bob. We have \(\sigma_{A'Z_0Z_1C} = \sigma_{A'Z_0} \otimes \sigma_C\) and \(\sigma_{A'Z_1C} = \rho_{A'YC}\). \(\square\)
Lemma 5.5 (Correctness). The protocol is perfectly correct.

Proof. If both players are honest, then $Z_0$, $Z_1$ and $C$ are independently distributed according to the required distributions. Furthermore, Bob always computes $Z_C$ as his output. □

The following theorem is an immediate consequence of Lemmas 5.3, 5.4, and 5.5.

Theorem 5.9. There exists a quantum protocol that uses $\kappa = O(\log 1/\varepsilon)$ commitments of size $b$, where $\kappa b = O(k + \log 1/\varepsilon)$, and implements a $(\frac{2}{1})$-OT$^k$ with an error of at most $\varepsilon$ according to Definition 5.5.
Bibliography


[DKS99] I. Damgård, J. Kilian, and L. Salvail. On the (im)possibility of basing oblivious transfer and bit com-


possibility of growing quantum bit commitments. Phys.

thesis, ETH Zurich, Switzerland, 2007. Available at

M. Naor, editor, Advances in Cryptology - EUROCRYPT
2007, volume 4515 of Lecture Notes in Computer Science,

[Wul09] J. Wullschleger. Oblivious transfer from weak noisy
channels. In O. Reingold, editor, Theory of Cryptography,
volume 5444 of Lecture Notes in Computer Science,

[WW04] S. Wolf and J. Wullschleger. Zero-error information and
applications in cryptography. In Proceedings of 2004 IEEE
Information Theory Workshop (ITW ’04), 2004.

[WW05a] S. Wolf and J. Wullschleger. New monotones and lower
bounds in unconditional two-party computation. In Ad-
varices in Cryptology — CRYPTO ’05, volume 3621 of Lecture

[WW05b] S. Wolf and J. Wullschleger. Oblivious transfer and
quantum non-locality. In Information Theory, 2005. ISIT

[WW06] S. Wolf and J. Wullschleger. Oblivious transfer is sym-
metric. In Advances in Cryptology — EUROCRYPT ’06,
volume 4004 of Lecture Notes in Computer Science, pages

[WW08a] S. Wehner and J. Wullschleger. Composable security
in the bounded-quantum-storage model. In Proceed-
ings of the 35th international colloquium on Automata, Lan-
guages and Programming, Part II, ICALP ’08, pages 604–


