On the Power of Two-Party Quantum Cryptography

Miroslava Sotáková

PhD Dissertation

Department of Computer Science
University of Aarhus
Denmark

On the Power of Two-Party Quantum Cryptography

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

by
Miroslava Sotáková
February 8, 2009

Abstract

This thesis focuses on questions in secure two-party quantum computation. In cryptography, more complicated protocols are usually composed from smaller building bricks – the protocols that implement simple functionalities known as *primitives*. It has been shown by Lo that in the model where the players are unbounded in computation time and memory size, it is not possible to achieve perfect security in the implementation of cryptographically interesting two-party primitives, even if the players are quantum. In this thesis, we extend those results by looking at the security limits of two-party quantum computation in more detail. We consider quantum protocols implementing *non-trivial* two-party primitives which are those with no secure classical protocol even against honest-but-curious adversaries. Under the sole assumption of correctness—which guarantees that honest players obtain their correctly distributed outcomes and nothing in addition — we show that *any* quantum protocol necessarily leaks forbidden information to a dishonest player. Furthermore, we provide a framework to quantify this leakage. All our results hold even against quantum honest-but-curious adversaries who honestly follow the protocol but purify their actions and apply a different measurement at the end of the protocol.

For several flavors of oblivious transfer, we determine the minimum leakage of any quantum protocol. In particular, we show that quantum protocols for oblivious transfer asymptotically leak *all* information to a honest-but-curious adversary as the length of the transmitted strings increases.

Furthermore, we generalize the framework by also considering protocols with the presence of a trusted third party, modeled by the state of the environment which does not interact with the players during the protocol's execution. We show that even in such a model, any non-leaking implementation of an arbitrary primitive is in fact, perfectly secure. It means that it only allows the players to access the information specified by the implemented functionality. This result does not follow immediately from the definition of a non-leaking implementation, since such an implementation may allow the players to get the information of their choice about the other party, unless some player wants to learn more than he would if he was honest. We also show that even if the environment enables the quantum players to implement some non-trivial primitives perfectly securely, they cannot amplify the cryptographic power of such primitives in an arbitrary way.

Another issue we look at is composability of two-party quantum protocols. To show that a protocol π can be self-composed, one would have to prove that

any attack of a real protocol using several instances of π as its sub-routines, can be simulated by an appropriate attack of an ideal protocol, using the instances of an ideal functionality ID_π corresponding to π as its sub-routines. Any attack of the ideal protocol consists of calls to ID_π defining the actions on single copies of π. On the other hand, in an attack of the real protocol also quantum operations acting coherently in more copies of π are allowed. In this work we show that in fact, no non-trivial two-party quantum protocol is self-composable. We do so by defining a generic protocol acting on several copies of π whose output cannot be reproduced and not even approximated by calls to the ideal functionality.

Acknowledgements

First of all, I would like to thank my supervisor Louis Salvail and the head of Aarhus Cryptology Group Ivan Damgård, for introducing me into the area of (quantum) cryptography and information theory, so new to me at the time I started to study at University of Aarhus. I am very grateful especially to Louis Salvail for all those long discussions that helped me to get deeper insight into the problems. Many thanks go to all the academic and non-academic folks at Department of Computer Science, and in particular to my study fellows who made the environment very friendly. Among them, I would especially like to thank my co-author Christian Schaffner for all the advice and help he offered to me, like an "older and experienced brother". My special thanks go also to Mikkel, Martin, and Claudio, for their will to help me with the administrative and technical problems related to handing-in this thesis. I address my gratitude to the members of Institute for Quantum Computation at University of Waterloo, and in particular to Debbie Leung for hosting me for five months filled with new experience and inspiration. I would like to thank my great friend Dávid Pál, together with Shai Ben-David and Tyler Lu from University of Waterloo, for extending my knowledge of other areas of theoretical computer science and new impulses that helped me to stay encouraged about scientific research. I would like to acknowledge Yevgeniy Dodis who provided me with a great working environment at New York University in the last months of my studies. I am also very grateful to my family who kept believing in me a lot more than I did, and to Joël Alwen for proof-reading and most of all, for his permanent moral support, strength, and optimism that were some of the essential forces helping me to finish this thesis.

Miroslava Sotáková,
Nová Lesná, December 31, 2008.

Contents

Chapter 1

Introduction

1.1 Cryptographic Models and Primitives

The need for secure communication is probably as old as the invention of writing. In the digital age, the tasks requiring security like encryption, key-agreement, authentication, identification, or voting are achieved through cryptographic *protocols*. The notion of security of a protocol is always related to a *cryptographic model* i.e., the environment in which the protocol is executed. The description of a model may involve specification of the limits of adversarial behavior (the number of dishonest parties and the way in which they are allowed to deviate from the instructions), computation space/time bounds, or the list of additional resources like specific communication channels, shared randomness, and oracles for certain cryptographic functionalities, available for using. A protocol is secure in the strongest sense, if it is secure against any number of dishonest parties with unlimited computational power, allowed to deviate from their honest behavior in an arbitrary way. The notion of security we investigate in this thesis is against weak adversaries, called *honest-but-curious*, that follow their computation instructions but store all information they can access. Otherwise, they are computationally unbounded. This model is interesting for at least two reasons. First, showing that there is no protocol implementing a given functionality securely even against this type of weak adversaries implies that no implementation can be secure against any stronger type of adversaries. Second, in the quantum world where *quantum honest-but-curious* behavior is equivalent to "indistinguishable from the honest one by the other party", a malicious (i.e., not just honest-but-curious) player can be detected by the other player and therefore, severely punished. Hence, in such a model it is often rational to behave in a honest-but-curious manner. The assumption of computational unboundedness is also well-justified, since infeasibility of tasks ensuring security of protocols against polynomial time adversaries, like integer factoring (RSA encryption [RSA78]), finding discrete logarithm (Diffie-Hellman key-exchange [DH76]), or lattice problems [AD97, GGH97], has never been formally proven. Furthermore, finding discrete logarithm and integer factoring are examples of problems that can be solved in polynomial time by a quantum computer [Sho97], even though no classical polynomial algorithm is known for

either of them.

Interesting cryptographic tasks can involve arbitrary number of parties. For a number of those, such as zero-knowledge proofs [GMR89] (a player wants to convince the other player that certain statement is true without revealing any information about its proof) or the millionaire problem [Yao82] (two millionaires want to know who is richer without disclosing any other information about the value of their properties), only two players are involved. In this thesis we focus on such setting.

In the cryptographic protocol design, reliable security is highly demanded. Protocols are therefore built from blocks, called *cryptographic primitives*, that implement specific low-level tasks and are realized by well-understood algorithms. Protocols are then proven to be secure by showing security (also in the composition) of its building blocks in a given cryptographic model. As an example of a primitive, we take a two-party primitive called *oblivious transfer*, first introduced by Rabin [Rab81]. Even though there are several variants of this primitive, all of them are equivalent in the sense that we can build any of them from several instances of another one [Cré87, CK88]. Probably the most well-known of these variants are 1-2-OT (one-out-of-two oblivious transfer) [Wie83, EGL82] and ROT (Rabin oblivious transfer) [Rab81].

In the first of these two variants, a sender Alice transmits two bits to Bob who decides which of them to receive. An implementation of 1-2-OT is secure, if it does not allow dishonest Alice to learn which of the two bits Bob has received and on the other hand, it prevents dishonest Bob from getting any information about the other one of Alice's bits. Rather surprisingly, it has been shown by Kilian [Kil88] that 1-2-OT is *universal* for two-party computation, which means that any two-party functionality can be securely implemented with several copies of this simple primitive. The second primitive – ROT, is simply a secure erasure channel. Alice sends Bob a single bit which is replaced by a uniformly random bit with probability 1/2. In a secure implementation of ROT, dishonest Alice does not learn whether the erasure happened and whatever Bob does (within the restrictions specified by the model) does not give him any information about the transmitted bit with probability 1/2.

Rather recently, Popescu and Rohrlich [PR94] introduced yet another primitive called *non-local box* (NL-box), as a machine modeling non-signaling nonlocality. It lets the two players generate an additive secret sharing of the product of their input bits x and y while keeping each party's input totally private. In other words, upon inputs x and y, the players receive output bits a and b satisfying $xy = a \oplus b$ and $\Pr[a = 0] = 1/2$. It has been shown in [WW05b] that one NLB together with one bit of communication allow for a simulation of 1-2-OT. It is not difficult to prove that in the model where we assume that the computational power of the players is unbounded and they only communicate via noiseless channels, it is not possible to implement 1-2-OT securely "from scratch". Probably the easiest way to do it is by showing impossibility of designing a secure protocol for an even weaker primitive introduced by Blum [Blu82], which is called *bit commitment*. This functionality is very important in cryptography, as it stands as an essential building block of most cryptographic protocols. Bit-commitment scheme lets one of the two players

commit to a bit b in such a way that the other player does not learn its value (we called this property *concealing*) and at the same time, there is a way for a committer to later convince the other party that the bit value was fixed at the time of the commitment and equals b (the commitment is then called *binding*). It is possible to build a protocol for bit commitment from several instances of a protocol for 1-2-OT, by letting Alice prepare many bit-pairs (x_0^i, x_1^i) such that $x_0^i \oplus x_1^i = b$ and letting Bob receive one bit of each pair. In the opening phase, Alice simply sends all of her bits to Bob. On the contrary, [MN05] shows that bit commitment is not sufficient for a secure implementation of oblivious transfer. We can easily prove that bit commitment cannot be implemented securely in the information-theoretic sense. Let us assume that a protocol for bit commitment hides the value of the committed bit perfectly. Then, since the verifier's view is exactly the same in both cases where $b = 0$ and $b = 1$, there exist complete protocol transcripts extending the verifier's view for both of the bit values. According to the choice of a transcript, the committer can reveal both $b = 0$ and $b = 1$ consistently with the view of the verifier. Bit commitment can be reduced to 1-2-OT, yielding that there is no secure protocol for 1-2-OT in the information-theoretic sense either.

1.2 Secure Two-Party Quantum Computation

Even though quantum communication provably allows multiple players to implement tasks with no secure classical protocols, which is most famously demonstrated by a protocol for secret-key distribution [BB84], quantum and classical cryptography often show similar limits in the two-party setting. Oblivious transfer [Lo97], bit commitment [May97, LC97], and even fair coin tossing [Kit03] are impossible to realize securely both classically and quantumly. We can show the impossibility of quantum bit commitment, by using a similar argument as in the classical case, and that we explain in more detail at the end of this section. On the other hand, quantum cryptography allows for some weak primitives[1] otherwise impossible in the classical world. For example, quantum coin-flipping protocols with maximum bias equal to $\frac{1}{4}$ exist[2] against any adversary while remaining impossible based solely on classical communication [Amb01]. Few other weak primitives are known to be possible with quantum communication while remaining impossible classically. Recall the definition of NL-box from the previous section. The sharing of one EPR pair allows to simulate an NL-box with symmetric error probability $\sin^2 \frac{\pi}{8}$ [PR94, BLM$^+$05]. Equivalently, Alice and Bob can implement *1-out-of-2 oblivious transfer* (1-2-OT) privately provided the receiver Bob gets the bit of his choice only with probability of error $\sin^2 \frac{\pi}{8}$ [Amb05]. Clearly, even with such imperfection these two primitives are impossible to realize in the classical world. This discussion naturally leads to the following questions:

- What is the cryptographic power of two-party quantum cryptography?

[1] These primitives are usually so weak that they cannot be amplified.

[2] In fact, protocols with better maximum bias are known for weak quantum coin flipping [Moc04, Moc05, Moc07].

and

- How does it relate to what is achievable in the classical setting?

On the one hand, quantum communication allows for primitives impossible in the classical world while on the other hand primitives like (any flavor of) oblivious transfer or bit commitment are impossible for similar reasons as in the classical world. Most standard primitives in two-party quantum cryptography have been shown impossible to implement securely against weak quantum adversaries reminiscent to the classical honest-but-curious (HBC) behavior [Lo97].

The idea behind these impossibility proofs is to consider parties that *purify* their actions throughout the protocol execution. This behavior is indistinguishable from the one specified by the protocol but guarantees that the joint quantum state held by Alice and Bob at any point during the protocol remains pure. The possibility for players to behave that way in any two-party protocol has important consequences. For instance, the impossibility of quantum bit commitment follows from this fact [May97, LC97]: After the commit phase, Alice and Bob share the pure state $|\psi_x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ corresponding to the commitment of bit x. Since a proper commitment scheme provides no information about x to the receiver Bob, it follows that $\mathrm{tr}_A |\psi_0\rangle\langle\psi_0| = \mathrm{tr}_A |\psi_1\rangle\langle\psi_1|$. In this case, there always exists a unitary $U_{0,1}$ acting only on Alice's side such that $|\psi_1\rangle = (U_{0,1} \otimes \mathbb{I}_B)|\psi_0\rangle$. In other words, if the commitment is concealing then Alice can open the bit of her choice by applying a suitable unitary transform only to her part. A similar argument allows to conclude that 1-2-OT is impossible [Lo97]: Suppose Alice is sending the pair of bits (b_0, b_1) to Bob through 1-2-OT. Since Alice does not learn Bob's selection bit, it follows that Bob can get bit b_0 before undoing the reception of b_0 and transforming it into the reception of b_1 using a local unitary transform similar to $U_{0,1}$ for bit commitment. For both these primitives, privacy implies that local actions can transform the honest execution with one input into the honest execution with another input.

1.3 Contributions

1.3.1 Modeling Quantum Protocols by Super-Embeddings

In this thesis, we investigate the cryptographic power of two-party quantum protocols against players that purify their actions. This *quantum honest-but-curious (QHBC)* behavior is the natural quantum version of the classical HBC behavior. We consider the general setting where Alice obtains random variable X and Bob random variable Y according to joint probability distribution $P_{X,Y}$. Any quantum protocol implementing $P_{X,Y}$ correctly will produce, when both parties purify their actions, a joint pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ that, when subsystems of A and B are measured in the computational basis, leads to outcomes X and Y with distribution $P_{X,Y}$. Such a state $|\psi\rangle$ is called a *quantum super-embedding*[3] of the *cryptographic primitive* $P_{X,Y}$. Conversely, any super-

[3] An embedding is called *super*-embedding, if the measurement of only a strict subset of registers A, B yields outcomes X, Y. The registers A and B of a *regular* quantum embedding of $P_{X,Y}$ only contain the values for X and Y.

embedding $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be produced in the QHBC model by the trivial protocol asking Alice to generate $|\psi\rangle$ before sending the quantum state in $\mathcal{H}_B$ to Bob. It follows that in order to understand the power of two-party quantum cryptography in the QHBC model, it suffices to investigate the cryptographic power of super-embeddings. In a super-embedding of $P_{X,Y}$, both extra registers A' and B' in $\mathcal{H}_A$ and $\mathcal{H}_B$ that are not measured in order to obtain X and Y do not give any extra information about Y and X respectively. Otherwise, the adversary could measure freely these extra registers leading to the implementation of a primitive different from $P_{X,Y}$. We say that a protocol for $P_{X,Y}$ is *correct* if, once purified, it generates a super-embedding of $P_{X,Y}$. Notice that if X and Y were provided privately to Alice and Bob—through a trusted third party for instance—then the expected amount of information one party gets about the other party's output is the minimal amount, quantified by the Shannon mutual information $I(X;Y)$ between X and Y.

We call a two-party primitive $P_{X,Y}$ *(cryptographically) non-trivial* if it cannot be generated in the HBC model. Answering the above two questions about the power of two-party cryptography requires to determine how well non-trivial primitives can be implemented by quantum super-embeddings.

1.3.2 Information Leakage of Super-Embeddings

Let A and B denote the quantum registers held by Alice and Bob respectively when they share a quantum embedding $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ for $P_{X,Y}$, which is a super-embedding with no additional registers held by the players. The information provided by B (resp. A) on random variable X (resp. Y), denoted by $S(X;B)$ (resp. $S(Y;A)$), is the expected amount of classical information required in addition to quantum state B (resp. A) in order to identify X (resp. Y) [DW03]. We simply define the *leakage* of super-embedding $|\psi\rangle$ for $P_{X,Y}$ as

$$\Delta_\psi := \max\{\, S(X;B) - I(X;Y)\,,\; S(Y;A) - I(Y;X)\,\}\,.$$

That is, the leakage is the maximum amount of extra information about the other party's output given the quantum state held by one party. It turns out that $S(X;B) = S(Y;A)$ holds for all super-embeddings, exhibiting a symmetry similar to its classical counterpart $I(X;Y) = I(Y;X)$ and therefore, the two quantities we are taking the maximum of in the definition of leakage above coincide. We then show that the leakage of any super-embedding for $P_{X,Y}$ is lower bounded by the leakage of some regular embedding of the same primitive. It follows that in order to lower bound the leakage of any correct implementation of a given primitive, it suffices to minimize the leakage over all its regular embeddings. We demonstrate that the only non-leaking embeddings are the ones for trivial primitives. Therefore, all embeddings for any non-trivial primitive $P_{X,Y}$ necessarily leak and so do all quantum protocols correctly implementing $P_{X,Y}$.

Determining the leakage of embedding $|\psi\rangle$ is in general not an easy task since it requires to find the eigenvalues of the reduced density matrix $\rho_A = \mathrm{tr}_B\,|\psi\rangle\langle\psi|$ (or equivalently $\rho_B = \mathrm{tr}_A\,|\psi\rangle\langle\psi|$). However, when $P_{X,Y}$ is such that the bit-length of either X or Y is short, the leakage of a given embedding of $P_{X,Y}$ can

be computed by diagonalizing the reduced density matrix in the Hilbert space of the lower dimension (i.e. we diagonalize ρ_A if X is short or ρ_B if Y is short), using the fact that $S(X;A) = S(Y;B)$. In order to find the minimum leakage of any correct quantum protocol for a given primitive, one has to minimize the leakage over all possible embeddings of that primitive. In general, this is a difficult problem. However, for simple primitives like 1-2-OT the minimum leakage can be explicitly computed to be $\frac{1}{2}$ bit. The same leakage is found for NL-box, since NL-box and 1-2-OT are locally equivalent [WW05b]. It follows that the bare correctness of a protocol for these two primitives implies that in average an extra $\frac{1}{2}$ bit is leaked towards each player. This bound is tight since there are embeddings leaking only $\frac{1}{2}$ bit. This is a stronger impossibility result than the ones described by [Lo97] since they assume perfect/statistical privacy against one party while our approach only assumes correctness. Both approaches apply even against QHBC adversaries. Similarly to 1-2-OT and SAND((denoting an additive secret-sharing generation of the bit-product xy without non-signaling property), we find the minimum leakage for Rabin OT (ROT^r) where r stands for the length of the string sent. When $r = 1$ (i.e. the standard Rabin bit-OT) the minimum leakage is about 0.311 bit, and for $r > 1$, the leakage approaches 1 exponentially in r. It follows that any correct implementation of ROT^r trivializes as r increases because the sender gets asymptotically all information about whether or not the bit sent has been received by Bob.

Furthermore, we show that a lower bound on the leakage of ROT^r also applies to string 1-2-OT (denoted by 1-2-OT^r where r is the length of the strings), due to the fact that it "contains" ROT^r. Finally, we lower-bound the leakage of the noisy version of 1-2-OT for noise rate $p < 0.15$.

1.3.3 Two-Party Cryptography from Limited Resources

A super-embedding of a primitive represents a protocol where Alice and Bob have the full control over the environment. Knowing that any super-embedding of a non-trivial primitive leaks information, it is tempting to ask what can be implemented without leakage at the presence of a trusted third party, in the case where its correlation with the players is limited. We model such protocols by pure states shared between the players and the environment, where Alice and Bob only have access to their parts and the uncertainty about the state of the environment from each player's perspective is upper-bounded. We show that in such a model, any (not necessarily correct) non-leaking implementation of any primitive is private. Notice that this statement does not follow immediately from the definition of a non-leaking implementation, since such an implementation might allow a player to get arbitrary information of her/his choice unless it lowers the uncertainty about the other party's output below $H(Y|X)$ on Alice's side and $H(X|Y)$ on Bob's side. Consequently, we show that a "hard" primitive cannot be implemented without leakage with just one call to the ideal functionality for an "easier" one.

1.3.4 Composability of Quantum Protocols

Finally, we look at another aspect of two-party quantum protocols: their ability to compose against quantum honest-but-curious adversaries (QHBC). In order to guarantee composability, the functionality of a quantum protocol should be modeled by some classical ideal functionality. An ideal functionality is a classical description of what the protocol achieves independently of the environment in which it is executed. If a protocol does not admit such a description then it can clearly not be used in any environment while keeping its functionality, and such a protocol would not compose securely in all applications. In particular, in this thesis we investigate composability of non-trivial quantum protocols. A super-embedding of $P_{X,Y}$ is called *trivial* if both parties can access at least the same amount of information about the functionality as it is possible in some classical protocol for $P_{X,Y}$ in the HBC model. Otherwise, it is said to be *non-trivial*. A quantum protocol is non-trivial if its bipartite purification results in a non-trivial super-embedding. We show that no non-trivial quantum protocol composes freely even if the adversary is restricted to be honest-but-curious. No ideal functionality, even with an uncountable set of rules, can fully characterize the behavior of a quantum protocol in all environments. This is clearly another severe limit to the cryptographic power of two-party quantum protocols.

It is not too difficult to show that any trivial embedding can be implemented by a quantum protocol that composes against QHBC adversaries. In the other direction, let $|\psi(\pi)\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a non-trivial super-embedding of $P_{X,Y}$ corresponding to the bipartite purification of quantum protocol π. We know that $|\psi(\pi)\rangle$ necessarily leaks information towards a QHBC adversary. Any ideal functionality ID_π for protocol π trying to account for honest-but-curious behaviors should allow to simulate all measurements applied either in $\mathcal{H}_A$ or $\mathcal{H}_B$ through an appropriate call to ID_π. One way to do this is to define ID_π by a function $[0..1] \times [0..1] \mapsto [0..1] \times [0..1]$ where $\mathsf{ID}_\pi(0,0)$ corresponds to the honest behavior on both sides: $\mathsf{ID}_\pi(0,0) = (x,y)$ with probability $P_{X,Y}(x,y)$ where (x,y) is encoded as a pair of real numbers. Other inputs to the ideal functionality allow for the simulation of different strategies mounted by the QHBC adversary. In its most general form, an ideal functionality could have an uncountable set of possible inputs in order to allow the simulation of all QHBC adversaries. We show that even allowing for these general ideal functionalities, composed non-trivial protocols cannot be modeled by one single ideal functionality. It means that for a protocol Π calling N times any non-trivial sub-protocol π , there is a QHBC strategy that cannot be modeled by arbitrarily many calls of ID_π, each of them acting locally on a single copy of π.

In order to achieve this, we provide a generic example of such a protocol. Protocol Π produces, as output, a real-value p that we call *payoff*. The payoff p represents how well the adversary can compare, without error, two factors of product states extracted from the N executions of protocol π. From a result of [KKB05], the product states are constructed in such a way that no individual measurement can do as well as the best coherent measurement. It follows that the payoff corresponding to any adversary restricted to deal with π through any ideal functionality would necessarily be lower than the one an adversary

applying coherent strategies on both parts of the product state could get. This implies that no ideal functionality for π would ever account for all QHBC strategies in Π. Moreover, the advantage of coherent strategies over individual ones can be made constant. The result follows.

1.4 Outline of the Thesis

In Chapter 2, we introduce mathematical concepts and cryptographic and information-theoretic notions and results used throughout the thesis. We define, motivate, and analyze the generality of modeling two-party quantum protocols by (super-)embeddings in Chapter 3. In Chapter 4, we define leakage of (super-)embeddings and show that only trivial primitives admit non-leaking (super-)embeddings. We also show that conversely, any non-trivial primitive has an embedding that does not trivialize it. These properties establish the relevance of the model. In Chapter 5, we explicitly find the minimum leakage of 1-2-OT, SAND, ROT^r, and 1-2-OT^r. In Chapter 6 we analyze the scenario where the two players are allowed to use a trusted third party, modeled by the state of the environment. In Chapter 7 we show that non-trivial two-party quantum protocols do not compose even against honest-but-curious adversaries. Finally, in Chapter 8 we discuss the possible directions for future research and open questions.

1.5 Related Work

Our approach allows for quantifying the minimum amount of leakage whereas standard impossibility proofs as the ones of [LC97, May97, Lo97, AKSW07] do not in general provide such quantification since the latter results assume privacy on one side in order to show that the protocol must be totally insecure on the other. By contrast, we derive lower bounds for the leakage of any correct implementation. At the first glance, our approach seems contradictory with standard impossibility proofs since embeddings leak the same amount towards both parties. To resolve this apparent paradox it suffices to observe that in the previous approach only the adversary purified its actions whereas in our case both parties do. If a honest player does not purify his actions then some leakage may be lost by the act of irreversibly and unnecessarily measuring some of his quantum registers.

In particular, our model also captures the scenario considered in [Col07], where Alice and Bob also compute the desired functionality by measuring their respective parts of a pure bipartite state in a fixed basis. [Col07] shows that in any correct implementation of certain primitives of the forms (XZ, YZ) or (XZ, Y), where $Z := f(X, Y)$, a honest-but-curious player can access more information about the other party's output than it is available through the ideal functionality. Unlike [Col07], in our work we deal with the fully general class of bipartite probability distributions and show that only the trivial ones can be implemented securely in the QHBC model. Furthermore, we introduce a

quantitative measure of protocol-insecurity that lets us answer which embedding allows the least effective cheating in the model of [Col07].

Another view of privacy of quantum protocols is presented in [Kla04]. Therein, privacy is expressed in terms of a quantity, called *privacy loss*, with the classical analogue first introduced in [ByCKO93]. It is defined to be the supremum of the amount of extra information that a quantum protocol provides to a cheating party given his/her honest output. Using the terminology introduced in our work, allowing a protocol to have non-zero privacy loss means to relax the requirement of correctness in super-embeddings. [Kla04] shows that there is a quantum protocol for the disjointness problem with quantum privacy loss exponentially lower than in any classical protocol. Furthermore, the paper points out surprising trade-offs between privacy loss and communication complexity, by showing that for the identified minimum problem, a tiny increase in the privacy loss reduces the communication cost exponentially. Both of these, undoubtedly very interesting results suggest to study quantum privacy loss deeper and for more general primitives, as well as how it relates to leakage defined in our work, which is the minimum amount of extra information about Alice's state divulged to Bob without requiring him to receive his honest output.

Chapter 2

Preliminaries

2.1 Notation and Basic Tools

In this chapter we introduce the notation and give a brief overview of the mathematical tools used throughout the thesis.

Most logarithms are to the base 2, which we denote by $\log(\cdot)$. When needed, the natural logarithm is denoted by $\ln(\cdot)$. Shannon binary entropy $H(p, 1-p) := -p\log p - (1-p)\log(1-p)$ is denoted by $h(p)$. By $A^\dagger$ we denote the complex adjoint of an operator A. By $\mathbb{C}^{n\times n}$ we denote the set of $n \times n$ complex matrices. The operator norm $\|T\|_\infty$ of an operator $T \in \mathbb{C}^{n\times n}$ is its largest singular value. *Trace norm* of an operator T is defined by $\|T\|_1 := \sum_i \sigma_i$, where σ_i denotes a singular value of T.

The following well-known inequality is important in analyzing convex and concave functions:

Lemma 2.1 (Jensen's inequality) *Let $f : \mathbb{R} \to \mathbb{R}$ be a convex function and let $x_1, \ldots, x_n \in \mathbb{R}$. Let $0 \le \alpha_1, \ldots, \alpha_n \le 1$ such that $\sum_{i=1}^n \alpha_i = 1$. Then*

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

For concave functions the inequality is in the opposite direction.

2.2 Probability Theory

For a discrete probability space (Ω, P) we denote by $P[\epsilon]$ the probability of an event $\epsilon \subseteq \Omega$, and by P_X the probability distribution of a random variable $X : \Omega \to \mathcal{X}$ for a finite set $\mathcal{X}$. We commonly define (Ω, P) implicitly by specifying the probabilities of the events from Ω for a given random variable. For two random variables with the joint probability distribution $P_{X,Y}$, the conditional probability distribution is defined by $P_{X|Y=y}(x) := \frac{P_{X,Y}(x,y)}{P_Y(y)}$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that $P_Y(y) > 0$. We denote the expected value of a random variable X by $\mathbb{E}(X)$.

The following inequality relates the probability of a random variable X taking a value larger than a constant to its expected value.

Lemma 2.2 (Markov's inequality) *For a random variable X defined on $\mathbb{R}_0^+$,*

$$\Pr[X \geq a] \leq \frac{\mathbb{E}(X)}{a}.$$

Proof. Assume that $\Pr[X \geq a] > \frac{p}{a}$. Then, $\mathbb{E}(X) > \frac{p}{a} \cdot a + (1 - \frac{p}{a}) \cdot 0 = p$. By setting $p \geq \mathbb{E}(X)$, we get a contradiction. □

2.3 Secure Two-Party Computation

All security questions we ask are with respect to *(quantum) honest-but-curious* adversaries. In the classical honest-but-curious adversarial model (HBC), the parties follow the instructions of a protocol but store all information available to them. Quantum honest-but-curious adversaries (QHBC), on the other hand, are allowed to behave in an arbitrary way that cannot be distinguished from their honest behavior by the other player. More on this type of adversaries can be found in Section 2.5.3. In this section we introduce several universal cryptographic two-party primitives. By universality we mean that any two-party secure function evaluation can be reduced to them. We present the completely randomized versions where players do not have inputs but receive randomized outputs instead. Throughout this thesis, the term *primitive* usually refers to the joint probability distribution defining its randomized version. The randomized and standard versions are easily seen to be equivalent for standard cryptographic primitives, in the sense that each of them can be transformed to the other one by local operations and noiseless communication. The randomized version of a given functionality can be implemented from the non-randomized one trivially, by letting the players pick their inputs at random. In the transformation from the randomized to the non-randomized version of a given primitive, the outputs in the randomized version are used for one-time pad encryption of inputs in the protocol for the non-randomized case. As an example, we take a functionality called *one-out-of-two oblivious transfer* (1-2-OT) [Wie83, EGL82], where sender Alice sends two bits to receiver Bob who chooses which of them he receives. The specification of the functionality requires that Alice does not learn which bit did Bob choose and at the same time, Bob does not get any information about the other one of Alice's bits. The randomized version of 1-2-OT is the following primitive: For $x_0, x_1, c, y \in \{0,1\}$, $P^{\text{OT}}_{X,Y}((x_0,x_1),(c,y)) = 1/8$ if and only if $y = x_c$. Assume that Alice and Bob share a blackbox for the randomized version of 1-2-OT. The following protocol [WW05b] for the standard version of 1-2-OT (with inputs) is then secure:

1. Bob picks the selection bit C and sends $C \oplus c$ to Alice.

2. Alice picks her input bits X_0 and X_1, and sends $(z_0, z_1) = (X_{C\oplus c} \oplus x_0, X_{C\oplus c\oplus 1} \oplus x_1)$ to Bob.

3. Bob computes $X_C = z_c \oplus x_c$.

Such a protocol is secure against Alice, since the message sent by Bob is a one-time pad of his selection bit B. This is due to the fact that in the randomized version of 1-2-OT, Alice does not get to know b. The protocol is also secure against Bob because in the message sent by Alice, $X_{B\oplus 1}$ is one-time padded with $x_{1\oplus b}$ which Bob does not learn in the secure implementation of randomized 1-2-OT.

It follows that the existence of secure protocols in the (quantum) honest-but-curious model for either version is equivalent to the existence of secure protocols for the other one.

Besides 1-2-OT, in this thesis we study the randomized versions of the following cryptographic primitives:

String Rabin OT (ROT^r) [Rab81]: Alice sends a random string of r bits to Bob who receives it with probability $1/2$, otherwise he receives a random string. Bob knows which of the two events happened but Alice does not learn any information about whether Bob has received the string she sent.

One-out-of-two String OT (1-2-OT^r) [Wie83, EGL82] Alice sends two random r-bit strings to Bob who decides which of them he receives. Bob does not learn any information about the other one of Alice's strings and Alice does not learn which of the strings has been received by Bob.

Additive sharing of AND (SAND) [PR94] Alice and Bob choose their respective input bits x and y, and receive the output bits a resp. b such that $a \oplus b = x \wedge y$ and $\Pr[a = 0] = 1/2$. They do not get any other information.

Noisy one-out-of-two OT (1-2-OT_p) Alice sends two bits to Bob who decides which of them he wants to receive. The selection bit is transmitted to him over a noisy channel with noise rate p. Bob does not learn any information about the other one of Alice's bits and Alice does not learn any information about Bob's selection bit.

The description of the randomized alternatives of the primitives defined above follows:

String Rabin OT (ROT^r): For $x \in \{0,1\}^r$ and $y \in \{0,1\}^r \cup \{\perp\}$:

$$P^{\text{ROT}^r}_{X,Y}(x,y) = \begin{cases} 2^{-r-1} & \text{if } x = y \text{ or } y = \perp, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to an execution of Rabin OT of a random binary string of length r.

One-out-of-two OT (1-2-OT): For $x_0, x_1, y, c \in \{0,1\}$:

$$P^{\text{OT}}_{X,Y}((x_0,x_1),(c,y)) = \begin{cases} \frac{1}{8} & \text{if } y = x_c, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution for the execution of one-out-of-two OT upon random input bits.

One-out-of-two String OT (1-2-OT^r): For $x_0, x_1, y \in \{0,1\}^r$ and $c \in \{0,1\}$, let

$$P^{\text{OT}^r}_{X,Y}((x_0,x_1),(c,y)) = \begin{cases} 2^{-2r-1} & \text{if } y = x_c, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to an execution of one-out-of-two r-bit string OT upon random inputs.

Additive Sharing of AND (SAND) For $x, y, a, b \in \{0,1\}$:

$$P^{\text{NL}}_{X,Y}((x,a),(y,b)) = \begin{cases} \frac{1}{8} & \text{if } xy = a \oplus b, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to the generation of an additive sharing for the AND of two random bits.

Noisy one-out-of-two OT (1-2-OT$_p$): For $x_0, x_1, y, c \in \{0,1\}$ and $p \in (0, 1/2)$:

$$P^{\text{OT}_p}_{X,Y}((x_0,x_1),(c,y)) = \begin{cases} \frac{1-p}{8} & \text{if } y = x_c, \\ \frac{p}{8} & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to an execution of one-out-of-two OT where the selected bit is received through a binary symmetric channel with error rate p.

Primitive $P^{\text{OT}}_{X,Y}$ is universal i.e., sufficient for any secure function evaluation, according to Kilian [Kil88]. Universality of ROT^r is implied by [Cré87], showing that ROT is equivalent to $P^{\text{OT}}_{X,Y}$. Universality of SAND follows from [WW05b] where its equivalence with 1-2-OT has been shown. Finally, universality of 1-2-OT$_p$ for $p < 0.22$ has been proven by [DKS99].

2.4 Classical Information Theory

In this section we introduce several information theoretical quantities. One of the very basic concepts of information theory is the entropy of a random variable, i.e. the measure of uncertainty associated to the given random variable. The most well-known of such measures is *Shannon entropy*.

Definition 2.1 (Shannon entropy [Sha48]) *The Shannon entropy of a discrete random variable X taking the values in $\{x_1, \ldots, x_n\}$ is*

$$H(X) = -\sum_{i=1}^{n} P_X(x_i) \log P_X(x_i).$$

Sometimes the notation $H(p_1, \ldots, p_n) = H(X)$ for $p_i := P_X(x_i)$ is used. As a function of n arguments, H is continuous, symmetric, and strictly concave, with the maximum $\log n = H(1/n, \ldots, 1/n)$.

Conditional entropy $H(X|Y)$ and mutual information $I(X;Y)$ are two standard information theoretical quantities, expressing how much entropy is left about X given Y, and how much information about X is available given Y, respectively. The definition implies that $I(X;Y)$ is symmetric, i.e. $I(X;Y) = I(Y;X)$.

Definition 2.2 Conditional entropy *of a random variable X given a random variable Y is* $H(X|Y) := H(X,Y) - H(Y)$. Mutual information *between random variables X and Y is* $I(X;Y) := H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y)$.

Definition 2.3 *Conditional mutual information between two random variables X and Y given Z is defined as*

$$I(X;Y|Z) := H(XZ) + H(YZ) - H(XYZ) - H(Z).$$

The following definition describes correlations in the sequence of random variables often related to natural random processes.

Definition 2.4 *A* Markov chain *is a sequence of random variables $X_0, \ldots, X_n$ with countable probability spaces, satisfying for $n \geq 0$*

$$\Pr[X_{n+1} = x_{n+1} | X_n = x_n, \ldots, X_0 = x_0] = \Pr[X_{n+1} = x_{n+1} | X_n = x_n].$$

For three random variables X, Y, Z forming a Markov chain (i.e. satisfying $\Pr[X = x|Y = y, Z = z] = \Pr[X = x|Y = y]$), we use the notation $X \leftrightarrow Y \leftrightarrow Z$. In terms of information theory, the Markov property of a triple of random variables can be expressed as follows:

$$X \leftrightarrow Y \leftrightarrow Z \Leftrightarrow H(X|YZ) = H(X|Y).$$

Equivalently, we can write

$$I(X;Z|Y) = H(XY) - H(Y) - (H(XZY) - H(YZ)) = H(X|Y) - H(X|YZ) = 0.$$

The following definition introduces a random variable describing the correlation between two random variables X and Y.

Definition 2.5 (Dependent part [WW04]) *For two random variables X, Y, let $f_X(x) := P_{Y|X=x}$. Then the* dependent part of X with respect to Y *is defined as $X \searrow Y := f_X(X)$.*

The dependent part $X \searrow Y$ is the minimum random variable computed from X such that $X \leftrightarrow X \searrow Y \leftrightarrow Y$ is a Markov chain [WW04]. It means that for any random variable $K = f(X)$ such that $X \leftrightarrow K \leftrightarrow Y$ is a Markov chain, there exists a function g such that $g(K) = X \searrow Y$. Immediately from the definition we get several other properties of $X \searrow Y$ [WW04]: $H(Y|X \searrow Y) = H(Y|X)$, $I(X;Y) = I(X \searrow Y; Y)$, and $X \searrow Y = X \searrow (Y \searrow X)$. The second and the third formula yield that $I(X;Y) = I(X \searrow Y; Y \searrow X)$.

The notion of dependent part has been further investigated in [FWW04, IMNW04, WW05a]. Wullschleger and Wolf have shown that quantities $H(X \searrow Y|Y)$ and $H(Y \searrow X|X)$ are monotones for two-party protocols [WW05a]. That is, none of these values can increase during classical two-party protocols. In particular, if Alice and Bob start without sharing any non-trivial cryptographic resource then classical two-party protocols can only produce (X, Y) such that: $H(X \searrow Y|Y) = H(Y \searrow X|X) = 0$, since $H(X \searrow Y|Y) > 0$ if and only if $H(Y \searrow X|X) > 0$ [WW05a]. Conversely, any primitive satisfying $H(X \searrow Y|Y) = H(Y \searrow X|X) = 0$ can be implemented securely in the HBC model. One such implementation is the following:

1. Bob samples a value from the distribution $P_{X \searrow Y}$ and obtains $P_Y^{x'}$ which is a distribution over $\mathcal{Y}$ conditioned on Alice's output. He sends the index x' of $P_Y^{x'}$ to Alice and samples his output y from $P_Y^{x'}$.

2. Alice picks her output x according to $P_{X|f_X(x)=P_Y^{x'}}$.

We call primitives satisfying $H(X \searrow Y|Y) = 0$ *trivial*.

2.5 Quantum Information Theory

In this section we introduce the basic notions in quantum information theory that we use in this thesis. For further reading on the topic, we refer to [NC00]. The state of a quantum-mechanical system in a Hilbert space $\mathcal{H}$ is described by a *density operator* ρ which is positive-semidefinite ($\rho = \rho^\dagger$, all eigenvalues are non-negative) such that $\mathrm{tr}(\rho) = 1$. A state ρ of a system in $\mathcal{H}$ is called *pure* if it can be written in the form $\rho = |\psi\rangle\langle\psi|$ for a unit vector $|\psi\rangle \in \mathcal{H}$. If a bipartite system is considered, we denote the subspaces of the associated Hilbert space held by Alice and Bob by $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Their respective registers are then denoted by A and B. Throughout this thesis, a state of $\mathcal{H}_A$ is denoted by $|\psi\rangle^A$ or ρ_A if needed. To simplify the notation, for pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ we sometimes use $|\psi_0, \psi_1\rangle$ or $|\psi_0\rangle|\psi_1\rangle$ instead of $|\psi_0\rangle \otimes |\psi_1\rangle$.

A *positive operator-valued measurement (POVM)* on $\mathcal{H}$ is a family $\mathcal{M} = \{M_x\}_{x \in X}$ of positive-semidefinite operators such that $\sum_{x \in X} M_x = \mathbb{I}_{\mathcal{H}}$. The probability distribution of the outcomes of a POVM $\mathcal{M}$ applied to state ρ is $P_X(x) = \mathrm{tr}(M_x \rho)$. In general, the evolution of a quantum system (involving e.g. unitary transforms, measurements, or noise application) in a state $\rho \in \mathbb{C}^{n \times n}$ can be described by a *quantum operation* $\mathcal{E} : \mathbb{C}^{n \times n} \to \mathbb{C}^{m \times m}$ which is a *completely positive* operator. Complete positivity means that for each $k \in \mathbb{N}$, the operator $\mathbb{I}_k \otimes \mathcal{E} : \mathbb{C}^{k \times k} \otimes \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k} \otimes \mathbb{C}^{m \times m}$ is positive. A quantum operation $\mathcal{E}$ can always be expressed in the *Kraus operator* sum representation which is

$$\mathcal{E}(\rho) = \sum_{k=1}^{n} A_k \rho A_k^\dagger$$

for (Kraus) operators A_k satisfying $\sum_{k=1}^{n} A_k^\dagger A_k = \mathbb{I}$.

A quantum operation on a bipartite system is called separable if the Kraus operators are all tensor products of two factors. The class of separable operations extends the *LOCC*-class (LOCC stands for *local operations and classical communication*). In a bipartite system, LOCC-operations are exactly those that can be performed by two players, each of them holding one part of the system, that are allowed to communicate only classically. The implementation of such an operation proceeds as follows: In each half-round, one player applies some operation on his/her part of the system and communicates the result classically to the other party. It has been shown by [BDF$^+$99] that quantum operations in the LOCC-class form a strict subset of the set of separable operations.

2.5.1 Quantum State Distingushability

In quantum protocols, the amount of accessible information depends on the ability of a player to identify a quantum state from a given set. For quantifying the distinguishability of quantum states, the following two measures are commonly used (for a broader survey on the topic see [FvdG99]). The *Kolmogorov distance* (also *trace norm distance*) $K(\rho_0, \rho_1)$ between two states ρ_0 and ρ_1 is defined by

$$K(\rho_0, \rho_1) := \max_{\mathcal{E} \in \mathcal{M}} K(p_0(\mathcal{E}), p_1(\mathcal{E})), \tag{2.1}$$

where $\mathcal{M}$ denote the set of all POVMs, $p_0(\mathcal{E}) = (p_1^{0,\mathcal{E}}, \ldots, p_m^{0,\mathcal{E}})$ and $p_1(\mathcal{E}) = (p_1^{1,\mathcal{E}}, \ldots, p_m^{1,\mathcal{E}})$ are the probabibility distributions of the outcomes of the measuremet $\mathcal{E}$ applied to ρ_0 and ρ_1, respectively, and $K(p_0(\mathcal{E}), p_1(\mathcal{E}))$ denotes the Kolmogorov distance of two probability distributions defined by

$$K(p_0(\mathcal{E}), p_1(\mathcal{E})) := \frac{1}{2} \sum_{i=1}^{m} |p_i^{0,\mathcal{E}} - p_i^{1,\mathcal{E}}|.$$

According to [FvdG99], $K(\rho_0, \rho_1)$ can equivalently be expressed as:

$$K(\rho_0, \rho_1) = \frac{1}{2} \|\rho_0 - \rho\|_1. \tag{2.2}$$

The statement can be proven by an explicit construction of the measurement $\mathcal{E}$ yielding the largest distance between the distributions $p_0(\mathcal{E})$ and $p_1(\mathcal{E})$, which is actually a projective measurement with probability 1 of a conclusive outcome (Helstrom [Hel76]).

The Kolmogorov distance between two states is closely related to the highest achievable probability of the right identification of a state sampled uniformly at random from the given pair of states. For such a probability, denoted by $q_{\text{corr}}(\rho_0, \rho_1)$, we get

$$q_{\text{corr}}(\rho_0, \rho_1) = \frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_1}{4}.$$

The claim easily follows from the equivalence between (2.1) and (2.2).

The *fidelity* (also *Bhattacharyya coefficient*) $B(\rho_0, \rho_1)$ between two states ρ_0 and ρ_1 is defined by

$$B(\rho_0, \rho_1) := \min_{\mathcal{E} \in \mathcal{M}} B(p_0(\mathcal{E}), p_1(\mathcal{E})),$$

where $\mathcal{M}$ denotes the set of POVMs and

$$B(p_0(\mathcal{E}), p_1(\mathcal{E})) := \sum_{i=1}^{m} \sqrt{p_i^{0,\mathcal{E}} p_i^{1,\mathcal{E}}}.$$

Equivalently, $B(\rho_0, \rho_1)$ can be expressed as [FvdG99]:

$$B(\rho_0, \rho_1) = \operatorname{tr} \sqrt{\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}},$$

where $\sigma = \sqrt{\rho}$ denote any positive-semidefinite matrix such that $\sigma^2 = \rho$. In the special case, for pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ we get

$$B(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = |\langle\psi_0|\psi_1\rangle|.$$

Kolmogorov distance and Bhattacharyya coefficient are related via the following inequalities [FvdG99]:

$$1 - B(\rho_0, \rho_1) \leq K(\rho_0, \rho_1) \leq \sqrt{1 - B^2(\rho_0, \rho_1)},$$

with the equality between the middle and the right term satisfied for any pair of pure states.

In the case of pure states, $B(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)$ determines the highest achievable probability of unambiguous identification of a state sampled uniformly at random from a given pair of states (which means that no error is allowed but an inconclusive outcome is allowed). Such a probability $q_c(\rho_0, \rho_1)$ can be shown to satisfy [Iva87, Die88, Per88]:

$$q_c(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = 1 - |\langle\psi_0|\psi_1\rangle|.$$

Above, we have seen two examples of the natural limits of state-distinguishability. Note that in the first case, we have specified what is the minimal probability of identification error given that the required probability of a conclusive outcome is 1. In the second example, we give an upper bound on the probability of a conclusive outcome given that the maximal probability of identification error is 0. Sometimes we are interested in the lowest probability of the state-identification error in the case where the probability of a measurement's conclusive outcome is fixed to any value, or on the other hand, we want to know the highest probability of a conclusive outcome given an arbitrary upper bound on the probability of error. The solution for these problems is given by the following lemma.

Lemma 2.3 ([CB98]) *Let the probability of a conclusive outcome and the error-probability of some POVM applied to a state, sampled uniformly at random from a pair of pure states* $(|\psi_0\rangle, |\psi_1\rangle)$*, be denoted by* q_c *and* q_{err}*, respectively. Then*

$$q_{\text{err}} \geq \frac{1}{2}\left(q_c - \sqrt{q_c^2 - (q_c - 1 + |\langle\psi_0|\psi_1\rangle|)^2}\right).$$

2.5.2 Von Neumann Entropy and Holevo Bound

Analogously to quantifying the uncertainty about a random variable by Shannon entropy, we can express the uncertainty present in a state of a quantum system in terms of *Von Neumann entropy*. Formally, the Von Neumann entropy of a state ρ is defined by

$$S(\rho) := -\operatorname{tr}(\rho \log \rho) = -\sum_{\lambda \in \sigma(\rho)} \lambda \log \lambda.$$

Von Neumann entropy is non-negative, takes the value 0 only for pure states, and is invariant under unitary transforms. It is strictly concave which means

that for $\{\gamma_i\}_{i=1}^k$ all positive and states $\{\rho_i\}_{i=1}^k$ we have

$$S\left(\sum_{i=1}^{k}\gamma_i\rho_i\right) \geq \sum_{i=1}^{k}\gamma_i S(\rho_i)$$

with the equality holding if and only if $\rho_1 = \rho_2 = \cdots = \rho_k$.

For a state ρ_A of $\mathcal{H}_A$ we sometimes denote $S(\rho_A)$ by $S(A)$. For a bipartite system in a joint pure state $|\psi\rangle^{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ we get that $S(A) = S(B)$, where by the states of the systems $\mathcal{H}_A$ and $\mathcal{H}_B$ we always mean reduced density operators $\mathrm{tr}_B\,|\psi\rangle\langle\psi|$ and $\mathrm{tr}_A\,|\psi\rangle\langle\psi|$, respectively. The claim follows from the fact that a pure bipartite state $|\psi\rangle \in \mathcal{H}_n \otimes \mathcal{H}_n$ can be written in the Schmidt form: $|\psi\rangle = \sum_{i=1}^n \sqrt{\lambda_i}|e_i\rangle|f_i\rangle$, yielding that $\rho_A = \sum_{i=1}^n \lambda_i|e_i\rangle\langle e_i|$, $\rho_B = \sum_{i=1}^n \lambda_i|f_i\rangle\langle f_i|$, and therefore, $S(A) = S(B) = H(\lambda_1, \ldots, \lambda_n)$.

The mutual information $S(A;B)$ between quantum systems A and B and the conditional Von Neumann entropy are defined similarly to their classical counterparts:

- $S(A|B) := S(A,B) - S(B)$, and
- $S(A;B) := S(A) + S(B) - S(A,B) = S(A) - S(A|B) = S(B) - S(B|A) = S(B;A)$.

In general, $S(A;B)$ and $S(A|B)$ are measures of information which are not easy to interpret. For instance, the conditional Von Neumann entropy $S(A|B)$ is negative when the system $\mathcal{H}_A \otimes \mathcal{H}_B$ is in a pure state but $\mathcal{H}_A$ alone is not. In this case, $S(A;B) > S(A)$. This is clearly impossible for their classical counterparts $H(X|Y)$ and $I(X;Y)$. Only relatively recently, an intuitive operational interpretation of conditional Von Neumann entropy has been given in the context of state merging [HOW07]. However, these quantum measures of information allow for a simple interpretation when the joint system AB has one of its subsystem classical while the other is quantum. Such states are called *cq*-states for *classical→quantum states*. Such a state with the classical register storing the values of random variable X is of the following form:

$$\rho_{XB} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|\,.$$

Cq-states are the ones describing a setting where quantum information is available about a classical random variable. For cq-state ρ_{XB}, the conditional Von Neumann entropy $S(X|B)$ is always non-negative and expresses the expected amount of classical information required to recover X from quantum state B provided many independent copies [Win99, DW03].

Let $R = \{(P_X(x), \rho_x\}_{x\in\mathcal{X}}$ be a source that produces ρ_x with probability $P_X(x)$. The quantum state produced by R is $\rho_R = \sum_{x\in\mathcal{X}} P_X(x)\rho_x$. The Holevo bound upper-bounds the amount of classical information about X that can be obtained by measuring ρ_R:

Theorem 2.1 (Holevo bound) *Let Y be the random variable describing the outcome of some measurement applied to ρ_R for $R = \{(P_X(x), \rho_x\}_{x\in\mathcal{X}}$. Then,*

$$I(X;Y) \leq S(\rho_R) - \sum_x P_X(x) S(\rho_x),$$

where the equality can be achieved if and only if $\{\rho_x\}_{x\in\mathcal{X}}$ are simultaneously diagonalizable.

The following statement shows that if the mutual information between the two registers of a cq-state $\rho = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$ is low, then the states ρ_x must be highly concentrated around the average state of the quantum register.

Theorem 2.2 (Average Encoding Theorem [KNTsZ01]) *Let B denote a quantum system storing the quantum part of a cq-state $\sigma = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_x$. Let $\rho := \sum_x P_X(x)\rho_x$. Then*

$$\sum_x P_X(x) \|\rho - \rho_x\|_1 \leq \sqrt{2(\ln 2) S(X;B)}.$$

2.5.3 Purification

The last notion we introduce in this section is the notion of purification of quantum states.

Almost all impossibility results in quantum cryptography rely upon a quantum honest-but-curious behavior of the adversary that we denote by QHBC. This behavior consists in *purifying* all actions of the honest players. Purifying means that instead of invoking classical randomness from a random tape, for instance, the adversary relies upon quantum registers holding all random bits needed. The operations to be executed from the random outcome are then performed quantumly without fixing the random outcomes. For example, suppose a protocol instructs a party to pick with probability p state $|\phi_0\rangle^C$ and with probability $1-p$ state $|\phi_1\rangle^C$ before sending it to the other party through the quantum channel C. The purified version of this instruction looks as follows: Prepare a quantum register in state $\sqrt{p}|0\rangle^R + \sqrt{1-p}|1\rangle^R$ holding the random process. Add a new register initially in state $|0\rangle^C$ before applying the unitary transform $U : |r\rangle^R|0\rangle^C \mapsto |r\rangle^R|\phi_r\rangle^C$ for $r \in \{0,1\}$ and send register C through the quantum channel and keep register R.

From the receiver's point of view, the purified behavior is indistinguishable from the one relying upon a classical source of randomness because in both cases, the state of register C is $\rho = p|\phi_0\rangle\langle\phi_0| + (1-p)|\phi_1\rangle\langle\phi_1|$. All operations invoking classical randomness can be purified similarly [LC97, May97]. The result is that measurements are postponed as much as possible and only extract information required to run the protocol in the sense that only when both players need to know a random outcome, the corresponding quantum register holding the random coin will be measured. If both players purify their actions then the joint state at any point during the execution will remain in pure state, until the very last step of the protocol when the outcomes are measured.

Chapter 3

Quantum Embeddings and Two-Party Protocols

3.1 Two-Party Protocols and their Super-Embeddings

We interpret a joint probability distribution $P_{X,Y}$ as *cryptographic primitive* providing X to honest player Alice and Y to honest player Bob. We consider cryptographic primitives with no inputs, which simplifies our treatment while remaining general since any quantum protocol with classical inputs can be run with all its inputs in superposition. It is easy to verify that the leakage (defined in Section 4.2) of a primitive with inputs in superposition corresponds to the leakage of the same primitive when its inputs are chosen according the probability distribution induced by the superposition. Our lower bounds for the leakage of cryptographic primitives with inputs (in Section 5) are derived for the natural setting of random and uniform inputs.

Let us first look at what we mean by saying that a protocol π correctly implements $P_{X,Y}$. The first natural requirement is that once the actions of π are purified by both players, measurements of registers A and B in the computational basis[1] provide joint outcome $(X,Y) = (x,y)$ with probability $P_{X,Y}(x,y)$.

Protocol π can use extra registers A' and B' on Alice's and Bob's side respectively providing them with (quantum) working space. The purification of all actions of π therefore generates a pure state $|\psi_\pi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$. However, protocol π implementing primitive $P_{X,Y}$ does not instruct the players to measure the extra registers $A'B'$ since the primitive implemented by π would be $P_{XYX'Y'}$ rather than $P_{X,Y}$ where X' and Y' denote the outcomes when A' and B' are measured. As registers A' and B' remain unmeasured in π, honest players could measure them to their liking. As the second requirement, we expect from a correct π that whatever measurements are applied to A' and B', it still produces outcome (x,y) according to $P_{X,Y}$ when measuring A and B. Formally, a correct protocol π for $P_{X,Y}$ should satisfy $S(X;YB') = S(Y;XA') = I(X;Y)$. This leads to our definition of correctness.

[1] It is clear that every quantum protocol for which the final measurement providing (x,y) with distribution $P_{X,Y}$ to the players is not in the computational basis can be transformed into a protocol of the described form by two additional local unitary transformations.

Definition 3.1 *A protocol π for $P_{X,Y}$ is* correct *if it satisfies $S(X;YB') = S(XA';Y) = I(X;Y)$ where A' and B' denote the extra working registers of Alice and Bob, respectively and $S(X;YB')$ is the von Neumann mutual information of Bob's quantum registers provided he measures $\mathcal{H}_B$ in order to get Y.*

In other words, measuring the working-space register of one party involved in a correct protocol π for $P_{X,Y}$ should not change the primitive implemented by π. An equivalent way of defining correct protocols is provided by the following lemma, where for quantum register A and classical random variables X and Y, $A \leftrightarrow X \leftrightarrow Y$ being a Markov chain means that $S(Y;A|X) = 0$, i.e. given X, the quantum register A does not give any information about Y.

Lemma 3.1 *A protocol π for $P_{X,Y}$ is correct if and only if $A' \leftrightarrow X \leftrightarrow Y$ and $X \leftrightarrow Y \leftrightarrow B'$ are Markov chains.*

Proof. $X \leftrightarrow Y \leftrightarrow B'$ is a Markov chain if and only if $S(X;B'|Y) = 0$. Equivalently,

$$\begin{aligned} 0 &= S(X;B'|Y) = H(XY) + S(YB') - H(Y) - S(XYB') \\ &= (H(X) + S(YB') - S(XYB')) - I(X;Y) = S(X;YB') - I(X;Y). \end{aligned}$$

For the same reason, $A' \leftrightarrow X \leftrightarrow Y$ being a Markov chain is equivalent to $S(XA';Y) = I(X;Y)$. □

It follows that a protocol π is correct if whenever one party learns her output, the extra register owned by this party does not provide any additional information about the other party's output.

In a correct protocol π for $P_{X,Y}$, honest players can always purify all their actions up to the final measurements providing X and Y. The resulting pure state (including extra working registers) is called a super-embedding of $P_{X,Y}$:

Definition 3.2 *The state $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$ is a super-embedding of $P_{X,Y}$ if it can be produced by the purification of some correct protocol for $P_{X,Y}$.*

We give an example of such transformation for a protocol implementing noisy 1-2-OT, with noise rate $p = \sin^2(\pi/8)$.

3.1.1 Correct Protocol for $P_{X,Y}^{\text{OT}_p}$ where $p = \sin^2(\pi/8)$

The following protocol has been suggested by [Amb05]:

1. Suppose Alice encodes her input bits (x_0, x_1) in the following way: $e(0,0) := |0\rangle$, $e(1,1) := |1\rangle$, $e(0,1) := |-\rangle$, $e(1,0) := |+\rangle$. She picks (x_0, x_1) and sends $e(x_0, x_1)$ to Bob.

2. If Bob wishes to receive the first bit of Alice, he measures his bit in the basis $\mathcal{B}_0 := (\cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle, \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle)$. If Bob wants to receive the second bit of Alice, he uses the other Breidbart basis $\mathcal{B}_1 := (\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle)$ to measure his bit.

It is easy to verify that in the protocol above, Bob obtains the correct value of the bit of his choise with probability $\cos^2(\pi/8)$ and also that such a protocol is private – it hides the other bit of Alice and Bob's choice bit perfectly. Even though choosing a different measurement allows Bob to reduce noise to 0 with certain probability, this protocol satisfies at least some condition – privacy, intuitively required from a good implementation of a noisy OT. We show that the protocol from above is correct according to Definition 3.1, by showing that purifying the players' action results into a super-embedding of the implemented functionality:

Purification

1. Set-up: Alice and Bob establish a shared EPR pair $|\Phi^+\rangle$ to replace communication with entanglement.

2. Alice encodes the parity of her bits into an additional register. Bob encodes his selection bit into an additional register. The resulting state shared between them is then $|+\rangle^{A_0}|\Phi^+\rangle^{A_1B_1}|+\rangle^{B_0}$.

3. Alice applies the Hadamard transform on A_1, conditioned on the state of A_0. After this step, the players share:

$$\begin{aligned} & \frac{1}{\sqrt{2}}\left(|0\rangle^{A_0}\left|\Phi^+\right\rangle^{A_1B_1} + |1\rangle^{A_0}\frac{|{+}0\rangle^{A_1B_1} + |{-}1\rangle^{A_1B_1}}{\sqrt{2}}\right)|+\rangle^{B_0} \\ = \; & \frac{1}{\sqrt{2}}\left(|0\rangle^{A_0}\left|\Phi^+\right\rangle^{A_1B_1} + |1\rangle^{A_0}\frac{|0{+}\rangle^{A_1B_1} + |1{-}\rangle^{A_1B_1}}{\sqrt{2}}\right)|+\rangle^{B_0} \end{aligned}$$

4. Bob applies a conditional rotation by $\pm\pi/8$ to B_1: If the state of $|B_0\rangle$ is $|0\rangle$ then he rotates the state of B_1 by $\pi/8$, and if it is $|1\rangle$ then he applies the rotation by $-\pi/8$ to B_1.

5. Alice applies a CNOT (controlled NOT) operation with control register A_1 to A_0, in order to let the state of A_0 encode the value of her first bit instead of the parity of her inputs.

In order to implement the desired functionality, it only remains to measure the players' registers in the computational basis. The final state $|\psi\rangle$ of the protocol above is the following super-embedding of randomized $P_{X,Y}^{\text{OT}_p}$ with $p = \sin^2(\pi/8)$, yielding that such a protocol is correct:

$$\begin{aligned} |\psi\rangle \;=\; & \frac{1}{2\sqrt{2}}\left(|000\rangle^{A_0A_1B_0} + |101\rangle^{A_0A_1B_0}\right)\left(\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle\right)^{B_1} \\ + \; & \frac{1}{2\sqrt{2}}\left(|010\rangle^{A_0A_1B_0} + |001\rangle^{A_0A_1B_0}\right)\left(\cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle\right)^{B_1} \\ + \; & \frac{1}{2\sqrt{2}}\left(|100\rangle^{A_0A_1B_0} + |111\rangle^{A_0A_1B_0}\right)\left(\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\right)^{B_1} \\ + \; & \frac{1}{2\sqrt{2}}\left(|110\rangle^{A_0A_1B_0} - |011\rangle^{A_0A_1B_0}\right)\left(-\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\right)^{B_1}. \end{aligned}$$

On the contrary, we give an example of an "unreasonable" protocol for 1-2-OT (even though it might not seem to be such on the first sight), which is not correct according to our definition.

3.1.2 Incorrect Protocol for 1-2-OT

Consider the following protocol for 1-2-OT:

1. Alice chooses her inputs (x_0, x_1) and Bob chooses the selection bit c.
2. Alice picks a random string $b \in \{0,1\}^n$ and a random sequence of bases $\mathcal{B} \in \{\mathcal{B}_0, \mathcal{B}_1\}^n$, where $\mathcal{B}_0 = (B_{0,0}, B_{0,1}) = (|0\rangle\langle 0|, |1\rangle\langle 1|)$ and $\mathcal{B}_1 = (B_{1,0}, B_{1,1}) = (|+\rangle\langle +|, |-\rangle\langle -|)$. For each $i \in \{1, \ldots, n\}$, she encodes the i-th position b_i of b by B_{i,b_i} and sends B_{i,b_i} to Bob.
3. Bob chooses a random sequence of bases $\mathcal{C} \in \{\mathcal{B}_0, \mathcal{B}_1\}^n$ and for each i, he measures B_{i,b_i} in basis $\mathcal{C}_i$.
4. Alice announces $\mathcal{B}$.
5. Bob constructs sets $S_{\text{good}} := \{i : \ \mathcal{B}_i = \mathcal{C}_i\}$ and $S_{\text{bad}} := \{i : \ \mathcal{B}_i \neq \mathcal{C}_i\}$. If he wants to receive the first bit of Alice ($c = 0$), he sends her $(S_0, S_1) := (S_{\text{good}}, S_{\text{bad}})$ and if he wants to receive Alice's second bit ($c = 1$), he sends her $(S_0, S_1) := (S_{\text{bad}}, S_{\text{good}})$.
6. Alice responds with (z_0, z_1) where $z_0 := x_0 \oplus \bigoplus_{i:i\in S_0} b_i$ and $z_1 := x_1 \oplus \bigoplus_{i:i\in S_1} b_i$.
7. Bob computes $x_c = z_c \oplus \bigoplus_{i:\ i\in S_{\text{good}}} b_i$.

Applying privacy amplification results into a protocol which is secure against Alice. However, it is not even close to being secure on Bob's side, since delaying his measurement in step 3 to the point where Alice announces $\mathcal{B}$ allows him to get the complete information about Alice's inputs. This is also the reason why purifying the players' action does not yield a super-embedding of 1-2-OT – Bob's additional register in such a case enables him to learn both of Alice's bits. Hence, such a protocol is not correct. One might hope that by letting Alice commit to $\mathcal{B}$ instead of sending it plain we get a secure protocol for 1-2-OT. If such a protocol was not correct, it would indicate that our definition of correctness is not well justified. However, such a transformation is not possible, since commitments in the information-theoretic sense do not exist.

Remember, we only consider attacks consisting of an arbitrary measurement applied to the adversary's registers (AA' for dishonest Alice and BB' for dishonest Bob) of a super-embedding in order to access information about the honest party's output, which is how a quantum honest-but-curious (QHBC) adversarial strategy can be translated into an adversarial measurement of a super-embedding.

Notice that the final state of the protocol from Section 3.1.1 implements the desired primitive with no extra registers available to the players. Such a super-embedding of a given primitive is then called an *embedding*.

3.2 Quantum Embeddings

Let $\Theta_{n,m} := \{\theta : \{0,1\}^n \times \{0,1\}^m \to [0 \dots 2\pi)\}$ be the set of functions mapping bit-strings of length $m+n$ to real numbers between 0 and 2π.

Definition 3.3 *For a joint probability distribution $P_{X,Y}$ where $X \in \{0,1\}^n$ and $Y \in \{0,1\}^m$, we define the set*

$$\mathcal{E}(P_{X,Y}) := \left\{ |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B : |\psi\rangle = \sum_{x,y} e^{i\theta(x,y)} \sqrt{P_{X,Y}(x,y)} |x,y\rangle^{AB}, \theta \in \Theta_{n,m} \right\},$$

and call any state $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ a quantum embedding *of the joint probability distribution $P_{X,Y}$.*

Clearly, any $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ produces (X,Y) according $P_{X,Y}$ since the probability $p_\psi(x,y)$ that Alice measures x and Bob measures y in the computational basis is $p_\psi(x,y) = |\langle\psi|x,y\rangle|^2 = P_{X,Y}(x,y)$.

In order to specify a particular embedding one only needs to give the description of the *phase function* $\theta(x,y)$. We denote by $|\psi_\theta\rangle \in \mathcal{E}(P_{X,Y})$ the quantum embedding of $P_{X,Y}$ with phase function θ. The function $\theta(x,y) := 0$ for all $x \in \{0,1\}^n, y \in \{0,1\}^m$ corresponds to what we call *canonical embedding* $|\psi_{\vec{0}}\rangle := \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle$.

We will show in Lemma 4.3 that the leakage of super-embeddings for a given primitive $P_{X,Y}$ can never be lower than the leakage of one embedding in $\mathcal{E}(P_{X,Y})$. Therefore, the minimum leakage of any correct protocol for primitive $P_{X,Y}$ can be found by looking at the set of embeddings $\mathcal{E}(P_{X,Y})$.

Chapter 4

Cryptography with Embeddings

We first define cryptographically *trivial* and *non-trivial* classical primitives and embeddings. We show that for any non-trivial classical primitive, its canonical quantum embedding is also non-trivial. We formally define the leakage of quantum super-embeddings and show that no super-embedding of a given primitive leaks less than a (regular) embedding of that primitive. We then prove that all embeddings of any non-trivial two-party cryptographic primitive leak information. In other words, the only primitives that correct two-party quantum protocols can implement correctly and without leakage are the trivial ones! This result can be seen as a quantum extension of the corresponding characterization for the cryptographic power of classical protocols in the HBC model. Whereas classical two-party protocols cannot achieve anything non-trivial, their quantum counterparts necessarily leak information when they implement non-trivial primitives.

4.1 Trivial Classical Primitives and Trivial Embeddings

Intuitively, a primitive $P_{X,Y}$ is *non-trivial* if X and Y cannot be generated between Alice and Bob in the classical HBC model. Formally, we define triviality via an entropic quantity related to the notion of *dependent part* (see Section 2.4).

Definition 4.1 *A primitive $P_{X,Y}$ is called* trivial *if it satisfies $H(X \searrow Y|Y) = 0$, and equivalently, also $H(Y \searrow X|X) = 0$. Otherwise, it is called* non-trivial.

It can easily be seen that all trivial primitives can be implemented securely (in such a way that only the information specified by the functionality is given to the players) in the HBC model. A secure protocol for $P_{X,Y}$ trivial is e.g. the following:

1. Alice samples $P_X^{y'}$ which is an event of $Y \searrow X$ from $P_{Y \searrow X}$ and announces its index y' to Bob. She then picks x with probability $P_X^{y'}(x)$.
2. Bob samples y from the distribution $P_{Y|Y \searrow X = P_X^{y'}}$

Clearly, by picking $P_X^{y'}$, Alice does not learn any information about Y which she is not allowed to, since $H(Y \searrow X|X) = 0$. We define a trivial embedding to be such that it allows the players to access at least the same amount of information concerning the implemented functionality, as in some protocol implementing the given functionality in the HBC model. The formal definition follows:

Definition 4.2 *An embedding* $|\psi\rangle^{AB} \in \mathcal{E}(P_{X,Y})$ *is* trivial *if either* $S(X \searrow Y|B) = 0$ *or* $S(Y \searrow X|A) = 0$. *Otherwise, we say that* $|\psi\rangle$ *is* non-trivial.

Notice that unlike in the classical case, $S(X \searrow Y|B) = 0 \Leftrightarrow S(Y \searrow X|A) = 0$ does not hold in general. As an example, consider a shared quantum state where the computational basis corresponds to the Schmidt basis for only one of its subsystems, say for A. Let $|\psi\rangle = \alpha|0\rangle^A|\xi_0\rangle^B + \beta|1\rangle^A|\xi_1\rangle^B$ be such that both subsystems are two-dimensional, $\{|\xi_0\rangle, |\xi_1\rangle\} \neq \{|0\rangle, |1\rangle\}$, $|\langle\xi_0|\xi_1\rangle| = 0$, and $|\langle\xi_0|0\rangle| \neq |\langle\xi_1|0\rangle|$. We then have $S(X|B) = 0$ and $S(Y|A) > 0$ while $X = X \searrow Y$ and $Y = Y \searrow X$.

Let $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ be trivial and assume without loss of generality that $S(Y \searrow X|A) = 0$. It follows that Alice holding register A can measure her part of the shared state to learn an event y' of $Y \searrow X$, specifying $P_{X|Y=y}$ for any event y of Y consistent with y' (such that $f_Y(y) = y'$). At this point, she chooses X according to the distribution that she has learned. An equivalent way of trivially generating (X, Y) classically is the following:

1. Alice picks $P_X^{y'}$ with probability $P_{Y \searrow X}(P_X^{y'})$ and announces its index y' to Bob. She samples x from the distribution $P_X^{y'}$.
2. Bob picks y with probability $P_{Y|Y \searrow X = P_X^{y'}}(y)$.

This argument shows why such an embedding $|\psi\rangle$ corresponds to a trivial implementation of $P_{X,Y}$. Of course, the same reasoning applies in case $S(X \searrow Y|B) = 0$ with the roles of Alice and Bob reversed. Conversely, the following lemma shows that any non-trivial $P_{X,Y}$ admits a non-trivial embedding.

Lemma 4.1 *If* $P_{X,Y}$ *is a non-trivial primitive then the canonical embedding* $|\psi_{\vec{0}}\rangle \in \mathcal{E}(P_{X,Y})$ *is also non-trivial.*

Proof. A non-trivial embedding of $P_{X,Y}$ can be created from a non-trivial embedding of $P_{X \searrow Y, Y \searrow X}$ by applying local unitary transforms. We therefore assume without loss of generality that $X = X \searrow Y$ and $Y = Y \searrow X$. Let

$$|\psi_{\vec{0}}\rangle := \sum_{x,y} \sqrt{P_{X,Y}(x,y)}|xy\rangle$$

be the canonical embedding of $P_{X,Y}$. Since $X = X \searrow Y$ and $Y = Y \searrow X$, it holds for any $x_0 \neq x_1$ that $P_{Y|X=x_0} \neq P_{Y|X=x_1}$. Furthermore, since $P_{X,Y}$ is non-trivial, there exist $x_0 \neq x_1$ and y_0 such that $P_{Y|X=x_0}(y_0) > 0$ and $P_{Y|X=x_1}(y_0) > 0$. The state $|\psi_{\vec{0}}\rangle$ can be written in the form:

$$|\psi_{\vec{0}}\rangle \quad = \quad \sqrt{P_X(x_0)}|x_0\rangle \sum_y \sqrt{P_{Y|X=x_0}(y)}|y\rangle + \sqrt{P_X(x_1)}|x_1\rangle \sum_y \sqrt{P_{Y|X=x_1}(y)}|y\rangle + |\psi'\rangle,$$

where $\operatorname{tr}(|x_0\rangle\langle x_0| \operatorname{tr}_B |\psi'\rangle\langle\psi'|) = \operatorname{tr}(|x_1\rangle\langle x_1| \operatorname{tr}_B |\psi'\rangle\langle\psi'|) = 0$. Since $P_{Y|X=x_0} \neq P_{Y|X=x_1}$, we get that $|\langle\varphi_{x_0}|\varphi_{x_1}\rangle| < 1$. Because all coefficients at $|y\rangle$ in the normalized vectors $|\varphi_{x_0}\rangle$ and $|\varphi_{x_1}\rangle$ are non-negative, and the coefficients at $|y_0\rangle$ are both positive, $\langle\varphi_{x_0}|\varphi_{x_1}\rangle \neq 0$. Therefore, the non-identical states $|\varphi_{x_0}\rangle$ and $|\varphi_{x_1}\rangle$ cannot be perfectly distinguished, which implies that Bob cannot learn whether $X = x_0$ or $X = x_1$ with probability 1. Therefore, the von Neumann entropy on Bob's side $S(B)$ is such that $S(B) < H(X)$. As $H(X \searrow Y|Y) > 0$ implies $H(Y \searrow X|X) > 0$, we can argue in the same way that $S(A) < H(Y)$ from which follows that $|\psi_{\vec{0}}\rangle$ is a non-trivial quantum embedding of $P_{X,Y}$. □

4.2 The Leakage of Quantum Embeddings

A perfect implementation of $P_{X,Y}$ would simply provide X to Alice and Y to Bob and do nothing else. The expected amount of information that one random variable gives about the other is $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y;X)$. Intuitively, we define the *leakage of a quantum super-embedding* $|\psi\rangle$ *of* $P_{X,Y}$ as the larger of the two following quantities: the extra amount of information Bob's quantum registers $\rho_{BB'} = \operatorname{tr}_{A,A'}(|\psi\rangle\langle\psi|)$ provide about X and the extra amount Alice's quantum state $\rho_{AA'} = \operatorname{tr}_{B,B'}(|\psi\rangle\langle\psi|)$ provide about Y respectively in comparison to "the minimum amount" $I(X;Y)$.

Definition 4.3 *Let* $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ *be a super-embedding of* $P_{X,Y}$*. We define the leakage* $\Delta_\psi(P_{X,Y})$ *of* $|\psi\rangle$ *viewed as an implementation of* $P_{X,Y}$ *as*

$$\Delta_\psi(P_{X,Y}) := \max\left\{S(X;BB') - I(X;Y), S(AA';Y) - I(X;Y)\right\}.$$

Furthermore, we say that a super-embedding $|\psi\rangle$ *is* δ-leaking *if* $\Delta_\psi(P_{X,Y}) \geq \delta$.

It is easy to see that the leakage of a super embedding is non-negative since $S(X;BB') \geq S(X;\tilde{B})$ if $\tilde{B}$ is the result of a quantum operation applied to BB'. Such an operation could be the tracing over B' and measurement in the computational basis of each qubit of B yielding $S(X;\tilde{B}) = I(X;Y)$.

For a general pure state in $\mathcal{H}_{ABA'B'}$, the quantities $S(X;BB') - I(X;Y)$ and $S(AA';Y) - I(X;Y)$ are not necessarily equal. However, according to the following lemma,

$$S(X;BB') - I(X;Y) = S(AA';Y) - I(X;Y)$$

holds in the case of a super-embedding. Hence, the definition of leakage is symmetric with respect to both players. Note that for a regular embedding $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ (where the work spaces A' and B' are trivial), this is easy to see. Notice that

$$S(X;B) = S(X) + S(B) - S(X,B) = H(X) + S(B) - H(X) = S(B),$$

and because $|\psi\rangle$ is pure, $S(A) = S(B)$. Therefore, $S(X;B) = S(A;Y)$ and the two quantities coincide.

Lemma 4.2 *Let $|\psi\rangle$ be a super-embedding of $P_{X,Y}$. Then,*

$$\Delta_\psi(P_{X,Y}) = S(X;BB') - I(X;Y) = S(AA';Y) - I(X;Y).$$

Proof. We have already shown that the statement is true in the case where both A' and B' are trivial. In the case where A' is trivial and B' is not, the Markov chain condition from Lemma 3.1 implies that $|\psi\rangle$ is of the form

$$|\psi\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)}|x,y\rangle^{AB}|\varphi^y\rangle^{B'},$$

hence, Bob can fix y_0 and apply a unitary transform $U^{BB'}$ on his part of the system, such that $U^{BB'}|y,\varphi^y\rangle = |y,\varphi^{y_0}\rangle$, and

$$\mathbb{I}_A \otimes U^{BB'}|\psi\rangle^{ABB'} = |\psi^*\rangle^{AB} \otimes |\varphi^{y_0}\rangle^{B'},$$

where $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$. In the resulting product state, $S(X;BB') - I(X;Y) = S(X;B) - I(X;Y) = S(A;Y) - I(X;Y)$, due to the fact that $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$. An analogous statement holds in the case where B' is trivial and A' is non-trivial.

We now assume that both A' and B' are non-trivial. A super-embedding of $P_{X,Y}$ can be written as $|\psi\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)}|x,y\rangle^{AB}|\varphi^{x,y}\rangle^{A'B'}$.

For every x and y, we can write the pure state

$$|\varphi^{x,y}\rangle^{A'B'} = \sum_{k=1}^{K} \sqrt{\lambda_k^{x,y}}|e_k^{x,y}\rangle^{A'}|f_k^{x,y}\rangle^{B'}$$

in Schmidt form. For the reduced density matrices, we obtain

$$\rho_{A'}^{x,y} = \sum_k \lambda_k^{x,y}|e_k^{x,y}\rangle\langle e_k^{x,y}|.$$

Since a super-embedding $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ of $P_{X,Y}$ is produced by a correct protocol, it satisfies

$$S(XA';B) = S(X;YB') = I(X;Y)$$

which by Lemma 3.1 is equivalent to $A' \leftrightarrow X \leftrightarrow Y$ and $X \leftrightarrow Y \leftrightarrow B'$ being Markov chains. It follows that for every x and $y \neq y'$, the reduced density matrices $\rho_{A'}^{x,y} = \rho_{A'}^{x,y'} = \rho_{A'}^{x}$ coincide and therefore, the eigenvalues $\lambda_k^{x,y}$ cannot depend on y. Because of $X \leftrightarrow Y \leftrightarrow B'$, they can neither depend on x. Hence, $|\varphi^{x,y}\rangle = \sum_k \sqrt{\lambda_k} e^{i\theta'(k,x,y)}|e_k^x\rangle|f_k^y\rangle$. The phase factors arise from the fact that from a reduced density matrix the global phases of the Schmidt-basis elements cannot be determined.

Let us fix a set of orthogonal states $\{|k\rangle\}_k$. We define the unitary $U^{AA'}$ to be the mapping of the orthonormal states $\{|e_k^x\rangle\}_k$ into the orthonormal states $\{|k\rangle\}_k$. Note that $U^{AA'}$ only acts on register A' conditioned on the x-value

in A. Analogously, let $U^{BB'}$ map the states $\{|f_k^y\rangle\}_k$ into $\{|k\rangle\}_k$. Applying $U^{AA'} \otimes U^{BB'}$ to $|\psi\rangle$ results into state

$$\begin{aligned} & \textstyle\sum_{x,y} \sqrt{P_{X,Y}(x,y)}|x,y\rangle^{AB} \sum_k \sqrt{\lambda_k} e^{i\theta'(k,x,y)}|k,k\rangle^{A'B'} \\ = \quad & \textstyle\sum_k \sqrt{\lambda_k} \left(\sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta'(k,x,y)}|x,y\rangle \right) |k,k\rangle \\ = \quad & \textstyle\sum_k \sqrt{\lambda_k}|\psi_k\rangle^{AB} \otimes |k,k\rangle^{A'B'}, \end{aligned}$$

where each $|\psi_k\rangle^{AB} \in \mathcal{E}(P_{X,Y})$. Cq-state $\rho_{XBB'}$ can now be written in the form:

$$\rho_{XBB'} = \sum_x P_X(x)|x\rangle\langle x| \otimes \sum_k \lambda_k |\phi_{x,k}, k\rangle\langle\phi_{x,k}, k|,$$

where $|\phi_{x,k}\rangle = \sum_y \sqrt{P_{Y|X=x}} e^{i\theta'(k,x,y)}|y\rangle$. Due to the second component, the states $|\phi_{x,k}, k\rangle$ are mutually orthogonal for each x. Therefore, for each x,

$$S\left(\sum_k \lambda_k |\phi_{x,k}, k\rangle\langle\phi_{x,k}, k| \right) = H(\lambda_1, \ldots, \lambda_K).$$

As a result we get that

$$S(XBB') = H(X) + \sum_x P_X(x) H(\lambda_1, \ldots, \lambda_K) = H(X) + H(\lambda_1, \ldots, \lambda_K)$$

and analogously,

$$S(AA'Y) = H(Y) + H(\lambda_1, \ldots, \lambda_K),$$

yielding the desired statement as follows:

$$\begin{aligned} S(X;BB') - I(X;Y) &= H(X) + S(BB') - S(XBB') - I(X;Y) \\ &= H(X) + S(BB') - (H(X) + H(\lambda_1, \ldots, \lambda_K)) - I(X;Y) \\ &= H(Y) + S(AA') - (H(Y) + H(\lambda_1, \ldots, \lambda_K)) - I(X;Y) \\ &= S(AA';Y) - I(X;Y). \end{aligned}$$

The equality $S(AA') = S(BB')$ follows from the purity of $|\psi\rangle$. □

The next lemma shows that super-embeddings leak at least as much as some regular embedding. In order to find lower bounds on the leakage, it is thus general enough to restrict our attention in the rest of the paper to regular embeddings.

Lemma 4.3 *Let $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ be a super-embedding of $P_{X,Y}$. Then there exists a regular embedding $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$ such that $\Delta_\psi(P_{X,Y}) \geq \Delta_{\psi^*}(P_{X,Y})$.*

Proof. In the case where A' and B' are both trivial, $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ and the statement holds trivially. In the case where A' is trivial and B' is not, we have shown in the proof of Lemma 4.2 that a super-embedding $|\psi\rangle$ of $P_{X,Y}$ is locally equivalent to a state $|\psi^*\rangle \otimes |\sigma\rangle$ for $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$ and a pure state $|\sigma\rangle$. An analogous statement holds if B' is trivial and A' is not. Therefore, in these two cases we get for some $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$ that $\Delta_\psi = \Delta_{\psi^*}$.

Now assume that both A' and B' are non-trivial. A super-embedding of $P_{X,Y}$ can be written as $|\psi\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)}|x,y\rangle^{AB}|\varphi^{x,y}\rangle^{A'B'}$.

In the proof of Lemma 4.2 we show the existence of two local unitary transforms $U^{AA'}$ and $U^{BB'}$ on Alice's and Bob's side that transform $|\psi\rangle$ into $\sum_k \sqrt{\lambda_k}|\psi_k\rangle^{AB} \otimes |k,k\rangle^{A'B'}$ for a set of orthogonal states $\{|k\rangle\}_k$ and $|\psi_k\rangle \in \mathcal{E}(P_{X,Y})$ for each k.

If Alice measures register A' or Bob measures B' in the basis $\{|k\rangle\}_k$, she/he transforms the state defined above into the state $|\psi_k\rangle^{AB} \otimes |k,k\rangle^{A'B'}$ with probability λ_k. Measuring register arbitrarily A' does not increase $S(AA';Y)$ on average, and analogously, measuring B' does not increase $S(X;BB')$ on average. This follows from Holevo bound (Theorem 2.1), yielding that

$$S(AA';Y) = S(A;Y) + S(A';Y|A) \geq S(A;Y) + S(K;Y|A) = S(AK;Y),$$

where K denotes the random variable associated with the measurement of register A' in the computational basis. Therefore, the leakage of $|\psi\rangle$ is at least the average leakage of one particular strategy, we get that $\Delta_\psi \geq \sum_k \lambda_k \Delta_{\psi_k}$. Hence, there must be k such that for $|\psi^*\rangle := |\psi_k\rangle$, it holds that $\Delta_\psi \geq \Delta_{\psi^*}$. □

The following statements concern the leakage of embeddings. The following definition serves to simplify the notation.

Definition 4.4 *Let $P_{X,Y}$ be an arbitrary primitive. We define*

$$\Delta_{P_{X,Y}} := \inf_{|\psi\rangle \in \mathcal{E}(P_{X,Y})} \Delta_\psi(P_{X,Y}).$$

The next lemma shows that in fact, in the definition above the infimum is achievable, implying that it can be replaced by "minimum".

Lemma 4.4 *For any primitive $P_{X,Y}$ there exists $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ such that*

$$\Delta_\psi(P_{X,Y}) = \Delta_{P_{X,Y}}.$$

Proof. The function $S_\psi(B)$ of $|\psi\rangle$ is continuous on the compact (closed and bounded) set of phases, which is $[0, 2\pi]^{|\mathcal{X}\times\mathcal{Y}|}$. Therefore, it has a minimum, yielding that function $\Delta_\psi(P_{X,Y}) = S_\psi(B) - I(X;Y)$ also has a minimum. □

In the following theorem we show that if for a quadruple of random variables X, Y, X', Y', X and Y are computable from X' and Y', respectively and furthermore, the extra information (besides X and Y) in X' and Y' is local (which is expressed by Markov chain properties), then there is an embedding of $P_{X,Y}$ leaking at most as much information as any given embedding of $P_{X',Y'}$.

Theorem 4.1 *Let X, X', Y, Y' be random variables such that $X' \leftrightarrow X \leftrightarrow Y'$ and $X' \leftrightarrow Y \leftrightarrow Y'$ are Markov chains and such that there exist deterministic functions f_X and f_Y with $f_X(X') = X$ and $f_Y(Y') = Y$. Then*

$$\Delta_{P_{X',Y'}} \geq \Delta_{P_{X,Y}}.$$

Proof. Since $X' \leftrightarrow X \leftrightarrow Y'$ and $X' \leftrightarrow Y \leftrightarrow Y'$ are Markov chains, we have that $I(X';Y') = I(X;Y)$. Therefore, showing that for some $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$ and any $|\psi\rangle \in \mathcal{E}(P_{X',Y'})$,

$$S_\psi(B) - I(X';Y') = \Delta_\psi(P_{X',Y'}) \geq \Delta_{\psi^*}(P_{X,Y}) = S_{\psi^*}(B) - I(X;Y)$$

is equivalent to proving $S_\psi(B) \geq S_{\psi*}(B)$. First, we show that there exists $|\tilde{\psi}\rangle \in \mathcal{E}(P_{X',Y})$ such that $S_\psi(B) \geq S_{\tilde{\psi}}(B)$, i.e. $\Delta_\psi(P_{X',Y'}) \geq \Delta_{\tilde{\psi}}(P_{X',Y})$. The existence of $|\psi^*\rangle$ such that $\Delta_{\tilde{\psi}}(P_{X',Y}) \geq \Delta_{\psi^*}(P_{X,Y})$ follows from an analogous argument.

State $|\psi\rangle$ can be written in the form:

$$|\psi\rangle = \sum_{x'y'} \sqrt{P_{X',Y'}(x',y')} e^{i\theta(x',y')} \big|x'y'\big\rangle.$$

For any realization y of Y, let $O_y := \{y' : \ f_Y(y') = y\}$. WLOG assume that $O_y = \{1, \ldots, k_y\}$. Let g be a bijection of the form $g(y') = (f_Y(y'), j_{y'})$, where $j_{y'} \in \{1, \ldots, k_{f_Y(y')}\}$. A pair (y, j) determines its g-preimage uniquely and therefore, in the following we sometimes encode y' by $f_Y(y')j_{y'} = yj$. Formally, there is a unitary transform U of Bob such that

$$\begin{aligned} \mathbb{I}_A \otimes U|\psi\rangle|0\rangle^B = & \sum_{x'y'} \sqrt{P_{X',Y'}(x',y')} e^{i\theta(x',y')} \big|x', f_Y(y')j_{y'}\big\rangle \\ = & \sum_{x'y} \sqrt{P_{X',Y}(x',y)} \big|x'y\big\rangle \sum_{j=1}^{k_y} \sqrt{P_{Y'|Y=y}(g^{-1}(y,j))} e^{i\theta(x',g^{-1}(y,j))} |j\rangle. \end{aligned} \tag{4.1}$$

Our goal for the rest of the proof is to transform the register containing j into a form where the order of the summations over $x'y$ and j in (4.1) can be reversed to get a state of the form

$$\frac{1}{\sqrt{t}} \sum_{j=1}^{t} \left|\hat{\psi}_j\right\rangle^{AB} |j\rangle^B,$$

where t is some normalization factor and each $|\hat{\psi}_j\rangle$ is in $\mathcal{E}(P_{X',Y})$. Our claim that there exists a state $|\tilde{\psi}\rangle \in \mathcal{E}(P_{X',Y})$ such that $S_{\tilde{\psi}}(B) \leq S_\psi(B)$ then follows from concavity of Von Neumann entropy i.e., from the fact that the average of the entropies of the states $\{\mathrm{tr}_A\, |\hat{\psi}_j\rangle\langle\hat{\psi}_j|\}_j$ is smaller than the entropy of their mixture which is equivalent to $\mathrm{tr}_A\, |\psi\rangle\langle\psi|$.

In order to reverse the order of summation in (4.1), we show that there exists a unitary W on Bob's system such that

$$(\mathbb{I}_A \otimes W)(\mathbb{I}_A \otimes U|\psi\rangle|0\rangle^B)|0\rangle^B = |\varphi\rangle = \frac{1}{\sqrt{t}} \sum_{z=1}^{t} \left|\hat{\psi}_z\right\rangle^{AB} |z\rangle^B,$$

where each $|\hat{\psi}_z\rangle$ is a quantum embedding of a joint random variable $\hat{X}\hat{Y}$, with the distribution arbitrarily close to the distribution of $X'Y$.

Equality (4.1) suggests to construct the states $|\hat{\psi}_z\rangle^{AB}$ by disentangling the register containing j from the registers containing $x'y$. This method will indeed lead us to the result but only after some pre-processing of the register containing j. First, we show how to split the register with j for each value of y into a uniform superposition of t values which Bob can measure afterwards to determine the index z of an embedding $|\hat{\psi}_z\rangle$. The uniformity over the register containing the indices ensures that measuring the index does not have any impact on the probability distribution $P_{X',Y}$ implemented by $|\hat{\psi}_z\rangle$.

Consider $t \in \mathbb{N}$ such that $0 < 1/t \ll \min_{y'}\{P_{Y'|Y=f_Y(y')}(y')\}$. We can ensure that each $y \in \mathcal{Y}$ is splitted into exactly t index-values z, by adaptively defining a function $[tP_{Y'|f_Y(Y')=y}(y')]_{y'} \in \{\lceil\ \rceil, \lfloor\ \rfloor\}$, indicating into how many values z a given y' such that $f_Y(y') = y$ splits. This procedure is elementary, but somewhat technical, and we postpone the detailed description to the end of the proof.

For an event y of Y, define $t_0 := 0$ and for $i \in \{1, \ldots, k_y\}$,

$$t_i := \sum_{j \le i} [tP_{Y'|f_Y(Y')=y}(yj)]_{yj}.$$

Let Bob's unitary transform W acting upon the registers containing Y, $j \in \{1, \ldots, k_Y\}$ and ancillas set to 0, be defined as follows:

$$W|yj\rangle|0\rangle = |y\rangle \frac{1}{\sqrt{[P_{Y'|f_Y(Y')=y}(yj)t]_{yj}}} \sum_{z=t_{j-1}+1}^{t_j} |z\rangle.$$

The definition of $[\ ]_{y'}$ implies that for each y: $t_{k_y} = t$, thus $z \in \{1, \ldots, t\}$. We can write

$$\begin{aligned} |\varphi\rangle := & \quad (\mathbb{I}_A \otimes W)((\mathbb{I}_A \otimes U)|\psi\rangle^{AB}|0\rangle^B)|0\rangle^B \\ = & \sum_{x'y} \sqrt{P_{X',Y}(x',y)}|x'y\rangle \sum_{j=1}^{k_y} \sqrt{\frac{P_{Y'|f_Y(Y')=y}(yj)}{[P_{Y'|f_Y(Y')=y}(yj)t]_{yj}}} e^{i\theta(x',yj)} \sum_{z=t_{j-1}+1}^{t_j} |z\rangle. \end{aligned} \tag{4.2}$$

For the term $\frac{P_{Y'|f_Y(Y')=y}(y)}{[P_{Y'|f_Y(Y')=y}(y')t]_{y'}}$ from (4.2) we have

$$\begin{aligned} \left| \frac{P_{Y'|f_Y(Y')=y}(y')}{[P_{Y'|f_Y(Y')=y}(y')t]_{y'}} - \frac{1}{t} \right| = & \quad \left| \frac{tP_{Y'|f_Y(Y')=y}(y') - [P_{Y'|f_Y(Y')=y}(y')t]_{y'}}{t[P_{Y'|f_Y(Y')=y}(y')t]_{y'}} \right| \\ \le & \quad \frac{1}{P_{Y'|f_Y(Y')=y}(y')t^2 - t} = \frac{1}{P_{Y'|f_Y(Y')=y}(y')t^2} + O\left(\frac{1}{t^3}\right). \end{aligned} \tag{4.3}$$

Now we can finally swap the summations to isolate z as promised earlier. From (4.2) and (4.3) follows that

$$\begin{aligned}|\varphi\rangle &= \sum_{x'y}\sqrt{P_{X',Y}(x',y)}\big|x'y\big\rangle\sum_{z=1}^{t}e^{i\theta'(x',y,z)}\sqrt{\frac{1}{t}+\frac{\varepsilon(y,z)}{t^2}}|z\rangle \\ &= \frac{1}{\sqrt{t}}\sum_{z=1}^{t}\left(\sum_{x'y}e^{i\theta'(x',y,z)}\sqrt{1+\frac{\varepsilon(y,z)}{t}}\sqrt{P_{X',Y}(x',y)}\big|x'y\big\rangle\right)|z\rangle,\end{aligned}$$

where $|\varepsilon(y,z)| \leq \frac{1}{\min_{y'}\{P_{Y'|Y=f_Y(y')}(y')\}}$ and since a pair (y,z) uniquely determines y' that it came from, $\theta'(x',y,z)=\theta(x',y')$ for y' corresponding to (y,z). If Bob measures z, the state $|\varphi\rangle$ collapses to

$$\left(\sum_{x'y}e^{i\theta'(x',y,z)}\sqrt{1+\frac{\varepsilon(y,z)}{t}}\sqrt{P_{X',Y}(x',y)}\big|x'y\big\rangle\right)\otimes|z\rangle = \left|\hat{\psi}_z\right\rangle\otimes|z\rangle.$$

The state $|\hat{\psi}_z\rangle$ lies in $\mathcal{E}(P_{\hat{X},\hat{Y}})$ for a joint probability distribution $P_{\hat{X},\hat{Y}}$ which is arbitrarily close to $P_{X',Y}$. The distance of the two distributions depends on the choice of t.

Hence, for any $\delta>0$ there is a way to pick a unitary transform W_δ (with t large enough) such that after applying W_δ and measuring z, the corresponding quantum systems satisfy $|S_{\tilde{\psi}_z}(B)-S_{\hat{\psi}_z}(B)|\leq\delta$ for some $|\tilde{\psi}_z\rangle\in\mathcal{E}(P_{X',Y})$.

Concavity of Von Neumann entropy together with the fact that the state $\frac{1}{\sqrt{t}}\sum_{z=1}^{t}|\hat{\psi}_z\rangle|z\rangle$ is locally equivalent to $|\psi\rangle$ imply that

$$\frac{1}{t}\sum_{z=1}^{t}S_{\hat{\psi}_z}(B)\leq S_\psi(B).$$

Therefore, $S_\psi(B)\geq\min_z\{S_{\hat{\psi}_z}(B)\}$, and $S_\psi(B)\geq\min_z\{S_{\tilde{\psi}_z}(B)\}-\delta$ for δ arbitrarily small.

Continuity of Von Neumann entropy yields that $S_\psi(B)\geq S_{\tilde{\psi}}(B)$ for some $|\tilde{\psi}\rangle\in\mathcal{E}(P_{X',Y})$, which is what we wanted to show.

Finally, it remains to give the correct definition of $[\,]_{y'}$: For any y let us start by setting $[tP_{Y'|f_Y(Y')=y}(y')]_{y'}:=\lfloor tP_{Y'|f_Y(Y')=y}(y')\rfloor$ for all $y':f_Y(y')=y$. We now increase the value of $[tP_{Y'|f_Y(Y')=y}(y')]_{y'}$ in steps and show that at some point, this value equals t. Let $0\leq i\leq k_y$. In the i-th step, replace $[\,]_{yi}=\lfloor\,\rfloor$ with $[\,]_{yi}=\lceil\,\rceil$. After k_y steps, $[\,]_{y'}=\lceil\,\rceil$ for all $y':f_Y(y')=y$. In every step the sum $\sum_{y',f_Y(y')=y}[tP_{Y'|f_Y(Y')=y}(y')]_{y'}$ increases by at most 1. Clearly, since $\sum_{y'}P_{Y'|f_Y(Y')=y}(y')=1$, we get that

$$\sum_{y',f_Y(y')=y}\lfloor tP_{Y'|f_Y(Y')=y}(y')\rfloor\leq t\quad\text{and}\quad\sum_{y',f_Y(y')=y}\lceil tP_{Y'|f_Y(Y')=y}(y')\rceil\geq t,$$

thus for some i, $\sum_{y',f_Y(y')=y}[tP_{Y'|f_Y(Y')=y}(y')]_{y'}=t$. □

As an immediate consequence of Theorem 4.1, we get that for any primitive $P_{X,Y}$, embeddings in $\mathcal{E}(P_{X,Y})$ leak at least as much as an embedding in

$\mathcal{E}(P_{X\searrow Y,Y\searrow X})$. This allows us to concentrate on random variables (X,Y) for which $X = X \searrow Y$ and $Y = Y \searrow X$. This property is satisfied by standard cryptographic primitives (see Section 2.3), since they are defined in a canonical form avoiding unnecessary redundancy in X and Y.

Corollary 4.1 *For any primitive $P_{X,Y}$,*

$$\Delta_{P_{X,Y}} \geq \Delta_{P_{X\searrow Y,Y\searrow X}}.$$

Proof. By definitions of $X \searrow Y$ and $Y \searrow X$, random variables $X \searrow Y, X, Y \searrow X$, and Y satisfy the conditions of Theorem 4.1. □

From Corollary 4.1 we conclude that the only primitives having non-leaking embeddings are the trivial ones. Hence, every non-trivial primitive necessarily leaks!

Theorem 4.2 *If there exists a non-leaking embedding $|\psi\rangle \in \mathcal{E}(P_{X,Y})$, then $P_{X,Y}$ is a trivial primitive.*

Proof. Corollary 4.1 implies that if there is a 0–leaking embedding of $P_{X,Y}$ than there is also a 0–leaking embedding of $P_{X\searrow Y,Y\searrow X}$. Let us therefore assume that $|\psi\rangle$ is a non-leaking embedding of $P_{X,Y}$ such that $X = X \searrow Y$ and $Y = Y \searrow X$. We can write $|\psi\rangle$ in the form $|\psi\rangle = \sum_x \sqrt{P_X(x)}|x\rangle|\varphi_x\rangle$, and define $\rho_B := \sum_x P_X(x)|\varphi_x\rangle\langle\varphi_x|$. The leakage of $|\psi\rangle$ can then be expressed as $\Delta_\psi(P_{X,Y}) = S(\rho_B) - I(X;Y)$. From the Holevo bound (Theorem 2.1) follows that for a random variable Z capturing the outcome of the measurement in the basis $\{|\varphi_x\rangle\}_x$, $S(\rho_B) = I(X;Z)$ if and only if $\{|\varphi_x\rangle\langle\varphi_x|\}_{x:P_X(x)>0}$ is an orthonormal set. The outcome of the measurement in the computational basis, captured by Y is then such that $X \leftrightarrow Z \leftrightarrow Y$ form a Markov chain. This follows from the fact that Z determines X completely hence, $H(Y|X) = H(Y|Z) = H(Y|ZX)$. Since $S(\rho_B) = I(X;Z) = I(X;Y)$, Z is the minimum (see the definition of dependent part in Section 2.4) random variable with this property, hence, $Z = Y \searrow X = Y$. It follows that $\{|\varphi_x\rangle\}_{x:P_X(x)>0}$ are the elements of the computational basis. The marginal Y is then completely determined by X, yielding that $H(Y \searrow X|X) = H(Y|X) = 0$. The primitive is therefore trivial. □

In the statement above we have shown than any correct protocol for non-trivial primitive leaks information. Notice that this is not immediately obvious from the fact that non-trivial primitives cannot be implemented securely in the QHBC model [Lo97], since e.g. an implementation of 1-2-OT that allows Bob to get either the bit of his choice or the parity of Alice's bits is non-leaking, yet insecure. However, in Chapter 6 we show that impossibility of a secure implementation of a given primitive in fact, implies that it is not possible to implement such a primitive without leakage. This result holds even in a more general model where we assume a presence of a (possibly restricted) trusted third party and with no correctness assumption.

4.3 Reducibility of Primitives and Their Leakage

One can ask the following question: Given two primitives $P_{X,Y}$ and $P_{X',Y'}$ such that $P_{X,Y}$ is reducible to $P_{X',Y'}$, what is the relationship between the leakage of $P_{X,Y}$ and the leakage of $P_{X',Y'}$? We will use the notion of reducibility in the following sense: We say that a primitive $P_{X,Y}$ is *reducible in the HBC model* to a primitive $P_{X',Y'}$ if in the HBC model, $P_{X,Y}$ can be securely implemented from (one call of) a secure implementation of $P_{X',Y'}$. The above question can also be generalized to the case where $P_{X,Y}$ can be computed from $P_{X',Y'}$ only with certain probability. Notice that the answer, even if we assume perfect reducibility, is not captured in our previous result from Lemma 4.3, since an embedding of $P_{X',Y'}$ is not necessarily a super-embedding of $P_{X,Y}$. However, under certain conditions we can show that

$$\Delta_{P_{X',Y'}} \geq \Delta_{P_{X,Y}}.$$

In Section 5.2, such a condition allows us to derive a lower bound on the leakage of $P_{X,Y}^{\mathrm{OT}^r}$.

Theorem 4.3 *Assume that primitives $P_{X,Y}$ and $P_{X',Y'} = P_{X'_0X'_1,Y'_0Y'_1}$ satisfy the condition:*

$$\sum_{x,y:P_{X'_0,Y'_0|X'_1=x,Y'_1=y}\simeq P_{X,Y}} P_{X'_1,Y'_1}(x,y) \geq 1-\delta,$$

where the relation $\simeq$ between two distributions means that they can only differ in the underlying probability space. Then,

$$\Delta_{P_{X',Y'}} \geq (1-\delta)\Delta_{P_{X,Y}}.$$

Proof. State $|\psi\rangle^{A_0A_1,B_0B_1} \in \mathcal{E}(P_{X',Y'})$ can be written in the form:

$$|\psi\rangle = \sum_{x\in\mathcal{X}'_1} \sqrt{P_{X'_1}(x)}|x\rangle^{A_1}|\psi_x\rangle^{A_0B},$$

where each $|\psi_x\rangle$ is an embedding of $P_{X'_0,Y'_0Y'_1|X'_1=x}$. Since

$$S_\psi(Y'|A) \leq S_\psi(Y'|A_0,X'_1) = \sum_x P_{X'_1}(x) S_{\psi_x}(Y'|A_0,X'_1=x),$$

for the leakage of $|\psi\rangle$ we obtain:

$$\begin{aligned}
\Delta_\psi(P_{X',Y'}) &= H(Y'|X') - S_\psi(Y'|A) \\
&\geq H(Y'|X') - \sum_x P_{X'_1}(x) S_{\psi_x}(Y'|A_0,X'_1=x) \\
&= \sum_x P_{X'_1}(x)(H(Y'|X'_0,X'_1=x) - S_{\psi_x}(Y'|A_0,X'_1=x)) \\
&= \sum_x P_{X'_1}(x)\Delta_{\psi_x}(P_{X'_0,Y'_0Y'_1|X'_1=x}).
\end{aligned}$$

..... By applying the same argument to each $|\psi_x\rangle$, we obtain that

$$\Delta_\psi(P_{X',Y'}) \geq \sum_{xy} P_{X'_1,Y'_1}(x,y)\Delta_{\psi_{x,y}}(P_{X'_0,Y'_0|X'_1=x,Y'_1=y}), \tag{4.4}$$

where each $|\psi_{x,y}\rangle$ is an embedding of $P_{X'_0,Y'_0|X'_1=x,Y'_1=y}$. For each (x,y) such that $P_{X'_0,Y'_0|X'_1=x,Y'_1=y} \simeq P_{X,Y}$ is satisfied, we get that

$$\Delta_{\psi_{x,y}}(P_{X'_0,Y'_0|X'_1=x,Y'_1=y}) \geq \Delta_{P_{X,Y}}.$$

Since $\sum_{x,y:P_{X'_0,Y'_0|X'_1=x,Y'_1=y}\simeq P_{X,Y}} P_{X'_1,Y'_1}(x,y) \geq 1-\delta$, we get from (4.4) that

$$\Delta_\psi(P_{X',Y'}) \geq (1-\delta)P_{X,Y}.$$

□

Notice that the statement above (for $\delta = 0$) does not follow from Lemma 4.3. Neither it does from Theorem 4.1, since the Markov chain conditions do not need to be satisfied in the situation considered by Theorem 4.3, which is the case e.g. for $P_{X,Y} = P^{\text{ROT}}_{X,Y}$ and $P_{X',Y'} = P^{\text{OT}}_{X,Y}$. On the other hand, neither the implication in the opposite direction is true, since e.g. the primitive $P_{X,Y_0Y_1=Y}$: $P_{X,Y}(0,(0,0)) = P_{X,Y}(0,(0,1)) = 3/16$, $P_{X,Y}(0,(1,0)) = P_{X,Y}(0,(1,1)) = P_{X,Y}(0,(1,2)) = 1/24$, $P_{X,Y}(1,(0,0)) = P_{X,Y}(1,(0,1)) = 1/16$, $P_{X,Y}(1,(1,0)) = P_{X,Y}(1,(1,1)) = P_{X,Y}(1,(1,2)) = 1/8$ (P_{X,Y_0} is a binary symmetric channel with noise rate $p = 1/4$), can be handled by Theorem 4.1 but not by Theorem 4.3. However, the proof of Theorem 4.1 contains a transformation of an embedding of $P_{X',Y'}$ into a state satisfying the conditions required to apply Theorem 4.3. Beyond this point, Theorem 4.1 follows from Theorem 4.3.

Chapter 5

The Leakage of Universal Cryptographic Primitives

In this chapter, we exhibit lower bounds on the leakage of some universal two-party primitives such as 1-out-of-2 Oblivious Transfer (1-2-OT), Rabin Oblivious Transfer (ROT), the additive sharing of an AND gate applied to two random bits (SAND), and the string and noisy versions of them. We refer to Section 2.3 for an overview and the formal definitions of these primitives. We note that Wolf and Wullschleger [WW05b] have shown that a randomized 1-2-OT can be transformed by local operations into an additive sharing of an AND. Therefore, our results for 1-2-OT below also apply to SAND. Each of these primitives is universal and can be seen as a cornerstone of two-party quantum computation.

For $P_{X,Y}^{\text{OT}^r}$ and $P_{X,Y}^{\text{OT}_p}$, the exact computation of the von Neumann entropies becomes difficult, since the number of possibilities for the phases increases exponentially in the number of qubits, hence, we only provide lower bounds on their leakage..

5.1 Minimum Leakage of ROT^r and 1-2-OT

First, we look at the leakage of the embeddings of Rabin String OT (ROT^r).

Theorem 5.1 *Any embedding of $P_{X,Y}^{\text{ROT}^r}$ is at least $(1 - O(r2^{-r}))$-leaking. For $r = 1$ any embedding is at least $(h(\frac{1}{4}) - \frac{1}{2}) \approx 0.311$-leaking. Furthermore, the leakage is the same for all embeddings of $P_{X,Y}^{\text{ROT}^r}$.*

Proof. Let

$$|\psi\rangle = \frac{1}{2^{\frac{r+1}{2}}} \sum_{x\in\{0,1\}^r} e^{i\theta(x,x)}|xx\rangle + \frac{1}{2^{\frac{r+1}{2}}} \left(\sum_{x\in\{0,1\}^r} e^{i\theta(x,\perp)}|x\rangle \right) |\perp\rangle,$$

where $\perp$ denotes an erasure, be a general form of an embedding of $P_{X,Y}^{\text{ROT}^r}$.

Define $|\varphi\rangle := \frac{1}{2^{r/2}} \sum_{x\in\{0,1\}^r} e^{i\theta(x,\perp)}|x\rangle$. If Bob guesses the value of Alice's string successfully, Alice gets an ensemble $\rho_0 = \frac{1}{2^r} \sum_{x\in\{0,1\}^r} |x\rangle\langle x|$. If an erasure occurs on Bob's side, Alice gets $\rho_1 = |\varphi\rangle\langle\varphi|$. We find $S(A)$ by computing the eigenvalues of $\rho_A := \frac{1}{2}(\rho_0 + \rho_1)$.

Since $\rho_0 = \frac{1}{2^r}\mathbb{I}_A$, $|v\rangle$ is an eigenvector of ρ_A if and only if it is an eigenvector of ρ_1. If $|v\rangle$ is an eigenvector of ρ_1 then either a) $|v\rangle = e^{i\theta}|\varphi\rangle$ or b) $\langle v|\varphi\rangle = 0$. If a) is true then

$$\rho_A|v\rangle = \frac{1}{2}(\rho_0|v\rangle + \rho_1|v\rangle) = \frac{1}{2}\left(1 + \frac{1}{2^r}\right)|v\rangle,$$

whereas in the case b),

$$\rho_A|v\rangle = \frac{1}{2}(\rho_0|v\rangle + \rho_1|v\rangle) = \frac{1}{2^{r+1}}.$$

The state ρ_A has eigenvalues $\{\frac{1}{2}+\frac{1}{2^{r+1}}, \frac{1}{2^{r+1}}\}$, where $\frac{1}{2^{r+1}}$ has multiplicity $2^r - 1$. $S(A)$ can then be computed as follows:

$$\begin{aligned} S(A) &= -\left(\frac{1}{2} + \frac{1}{2^{r+1}}\right)\log\left(\frac{1}{2} + \frac{1}{2^{r+1}}\right) + \frac{2^r - 1}{2^{r+1}}(r+1) \\ &= \left(\frac{1}{2} + \frac{1}{2^{r+1}}\right)\left(1 - \frac{1}{\ln 2 \cdot 2^r} + o\left(\frac{1}{2^r}\right)\right) + \frac{r+1}{2} - \frac{r+1}{2^{r+1}} = \frac{r}{2} + 1 - O\left(\frac{r}{2^r}\right). \end{aligned}$$

Since $I(X;Y) = \frac{r}{2}$, for the leakage we get:

$$\Delta_\psi(P^{\text{ROT}^r}_{X,Y}) = S(A) - I(X;Y) = 1 - O\left(\frac{r}{2^r}\right).$$

As we can see, the leakage does not depend on the phase-function θ. □

In the following theorem we minimize the leakage of an embedding of $P^{\text{OT}}_{X,Y}$.

Theorem 5.2 *Any $|\psi\rangle \in \mathcal{E}(P^{\text{OT}}_{X,Y})$ is at least $\frac{1}{2}$-leaking. The leakage is minimized by the canonical embedding.*

Proof. Let

$$|\psi\rangle = \frac{1}{2\sqrt{2}} \sum_{x_0,x_1,c\in\{0,1\}} e^{i\theta(x_0x_1,cx_c)}|x_0x_1\rangle|cx_c\rangle$$

be an embedding of $P^{\text{OT}}_{X,Y}$. Without loss of generality assume that $\theta(00,00) = 0$. Notice that for the local phase-change transforms

$$\begin{aligned} U^A &:= |00\rangle\langle 00| + \exp(i\theta(01,00))|01\rangle\langle 01| + \exp(i(\theta(10,10) - \theta(00,10)))|10\rangle\langle 10| \\ &+ \exp(i(\theta(10,10) + \theta(11,01) - \theta(00,10) - \theta(10,01)))|11\rangle\langle 11|, \\ U^B &:= |00\rangle\langle 00| + \exp(i(\theta(00,10) + \theta(10,01) - \theta(10,10)))|01\rangle\langle 01| \\ &+ \exp(i\theta(00,10))|10\rangle\langle 10| + \exp(i(\theta(01,11) - \theta(01,00)))|11\rangle\langle 11|, \end{aligned}$$

we get

$$U^A \otimes U^B|\psi\rangle = |\psi'\rangle = \frac{1}{2}(|0+\rangle|00\rangle + |1+\rangle|01\rangle + |+0\rangle|10\rangle + \frac{|0\rangle + e^{i\omega}|1\rangle}{\sqrt{2}}|1\rangle|11\rangle),$$

where $\omega = \theta(00,10) + \theta(01,00) + \theta(10,01) + \theta(11,11) - \theta(01,01) - \theta(10,10) - \theta(11,01)$.

Let A' denote Alice's quantum system for Alice and Bob sharing $|\psi'\rangle$. Since $S(A) = S(A')$, we can minimize $S(A')$ in order to minimize $S(A)$. Assume that Alice and Bob share $|\psi'\rangle$. For Bob's selection bit $c = 0$, Alice gets an ensemble $\rho_0 = \frac{1}{2}(|0+\rangle\langle 0+| + |1+\rangle\langle 1+|)$, whereas for $c = 1$, she gets $\rho_1 = \frac{1}{2}(|+0\rangle\langle +0| + (|01\rangle + e^{i\omega}|11\rangle)(\langle 01| + e^{-i\omega}\langle 11|))$, where $\rho_{A'} = \frac{1}{2}(\rho_0 + \rho_1)$. By solving the characteristic equation of $\rho_{A'}$ we get the set of eigenvalues $\{\frac{1}{4}(1 \pm \cos\frac{\omega}{4}), \frac{1}{4}(1 \pm \sin\frac{\omega}{4})\}$. $S(A')$ can then be expressed as follows:

$$S(A') = 1 + \frac{h(\frac{1-\cos(\omega/4)}{2}) + h(\frac{1-\sin(\omega/4)}{2})}{2}.$$

By computing the second derivative of $f(x) = h(\frac{1-\sqrt{x}}{2})$, we get that $f''(x) \leq 0$ in $[0, 1]$, implying that f is concave in $[0, 1]$. For $\alpha \in [0, 1]$, Jensen's inequality yields that $\frac{f(0)+f(1)}{2} \leq f(\alpha)$, and therefore, $\frac{f(0)+f(1)}{2} \leq \frac{f(\alpha)+f(1-\alpha)}{2}$. Consequently, the minimum of $h(\frac{1-\cos(\omega/4)}{2}) + h(\frac{1-\sin(\omega/4)}{2}) = f(\cos^2\frac{\omega}{4}) + f(\sin^2\frac{\omega}{4})$ is achieved for $\omega = 0$ and in this case, $S(A') = \frac{3}{2}$.

Finally, we can conclude that the leakage is minimal for the canonical embedding and $\Delta_\psi(P_{X,Y}) = S(A) - I(X;Y) = S(A') - I(X;Y) \geq \frac{3}{2} - 1 = \frac{1}{2}$. □

There is also a more direct way to interpret this quantity in the case of the canonical embedding $|\psi_{\vec{0}}\rangle$ for $P^{\text{OT}}_{X,Y}$: If Alice and Bob share a single copy of $|\psi_{\vec{0}}\rangle$ then there exist POVMs for both of them which reveal Bob's selection bit to Alice, and the XOR of Alice's bits to Bob, both with probability $\frac{1}{2}$. Let $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ denote the Bell states, and $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Observe that the canonical embedding $|\psi_{\vec{0}}\rangle$ of $P^{\text{OT}}_{X,Y}$ can be expressed as follows:

$$|\psi_{\vec{0}}\rangle = \frac{1}{2}|\Psi^-\rangle \otimes \frac{|\Psi^-\rangle - |\Phi^-\rangle}{\sqrt{2}} + \frac{1}{2}|\Phi^-\rangle \otimes \frac{|\Psi^+\rangle - |\Phi^+\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}|{+}{+}\rangle|{+}{+}\rangle.$$

In order to get the value $x_0 \oplus x_1$ of Alice's bits x_0 and x_1, Bob can use POVM $\mathsf{B} = \{\mathsf{B}_0, \mathsf{B}_1, \mathsf{B}_?\}$ where $\mathsf{B}_0 := \frac{1}{2}(|\Psi^-\rangle - |\Phi^-\rangle)(\langle\Psi^-| - \langle\Phi^-|)$, $\mathsf{B}_1 := \frac{1}{2}(|\Psi^+\rangle - |\Phi^+\rangle)(\langle\Psi^+| - \langle\Phi^+|)$, and $\mathsf{B}_? := |{+}{+}\rangle\langle{+}{+}|$. It is easy to verify that Bob gets outcome B_z for $z \in \{0, 1\}$ (in which case $x_0 \oplus x_1 = z$ with certainty) with probability $\frac{1}{2}$. Alice's POVM can be defined as $\mathsf{A} = \{\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_?\}$ where $\mathsf{A}_0 := |{-}{+}\rangle\langle{-}{+}|$, $\mathsf{A}_1 := |{+}{-}\rangle\langle{+}{-}|$, and $\mathsf{A}_? := \mathbb{I}_2 - \mathsf{A}_0 - \mathsf{A}_1$. By inspection we easily find that the probability for Alice to get Bob's selection bit is $1 - \text{tr}((\mathsf{A}_? \otimes \mathbb{I}_2)|\psi_{\vec{0}}\rangle\langle\psi_{\vec{0}}|) = \frac{1}{2}$. For any embedding of $P^{\text{OT}}_{X,Y}$ we can construct similar POVMs revealing the XOR of Alice's bits to Bob and Bob's selection bit to Alice with probability strictly more than $\frac{1}{4}$.

Based on the examples of $P^{\text{ROT}^r}_{X,Y}$ and $P^{\text{OT}}_{X,Y}$ it is tempting to conjecture that the leakage is always minimized for the canonical embedding, which agrees with the geometric intuition that the minimal pairwise distinguishability of quantum states in a mixture minimizes the von Neumann entropy of the mixture. As shown in [JS00] however, this is not always the case. They show that in a quantum system of dimension at least three, the following situation can happen: For two sets of pure states $\{|u_i\rangle\}_{i=1}^n$ and $\{|v_i\rangle\}_{i=1}^n$ such that for

all i, j satisfying $|\langle u_i|u_j\rangle| \leq |\langle v_i|v_j\rangle|$, there exist probabilities p_i such that for $\rho_u := \sum_{i=1}^n p_i |u_i\rangle\langle u_i|$, $\rho_v := \sum_{i=1}^n p_i |v_i\rangle\langle v_i|$, it holds that $S(\rho_u) < S(\rho_v)$. As we can see, although each pair $|u_i\rangle$, $|u_j\rangle$ is more distinguishable than the corresponding pair $|v_i\rangle$, $|v_j\rangle$, the overall ρ_u provides us with less uncertainty than ρ_v. It follows that although for the canonical embedding $|\psi_{\vec{0}}\rangle = \sum_y |\varphi_y\rangle|y\rangle$ of $P_{X,Y}$ the mutual overlaps $|\langle\varphi_y|\varphi_{y'}\rangle|$ are clearly maximized, it does not necessarily imply that $S(A)$ in this case is minimal over $\mathcal{E}(P_{X,Y})$.

5.2 Lower Bounds on the Leakage of 1-2-OT^r and 1-2-OT$_p$

1-2-OT^r and 1-2-OT$_p$ are primitives where the direct evaluation of the leakage for a general embedding $|\psi_\theta\rangle$ is hard to compute. Instead of computing $S(A)$ directly, we show how to derive lower bounds on the leakage in such cases.

5.2.1 Lower Bound on the Leakage of $P_{X,Y}^{\text{OT}^r}$

Theorem 5.3 *Any embedding $|\psi\rangle$ of $P_{X,Y}^{\text{OT}^r}$ is $(1 - O(r2^{-r}))$-leaking.*

Proof. We use Theorem 4.3 to show that any embedding of $P_{X,Y}^{\text{OT}^r}$ leaks at least as much as an embedding of $P_{X,Y}^{\text{ROT}^r}$. Let (A_0, A_1) and B denote Alice's and Bob's respective registers. Then $|\psi\rangle^{A_0A_1B} \in \mathcal{E}(P_{X,Y}^{\text{OT}^r})$ can be written in the form:

$$|\psi\rangle = \frac{1}{2^{r/2}} \sum_{x\in\{0,1\}^r} |x\rangle^{A_1} |\psi^x\rangle^{A_0B},$$

where each

$$|\psi^x\rangle = \frac{1}{2^{(r+1)/2}} \left(\sum_{x'\in\{0,1\}^r} \left(e^{i\theta(x',x,0)} \big|x'\big\rangle^{A_0} \big|0,x'\big\rangle^{B} + e^{i\theta(x',x,1)} \big|x'\big\rangle^{A_0} |1,x\rangle^{B} \right) \right)$$

can be viewed as an embedding of $P_{X,Y}^{\text{ROT}^r}$. According to Theorem 4.3 and Theorem 5.1, we get that

$$\Delta_{P_{X,Y}^{\text{OT}^r}} \geq \Delta_{P_{X,Y}^{\text{ROT}^r}} = 1 - O(r/2^r).$$

□

5.2.2 Lower Bound on the Leakage of $P_{X,Y}^{\text{OT}_p}$

In the following, we provide a lower bound on the leakage of $P_{X,Y}^{\text{OT}_p}$ for $p < \sin^2(\pi/8) \approx 0.15$. Notice that in fact, the leakage is strictly positive for any embedding of $P_{X,Y}^{\text{OT}_p}$ with $p < 1/4$, since for $p < 1/4$, $P_{X,Y}^{\text{OT}_p}$ is a non-trivial primitive. On the other hand, for $P_{X,Y}^{\text{OT}_{1/4}}$ is a trivial primitive implemented securely by the following protocol in the classical HBC model:

1. Alice chooses randomly between her input bits x_0 and x_1 and sends the chosen value x_a to Bob.

2. Bob chooses his selection bit c uniformly at random and sets $y := x_a$.

Equality $x_c = y$ is satisfied if either $a = c$, which happens with probability $1/2$, or if $a \neq c$ and $x_a = x_{1-a}$, which happens with probability $1/4$. Since the two events are disjoint, it follows that $x_c = y$ with probability $3/4$ and that the protocol implements $P_{X,Y}^{\text{OT}_{1/4}}$. The implementation is clearly secure against honest-but-curious Alice, since she does not receive any message from Bob. It is also secure against Bob, since he receives only one bit from Alice. By letting Alice randomize the value of the bit she is sending, the players can implement $P_{X,Y}^{\text{OT}_p}$ securely for any value $1/4 < p \leq 1/2$.

Theorem 5.4 *If* $p < \frac{1}{2} - \frac{1}{2\sqrt{2}}$ *then*

$$\Delta_{P_{X,Y}^{\text{OT}_p}} \geq \frac{(1/2 - p - \sqrt{p(1-p)})^2}{8 \ln 2}.$$

Proof. First, we show that for any embedding of P_{X,Y_0Y_1} such that Y_0 and Y_1 are independent,

$$S(A; Y_0Y_1) \leq S(A; Y_0) + S(A; Y_1).$$

We can write

$$\begin{aligned} S(A; Y_0) + S(A; Y_1) &= H(Y_0) + H(Y_1) - S(Y_0|A) - S(Y_1|A) \\ &= H(Y_0Y_1) - S(Y_0|A) - S(Y_1|A) \\ &\leq H(Y_0Y_1) - S(Y_0Y_1|A) = S(A; Y_0Y_1). \end{aligned} \tag{5.1}$$

Let X, Y_0, Y_1 be random variables corresponding to Alice's pair of bits, Bob's selection bit, and its value, respectively. For $P_{X,Y}^{\text{OT}_p}$ we have that $I(X; Y_0Y_1) = 1 - h(p)$. $S(A; Y_0Y_1)$ can then be lower-bounded by

$$S(A; Y_0Y_1) \geq S(A; Y_0) + S(A; Y_1) \geq S(A; Y_0) + (1 - h(p)).$$

Hence, for computing the lower bound on $S(A; Y_0Y_1)$, we only need to compute the lower bound on $S(A; Y_0)$. A state $|\psi\rangle \in \mathcal{E}(P_{X,Y}^{\text{OT}_p})$ can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle^{AB_1}|0\rangle^{B_0} + |\psi_1\rangle^{AB_1}|1\rangle^{B_0}).$$

Let $\rho_A^0 := \text{tr}_{B_1} |\psi_0\rangle\langle\psi_0|$ and $\rho_A^1 := \text{tr}_{B_1} |\psi_1\rangle\langle\psi_1|$.
By applying Theorem 2.2, we get that

$$\|\rho_A^0 - \rho_A^1\|_1 \leq \sqrt{8(\ln 2) S(A; Y_0)},$$

and therefore,

$$\frac{\|\rho_A^0 - \rho_A^1\|_1^2}{8 \ln 2} \leq S(A; Y_0). \tag{5.2}$$

The trace norm of $\rho_A^0 - \rho_A^1$ yields an upper bound on the entries of the matrix:

$$|(\rho_A^0 - \rho_A^1)_{ij}| \leq \|\rho_A^0 - \rho_A^1\|_1. \tag{5.3}$$

We can write the state $|\psi\rangle$ in the form:

$$|\psi\rangle = \frac{1}{2}\sum_{y_0,y_1} |\varphi_{y_0,y_1}\rangle^A |y_0,y_1\rangle^{B_0B_1},$$

where

$$\begin{aligned}
|\varphi_{0,y}\rangle &= \sqrt{\frac{1-p}{2}}\sum_{x=0}^{1} e^{i\theta(y,x,0,y)}|y,x\rangle^A|0,y\rangle^{B_0B_1} + \sqrt{\frac{p}{2}}\sum_{x=0}^{1} e^{i\theta(y,x,0,1-y)}|y,x\rangle^A|0,1-y\rangle^{B_0B_1} \\
|\varphi_{1,y}\rangle &= \sqrt{\frac{1-p}{2}}\sum_{x=0}^{1} e^{i\theta(x,y,1,y)}|x,y\rangle^A|1,y\rangle^{B_0B_1} + \sqrt{\frac{p}{2}}\sum_{x=0}^{1} e^{i\theta(x,y,1,1-y)}|x,y\rangle^A|1,1-y\rangle^{B_0B_1}.
\end{aligned}$$

By evaluating the entries of $(\rho_A^0 - \rho_A^1)$ we get a simple lower bound on $|(\rho_A^0 - \rho_A^1)_{ij}|$ for $i \neq j \in \{0,\ldots,3\}$:

$$|(\rho_A^0 - \rho_A^1)_{ij}| \geq \frac{1-2p}{4} - \frac{\sqrt{(1-p)p}}{2} \tag{5.4}$$

hence, from (5.3) follows that

$$\|\rho_A^0 - \rho_A^1\|_1 \geq \frac{1-2p}{4} - \frac{\sqrt{(1-p)p}}{2},$$

yielding due to (5.1) and (5.2) that

$$S(A;Y_0Y_1) \geq 1 - h(p) + S(A;Y_0) \geq 1 - h(p) + \frac{(1/2 - p - \sqrt{(1-p)p})^2}{32\ln 2}.$$

The lower-bound is non-trivial if $1/2 - p - \sqrt{(1-p)p} > 0$, which is true for $p < \frac{1}{2} - \frac{1}{2\sqrt{2}}$. The results yields the following lower-bound on the leakage of $P_{X,Y}^{\mathrm{OT}_p}$:

$$\Delta_{P_{X,Y}^{\mathrm{OT}_p}} \geq \frac{(1/2 - p - \sqrt{(1-p)p})^2}{32\ln 2}.$$

However, this lower-bound is very loose, since for $p = 0$ we get that

$$\Delta_{P_{X,Y}^{\mathrm{OT}}} \geq \frac{1}{128\ln 2} \approx 0.011,$$

which is much weaker than the optimal

$$\Delta_{P_{X,Y}^{\mathrm{OT}}} \geq \frac{1}{2}.$$

□

It remains to mention that by using more careful analysis of the phases of $|\varphi_{0.y}\rangle$ and $|\varphi_{1,y}\rangle$, the lower bound on the absolute value of the outside-diagonal entries from (5.4) can be improved, yielding a non-trivial lower bound on the leakage for $p > 0.15$ and eventually, even for any $p < 1/4$. It is possible that for the values of p close to $1/4$, using Average Encoding Theorem (Theorem 2.2) yields a lower bound with a better ratio compared to the real value of the minimum leakage of an embedding of $P_{X,Y}^{\mathrm{OT}_p}$.

Chapter 6

Two-Party Cryptography from Limited Resources

As we have shown in the Chapter 4, it is not possible to implement non-trivial primitives with no leakage from scratch. A natural question arising from our conclusions is then: What happens if we allow the players to rely in some way on a trusted third party? In such a model, a two-party quantum protocol is represented by an ensemble $\sum_e P_E(e)|e\rangle\langle e| \otimes |\psi_e\rangle\langle\psi_e|$, shared between a pair of players and the environment who do not interact. An ensemble ρ_{EAB} implements a primitive $P_{X,Y}$, if measuring Alice's and Bob's registers in the computational basis yields a distribution $P_{X',Y'}$ such that $P_{X,Y}$ is locally computable from $P_{X',Y'}$. We also consider correct implementations of $P_{X,Y}$, where the meaning of *correctness* is the same as for embeddings:

Definition 6.1 *An ensemble $\rho_{EABA'B'} = \sum_e P_E(e)|e\rangle\langle e| \otimes |\psi_e\rangle\langle\psi_e|$ where for each e, $|\psi_e\rangle \in \mathcal{H}_{ABA'B'}$, is a* correct implementation *of $P_{X,Y}$, if measuring registers A and B of $\rho_{EABA'B'}$ in the computational basis yields the distribution $P_{X,Y}$ and the ensemble satisfies $S(X;YB') = S(XA';Y) = I(X;Y)$.*

In the following, we often use a pure state $|\psi\rangle^{EABA'B'} := \sum_e \sqrt{P_E(e)}|e\rangle^E|\psi_e\rangle^{ABA'B'}$ to describe the state of a protocol instead of an ensemble, but we emphasize that the environment we consider is always classical and corresponds to the measurement of the register E of $|\psi\rangle$ in the computational basis. We also use $\rho_{AB} := \mathrm{tr}_E\,|\psi\rangle\langle\psi|$ to denote only the state held by Alice and Bob. Such a model is general enough, since analogously to the case of embeddings, we can assume that at any step of the protocol's execution, the state shared by the honest-but-curious players is pure given the state of the environment. Our results concerning embeddings capture the case where the environment does not hide any information from the players. On the other hand, if the environment can store an arbitrary amount of information, then any primitive can be implemented privately. The notion of privacy we consider is defined as follows:

Definition 6.2 *And implementation ρ_{AB} of $P_{X,Y}$ is* private *if any information about X that Bob can learn from measuring his part of ρ_{AB}, he can also learn from his output Y of the ideal functionality for $P_{X,Y}$, and analogously if any*

information about Y that Alice can learn from ρ_{AB}, she can also learn through the ideal functionality for $P_{X,Y}$.

An example of a private implementation of a primitive $P_{X,Y}$ is the following one:

$$|\psi\rangle^{EAB} = \sum_{x',y'} \sqrt{P_{X\searrow Y,Y\searrow X}(x',y')}\big|x',y'\big\rangle^{E} \sum_{x,y} \sqrt{P_{X,Y|X\searrow Y=x',Y\searrow X=y'}(x,y)}|x,y\rangle^{AB}., \tag{6.1}$$

We define the leakage of ρ_{AB} analogously to the leakage of a super-embedding:

Definition 6.3 *The leakage of an implementation ρ_{AB} of $P_{X,Y}$ is defined by:*

$$\Delta_{\rho_{AB}} := \max(S_{\rho_{AB}}(X;B) - I(X;Y), S_{\rho_{AB}}(A;Y) - I(X;Y)).$$

The following lemma shows that analogously to the case of super-embeddings, a correct implementation of $P_{X,Y}$ leaks at least as much as some implementation of $P_{X,Y}$ with no extra registers held by the players and no increase in the size of the environment. In the latter case, let $\mathcal{E}(\psi) := \{e :\ P_E(e) > 0\}$ where E is the environment register associated with state $|\psi\rangle^{EAB}$.

Lemma 6.1 *Let $|\psi\rangle^{EABA'B'}$ be a correct implementation of $P_{X,Y}$. Then there exists an implementation $|\psi'\rangle^{EAB} = \sum_{e,x,y} \alpha_{e,x,y}|e,x,y\rangle$ of $P_{X,Y}$ such that $|\mathcal{E}(\psi')| \leq |\mathcal{E}(\psi)|$ (hence, $H_{\psi'}(E) \leq \log|\mathcal{E}(\psi)|$) and*

$$\Delta_{\rho_{AB}}(P_{X,Y}) \geq \Delta_{\rho'_{AB}}(P_{X,Y}),$$

for $\rho'_{AB} := \mathrm{tr}_E\,|\psi'\rangle\langle\psi'|$.

Proof. State $|\psi\rangle^{EABA'B'}$ can be written in the form:

$$\begin{aligned}
|\psi\rangle^{EABA'B'} &= \sum_{e,x,y} \sqrt{P_{E,X,Y}(e,x,y)}|e,x,y\rangle^{EAB}|\psi_{e,x,y}\rangle^{A'B'} \\
&= \sum_{e,x,y} \sqrt{P_{E,X,Y}(e,x,y)}|e,x,y\rangle^{EAB} \sum_{k=1}^{K} \sqrt{\lambda^k_{e,x,y}}\left|a^k_{e,x,y}\right\rangle^{A'} \left|b^k_{e,x,y}\right\rangle^{B'},
\end{aligned}$$

where $\sum_k \sqrt{\lambda^k_{e,x,y}}|a^k_{e,x,y}\rangle^{A'}|b^k_{e,x,y}\rangle^{B'}$ is the Schmidt decomposition of $|\psi_{e,x,y}\rangle^{A'B'}$. We can write

$$\begin{aligned}
S(X;YB') &= H(X) + S(YB') - S(XYB') \\
&= I(X;Y) + \sum_y P_Y(y) S\left(\sum_{e,x} P_{E,X|Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}|\right) \\
&- \sum_{x,y} P_{X,Y}(x,y) S\left(\sum_e P_{E|X=x,Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}|\right).
\end{aligned}$$

Correctness of $|\psi\rangle$ implies $S_\psi(X;YB') - I(X;Y) = 0$ which due to strict concavity of Von Neumann entropy and Jensen's inequality holds if and only if for each y, the following is true:

$$\forall x : \sum_{e,x} P_{E,X|Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}| = \sum_{e} P_{E|X=x,Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}|.$$

Analogously, from $S(XA';Y) = I(X;Y)$ we get that for any fixed x and all y:

$$\sum_{e,y} P_{E,Y|X=x}(e)\,\mathrm{tr}_{B'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}| = \sum_{e} P_{E|X=x,Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}|.$$

Since $\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}| = \mathrm{tr}_{B'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}|$, it follows that for all (x,y):

$$\begin{aligned}\sum_k \sum_e P_{E|(X,Y)=(x,y)}(e)\lambda^k_{e,x,y}\left|b^k_{e,x,y}\right\rangle\left\langle b^k_{e,x,y}\right| &= \sum_e P_{E|(X,Y)=(x,y)}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}| \\ = \sum_{e,x} P_{E,X|Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}| &= \sum_{e,y} P_{E,Y|X=x}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}|,\end{aligned}$$

yielding that for each k, $\sum_e P_{E|X=x,Y=y}(e)\lambda^k_{e,x,y}$ is independent of (x,y). Furthermore, the equality

$$\begin{aligned}\sum_k \sum_e P_{E|(X,Y)=(x,y)}(e)\lambda^k_{e,x_y}\left|b^k_{e,x,y}\right\rangle\left\langle b^k_{e,x,y}\right| &= \sum_{e,x} P_{E,X|Y=y}(e)\,\mathrm{tr}_{A'}\,|\psi_{e,x,y}\rangle\langle\psi_{e,x,y}| \\ &= \sum_{e,x} P_{E,X|Y=y}(e)\sum_k \lambda^k_{e,x,y}\left|b^k_{e,x,y}\right\rangle\left\langle b^k_{e,x,y}\right|\end{aligned}$$

implies that $|b^k_{e,x,y}\rangle$ is independent of x. Analogously, we conclude that $|a^k_{e,x,y}\rangle$ is independent of y. It follows that there are unitary transforms U^A and U^B acting on $\mathcal{H}_{AA'}$ and $\mathcal{H}_{BB'}$, respectively, such that for $|\tilde{\psi}\rangle := \mathbb{I}_E \otimes U^A \otimes U^B|\psi\rangle^{ABEA'B'}$ we get:

$$\left|\tilde{\psi}\right\rangle = \sum_{x,y} |x,y\rangle^{AB}\sqrt{P_{X,Y}(x,y)}\sum_e \sqrt{P_{E|(X,Y)=(x,y)}(e)}|e\rangle^E \mathrm{e}^{i\theta(e,x,y,k)}\sqrt{\lambda^k_{e,x,y}}|k,k\rangle^{A'B'}$$

In order to learn some information about Bob's output, Alice can measure her register A' in the computational basis and thereby convert $|\tilde{\psi}\rangle$ into the state $|\psi_k\rangle^{ABE} \otimes |k\rangle^{B'}$, where

$$|\psi_k\rangle^{ABE} = \mu\sum_{x,y}\sqrt{P_{X,Y}(x,y)}|x,y\rangle^{AB}\sum_e \sqrt{P_{E|(X,Y)=(x,y)}(e)}\mathrm{e}^{i\theta(e,x,y,k)}\sqrt{\lambda^k_{e,x,y}}|e\rangle^E,$$

with μ being a normalization constant. Since $\sum_e P_{E|(X,Y)=(x,y)}\lambda^k_{e,x,y}$ is the same value for all pairs (x,y), μ satisfies:

$$\mu\sum_e P_{E|(X,Y)=(x,y)}(e)\lambda^k_{e,x,y} = 1.$$

The probability that by measuring the registers A and B in the computational basis, the players obtain the joint outcome (x,y) is then $P_{X,Y}(x,y)$. Thus

for each k, $|\psi_k\rangle$ implements $P_{X,Y}$ with no extra registers. Since due to Holevo bound (Theorem 2.1), a measurement of register B' does not increase $S(X;BB')$ (and hence, decrease $S(X|BB')$) on average, we get that for some k,

$$S_{\mathrm{tr}_E |\psi_k\rangle\langle\psi_k|}(X|B) \geq S_{\rho_{AB}}(X|BB'),$$

yielding that for $|\psi'\rangle := |\psi_k\rangle$:

$$\Delta_{\rho'_{AB}}(P_{X,Y}) = \Delta_{\mathrm{tr}_E |\psi'\rangle\langle\psi'|}(P_{X,Y}) \leq \Delta_{\rho_{AB}}(P_{X,Y}).$$

For such $|\psi'\rangle^{EAB}$, $\mathcal{E}(\psi') \subseteq \mathcal{E}(\psi)$, yielding that $|\mathcal{E}(\psi')| \leq |\mathcal{E}(\psi)|$. □

We now show that any non-leaking implementation of $P_{X,Y}$ is in fact, private. Furthermore, such an implementation not only prevents Bob from getting any other information about X than he is allowed to get from the ideal functionality for $P_{X,Y}$, but also, he cannot get any other information about the state of Alice's register than he is given by the ideal functionality, and analogously if the roles of the players are switched. The statement holds regardless of whether the implementation is correct i.e., even if the extra registers of Alice and Bob do not satisfy Definition 6.1. Notice, that this fact does not follow immediately from the definition of a non-leaking implementation, since in such an implementation, the players are allowed to get any information of their choice unless it would mean that the uncertainty about the other party's output decreases below $H(X|Y)$ on Bob's side and $H(Y|X)$ on Alice's side.. As an example of a non-leaking but not even close to private implementation we can take the one of 1-2-OT where Bob can choose to either get the value of his selection bit or the parity of Alice's bits. In both of these cases, his uncertainty about Alice's part remains one bit, hence such an implementation is non-leaking nevertheless, it is not private.

Theorem 6.1 *Let $|\psi\rangle^{EAB}$ be a non-leaking (not necessarily correct) implementation of $P_{X,Y}$. Then $|\psi\rangle^{EAB}$ implements $P_{X,Y}$ privately. Furthermore, in such an implementation, ρ_{AB} is locally equivalent to $\sum_{x',y'} P_{X\searrow Y,Y\searrow X}(x',y')|x',y'\rangle\langle x',y'|$.*

Proof. Here we assume that in $|\psi\rangle^{EAB}$, Bob's entire register is used to compute Y i.e., there are no additional registers on his side. We can view such an implementation as an embedding-analogue. This is without loss of generality because for $\tilde{Y}$ capturing the result of a measurement of only a part of Bob's register, we get that

$$S(X;B) \geq I(X;Y) \geq I(X;\tilde{Y}).$$

It follows that for $|\psi\rangle^{EAB}$ non-leaking, $I(X;Y) = I(X;\tilde{Y})$ has to be satisfied. Since $\tilde{Y}$ is a deterministic function of Y, we obtain $Y \searrow X = \tilde{Y} \searrow X$. Hence, anything we conclude for $Y \searrow X$ also applies to $\tilde{Y} \searrow X$, yielding the validity of the proof for the case where Y captures a measurement of only a part of Bob's register.

Because $|\psi\rangle^{EAB}$ is 0–leaking, we have that $S(X;B) = I(X;Y)$, which by Holevo bound (Theorem 2.1) implies that $\mathrm{tr}_{EA} |\psi\rangle\langle\psi|$ can be written as

$$\mathrm{tr}_{EA} |\psi\rangle\langle\psi| = \sum_x P_X(x) \,\mathrm{tr}_E |\varphi_x\rangle\langle\varphi_x|,$$

where all $\mathrm{tr}_E |\varphi_x\rangle\langle\varphi_x|$ are simultaneously diagonalizable. If the common diagonal basis of these states is $\{|z\rangle\}_z$, then the cq-state shared between Alice tracing out her part and Bob is

$$\rho_{XB} = \sum_{z'} \left(\sum_x \left(P_{X|f_Z(z)=z'}(x) |x\rangle\langle x| \right) \right) \sigma^{z'},$$

where $f_Z(Z) := Z \searrow X$ and

$$\sigma^{z'} := \sum_{z:f_Z(z)=z'} a_z |z\rangle\langle z|.$$

This is a purely classical state, implementing the distribution $P_{X,Z}$ securely on Bob's side. Any information that Bob can learn about the distribution of X is via the distribution of $Z \searrow X$ that he learns by measuring his part. Hence, for the honest measurement of Bob captured by Y, we have that $X \leftrightarrow Z \searrow X \leftrightarrow Y \searrow X$ is a Markov chain. From the assumption $S(X;B) = I(X;Y)$ we get:

$$S(X;B) = I(X;Z) = I(X;Z \searrow X) = I(X;Y) = I(X;Y \searrow X),$$

yielding that $S(X|Y \searrow X) = S(X|Z \searrow X)$. Due to the Markov chain property,

$$S(X|Z \searrow X, Y \searrow X) = S(X|Z \searrow X),$$

implying that

$$S(X|Y \searrow X, Z \searrow X) = S(X|Y \searrow X),$$

i.e. $X \leftrightarrow Y \searrow X \leftrightarrow Z \searrow X$ is also a Markov chain. Since both $Z \searrow X$ and $Y \searrow X$ are minimal random variables W_Z, W_Y such that $X \leftrightarrow W_Z \leftrightarrow X \searrow Z$ and $X \leftrightarrow W_Y \leftrightarrow Y \searrow X$ are Markov chains, we get that $Z \searrow X = Y \searrow X$. Then ρ_{XB} can be written as:

$$\rho_{XB} = \sum_{y'} \sum_x \left(P_{X|f_Y(y)=y'}(x) |x\rangle\langle x| \right) \rho^{y'},$$

where the support of each of $\rho^{y'}$ only contains y-values such that $f_Y(y) = y'$. It follows that then, ρ_{XB} privately implements $P_{X,Y\searrow X}$ on Bob's side. Analogously, $S(A;Y) = I(X;Y)$ implies that ρ_{AY} privately implements $P_{Y\searrow X,Y}$ on Alice's side. In such a case, $\mathrm{tr}_E |\psi\rangle\langle\psi| = \mathrm{tr}_E |\psi'\rangle\langle\psi'|$ for $|\psi'\rangle^{EAB}$ satisfying

$$\left|\psi'\right\rangle^{EAB} = \sum_{x',y'} \sqrt{P_{X\searrow Y,Y\searrow X}(x',y')} \left|x',y'\right\rangle^E \left|\omega_{x',y'}\right\rangle^{AB}$$

where

$$\left|\omega_{x',y'}\right\rangle^{AB} = \sum_{x,y:f_X(x)=x',f_Y(y)=y'} \alpha^{x,y} |x,y\rangle.$$

For $S(X;B)$ we then get that

$$\begin{aligned} S(X;B) &= I(X \searrow Y; Y \searrow X) + \sum_{x',y'} P_{X\searrow Y,Y\searrow X}(x',y') S(\mathrm{tr}_A \left|\omega_{x',y'}\right\rangle\!\left\langle\omega_{x',y'}\right|) \\ &= I(X;Y) + \sum_{x',y'} P_{X\searrow Y,Y\searrow X}(x',y') S(\mathrm{tr}_A \left|\omega_{x',y'}\right\rangle\!\left\langle\omega_{x',y'}\right|). \end{aligned}$$

Hence, equality $S(X;B) = I(X;Y)$ can hold only if all $|\omega_{x',y'}\rangle$ are product states, yielding that there are local unitary transforms U^A and U^B acting on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, such that

$$\mathbb{I}_E \otimes U^A \otimes U^B \big|\psi'\big\rangle = \sum_{x',y'} \sqrt{P_{X\searrow Y, Y\searrow X}(x',y')}\big|x',y'\big\rangle^E \big|x',y'\big\rangle^{AB}.$$

Therefore, $\mathrm{tr}_E\,|\psi\rangle\langle\psi| = \mathrm{tr}_E\,|\psi'\rangle\langle\psi'|$ does not allow Alice and Bob to learn anything more about the states of B and A (and therefore, also the values of Y and X), respectively, than they obtain from $X \searrow Y$ and $Y \searrow X$, concluding that $|\psi\rangle^{EAB}$ is a private implementation of $P_{X,Y}$. □

The statement that we just proved has several consequences, formulated in the following lemmas.

Lemma 6.2 *A non-leaking implementation of a primitive $P_{X,Y}$ satisfies $S(E|B) \geq H(X \searrow Y|Y)$ and $S(E|A) \geq H(Y \searrow X|X)$.*

Proof. In a non-leaking implementation $|\psi\rangle^{EAB}$ of $P_{X,Y}$, ρ_{AB} is locally equivalent to $\sigma := \sum_{x',y'} P_{X\searrow Y, Y\searrow X}|x',y'\rangle\langle x',y'|$ according to Theorem 6.1. For Alice measuring her part, we obtained the following cq-state shared among the three parties:

$$\rho_{XEB} = \sum_{x'} P_{X\searrow Y}(x')\big|x'\big\rangle\big\langle x'\big| \otimes |\varphi_{x'}\rangle\langle\varphi_{x'}|,$$

where from Bob's perspective, $|\varphi_{x'}\rangle$ must be equivalent to

$$|\varphi_{x'}\rangle^{EB} = \sum_{y'} \sqrt{P_{Y\searrow X|X\searrow Y=x'}(y')}\big|y'\big\rangle^E \big|y'\big\rangle^B,$$

in order to obtain the desired form of σ. It follows that then,

$$S(E|A) = S(E|X) \geq H(Y \searrow X|X \searrow Y) = H(Y \searrow X|X).$$

On Bob's side, the inequality $S(E|B) \geq H(X \searrow Y|Y)$ can be proven analogously. □

The lower bound from the lemma above can always be achieved e.g. by formula (6.1). The result we have shown is analogous to the one holding in the purely classical case where the players implement a distribution with the help of a trusted third party. Here, let E be the random variable corresponding to the information held by the trusted third party Elena. Then the result of [WW05a] showing that $H(X \searrow Y|Y)$ and $H(Y \searrow X|X)$ are non-increasing monotones for classical two-party computation, implies that in any private classical protocol for $P_{X,Y}$, $H(E|X) \geq H(Y \searrow X|X)$ and $H(E|Y) \geq H(X \searrow Y|Y)$. The claim can be shown simply, as follows: Assume that Bob and Elena act as only one player and implement a distribution $P_{X,Y}$ in such a way that Alice does not learn any more information than she is supposed to. We can view such a

protocol as a two-party protocol built from scratch that implements $P_{X,Y}$ trivially, yet securely against Alice. The views of both parties are then captured by random variables X and YE. According to [WW05a], we get

$$H(X \searrow YE|E,Y) = 0.$$

The definition of the dependent part directly implies that

$$H(X \searrow Y|E,Y) \leq H(X \searrow YE|E,Y) = 0,$$

hence, $H(X \searrow Y|E,Y) = 0$. We can write:

$$H(X \searrow Y|Y) \leq H(X \searrow Y|E,Y) + H(E|Y) = H(E|Y).$$

Analogously, $H(E|X) \geq H(Y \searrow X|X)$. It follows that the amounts of information needed to be kept by the trusted third party/environment in both classical and quantum case are equal. The lower bounds on $H(E|X)$ and $H(E|Y)$ are achieved by a private classical protocol for $P_{X,Y}$ involving the trusted third party who picks the values of $X \searrow Y$ and $Y \searrow X$ and distributes them to the players.

The following lemma says that at any moment in a quantum protocol using a (perfect) blackbox for $P_{X,Y}$, $S(E|A)$ and $S(E|B)$ can be considered to be upper-bounded by $H(Y \searrow X|X)$ and $H(X \searrow Y|Y)$, respectively.

Lemma 6.3 *Consider a quantum protocol equipped with a blackbox for $P_{X,Y}$. From the players' perspectives, such a protocol is indistinguishable from a protocol where $S(E|A) \leq H(Y \searrow X|X)$ and $S(E|B) \leq H(X \searrow Y|Y)$ during the entire protocol execution.*

Proof. From the players' points of view, a blackbox for $P_{X,Y}$ is locally equivalent to the state $\sigma_{AB} = \sum_{x',y'} P_{X\searrow Y,Y\searrow X}(x',y')|x',y'\rangle\langle x',y'|$ which is purely classical and satisfies $\sigma_{AB} = \mathrm{tr}_E\,|\psi\rangle\langle\psi|$ for

$$|\psi\rangle^{EAB} = \sum_{x',y'} \sqrt{P_{X\searrow Y,Y\searrow X}(x',y')}\big|x',y'\big\rangle^{E}\big|x',y'\big\rangle^{AB}.$$

For such $|\psi\rangle$, we have that $S(E|A) = H(Y \searrow X|X)$ and $S(E|B) = H(X \searrow Y|Y)$. Since there is no interaction between the players and the environment, the protocol built upon $|\psi\rangle$ and the same protocol using a different perfect implementation of $P_{X,Y}$ are indistinguishable from both players' perspectives. The bits that each player receives from a blackbox for $P_{X,Y}$ are only classically correlated with the environment and with the outcome of the other player. It follows that at any moment of the protocol's execution, honest-but-curious players can measure their parts of the blackbox output, store their respective classical outcomes, and proceed further without being detected. Such a measurement on Alice's side extracts incomplete information about the environment which therefore partially collapses. If the measurement takes place at the beginning of the computation, where it is not preceded by any non-invertible operation such as another measurement, then Alice's uncertainty about the environment at

this point is $H(Y \searrow X|X)$. Since the environment remains unaffected during the protocol's run, $S(E|A)$ cannot exceed this value at any time later. □

As an immediate consequence of the previous three statements we get the following theorem:

Theorem 6.2 *Suppose that primitives $P_{X,Y}$ and $P_{X',Y'}$ satisfy $H(X' \searrow Y'|Y') > H(X \searrow Y|Y)$ or $H(Y' \searrow X'|X') > H(Y \searrow X|X)$. Then any implementation of $P_{X',Y'}$ using just one call to the ideal functionality for $P_{X,Y}$ leaks information.*

Proof. WLOG assume that $H(Y' \searrow X'|X') > H(Y \searrow X|X)$. There is a blackbox implementation of $P_{X,Y}$ of the form given by (6.1), where $S(E|A) = H(Y \searrow X|X)$. According to Lemma 6.3, the protocol for $P_{X',Y'}$ built upon such a blackbox is indistinguishable from the same protocol using a different blackbox for $P_{X,Y}$. Furthermore, $S(E|A) \leq H(Y \searrow X|X)$ during the entire run of the protocol using the blackbox in the form (6.1). However, Lemma 6.2 yields that in any non-leaking implementation of $P_{X',Y'}$, $S(E|A) \geq H(Y' \searrow X'|X')$ must hold. Since $H(Y' \searrow X'|X') > H(Y \searrow X|X)$, the claim follows. □

Corollary 6.1 *Let $P_{X,Y}$ be a non-trivial primitive. Then any implementation of M copies of $P_{X,Y}$ using $m < M$ perfect instances of $P_{X,Y}$ leaks information.*

Proof. The primitives $P_{\tilde{X},\tilde{Y}} := (P_{X,Y})^m$ and $P_{\tilde{X}',\tilde{Y}'} := (P_{X,Y})^M$ satisfy

$$H(\tilde{Y} \searrow \tilde{X}|\tilde{X}) = mH(Y \searrow X|X), \quad H(\tilde{Y}' \searrow \tilde{X}'|\tilde{X}') = MH(Y \searrow X|X).$$

Non-triviality of $P_{X,Y}$ implies $H(Y \searrow X|X) > 0$, yielding that then,

$$H(\tilde{Y}' \searrow \tilde{X}'|\tilde{X}') > H(\tilde{Y} \searrow \tilde{X}|\tilde{X}).$$

The rest follows from Theorem 6.2. □

Theorem 6.1 shows that if we require an implementation to be non-leaking, then being quantum in our model does not give the players any advantage, in the sense that they still need the same amount of correlation with the environment as when they are classical. This leaves many unanswered questions, arising mostly from the problem of how much correlation with the environment the players need in order to implement a given primitive with bounded leakage. We summarize these questions in Chapter 8. Consequently, it seems that analyzing two-party quantum computation via certain kind of "monotones" as we did in this chapter might be rather powerful and deserves deeper investigation.

Chapter 7

Only Trivial Protocols Can Be Composed

In this chapter we show that quantum protocols even characterized only by the embeddings of the corresponding primitives (i.e. without considering whether or not that state can be distributed fairly) do not compose without allowing the adversary to mount joint attacks that cannot be simulated by attacks applied to individual copies. We are allowed to make this simplification because any attack of a super-embedding of a primitive can be modeled by an at least equally efficient (in terms of the amount of extra information accessible by a cheater) attack of the associated protocol. We define trivial protocols to be such that produce trivial super-embeddings.

Definition 7.1 *A correct protocol for a primitive $P_{X,Y}$ is* trivial*, if the super-embedding produced by such a protocol is trivial. Otherwise, it is called* non-trivial*.*

In order to show non-composability of a non-trivial super-embedding $|\psi\rangle \in \mathcal{H}_{ABA'B}$ of a primitive $P_{X,Y}$, satisfying t $S_\psi(X \searrow Y|BB') > 0$ and $S_\psi(Y \searrow X|AA') > 0$, it is sufficient to show that no non-trivial embedding of $P_{X,Y}$ can be composed, for the following reason: In the proof of Lemma 4.2 we have shown that by measuring register A' of $|\psi\rangle$, Alice converts $|\psi\rangle$ into $|\psi_k\rangle$ for some $k \in \{1, \ldots, K\}$, which is an embedding of $P_{X,Y}$. If she performs such a measurement on many copies of $|\psi\rangle$, with high probability at least some constant fraction of them collapses into the same non-trivial embedding of $P_{X,Y}$. Non-composability of such an embedding then implies non-composability of super-embedding $|\psi\rangle$ of $P_{X,Y}$. The protocol composability questions can therefore be reduced to investigating composability of these embeddings.

In the following, we formalize the weakness of non-composability inherent to any two-party quantum protocol, preventing us from building strong cryptographic primitives even from non-trivial weak ones. This is in a sharp contrast with quantum key distribution – a three-party game that can be shown to be universally composable [BHL$^+$05].

Composability of quantum protocols has been studied by Ben-Or and Mayers [BM02, BM04] and by Unruh [Unr04]. The former approach is an extension of Canetti's framework [Can01] to the quantum case while the latter is an extension of Backes, Pfitzmann, and Waidner [BPW04]. We are going to consider

a weaker version of composability called *weak composability* and show that almost no quantum protocol satisfies it. Informally, we call a quantum two-party protocol weakly self-composable if any adversarial strategy acting, possibly coherently, upon n independent copies of the protocol is equivalent to a strategy which acts individually upon each copy of the protocol.

7.1 Ideal Functionalities

In order to guarantee composability, the functionality of a quantum protocol should be modeled by some classical ideal functionality. An ideal functionality is a classical description of what the protocol achieves independently of the environment in which it is executed. If a protocol does not admit such a description then it can clearly not be used in any environment while keeping its functionality, and such a protocol would not compose securely in all applications.

In the following, let $\mathcal{H}_A$ and $\mathcal{H}_B$ denote Alice's and Bob's quantum systems, respectively, and let $\mathcal{X}$ and $\mathcal{Y}$ denote the set of classical outcomes of Alice's and Bob's final measurements.

Intuitively, a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ implements the ideal functionality ID_ψ if whatever the adversary does on his/her part of $|\psi\rangle$, there exists a classical input to ID_ψ for the adversary that produces the same view. The ideal functionality ID_ψ accepts inputs for Alice and for Bob in [0..1], where the elements of [0..1] encode all possible strategies for both parties. When a party inputs 0 to ID_ψ, the outcome of measuring this party's part of $|\psi\rangle$ in the computational basis, encoded by a number in [0..1] is returned to the party. This corresponds to the honest behavior. When $m \in [0..1]$ is input to ID_ψ, a measurement depending upon m is applied to register $\mathcal{H}_A$ (resp. $\mathcal{H}_B$) of $|\psi\rangle$ and the classical outcome is returned to Alice (resp. Bob). Such a measurement acts only locally on the specified system. Clearly, for ID_ψ to be of any cryptographic value, the set of possible strategies should be small, otherwise it would be very difficult to characterize exactly what ID_ψ achieves. As we are going to show next, even if $|\psi\rangle$ implements such an ID_ψ where [0..1] is used to encode all possible POVMs in $\mathcal{H}_A$ and $\mathcal{H}_B$ then all adversarial strategies against $|\psi\rangle^{\otimes n}$ cannot be modeled by calls to n copies of ID_ψ.

We write $\mathsf{ID}_\psi(m, 0) = (\tilde{w}, z)$ for the ideal functionality corresponding to pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ with honest Bob and dishonest Alice using strategy $m \in (0..1]$. The output $\tilde{w}$ is provided to Alice and $z \in [0..1]$ encoding an event in $\mathcal{Y}$ to Bob. Similarly, we write $\mathsf{ID}_\psi(0, m) = (z, \tilde{w})$ when Alice is honest and Bob is dishonest and is using strategy $m \in (0..1]$. Notice that an ideal functionality for state $|\psi\rangle$ is easy to implement by letting ID_ψ simulate Alice's and Bob's strategies through a classical interface.

In general, ID_ψ returns one party's output as soon as its strategy has been specified. The ideal functionality never waits for both parties before returning the outcomes. This models the fact that shared pure states never signal from one party to the other. The ideal functionality ID_ψ can be queried by one party more than once with different strategies. The ideal functionality keeps track

of the residual state after one strategy is applied. If a new strategy is applied then it is applied to the residual state. This feature captures the fact that the first measurement can be applied before knowing how to refine it, which may happen when Alice and Bob are involved in an interactive protocol using only classical communication from shared state $|\psi\rangle$. Dishonest Alice may measure partially her part of $|\psi\rangle$ before announcing the outcome to Bob. Bob could then send information to Alice allowing her to refine her measurement of $|\psi\rangle$ dependently of what she received from him. This procedure can be simulated using ID_ψ after specifying a partial POVM for Alice's first measurement among the set of POVMs encoded by the elements of [0..1]. Then, Alice refines her first measurement by specifying a new POVM represented by an element of [0..1] to the ideal functionality ID_ψ.

7.2 Simulation

A pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ implements the ideal functionality ID_ψ if any attack implemented via POVM $\mathcal{M}$ by adversary Alice (resp. adversary Bob) can be simulated by calling the ideal functionality with some $m \in [0..1]$. The attack in the simulated world calls ID_ψ only once as it is in the real case. The ideal functionality ID_ψ therefore refuses to answer more than one query per party. Remember also that ID_ψ returns the outcome to one party as soon as the party's strategy is specified irrespectively of whether the other party has specified its own.

First, let us show on an example what do we mean by simulation of an attack using the calls to the ideal functionality.

Example 7.1 *Consider that Alice and Bob are sharing* $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *which is an embedding of the joint probability distribution* $P_{X,Y}$ *with* $P_{X,Y}(0,0) = P_{X,Y}(1,1) = 1/2$. *Alice's and Bob's honest measurement happen to be in the Schmidt basis. We can define the ideal functionality* ID_{EPR} *as follows:*

$$\mathsf{ID}_{\text{EPR}}(0,0) = (x,x) \text{ with prob. } \tfrac{1}{2}.$$

Since both players are measuring in the Schmidt basis, it follows that ID_{EPR} *models any adversarial behavior.* ID_{EPR} *is an ideal functionality for* $|\Psi^+\rangle$ *even in a context where it is a part of a larger system. However,* $|\Psi^+\rangle$ *is a trivial embedding!*

Notice that any strategy against $|\Psi^+\rangle^{\otimes m}$ can be simulated by appropriate calls to m copies of ID_{EPR}. In other words, $|\psi^+\rangle$ is self-composable in a weak sense. In the following section we show that in fact, all weakly self-composable embedding of joint probability distributions are trivial.

7.3 Self-Composability of Embeddings

We define the *classical weak self-composability* of an embedding $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ of a joint probability distribution $P_{X,Y}$ as its ability to be composed with itself

without allowing the adversary to get information about X resp. Y that is not available through calls to independent copies of ID_ψ.

Definition 7.2 *An embedding $|\psi\rangle$ of $P_{X,Y}$ is* weakly self-composable *if there exists an ideal functionality ID_ψ such that all attacks against $|\psi\rangle^{\otimes m}$ for any $m > 0$ can be simulated by appropriate calls to m ideal functionalities ID_ψ.*

Next, we show that only (not necessarily all) trivial embeddings can be weakly self-composed. The idea behind this result is the definition of a protocol computing a function, between Alice and Bob sharing $|\psi\rangle^{\otimes m}$ such that Bob can make the expected value of the function strictly larger provided he has the capabilities to measure his part of $|\psi\rangle^{\otimes m}$ coherently rather than individually. Only individual measurements can be performed by Bob if ID_ψ is modelling the behavior of $|\psi\rangle$ in any situation. Consider that Alice and Bob are sharing a non-trivial embedding $|\psi\rangle$ of $P_{X,Y}$ that can be written as:

$$|\psi\rangle = \sum_{x\in\mathcal{X}} \sqrt{P_X(x)}|x\rangle^A|\psi_x\rangle^B. \tag{7.1}$$

We show in Lemma 7.1 that $|\psi\rangle$ being non-trivial (i.e. $S(X \searrow Y|\rho_B) > 0$) implies the existence of $x_0 \neq x_1 \in \mathcal{X}$ such that

$$0 < |\langle\psi_{x_0}|\psi_{x_1}\rangle|^2 < 1. \tag{7.2}$$

Protocol 7.1 challenges Bob to *identify* in some sense the state of two positions chosen uniformly and at random among the following possibilities:

$\{|\psi_{x_0}\rangle|\psi_{x_0}\rangle, |\psi_{x_0}\rangle|\psi_{x_1}\rangle, |\psi_{x_1}\rangle|\psi_{x_0}\rangle, |\psi_{x_1}\rangle|\psi_{x_1}\rangle\}$. We will show that Bob, restricted to interact with his subsystem through the ideal functionality ID_ψ, cannot make the expected value of a certain function as large as when it is allowed to interact unconditionally (i.e. *coherently*) with his subsystem. We now prove that such $x_0, x_1 \in \mathcal{X}$ exist for any non-trivial embedding.

Lemma 7.1 *If $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a non-trivial embedding of $P_{X,Y}$ then there exist $x_0, x_1 \in \mathcal{X}$ such that $|\psi_{x_0}\rangle$ and $|\psi_{x_1}\rangle$ satisfy*

$$0 < |\langle\psi_{x_0}|\psi_{x_1}\rangle| < 1.$$

Proof. Let us write $|\psi\rangle$ as,

$$|\psi\rangle = \sum_{x\in\mathcal{X}} \sqrt{P_X(x)}|x\rangle^A|\psi_x\rangle^B. \tag{7.3}$$

Let $\{|\psi_1^*\rangle, \ldots, |\psi_\ell^*\rangle\} \subseteq \{|\psi_x\rangle\}_{x\in\mathcal{X}}$ be the set of different states $|\psi_x\rangle$ available to Bob when Alice measures X. Equation (7.3) can be re-written as,

$$|\psi\rangle = \sum_{j=1}^{\ell} \left(\sum_{\substack{x\in\mathcal{X}:\\ |\psi_x\rangle=|\psi_j^*\rangle}} e^{i\theta(x)}\sqrt{P_X(x)}|x\rangle \right) \otimes |\psi_j^*\rangle, \tag{7.4}$$

for some $\theta(x) \in [0 \dots 2\pi)$.

If $\{|\psi_j^*\rangle\}_{j=1}^{\ell}$ are mutually orthogonal then if Bob measures in this basis no uncertainty about $X \searrow Y$ is left contradicting the fact that $S(X \searrow Y|\rho_B) > 0$. □

In Protocol 7.1 Alice asks Bob to compare the two pure states on his side. In the next section we define a game related to the state comparison problem and show that there is a coherent strategy which in this game can succeed strictly better than any separable one, and therefore also LOCC strategy on Bob's registers.

CHALLENGE:

1. Let $p := 0$ and let Alice and Bob both know $x_0, x_1 \in \mathcal{X}$ such that $0 < |\langle\psi_{x_0}|\psi_{x_1}\rangle| = \tau < 1$ is satisfied.
2. Alice gets $X^m = X_1, \dots, X_m$ by measuring her part in all m copies of $|\psi\rangle$ in the computational basis. She identifies 4 positions $1 \leq i \neq i', j \neq j' \leq m$ such that $X_i = X_{i'} = x_0$ and $X_j = X_{j'} = x_1$. If such four positions do not exist then Alice announces to Bob that $p = 0$ and aborts.
3. Alice picks $(h, h') \in \{i, i', j, j'\}$ with $h \neq h'$ such that $(X_h, X_{h'}) = (\alpha, \beta)$ with probability $1/4$ for any choice of $\alpha, \beta \in \{x_0, x_1\}$ and announces (h, h') to Bob.
4. Bob sends $b \in \{0, 1, ?\}$ to Alice, guessing whether the pair of pure states on the positions h, h' is one of $A_0 := \{|\psi_{x_0}\rangle|\psi_{x_0}\rangle, |\psi_{x_1}\rangle|\psi_{x_1}\rangle\}$, $\mathsf{A}_1 := \{|\psi_{x_0}\rangle|\psi_{x_1}\rangle, |\psi_{x_1}\rangle|\psi_{x_0}\rangle\}$, or responds by "don't know".
5. Alice sets the payoff value p: $p := -c$ if Bob responded incorrectly, $p := 0$ if he answered "don't know", and $p := 1$ if he answered the challenge correctly.

Figure 7.1: A state comparison challenge to Bob.

7.4 State-Comparison Game with a Separably Inapproximable Coherent Strategy

Consider the challenge from Protocol 7.1. In the game defined by this protocol, Alice lets Bob compare two states defined by a non-trivial embedding of a given primitive, which are either identical or different, but not orthogonal. Bob is allowed to response inconclusively however, for such an answer he obtains 0 points. On the other hand, if his guess is right, he obtains 1 point and if it is wrong, he obtains $-c$ points for some positive number c which we determine later. We call his score *payoff*. With respect to the game defined by Protocol 7.1, let the maximal achievable expected payoff over the set of all measurement strategies be denoted by $p_{\max}$. In this section we show that there exists c such that the maximal average payoff $p_{\max}$ can be only achieved with a strategy

coherent on the registers corresponding to the two factors of Bob's product state. Furthermore, we show that for such a c there is a constant gap between the maximal payoff achievable with a separable strategy and $p_{\max}$. Separable measurements on a quantum system consisting of two subsystems are such that any of their elements M is in the form $M = \sum_{i,j} F_i^0 \otimes F_j^1$, where F_i^0, F_j^1 are the operators acting on the respective subsystems of the given system. According to [BDF+99], separable measurements form a strict superset of all LOCC measurements.

It is shown in [KKB05] that for $0 < \tau < 1$, the optimal no-error measurement is always coherent. Furthermore, they prove that the highest success rate achievable by a separable unambiguous measurement is $(1-\tau)^2$ whereas the optimal measurement has a success rate $(1-\tau)$.

Fix the value of $0 < \tau < 1$. For c sufficiently large the best coherent strategy is to apply the best unambiguous measurement with the correct-answer rate $1-\tau$, and to output *don't know* for an uncertain result. Therefore, for some c we have $p_{\max} = 1-\tau$. Let p_s denote the supremum of average payoffs in the game from Protocol 7.1 achievable by separable strategies.

Theorem 7.1 *In the game from Protocol 7.1 there exists $c > 0$ such that $p_s \leq p_{\max} - f(\tau)$, where $f(\tau) > 0$ whenever $0 < \tau < 1$.*

Before proving the actual theorem, we introduce a useful lemma.

Lemma 7.2 *Let $|\varphi_0\rangle, |\varphi_1\rangle \in \mathcal{H}$ be pure states such that $|\langle\varphi_0|\varphi_1\rangle| = \tau$. For a discrimination strategy $\mathcal{S}$ with three possible outcomes 0, 1, and "don't know", let q_c denote the probability of a conclusive answer and q_{err} the probability of a wrong answer. Then,*

$$q_c \leq 2q_{\text{err}} + 1 - \tau + 2\sqrt{q_{\text{err}}(1-\tau)}.$$

Proof. According to Lemma 2.3,

$$q_{\text{err}} \geq \frac{1}{2}\left(q_c - \sqrt{q_c^2 - (q_c - (1-\cos\theta))^2}\right).$$

Equivalently, we get:

$$\sqrt{q_c^2 - (q_c - (1-\cos\theta))^2} \geq q_c - 2q_{\text{err}}.$$

By squaring both sides of the inequality we obtain:

$$\begin{aligned} 2q_c(1-\cos\theta) - (1-\cos\theta)^2 &\geq q_c^2 + 4q_{\text{err}}^2 - 4q_c q_{\text{err}} \\ q_c^2 - q_c(4q_{\text{err}} + 2(1-\tau)) + (1-\tau)^2 + 2q_{\text{err}}^2 &\leq 0. \end{aligned} \tag{7.5}$$

By solving the quadratic equation

$$q_c^2 - q_c(4q_{\text{err}} + 2(1-\tau)) + (1-\tau)^2 + 2q_{\text{err}}^2 = 0,$$

we get the solutions $2q_{\text{err}} + 1 - \tau \pm 2\sqrt{q_{\text{err}}(1-\tau)}$, implying the solutions of (7.5) to be

$$q_c \leq 2q_{\text{err}} + 1 - \tau + 2\sqrt{q_{\text{err}}(1-\tau)}.$$

□

Proof Theorem7.1. The method we use is the following: For given parameters $\tau, c \in \mathbb{R}$ such that $0 < \tau < 1$ and $c > 0$, and an additional parameter $k > 0$, we divide the set of all separable measurements into three subsets according to the probability q_{err} of Bob's incorrect (conclusive) answer in the state-comparison, expressed as a function of c, k, and τ. We construct an upper bound on p_s in each of the three sets separately and dependently on c, k, and τ. Finally, we find the conditions for c and k such that in all three sets we get $p_s \leq p_{\max} - f(\tau)$ for some $f(\tau) > 0$.

[KKB05] shows that the best separable unambiguous strategy for solving the 2-out-of-2 state comparison problem is applying the best unambiguous measurements on each part of Bob's register independently. Lemma A.2 (see Appendix A) says that the payoff achieved by such a strategy in the case where probability q_{err} is small, is close to the optimal payoff. The analysis of such a situation is captured in the first of the three cases, where we consider the separable measurements with $q_{\text{err}} \leq \frac{1}{2k(c+1)}$.

1. ($q_{\text{err}} \leq \frac{1}{2k(c+1)}$) Lemma A.2 shows that to any separable measurement $\mathcal{M} = (E_0, E_1, E_?)$ with probability of error $q_{\text{err}} \leq \frac{1}{2(c+1)k}$ and the expected payoff p, there exists a separable measurement $\mathcal{M}' = (E'_0, E'_1, E'_?)$ with the expected payoff p', satisfying $p \leq p' + \frac{1}{k} + O(1/\sqrt{c})$, such that its elements can be written in the form:

$$E'_0 = G^0_0 \otimes G^1_0 + G^0_1 \otimes G^1_1, \quad E'_1 = G^0_0 \otimes G^1_1 + G^0_1 \otimes G^1_0, \quad E'_? = 1 - E'_0 - E'_1,$$

where the upper index of G^β_α refers to the subsystem and the lower index determines the guess of the state of the corresponding subsystem.

The upper bound on the value of p' which we compute next, can then be used to upper bound p. Consider an extended problem where Bob is supposed to identify each factor of his product state (in contrast to just comparing the factors in the game). Let q^0_{err}, q^1_{err}, and q^0_c, q^1_c denote the probabilities of Bob's incorrect resp. conclusive answers in each of his subsystems. Then the probability of comparing the states incorrectly can be expressed as follows:

$$q_{\text{err}} = q^0_{\text{err}}(q^1_c - q^1_{\text{err}}) + q^1_{\text{err}}(q^0_c - q^1_{\text{err}}) = q^1_c q^0_{\text{err}} + q^1_c q^1_{\text{err}} - 2q^0_{\text{err}} q^1_{\text{err}}.$$

For separable strategies for which $q^1_c < 1-\tau-2/k$ or $q^0_c < 1-\tau-2/k$, we obtain $p' < 1-\tau-2/k$ and hence, $p < 1-\tau-1/k+O(1/\sqrt{c})$ due to Lemma A.2. For c sufficiently large we then get:

$$p_{\max} - p \geq \frac{1}{2k}. \tag{7.6}$$

Next, we discuss the case (not disjoint with the previous one) where both $q^0_c, q^1_c \geq 1 - \tau - 1/k =: \gamma$, which implies that

$$q_{\text{err}} \geq \gamma(q^0_{\text{err}} + q^1_{\text{err}}) - 2q^0_{\text{err}} q^1_{\text{err}}. \tag{7.7}$$

For upper bounding the probability q^0_c of a conclusive answer of the measurement $\mathcal{M}'$ we use Lemma 7.2 (an analogous formula holds for q^1_c):

$$q^0_c \leq 2q^0_{\text{err}} + 1 - \tau + 2\sqrt{q^0_{\text{err}}(1-\tau)}.$$

The probability of correct state-identification in the first of Bob's subsystems then satisfies:

$$q_c^0 - q_{\text{err}}^0 \leq q_{\text{err}}^0 + 1 - \tau + 2\sqrt{q_{\text{err}}^0(1-\tau)}. \tag{7.8}$$

Inequalities (7.7) and (7.8) give us an upper bound on p' for $c > 9$:

$$\begin{aligned} p' \leq & \quad -cq_{\text{err}} + q_{\text{err}}^0 q_{\text{err}}^1 \\ + & \quad (q_{\text{err}}^0 + 1 - \tau + 2\sqrt{q_{\text{err}}^0(1-\tau)})(q_{\text{err}}^1 + 1 - \tau + 2\sqrt{q_{\text{err}}^1(1-\tau)}) \\ \leq & \quad -cq_{\text{err}} + (1-\tau)^2 + 2(\sqrt{q_{\text{err}}^0} + \sqrt{q_{\text{err}}^1}) + 9q_{\text{err}} \\ \leq & \quad (1-\tau)^2 + \frac{4\sqrt{q_{\text{err}}}}{\sqrt{\gamma}} \leq (1-\tau)^2 + \frac{4}{\sqrt{2\gamma k(c+1)}} \end{aligned}$$

hence by Lemma A.2, $p \leq (1-\tau)^2 + \frac{4}{\sqrt{2\gamma k(c+1)}} + \frac{1}{k} + O(1/\sqrt{c})$. For c sufficiently large we get:

$$p \leq (1-\tau)^2 + \frac{2}{k}. \tag{7.9}$$

2. Second, we assume that $\frac{1}{2k(c+1)} < q_{\text{err}} \leq \frac{1}{256(1-\tau)}$. To upper bound the probability of comparing the states correctly, we use the same argument as in (7.8) and get that:

$$q_c - q_{\text{err}} \leq q_{\text{err}} + 1 - \tau + 2\sqrt{q_{\text{err}}(1-\tau)},$$

where q_c denotes the probability of a conclusive outcome. This inequality implies the upper bound on p:

$$p \leq -cq_{\text{err}} + (q_c - q_{\text{err}}) \leq -\frac{c-1}{c+1} \cdot \frac{1}{2k} + 1 - \tau + 2\sqrt{q_{\text{err}}(1-\tau)},$$

yielding that for c sufficiently large,

$$p \leq -\frac{1}{2k} + 1 - \tau + 2\sqrt{q_{\text{err}}(1-\tau)}. \tag{7.10}$$

Consequently, we have three upper bounds on the value of p, given by (7.6), (7.9), and (7.10): $B_0 := 1 - \tau - \frac{1}{2k}$, $B_1 := (1-\tau)^2 + \frac{2}{k}$, and $B_2 := 1 - \tau + 2\sqrt{q_{\text{err}}(1-\tau)} - \frac{1}{2k}$. Since $B_2 \geq B_0$, we only have to find $f(\tau)$ and k such that $B_1, B_2 \leq (1-\tau) - f(\tau)$, or equivalently:

$$\begin{aligned} 2f(\tau) + 4\sqrt{q_{\text{err}}(1-\tau)} & \leq \frac{1}{k} \leq \frac{\tau(1-\tau) - f(\tau)}{2} \\ \frac{5}{2}f(\tau) & \leq \frac{\tau(1-\tau)}{2} - 4\sqrt{q_{\text{err}}(1-\tau)}. \end{aligned}$$

It is easy to verify that for $d \leq \frac{1}{256(1-\tau)}$, the two inequalities are satisfied for $k := \frac{20}{9\tau(1-\tau)}$ and $f(\tau) := \frac{\tau(1-\tau)}{10}$. Thus, there exists $c > 0$ such that in any separable strategy with the probability of error $q_{\text{err}} \leq \frac{1}{256(1-\tau)}$ and the expected payoff p:

$$p \leq p_{\max} - \frac{\tau(1-\tau)}{10}.$$

3. For separable strategies with the probability of error $q_{\text{err}} > \frac{1}{256(1-\tau)}$, we can simply set $c > 256(1-\tau)$ which ensures that the payoff $p \leq 0$.

Set c to be the maximum over the values required by the discussed subcases. For such a c and any separable strategy, the corresponding expected payoff p satisfies $p \leq p_{\max} - \frac{\tau(1-\tau)}{10}$, yielding that

$$p_{\max} - p_s \geq \frac{\tau(1-\tau)}{10}.$$

□

7.5 Non-Trivial Embeddings Cannot Be Composed

As a straightforward corollary of Theorem 7.1, we now get that there exists a constant c such that any Bob restricted to interact with his system through the ideal functionality $\mathsf{ID}_{\psi}^{\otimes m}$ can never get the expected value of p as large and not even close as with the best coherent strategy. This remains true for any possible description of the ideal functionality since even if ID_{ψ} allowed to specify an arbitrary POVM then the ideal functionality would not be as good as the best coherent strategy.

Notice that any strategy Bob may use for querying the ideal functionality ID_{ψ} for both systems involved in order to pass the challenge with success, can also be carried by two parties restricted to local quantum operation and classical communication (LOCC). This is because ID_{ψ} only returns classical information. Local quantum operations can be performed by asking ID_{ψ} to apply a POVM to a local part of $|\psi\rangle$.

We now formally prove that non-trivial embeddings do not compose since Bob can always succeed better in Protocol 7.1 if he could measure all his registers coherently.

Theorem 7.2 *No non-trivial embedding of a primitive $P_{X,Y}$ is weakly self-composable.*

Proof. Let $|\psi\rangle = \sum_{x\in\mathcal{X}} \sqrt{P_X(x)}|x\rangle|\psi_x\rangle$ be a non-trivial embedding of $P_{X,Y}$. According to Lemma 7.1 there exist $x_0, x_1 \in \mathcal{X}$ such that $0 < |\langle\psi_{x_0}|\psi_{x_1}\rangle| < 1$. Theorem 7.1 then implies that there is $c \in \mathbb{R}^+$ such that in Protocol 7.1 played with $|\psi_{x_0}\rangle$ and $|\psi_{x_1}\rangle$ satisfying the condition above, the expected payoff achievable by the best coherent strategy is strictly better than what can be achieved by separable i.e. also LOCC strategies. By definition of weak self-composability it means that the non-trivial embedding $|\psi\rangle$ of $P_{X,Y}$ is not weakly self-composable. □

Corollary 7.1 *No non-trivial (correct) two-party quantum protocol is weakly self-composable.*

Proof. The statement follows from the fact that any quantum honest-but-curious attack of a super-embedding can be modeled by an attack of the corresponding two-party protocol. In the proof of Lemma 4.2, we have shown that for

any party there is a measurement converting a super-embedding $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ of a primitive $P_{X,Y}$ into an embedding $|\psi_k\rangle$ of $P_{X,Y}$ for some $k \in \{1, \ldots, K\}$. The other party can also learn the index k by measuring his/her additional register. Non-composability of non-trivial quantum two-party protocols for $P_{X,Y}$ then follows from non-composability of non-trivial embeddings of $P_{X,Y}$ by including a pre-stage into the game from Protocol 7.1. In this stage, Alice and Bob convert each of many super-embeddings of $P_{X,Y}$ corresponding to the protocol copies into an embedding of $P_{X,Y}$ known to both parties. This conversion results into a non-trivial embedding of $P_{X,Y}$ with constant probability. This is because if all embeddings in the conversion-range were trivial, then the measurement converting the super-embedding into embeddings could be used as a part of a measurement revealing $X \searrow Y$ completely to Bob, or revealing $Y \searrow X$ completely to Alice. Hence, such a super-embedding and the corresponding protocol would then be trivial. Due to the law of large numbers, from several copies of a super-embedding Alice obtains at least some constant fraction of the same non-trivial embeddings except of probability negligible in the number of copies. Alice and Bob then play the game from Protocol 7.1, using the subset of copies where Alice obtained the same non-trivial embedding. □

Finally, let us mention several facts related particularly to (non-)composability of trivial two-party quantum protocols implementing trivial primitives. Clearly, every trivial primitive has a protocol which is composable against quantum honest-but-curious adversaries, namely the classical one implementing the primitive securely in the HBC model. Formally, for a trivial $P_{X,Y}$ we show composability of quantum protocols implementing only $P_{X\searrow Y,Y\searrow X}$ (which corresponds to secure implementation in the HBC model) instead of $P_{X,Y}$, where the desired distribution $P_{X,Y}$ is obtained from the implementation of $P_{X\searrow Y,Y\searrow X}$ by local randomization. Since a trivial primitive satisfies $H(X \searrow Y|Y \searrow X) = H(Y \searrow X|X \searrow Y) = 0$ or in other words, the implemented dependent parts are accessible to both parties already in one protocol copy, coherent attacks do not help in getting any more information. Because the rest of X and Y is computed purely locally, there is no attack, individual or coherent, revealing any information about the result of this operation.

On the other hand, not all protocols for trivial primitives are composable. As an example let us take a protocol for a primitive $P_{X,Y}$ defined by $P_{X,Y}(0,0) = P_{X,Y}(1,0) = 3/8$, $P_{X,Y}(0,1) = P_{X,Y}(1,1) = 1/8$, represented by the following embedding:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right) + \frac{1}{\sqrt{2}}|1\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\right).$$

Such an embedding (and therefore, the corresponding protocols) is trivial because it implements a trivial primitive. Formally, $0 = H(X \searrow Y|Y)$ and $H(X \searrow Y|Y) \geq S(X \searrow Y|B)$ imply that $S(X \searrow Y|B) = 0$. On the other hand, the states

$$|\psi_0\rangle := \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle, \qquad |\psi_1\rangle := \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$$

that Bob gets for Alice's respective outcomes 0 and 1 of the measurement in the canonical basis, satisfy the condition $0 < |\langle\psi_0|\psi_1\rangle| < 1$ from Protocol 7.1. Hence, the arguments from the proof of Theorem 7.1 apply, yielding that $|\psi\rangle$ cannot be composed.

Chapter 8

Conclusion and Open Problems

8.1 Summary of the Results

We have provided a quantitative extension of qualitative impossibility results for two-party quantum cryptography. All non-trivial primitives leak information when implemented by quantum protocols. Notice that demanding a protocol to be non-leaking is generally weaker than demanding it to be private. For instance, consider a protocol implementing 1-2-OT but allowing a curious receiver with probability $\frac{1}{2}$ to learn both bits simultaneously or with probability $\frac{1}{2}$ to learn nothing about them. Such a protocol for 1-2-OT would be non-leaking but nevertheless insecure. Consequently, Theorem 4.2 not only tells us that any quantum protocol implementing a non-trivial primitive must be insecure, but also that a privacy breach will reveal itself as leakage. Hence, possibility of a non-leaking implementation and possibility of a private implementation of a given primitive are equivalent. We strengthened the above result by showing that this is true even if the players are allowed to interact with the trusted third party and if we allow the implementation to violate the correctness condition. This is implied by Theorem 6.1, showing that in such a scenario, 0–leakage implies privacy. The statement also applies to trivial primitives which is not uninteresting, since an implementation of a trivial primitive is not automatically private. As an example we can take an insecure embedding $\frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)$ of $P_{X,Y}$ satisfying $P_{X,Y}(a,b) = 1/4$ for any $a, b \in \{0,1\}$. In addition, in Chapter 7 we have shown that two-party quantum protocols not only leak information but also that when composed, almost none of them is resilient against coherent attacks.

Our framework allows to quantify the leakage of any two-party quantum protocol correctly implementing a primitive. Such impossibility results are stronger than standard ones since they only rely on the cryptographic correctness of the protocol. Furthermore, we present lower bounds on the leakage of some universal two-party primitives and explain the techniques used to establish these lower bounds.

In addition to the primitives we have considered, another one deserves to be mentioned – the *binary symmetric channel* (BSC) can be used as a cryptographic resource [CK88, Cré97, DKS99]. For BSC with noise $0 \leq p := \sin^2 \varphi \leq \frac{1}{2}$

the minimal leakage over its embeddings can be evaluated to $h(\frac{1-\sin(2\varphi)}{2}) + h(\frac{1-\cos(2\varphi)}{2}) - 1$. Moreover, canonical embeddings always minimize the leakage. As an example, the standard BB84 coding scheme can be seen as a BSC with $p = 1/4$ when the encoding and decoding bases remain private. However, its purification (which is equivalent to one EPR pair) leads to an embedding that leaks half a bit, which is more than three times the leakage of the canonical embedding of a BSC with $p = 1/4$.

8.2 Leakage – Bounds and Applications

A natural open question is to find a way to identify good embeddings for a given primitive. In particular, how far can the leakage of the canonical embedding be from the best one? Such a characterization, even if only applicable to special primitives, would allow to lower bound their leakage and would also help understanding the power of two-party quantum cryptography in a more concise way.

It would also be interesting to find a measure of cryptographic non-triviality for two-party primitives and to see how it relates to the minimum leakage of any implementation by quantum protocols. For instance, is it true that quantum protocols for two-party primitive $P_{X,Y}$ leak more as the minimum (total variation) distance between $P_{X,Y}$ and any trivial primitive increases?

Another question we leave for future research is to define and investigate leakage in a one-shot setting instead of in the asymptotic regime. Results in the one-shot setting have already been established for data compression [RW05], channel capacities [RWW06], state-merging [WR07,Ber08] and other (quantum-) information-theoretic tasks.

Furthermore, it is tempting to investigate what are the interesting applications of leakage, considered also for protocols using environment as a trusted third party. In particular, how well does leakage reflect privacy of cryptographic protocols? Privacy of an implementation of a given primitive can be measured e.g. in terms of amplification, in the case where it is possible and in the following sense: The fewer copies of such an implementation are needed to implement one copy of the same primitive almost privately, the better is the implementation. By "almost private" implementation of a given primitive we mean that it allows any player to get just a little bit different information about the other party's honest output than he/she is given by the ideal functionality for this primitive (i.e., a protocol for 1-2-OT which allows Bob to get either the bit of his choice or the parity of Alice's bits is not even approximately private). Notice that in this sense, protocols with low leakage are "good" protocols. It follows from the fact that any non-leaking protocol is also private (Theorem 6.1) and continuity of leakage, yielding that protocols with low leakage are close to being private. Hence, for a given primitive $P_{X,Y}$ and a given threshold specifying how insecure (non-private) an implementation can be, there exists ϵ such that only one copy of a protocol for $P_{X,Y}$ with leakage ϵ also implements $P_{X,Y}$ within the given threshold concerning privacy. It would be interesting to know what happens if we allow the leakage to be higher. Namely, how many copies of an implemen-

tation with bounded leakage are needed to implement a given primitive within a given privacy threshold?

8.3 Amplification of Two-Party Resources

In Chapter 6, we extended the definition of leakage to protocols involving the environment acting as a trusted third party, and showed how much correlation between the players and the environment is needed for implementing a given primitive without leakage. Again, we consider only correct protocols. If we allow leakage to be non-zero, we can define the following function:

Definition 8.1 *Let* $s_{P_{X,Y}} : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ *be defined as follows:*

$$s_{P_{X,Y}}(\epsilon) := \inf_{|\psi\rangle^{EAB}:\Delta_{\rho_{AB}}(P_{X,Y})\leq\epsilon} \max(S(E|A), S(E|B)).$$

In the first place, it would be very interesting to learn how leakage and the function $s_{P_{X,Y}}$ are related, by investigate the case where $\epsilon > 0$. Second, it would be of interest to study how quantum protocols equipped with the environment compare to classical protocols which make use of a trusted third party. Analogously to the quantum case, in the classical honest-but-curious model, the leakage of protocol π for $P_{X,Y}$, providing Alice and Bob with their respective views V_A and V_B can be defined by

$$\Delta_\pi^c(P_{X,Y}) := \max(H(X|Y) - H(X|YV_B), H(Y|X) - H(Y|XV_A).$$

This definition coincides with the definition of *privacy loss*, introduced by [ByCKO93]. Then we can define:

$$\Delta_{P_{X,Y}}^c := \inf_{V_A,V_B} \max(H(X|Y) - H(X|YV_B), H(Y|X) - H(Y|XV_A)).$$

Quantum privacy loss has been introduced by [Kla04], and is defined as the maximum amount of extra information that a quantum honest-but-curious player can get about the other party's output. In terms of "incorrect" implementations $|\psi\rangle \in \mathcal{H}_E \otimes \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ of $P_{X,Y}$, this amount equals $S_{\mathrm{tr}_E |\psi\rangle\langle\psi|}(X; YB') - I(X;Y)$. Klauck shows that for the disjointness problem, there is a quantum protocol with exponentially lower privacy loss than a classical one [Kla04]. It is tempting to ask: Can we conclude something similar for the leakage in the classical and the quantum scenarios? Notice that even though the definition of leakage and the definition of privacy loss agree if we consider classical protocols, they differ in the quantum case.

Furthermore, [Kla04] shows that there are problems for which a tiny relaxation in privacy-loss requirements allows for an exponential reduction of the communication cost. It would be very interesting to know whether a similar phenomenon can also occur with respect to the quantities we discuss in this work, namely, can the decrease of $s_{P_{X,Y}}$ be exponentially fast in the size of its argument? If for certain primitives the answer was yes, this fact could be demonstrated in a rather interesting way. For instance, consider Alice and

Bob preparing M instances of 1-2-OT from only m of them. These can be implemented via a tripartite state satisfying $S(E|A) = S(E|B) = m$ hence, $s_{P_{X,Y}^{\text{OT}^m}}(0) \leq m$. Trivial upper-bound on the leakage of such an implementation of M copies of 1-2-OT is then easy to obtain. Simply, let the players implement m 1-2-OTs perfectly from the blackboxes and the rest of them by embeddings. For such a protocol π we get:

$$\Delta_\pi(P_{X,Y}) = (M-m)\Delta_{P_{X,Y}^{\text{OT}}} = \frac{M-m}{2}.$$

Notice that $\Delta_\pi(P_{X,Y}) = 0$ can only hold if $S(E|A) = H_{P_{X,Y}^{\text{OT}^M}}(Y \searrow X|X) = M$, yielding that $m = M$.

Can the players use the m calls to the blackbox any better, for instance, "split" the power of m copies of 1-2-OT in such a way that each one of M implemented copies would leak less than $\frac{M-m}{2m}$? Such a magical amplification of multiple copies of 1-2-OT (or other primitive) from a few calls to the associated ideal functionality could be a demonstration of the fact that a small increase in the leakage can lead to a significant reduction in the required amount of the correlation between the players and the environment. On the other hand, upper-bounding how fast $s_{P_{X,Y}}$ decreases would give us a bound on how well can a given functionality be amplified.

Bibliography

[AD97] Miklos Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *29th Annual ACM Symposium on Theory of Computing (STOC)*, pages 284–293, 1997.

[AKSW07] Giacomo Mauro D' Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 76(3):032328, 2007.

[Amb01] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping". In *33rd Annual ACM Symposium on Theory of Computing (STOC)*, 2001.

[Amb05] Andris Ambainis. personal communication, 2005.

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

[BDF+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070–1091, February 1999.

[Ber08] Mario Berta. Single-shot quantum state merging. Master's thesis, ETH Zurich, 2008.

[BHL+05] Michael Ben-Or, Michal Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference (TCC)*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406. Springer, 2005.

[BLM+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefan Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Physical Review A*, 71:022101, 2005.

[Blu82] M. Blum. Coin flipping by telephone. In *Proceedings of 24th IEEE Spring Computer Conference*, pages 133–137, 1982.

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

[BM04] Michael Ben-Or and Dominic Mayers. General security definition and composability for quantum and classical protocols, September 2004. `http://arxive.org/abs/quant-ph/0409062`.

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

[ByCKO93] Reuven Bar-yehuda, Benny Chor, Eyal Kushilevitz, and Alon Orlitsky. Privacy, additional information, and communication. *IEEE Transactions on Information Theory*, 39:55–65, 1993.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 136–145, 2001.

[CB98] Anthony Chefles and Stephen M. Barnett. Quantum state separation, unambiguous discrimination, and exact cloning. *J. Phys. A*, 31(50):10097–10103, 1998. `http://front.math.ucdavis.edu/9808.4018`.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions. In *29th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 42–53, 1988.

[Col07] Roger Colbeck. The impossibility of secure two-party classical computation. `http://arxiv.org/abs/0708.2843`, August 2007.

[Cré87] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In *Advances in Cryptology—CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*. Springer, 1987.

[Cré97] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In *Advances in Cryptology—EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 306–317. Springer, 1997.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[Die88] Dennis Dieks. Overlap and distinguishability of quantum states. *Physical Letters A*, 126:303–307, 1988.

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *Advances in Cryptology—EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 1999.

[DW03] Igor Devetak and Andreas Winter. Classical data compression with quantum side information. *Phys. Rev. A*, 68(4):042301, Oct 2003.

[EGL82] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*. Plenum Press, 1982.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45:1216–1227, 1999.

[FWW04] Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger. Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In *Advances in Cryptology—CRYPTO '04*, volume 3152 of *Lecture Notes in Computer Science*, pages 562–579. Springer, 2004.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Eliminating decryption errors in the ajtai-dwork cryptosystem. In *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 105–111. Springer, 1997.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[Hel76] Carl W. Helstrom. Quantum detection and estimation theory. *Academic Press, New York*, 1976.

[HOW07] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Comm. Math. Phys.*, 269(1):107–136, 2007.

[IMNW04] Hideki Imai, Jörn Müller-Quade, Anderson Nascimento, and Andreas Winter. Rates for bit commitment and coin tossing from noisy correlation. In *Proceedings of 2004 IEEE International Symposium on Information Theory*, pages 47–47, June 2004.

[Iva87] I. D. Ivanović. How to differentiate between non-orthogonal states. *Physical Letters A*, 123:257–259, 1987.

[JS00] Richard Jozsa and Jürgen Schlienz. Distinguishability of states and von neumann entropy. *Phys. Rev. A*, 62(1):012301, Jun 2000.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 20–31, 1988.

[Kit03] A. Kitaev. Quantum coin-flipping. presented at QIP'03. A review of this technique can be found in `http://lightlike.com/~carlosm/publ`, 2003.

[KKB05] Matthias Kleinmann, Hermann Kampermann, and Dagmar Bruss. On the generalization of quantum state comparison. *Phys. Rev. A*, 72(032308), 2005. `http://arxiv.org/abs/quant-ph/0503012`.

[Kla04] Hartmut Klauck. On quantum and approximate privacy. *Theory of Computing Systems*, 37(1):221–246, 2004. `http://arxiv.org/abs/quant-ph/0110038`, also in the proceedings of STACS '2002.

[KNTsZ01] Hartmut Klauck, Ashwin Nayak, Amnon Ta-shma, and David Zuckerman. Interaction in quantum communication and the complexity of set disjointness. In *In Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 124–133, 2001.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? In *Physical Review Letters* [PRL97], pages 3410–3413.

[Lo97] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. In *Physical Review Letters* [PRL97], pages 3414–3417.

[MN05] Tal Moran and Moni Naor. Basing cryptographic protocols on tamper-evident seals. In *32nd International Colloquium on Automata, Languages and Programming (ICALP)*, volume 3580 of *Lecture Notes in Computer Science*, pages 285–297. Springer, 2005.

[Moc04] Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *45th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 2–11, 2004.

[Moc05] Carlos Mochon. A large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72:022341, 2005.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias, 2007. `http://arxiv.org/abs/0711.4114`.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2000.

[Per88] How to differentiate between non-orthogonal states. *Physical Letters A*, 128:19, 1988.

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[PRL97] *Physical Review Letters*, volume 78, April 1997.

[Rab81] M. Rabin. How to exchange secrets by oblivious transfer. Technical report, Harvard Aiken Computation Lab, 1981.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[RW05] Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *Advances in Cryptology—ASIACRYPT 2005*, Lecture Notes in Computer Science, pages 199–216. Springer, 2005.

[RWW06] Renato Renner, Stefan Wolf, and Juerg Wullschleger. The single-serving channel capacity. In *Proceedings of the International Symposium on Information Theory (ISIT)*. IEEE, July 2006. available at http://arxiv.org/abs/cs.IT/0608018.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *Bell Telephone System Technical Publications*, 1948.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[Unr04] Dominique Unruh. Simulatable security for quantum protocols. `http://arxiv.org/abs/quant-ph/0409125`, 2004.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Original manuscript written circa 1970.

[Win99] Andreas Winter. *Coding Theorems of Quantum Information Theory*. PhD thesis, Department of Mathematics, University of Bielefeld, 1999.

[WR07] Andreas Winter and Renato Renner. Single-shot state merging, 2007. unpublished note.

[WW04] Stefan Wolf and Jürg Wullschleger. Zero-error information and applications in cryptography. In *IEEE Information Theory Workshop (ITW)*, San Antonio, Texas, October 2004.

[WW05a] Stefan Wolf and Jürg Wullschleger. New monotones and lower bounds in unconditional two-party computation. In *Advances in Cryptology—CRYPTO '05*, volume 3621 of *Lecture Notes in Computer Science*, pages 467–477. Springer, 2005.

[WW05b] Stefan Wolf and Jürg Wullschleger. Oblivious transfer and quantum non-locality. In *International Symposium on Information Theory (ISIT 2005)*, pages 1745–1748, 2005.

[Yao82] Andrew C. Yao. Protocols for secure computations. In *23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 1982.

Appendix A

Lemma A.2 from the proof of Theorem 7.1

Before starting with the actual Lemma A.2, we formulate and prove an auxiliary lemma, needed for the main proof.

Lemma A.1 *Let $f : \mathbb{R}^+ \to \mathbb{C}^{2\times 2}$ be a function mapping c positive into a positive-semidefinite operator $F_c \in \mathbb{C}^{2\times 2}$ such that $\|F_c\|_\infty = 1$ and for some unit vector $|v_0\rangle \in \mathbb{C}^2$, $\langle v_0|F_c|v_0\rangle \in O(1/c)$. Then the dominant eigenvector of F_c is of the form $\gamma_0^c|v_0\rangle + \gamma_1^c|v_1\rangle$, where $\langle v_0|v_1\rangle = 0$, $|\gamma_0^c|^2 + |\gamma_1^c|^2 = 1$, and $|\gamma_0^c|^2 \in O(1/c)$. Furthermore, the second largest eigenvalue λ_c of F_c satisfies $\lambda_c \in O(1/c)$.*

Proof. Let us write F_c in the form: $F_c = M_c^\dagger M_c$, for a matrix $M_c \in \mathbb{C}^{2\times 2}$. This is possible due to the fact that F_c is positive-semidefinite. We define $|u_0\rangle := M_c|v_0\rangle$ and $|u_1\rangle := M_c|v_1\rangle$. According to the assumption, $\langle u_0|u_0\rangle \in O(1/c)$. Let us write the (unit) dominant eigenvector of F_c in the basis $\{|v_0\rangle, |v_1\rangle\}$ as:

$$|w\rangle = \gamma_0^c|v_0\rangle + \gamma_1^c|v_1\rangle.$$

It follows that

$$1 = \langle w|F_c|w\rangle = |\gamma_0^c|^2\langle u_0|u_0\rangle + |\gamma_1^c|^2\langle u_1|u_1\rangle + 2\mathrm{Re}(\overline{\gamma_0^c}\gamma_1^c\langle u_0|u_1\rangle).$$

Assume that there exists an unbounded increasing sequence of positive numbers such that for its elements c, we get $|\gamma_1^c|^2 = 1 - \Theta(1/c^\delta)$ for $1/2 \leq \delta < 1$. From $\langle u_0|u_0\rangle \in O(1/c)$ we get that $|\overline{\gamma_0^c}\gamma_1^c\langle u_0|u_1\rangle| \in \Theta(1/c^\delta)$ and $|\langle u_0|u_1\rangle| \in O(1/\sqrt{c})$, yielding that

$$|\gamma_0^c| \in \omega(1/c^{\delta-1/2}).$$

Since $|w\rangle$ is a unit vector, for some k positive, we get

$$1 = |\gamma_1^c|^2 + |\gamma_0^c|^2 \geq 1 - \frac{k}{c^\delta} + |\gamma_0^c|^2,$$

and thus, $|\gamma_0^c|^2 \in O(1/c^\delta)$. From the two conditions we conclude that

$$|\gamma_0^c|^2 \in \omega(1/c^{2\delta-1}) \cap O(1/c^\delta),$$

yielding that $\delta = 1$, since the intersection of the two sets has to be non-empty. Therefore, the function f satisfies

$$|\gamma_0^c|^2 \in O(1/c) \tag{A.1}$$

on the entire domain.

Now we upper bound the second largest eigenvalue of F_c. Since the second eigenvector $|w^\perp\rangle$ of F_c is orthogonal to its dominant eigenvector, it can be written in the form:

$$\left|w^\perp\right\rangle = \tilde{\gamma}_1^c|v_0\rangle + \tilde{\gamma}_0^c|v_1\rangle,$$

where $|\tilde{\gamma}_1^c| = |\gamma_1^c|$ and $|\tilde{\gamma}_0^c| = |\gamma_0^c|$. We get that

$$\lambda_c = \left\langle w^\perp\middle|F_c\middle|w^\perp\right\rangle = |\tilde{\gamma}_1^c|^2\langle u_0|u_0\rangle + |\tilde{\gamma}_0^c|^2\langle u_1|u_1\rangle + 2\mathrm{Re}(\overline{\tilde{\gamma}_1^c}\tilde{\gamma}_0^c\langle u_0|u_1\rangle).$$

From the assumption $\langle u_0|u_0\rangle \in O(1/c)$ and (A.1) we conclude that

$$\lambda_c \in O(1/c).$$

□

Lemma A.2 *Let $c, k > 0$. Consider the game from Prot. 7.1 and let X and Y denote the respective registers of Bob, corresponding to Alice's choices of h and h'. To any strategy based on the outcomes of a separable measurement $\mathcal{M} = (E_0, E_1, E_?)$ on $\mathcal{H}_X \otimes \mathcal{H}_Y$ with probability of error $q_{\mathrm{err}} \leq \frac{1}{2(c+1)k}$ and the expected payoff p, there exists a strategy using a separable measurement $\mathcal{M}' = (E'_0, E'_1, E'_?)$ in the form:*

$$E'_0 = G_0^0 \otimes G_0^1 + G_1^0 \otimes G_1^1, \quad E'_1 = G_0^0 \otimes G_1^1 + G_1^0 \otimes G_0^1, \quad E'_? = 1 - E'_0 - E'_1$$

with the expected payoff p', satisfying:

$$|p - p'| \in \frac{1}{k} + O(1/\sqrt{c}).$$

Proof. For simplicity of the notation, let us define $|\psi_0\rangle := |\psi_{x_0}\rangle$ and $|\psi_1\rangle := |\psi_{x_1}\rangle$, where $|\psi_{x_0}\rangle$ and $|\psi_{x_1}\rangle$ come from Prot. 7.1.

Every element of a separable measurement on $\mathcal{H}_X \otimes \mathcal{H}_Y$ can be written as a sum of tensor products of positive semi-definite operators. In particular, the elements of $\mathcal{M}$ can be written in the form:

$$E_{b(x,y)} := \sum_{x,y} F^0_{b(x,y),x} \otimes F^1_{b(x,y),y}.$$

Operators $F^0_{b(x,y),x} \otimes F^1_{b(x,y),y}$ can be viewed as the elements of a new measurement $\mathcal{N}$, refining $\mathcal{M}$. Since the states $|\psi_0\rangle$ and $|\psi_1\rangle$ span a 2-dimensional Hilbert space, all operators $F^0_{b_{x,y},x}$ and $F^1_{b_{x,y},y}$ can be restricted to correspond to 2×2 matrices in some basis of this space.

The function $b : (x, y) \to \{0, 1, ?\}$ is a post-processing function of the outcomes of $\mathcal{N}$, determining the outcome of $\mathcal{M}$ (0 corresponds to the states being

equal, 1 to them being different, and ? denotes an inconclusive answer). Let A denote the sets of all pairs (x, y) of outcomes of $\mathcal{N}$. To every pair $(x, y) \in A$ we assign $(q_x^0, q_y^1) \in [0, 1/2]^2$ – the probabilities of error in guessing the factor states of $\mathcal{H}_X$ and $\mathcal{H}_Y$, conditioned on measuring x and y, respectively. Let W_0 and W_1 denote the random variables assigned to the states of $\mathcal{H}_X$ and $\mathcal{H}_Y$, respectively. The probability space of both W_0 and W_1 is $\{0, 1\}$, since the state of either of the subsystems is $|\psi_0\rangle$ or $|\psi_1\rangle$. For $\zeta \in \{0, 1\}$, let $x \to \zeta$, $y \to \zeta$ stand for $\Pr[W_0 = 1 - \zeta|x], \Pr[W_1 = 1 - \zeta|y] \leq \frac{1}{2(c+1)}$, respectively, where the probabilities are conditioned on the outcomes of $\mathcal{N}$ in the respective subsystems. Consider measurement $\mathcal{M}^* := (E_0^*, E_1^*, E_?^*)$ with the same refined set of outputs A as $\mathcal{M}$ (which now will be indexed differently) in the following form:

$$E_0^* = E_{0,0}^* + E_{1,1}^*, \qquad E_1^* = E_{0,1}^* + E_{1,0}^*, \qquad E_?^* = \mathbb{I} - E_0^* - E_1^*,$$

where

$$E_{\alpha,\beta}^* := \sum_{x \to \alpha, y \to \beta} F_{\alpha,x}^0 \otimes F_{\beta,y}^1. \tag{A.2}$$

We show that the difference of the expected payoff p of $\mathcal{M}$ and the expected payoff p^* of $\mathcal{M}^*$ satisfies:

$$|p - p^*| \leq \frac{1}{k}. \tag{A.3}$$

Since the refined sets of possible outcomes of both $\mathcal{M}^*$ and $\mathcal{M}$ are the same, the two measurements only differ in the post-processing functions denoted by b and b^*, respectively. In other words, $\mathcal{M}^*$ differs from $\mathcal{M}$ in the arrangement of the same set of summands in the three sums defining measurement elements $(E_0, E_1, E_?)$ and $(E_0^*, E_1^*, E_?^*)$.

Consider any strategy which upon measuring (x, y) yields a conclusive answer. For the corresponding expected payoff $p_{x,y}$ conditioned on measuring (x, y) we then get:

$$\begin{aligned} p_{x,y} = \quad & (1 - q_x^0)(1 - q_y^1) + q_x^0 q_y^1 - c(q_x^0(1 - q_y^1) + (1 - q_x^0)q_y^1) \\ = \quad & 1 - (c + 1)(q_x^0 + q_y^1 - 2q_x^0 q_y^1). \end{aligned} \tag{A.4}$$

If on the other hand, measuring (x, y) implies the answer of $\mathcal{M}$ to be inconclusive, the expected payoff conditioned on measuring (x, y) will be 0. Consequently, the optimal post-processing strategy (with the maximum payoff) should output $b(x, y) =?$ for every (x, y) satisfying $q_x^0 + q_y^1 - 2q_x^0 q_y^1 > \frac{1}{c+1}$, otherwise it outputs a conclusive answer. In particular, the output should be inconclusive for all pairs (x, y) such that $q_x^0 > \frac{1}{c+1}$ or $q_y^1 > \frac{1}{c+1}$, and conclusive if both $q_x^0, q_y^1 \leq \frac{1}{2(c+1)}$.

However, only the knowledge that $(q_x^0, q_y^1) \in [0, \frac{1}{c+1}]^2 \setminus [0, \frac{1}{2(c+1)}]^2$ does not allow us to determine what is the best output in order to maximize the payoff. We analyze this problem with respect to the probability of error allowed for the post-processing function.

We assume that the answer of $\mathcal{N}$ with the post-processing function b can be false with probability at most $q_{\text{err}} \leq \frac{1}{2k(c+1)}$. According to Markov's inequality, measuring (x, y) such that either $q_x^0 > kq_{\text{err}}$ or $q_y^1 > kq_{\text{err}}$ does not allow to

output a conclusive answer with probability larger than $1/k$. Thus, for either $q_x^0 > \frac{1}{2(c+1)}$ or $q_y^1 > \frac{1}{2(c+1)}$, the answer cannot be conclusive with probability larger than $1/k$. In the latter we analyze the difference of the expected payoffs for the post-processing function b and for a newly defined b^* such that for any (x, y) satisfying $q_x^0 > \frac{1}{2(c+1)}$ or $q_y^1 > \frac{1}{2(c+1)}$, the output is $b^*(x, y) =?$.

Consider every pair (x, y) such that by modifying $b(x, y)$ into $b^*(x, y)$, $p_{x,y}$ decreases and compute the difference of $p_{x,y}$ and p^*_{xy} in this case. We have that either $q_x^0 \in (\frac{1}{2(c+1)}, \frac{1}{c+1}]$ or $q_y^1 \in (\frac{1}{2(c+1)}, \frac{1}{c+1}]$, yielding that

$$p_{x,y} = 1 - (c+1)(q_x^0 + q_y^1 - 2q_x^0 q_y^1) < \frac{1}{2}.$$

It means that for every pair (x, y) for which the value of the post-processing function was modified, $p_{x,y}$ decreased by at most $1/2$. However, since the answer of $\mathcal{M}$ is false with probability at most q_{err}, the functions b and b^* cannot differ anywhere except for a set of (x, y) measured with probability at most $1/k$, concerning that $q_{\text{err}} \leq \frac{1}{2k(c+1)}$. This gives us

$$|p - p^*| \leq \frac{1}{k}. \tag{A.5}$$

We have shown that a separable measurement $\mathcal{M}$ can be approximated by a separable measurement $\mathcal{M}^*$ in the special form. In the following we show that $\mathcal{M}^*$ can be approximated by a measurement in the form from the statement up to a difference in payoffs which is in $O(1/\sqrt{c})$. The statement of the lemma then follows from the triangle inequality.

Our next goal is to construct a measurement $\mathcal{M}' = (E'_0, E'_1, E'_?)$ in the form:

$$E'_0 = G^0_{00} \otimes G^1_{00} + G^0_{11} \otimes G^1_{11}, \quad E'_1 = G^0_{01} \otimes G^1_{01} + G^0_{10} \otimes G^1_{10}, \quad E'_? = \mathbb{I} - E'_0 - E'_1,$$

approximating the measurement $\mathcal{M}^*$ with respect to the expected payoff. In the definition of the elements of $\mathcal{M}'$, the upper index of G^ζ_{ab} specifies the subsystem, the first bit of the lower index determines the outcome in the first subsystem, and the second bit of the lower index determines the outcome in the second subsystem.

Consider the previously constructed measurement $\mathcal{M}^*$. Fix $\alpha, \beta \in \{0, 1\}$ and define $F_x^0 := \frac{F^0_{\alpha,x}}{\|F^0_{\alpha,x}\|_\infty}$, $F_y^1 := \frac{F^1_{\beta,y}}{\|F^1_{\beta,y}\|_\infty}$, $\mu_{x,y} := \|F^0_{\alpha,x}\|_\infty \cdot \|F^1_{\beta,y}\|_\infty$. First, we construct positive-semidefinite operators $\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}$, approximating

$$E^*_{\alpha,\beta} = \sum_{x \to \alpha, y \to \beta} \mu_{x,y} F_x^0 \otimes F_y^1$$

(defined by (A.2)), where the guesses of α and β conditioned on measuring F_x^0 and F_y^1 are incorrect with probability at most $\frac{1}{2(c+1)}$. We require these operators to satisfy:

1. $p_{E^*_{\alpha,\beta}} = p_{\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}}$, where $p_{E^*_{\alpha,\beta}}$ and $p_{\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}}$ denote the expected payoffs conditioned on measuring $E^*_{\alpha,\beta}$ and $\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}$, respectively.

2. For all $\zeta_0, \zeta_1, \alpha, \beta \in \{0,1\}$:

$$\left|\langle\psi_{\zeta_0}, \psi_{\zeta_1}|\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}|\psi_{\zeta_0}, \psi_{\zeta_1}\rangle - \langle\psi_{\zeta_0}, \psi_{\zeta_1}|E^*_{\alpha,\beta}|\psi_{\zeta_0}, \psi_{\zeta_1}\rangle\right| \in O(1/\sqrt{c}),$$

3. $\|\sum_{\alpha,\beta} \tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}\|_\infty \in 1 + O(1/c)$.

We now describe the construction of operators $\tilde{G}^0_{\alpha,\beta}$ and $\tilde{G}^1_{\alpha,\beta}$. The respective dominant eigenvectors of F^0_x and F^1_y can be written as

$$\begin{aligned} |w_0\rangle &= \gamma^0_{0,x}|\psi_{1-\alpha}\rangle + \gamma^0_{1,x}\left|\psi^\perp_{1-\alpha}\right\rangle, \\ |w_1\rangle &= \gamma^1_{0,y}|\psi_{1-\beta}\rangle + \gamma^1_{1,y}\left|\psi^\perp_{1-\beta}\right\rangle, \end{aligned}$$

where for each $\zeta \in \{0,1\}$, $|\psi^\perp_\zeta\rangle$ denotes the unit vector spanned by $|\psi_0\rangle$ and $|\psi_1\rangle$, orthogonal to $|\psi_\zeta\rangle$. According to Lemma A.1, there exists κ positive such that for each x and y, $|\gamma^0_{0,x}|^2 \leq \frac{\kappa}{c}$ and $|\gamma^1_{0,y}|^2 \leq \frac{\kappa}{c}$. We define operators $\tilde{G}^0_{\alpha,\beta}$ and $\tilde{G}^1_{\alpha,\beta}$ by

$$\begin{aligned} \tilde{G}^0_{\alpha,\beta} &:= \left(1 - \frac{\kappa}{c}\right) \cdot \sqrt{\sum_{x,y} \mu_{x,y}}\left|\psi^\perp_{1-\alpha}\right\rangle\!\left\langle\psi^\perp_{1-\alpha}\right| + \nu_0(c)|\psi_{1-\alpha}\rangle\langle\psi_{1-\alpha}|, \\ \tilde{G}^1_{\alpha,\beta} &:= \left(1 - \frac{\kappa}{c}\right) \cdot \sqrt{\sum_{x,y} \mu_{x,y}}\left|\psi^\perp_{1-\beta}\right\rangle\!\left\langle\psi^\perp_{1-\beta}\right| + \nu_1(c)|\psi_{1-\beta}\rangle\langle\psi_{1-\beta}| \end{aligned}$$

for non-negative functions $\nu_0, \nu_1 \in O(1/c)$ chosen to be such that

$$p_{E^*_{\alpha,\beta}} = p_{\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}}.$$

Such a choice of parameters is possible, due to the fact the the probability of a wrong guess, conditioned on the outcome $E^*_{\alpha,\beta}$ is in $O(1/c)$. Since operators $\{E^*_{\alpha,\beta}\}_{\alpha,\beta}$ form a valid POVM, after projecting them by a projector $P := |\psi^\perp_{1-\alpha}\rangle\langle\psi^\perp_{1-\alpha}| \otimes |\psi^\perp_{1-\beta}\rangle\langle\psi^\perp_{1-\beta}|$, we get a valid POVM on the support of P. In other words, $\{PE^*_{\alpha,\beta}P\}_{\alpha,\beta}$ form a POVM and therefore, also the operators

$$J_{\alpha,\beta} := \left(1 - \frac{\kappa}{c}\right) \cdot \left(\sum_{x \to \alpha, y \to \beta} \mu_{x,y}\right) \left|\psi^\perp_{1-\alpha}\right\rangle\!\left\langle\psi^\perp_{1-\alpha}\right| \otimes \left|\psi^\perp_{1-\beta}\right\rangle\!\left\langle\psi^\perp_{1-\beta}\right|,$$

lower-bounding $PE^*_{\alpha,\beta}P$, form valid POVMs. From the condition

$$\|\sum_{\alpha,\beta} J_{\alpha,\beta}\|_\infty \leq 1,$$

we conclude that

$$\|\sum_{\alpha,\beta} \tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}\|_\infty \in 1 + O(1/c). \tag{A.6}$$

It remains to show that

$$\forall \zeta_0, \zeta_1, \alpha, \beta \in \{0,1\} : \left|\langle\psi_{\zeta_0}, \psi_{\zeta_1}|\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}|\psi_{\zeta_0}, \psi_{\zeta_1}\rangle - \langle\psi_{\zeta_0}, \psi_{\zeta_1}|E^*_{\alpha,\beta}|\psi_{\zeta_0}, \psi_{\zeta_1}\rangle\right| \in O(1/\sqrt{c}).$$

By definition of $\tilde{G}^0_{\alpha,\beta}$ and $\tilde{G}^1_{\alpha,\beta}$, this is true if $\zeta_0 \neq \alpha$ or $\zeta_1 \neq \beta$. We now discuss the remaining case. It follows from Lemma A.1, applied to each $F^0_x \otimes F^1_y$ and the construction of $\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}$ that

$$\left\| \sum_{x\to\alpha, y\to\beta} \mu_{x,y} F^0_x \otimes F^1_y - \tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta} \right\|_\infty \in O(1/\sqrt{c}).$$

Hence, also

$$\left| \langle \psi_\alpha, \psi_\beta | \tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta} | \psi_\alpha, \psi_\beta \rangle - \langle \psi_\alpha, \psi_\beta | E^*_{\alpha,\beta} | \psi_\alpha, \psi_\beta \rangle \right| \in O(1/\sqrt{c}).$$

We have defined a set of operators $\{\tilde{G}^0_{\alpha,\beta} \otimes \tilde{G}^1_{\alpha,\beta}\}_{\alpha,\beta}$, almost forming a POVM due to the condition (iii). Therefore, we can re-scale the elements of the set by a factor in $1 - O(1/c)$, and thereby create a POVM $\{G^0_{\alpha,\beta} \otimes G^1_{\alpha,\beta}\}_{\alpha,\beta}$. Due to the condition (i), the expected payoffs conditioned on measuring either $E^*_{\alpha,\beta}$ or $G^0_{\alpha,\beta} \otimes G^1_{\alpha,\beta}$ are the same. Finally, due to the condition (ii), the probabilities of measuring an outcome from $\{E^*_{\alpha,\beta}\}_{\alpha,\beta}$ and an outcome from $\{G^0_{\alpha,\beta} \otimes G^1_{\alpha,\beta}\}_{\alpha,\beta}$ differ by a value in $O(1/\sqrt{c})$. Hence, if the probability of a conclusive answer of $\mathcal{M}^*$ is constant then the measurement with elements

$$E''_0 := G^0_{0,0} \otimes G^1_{0,0} + G^0_{1,1} \otimes G^1_{1,1}, \quad E''_1 := G^0_{0,1} \otimes G^1_{0,1} + G^0_{1,0} \otimes G^1_{1,0}, \quad E''_? := \mathbb{I} - E'_0 - E'_1$$

gives a conclusive answer with probability lower by at most a value in $O(1/\sqrt{c})$, and differs from $\mathcal{M}^*$ in its payoff by a value in $O(1/\sqrt{c})$. According to [KKB05], the state of each of the two subsystems after applying the measurement given above is independent of the outcome in the other one. Therefore, in order to achieve certain expected payoff, the local measurements can be optimized separately. It follows that the payoff of measurement $(E''_0, E''_1, E''_?)$ can be matched by the payoff p' of some measurement $\mathcal{M}'$ in the form:

$$E'_0 = G^0_0 \otimes G^1_0 + G^0_1 \otimes G^1_1, \quad E'_1 = G^0_0 \otimes G^1_1 + G^0_1 \otimes G^1_0, \quad E'_? = \mathbb{I} - E'_0 - E'_1.$$

By applying (A.3) and the triangle inequality, we finally get that

$$|p - p'| \in O(1/k) + O(1/\sqrt{c}).$$

□