לקראת אי ההיתכנות של הגברת פרטיות תחת הנחות של חוסר יכולת לאותת אחורה בזמן

ע"י
רתם ארנון פרידמן

יולי, 2012

תקציר

בשנים האחרונות גברה ההתעניינות בהוכחת פרוטוקולים קריפטוגרפים, כגון פרוטוקולים קוונטיים להחלפת מפתחות, מהנחה אחת ויחידה שקובעת כי אליס ובוב לא יכולים לאותת אחד לשני בעזרת המערכות שלהם. את ההנחה הזאת ניתן להצדיק ע"י כך שאליס ובוב יבצעו את המדידות שלהם באזורי מרחב-זמן מנותקים אחד מהשני (ואז חוסר היכולת לאותת יובטח לנו מתורת היחסות) או ע"י מיגון פיזי של המערכות שלהם בצורה כזו שאותות לא יכולים לצאת או להיכנס. למרבה הצער, הוכח ב-[11] כי לא משנה באיזו פונקציית גיבוב נשתמש, לא תיתכן הגברת פרטיות אם ההנחה היחידה על המערכת היא שאליס ובוב לא יכולים לאותת אחד לשני (בעוד אותות כן יכולים לעבור בין תתי המערכות של אליס לדוגמא).

בעבודה זו אנו מקטינים את הפער בין ההנחות של [11] להנחות הפיזיקאליות הרלוונטיות מבחינה ניסיונית, אשר קובעות כי המערכות של אליס ובוב לא יכולות לאותת אחורה בזמן. אנו מתייחסים לקבוצת הנחות קרובה לתנאים אלו ומוכיחים כי תוצאת האי היתכנות של [11] עדיין תקפה.

TEL-AVIV UNIVERSITY
RAYMOND AND BEVERLY SACKLER
FACULTY OF EXACT SCIENCES
BLAVATNIK SCHOOL OF COMPUTER SCIENCE

Towards the Impossibility of Non-Signalling Privacy Amplification from Time-Like Ordering Constraints

Submitted as a partial fulfillment of the
requirements towards Master of Science degree
Tel Aviv University
School of Computer Science

by
Rotem Arnon Friedman

Under the supervision of
Prof. Amnon Ta-Shma

July, 2012

Acknowledgments

Abstract

In the past few years there was a growing interest in proving the security of cryptographic protocols, such as key distribution protocols, from the sole assumption that the systems of Alice and Bob cannot signal to each other. This can be achieved by making sure that Alice and Bob perform their measurements in a space-like separated way (and therefore signalling is impossible according to the non-signalling postulate of relativity theory) or even by shielding their apparatus. Unfortunately, it was proven in [11] that, no matter what hash function we use, privacy amplification is impossible if we only impose non-signalling conditions between Alice and Bob and not within their systems.

In this letter we reduce the gap between the assumptions of [11] and the physical relevant assumptions, from an experimental point of view, which say that the systems can only signal forward in time within the systems of Alice and Bob. We consider a set of assumptions which is very close to the conditions above and prove that the impossibility result of [11] still holds.

Contents

Chapter 1

Introduction and Contribution

1.1 Non-signalling cryptography

In the past few years there was a growing interest in proving the security of cryptographic protocols, such as quantum key distribution (QKD) protocols, from the sole assumption that the system on which the protocol is being executed does not allow for signalling between Alice and Bob. One way to make sure that this assumption holds is for Alice and Bob to have secured shielded laboratories, such that information cannot leak outside. It could also be ensured by performing Alice's and Bob's measurements in a space-like separated way; this way, relativity theory predicts the impossibility of signalling between them. For this reason, such cryptographic protocols are sometimes called "relativistic protocols". Since the condition that information cannot leak outside is a necessary condition in any cryptographic protocol (otherwise the key could just leak out to the adversary, Eve), basing the security proof on this condition alone will mean that the protocol has minimal assumptions.

We consider families of protocols which have two special properties. First, the security of the protocols is based only on the observed correlations of Alice's and Bob's measurements outcomes and not on the physical apparatus they use. I.e., the protocols are device-independent [17, 19]. In device-independent protocols, we assume that the system of Alice and Bob was prepared by the adversary Eve. Note that although the system was created by Eve, Alice and Bob have to be able to make sure that information does not leak outside by shielding the systems. Alice and Bob therefore perform some (unknown) measurements on their system and privacy should be concluded only from the correlations of the outcomes.

Second, in the protocols that we consider, the adversary is limited only by the non-signalling principle and not by quantum physics (i.e., super-quantum adversary). By combining these two properties together we can say that quantum physics guarantees the protocol to work, but the security is completely independent of quantum physics.

1.2 Systems and correlations

For two correlated random variables X, U over $\Lambda_1 \times \Lambda_2$, we denote the conditional probability distribution of X given U by $P_{X|U}(x|u) = Pr(X = x|U = u)$.

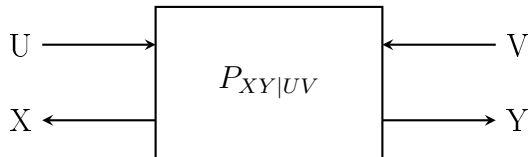A bipartite system is defined by the joint input-output behavior $P_{XY|UV}$ (see Figure 1.2.1).

Figure 1.2.1: A bipartite system

In a system $P_{XY|UV}$ U and X are usually Alice's input and output respectively, while V and Y are Bob's input and output. We denote Alice's interface of the system by $X(U)$ and Bob's interface by $Y(V)$. In a similar way, when considering a tripartite system $P_{XYZ|UVW}$ Eve's interface of the system is denoted by $Z(W)$.

We are interested in non-local systems - systems which cannot be described by shared randomness of the parties. Bell proved in [3] that entangled quantum states can display non-local correlations under measurements. Bell's work was an answer to Einstein, Podolsky, and Rosen's claim in [1] that quantum physics is incomplete and should be augmented by classical variables determining the behavior of every system under any possible measurement. In this letter we deal with a specific type of Bell inequality, called the CHSH inequality after [7].

We can think about the CHSH inequity as a game. In the CHSH game Alice and Bob share a bipartite system $P_{XY|UV}$. Alice gets a random input U, Bob gets a random input V and the goal is that the outputs of Alice and Bob, X and Y respectively, will satisfy $X \oplus Y = U \cdot V$. For all local systems the probability of winning the game satisfies $\Pr[X \oplus Y = U \cdot V] \leq 0.75$. This can be easily seen from the fact that only three out of the four conditions represented by $\Pr[X \oplus Y = U \cdot V] = 1$ can be satisfied together. If a system violates the inequality then it is non-local.

Definition 1.2.1. (CHSH non-locality). A system $P_{XY|UV}$ is non-local if $\sum_{u,v} \frac{1}{4} \Pr[X \oplus Y = u \cdot v] > 0.75$.

When measuring entangled quantum states, one can achieve roughly 85%; this is a Bell inequality violation. The maximal violation of the CHSH inequality, i.e. $\sum_{u,v} \frac{1}{4} \Pr[X \oplus Y = u \cdot v] = 1$ for any u, v, is achieved by the following system, called a Popescu-Rohrlich box, or a PR-box [20].

		U = 0		U = 1	
V \ X	Y \ X	0	1	0	1
0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0
0	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$
1	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0

Figure 1.2.2: PR-box

Definition 1.2.2. (PR-box). A PR box is the following bipartite system $P_{XY|UV}$: For each input pair (u, v), the random variables X and Y are uniform bits and we have $\sum_{u,v} \frac{1}{4} \Pr[X \oplus Y = u \cdot v] = 1$ (see Figure 1.2.2).

As seen from Figure 1.2.2 the outputs are perfectly random, and since the correlations are non-local, they cannot be described by pre-shared randomness. I.e., PR-boxes correspond to perfect secrecy. This implies that PR-boxes could have been a good resource for cryptographic protocols. Unfortunately, perfect PR-boxes do not exist in nature; as was proven by Tsirelson [6], quantum physics is non-local, but not maximally. Therefore, for a protocol which can be implemented using quantum systems, we should consider approximations of PR-boxes, or PR-boxes with some error. For example, an 85%-approximations can be achieved with maximally entangled qubits. For a more general treatment we can define the following.

Definition 1.2.3. (Unbiased PR-box with error ε). An unbiased PR-box with error ε is the following bipartite system $P_{XY|UV}$: For each input pair (u, v), the random variables X and Y are uniform bits and we have $\Pr[X \oplus Y = u \cdot v] = 1 - \varepsilon$ (see Figure 1.2.3).

Note that the error here is the same error for all inputs. In a similar way we can define different errors for different inputs.

Definition 1.2.4.

Using this notation, systems $P_{XY|UV}$ which approximate the PR-box with error $\varepsilon \in [0, 0.25)$ are non-local. For a proof that any unbiased PR-box with error $\varepsilon < 0.25$ "holds" some secrecy, see

V\X, U\Y		U=0		U=1	
		X=0	X=1	X=0	X=1
0	0	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$
	1	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$
1	0	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$
	1	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$

Figure 1.2.3: Unbiased PR-box with error ε

for example Lemma 5 in [12]. While PR-Boxes correspond to perfect secrecy, PR-boxes with error correspond to partial secrecy. The problem is that the amount of secrecy (defined formally in Section 2.3) which can be achieved from a quantum system is not enough for our purposes. Therefore we must have some privacy amplification protocol in order for such systems to be useful.

1.3 Privacy amplification

In the privacy amplification problem we consider the following scenario. Alice and Bob share information that is only partially secret with respect to an adversary Eve. Their goal is to distill this information to a shorter string, the key, that is completely secret. The problem was introduced in [4, 5] for classical adversaries and in [13] for quantum adversaries. In our case, Alice and Bob want to create a secret key using a system $P_{XY|UV}$ while Eve, who is only limited by the non-signalling principle, tries to get some information about it.

Assume that Alice and Bob share a system from which they can create a partially secret bit string X. Information theoretically, if there is some entropy in one system, we can hope that by using several systems we will have enough entropy to create a more secure key. The idea behind privacy amplification is to consider Alice's and Bob's system as a black box, take several such systems which will produce several partially secret bit strings $X_1, ..., X_n$ and then apply some hash function f (which might take a short random seed as an additional input) to $X_1, ..., X_n$, in order to receive a shorter but more secret bit string K, which will act as the key.

The amount of secrecy, as will be defined formally in Section 2.3, is usually measured by the distance of the actual system of Alice, Bob and Eve from an ideal system, in which the key is uniformly distributed and not correlated to the information held by Eve. We will denote this distance by $d(K|E)$,

4

where E is Eve's system. We say that a system generating a key is ϵ-indistinguishable from an ideal system if $d(K|E) \leq \epsilon$ for some small $\epsilon > 0$. Therefore, the problem of privacy amplification is actually the problem of finding such a 'good' function f.

Privacy amplification is said to be possible when ϵ is a decreasing function of n, the number of systems held by Alice and Bob. In order to prove an impossibility result it is enough to give a specific system, in which each of the subsystems holds some secrecy, but this secrecy cannot be amplified by using any hash function - the distance from uniform remains high, no matter what function Alice and Bob apply to their output bits and how many systems they share.

In the classical scenario, this problem can be solved almost optimally by extractors [18, 21]. Although not all classical extractors work against quantum adversaries [9], some very good extractors do, for example, [8]. Since we consider a super-quantum adversary, we cannot assume that protocols which work for the classical and quantum case, will stay secure against a more powerful adversary. Therefore a different treatment is needed when considering non-signalling adversaries.

1.4   Related work

Barrett, Hardy, and Kent have shown in [2] a protocol for QKD which is based only on the assumption that Alice and Bob cannot signal to each other. Unfortunately, the suggested protocol cannot tolerate any errors caused by noise in the quantum channel and is inefficient in the number of quantum systems used in order to produce one secure bit. This problem could have been solved by using a privacy amplification protocol, which works even when the adversary is limited only by the non-signalling principle. Unfortunately, it was proven in [11] that such a privacy amplification protocol does not exist if signalling is possible within the laboratories of Alice and Bob.

On the contrary, in [12], [15] and [16] it was proven that if we assume full non-signalling conditions, i.e., that any subset of systems cannot signal to any other subset of systems, QKD which is based only on the non-locality of the correlations is possible. In particular, the step of privacy amplification is possible.

In the gap between these two extreme cases little has been known. There is one particular set of assumptions of special interest from an experimental point of view; the set of assumptions which says that the systems can only signal forward in time within the systems of Alice and Bob. For this setting it was only known that privacy amplification using the XOR or the AND function is impossible [14].

1.5   Contribution

In this letter we reduce the gap between the assumptions of [11], in which signalling is impossible only between Alice and Bob, and the physical relevant assumptions which says that the systems can only signal forward in time within the systems of Alice and Bob. We consider a set of assumptions which is very close to the conditions which only allow to signal forward in time and prove that the impossibility result of [11] still holds.

Since our set of assumptions differs only a bit from the assumptions of signalling only forward in time, called "backward non-signalling", we can highlight the specific assumptions which might make the difference between possibility and impossibility results. If the adversary does not necessarily need to exploit these specific assumptions, then privacy amplification will be impossible also in the physical assumptions of "backward non-signalling" systems. On the other hand, if privacy amplification will be proved to be possible we will know that the power of the adversary arises from these assumptions.

The proof given here is an extension of the proof in [11]. We prove that the adversarial strategy suggested in [11] is still valid under stricter non-signalling assumptions (Theorem 3.2.2), and as a consequence also under the assumption of an "almost backward non-signalling" system (Corollary 3.2.4). This will imply that privacy amplification against non-signalling adversaries is impossible under our stricter assumptions (which include a lot more non-signalling conditions than in [11]), as stated formally in Theorem 3.2.2.

1.6   Outline

The rest of this letter is organized as follows. In Chapter 2 we describe several different non-signalling conditions and explain the model of non-signalling adversaries. In Chapter 3 we define a specific system which respects many non-signalling conditions and yet we cannot use privacy amplification in order to create an arbitrary secure bit from it. In addition, we prove that an impossibility result for our set of assumptions implies an impossibility result for "almost backward non-signalling" systems (Corollary 3.2.4). In Chapter 4 we prove our main theorem, Theorem 3.2.2. We conclude in Chapter 5.

Chapter 2

Preliminaries

2.1 Notations

We denote the set $\{1, ..., n\}$ by $[n]$. For any string $x \in \{0,1\}^n$ and any subset $I \subseteq [n]$, x_i stands for the i'th bit of x and $x_I \in \{0,1\}^{|I|}$ stands for the string formed by the bits of x at the positions given by the elements of I. $\overline{I}$ is the complementary set of I, i.e., $\overline{I} = [n]/I$. $x_{\overline{i}}$ is the string formed by all the bits of x except for the i'th bit.

For two correlated random variables X, U over $\Lambda_1 \times \Lambda_2$, we denote the conditional probability distribution of X given U as $P_{X|U}(x|u) = Pr(X = x|U = u)$.

2.2 Non-signalling systems

We start by formally defining the different types of non-signalling systems and conditions which will be relevant in this letter.

Definition 2.2.1. (Fully non-signalling system). An n-party conditional probability distribution $P_{X|U}$ over $X, U \in \{0,1\}^n$ is called a fully non-signalling system if for any set $I \subseteq [n]$,

$$\forall x_{\overline{I}}, u_I, u'_I, u_{\overline{I}} \sum_{x_I \in \{0,1\}^{|I|}} P_{X|U}(x_I, x_{\overline{I}}|u_I, u_{\overline{I}}) = \sum_{x_I \in \{0,1\}^{|I|}} P_{X|U}(x_I, x_{\overline{I}}|u'_I, u_{\overline{I}}).$$

This definition implies that any group of parties cannot infer from their part of the system which inputs were given by the other parties. A measurement of a subset I of the parties does not change the statistics of the outcomes of parties $\overline{I}$; the marginal system they see is the same for all inputs of the other parties. This means that different parties cannot signal to other parties using only the system.

Note that this type of condition is not symmetric. The fact that parties I cannot signal to parties $\bar{I}$ does not imply that parties $\bar{I}$ cannot signal to parties I. The fully non-signalling conditions can also be written in the following way.

Lemma 2.2.2. *(Lemma 2.7 in [10]). An n-party system $P_{X|U}$ over $X, U \in \{0,1\}^n$ is a fully non-signalling system if and only if for all $i \in [n]$,*

$$\forall x_{\bar{i}}, u_i, u'_i, u_{\bar{i}} \sum_{x_i \in \{0,1\}} P_{X|U}(x_i, x_{\bar{i}}|u_i, u_{\bar{i}}) = \sum_{x_i \in \{0,1\}} P_{X|U}(x_i, x_{\bar{i}}|u'_i, u_{\bar{i}}).$$

In order to make sure that the fully non-signalling conditions as in Definition 2.2.1 hold one will have to create the system such that each of the $2n$ subsystems is space-like separated from all the others, or shielded, to exclude signalling. This is of course impractical from an experimental point of view. Therefore, we need to consider more practical, weaker, conditions. A minimal requirement needed for any useful system is that Alice cannot signal to Bob and vice versa[1]. We stress that this is an assumption, since the non-signalling condition cannot be tested (not even with some small error) using a parameter estimation protocol as a previous step. This assumption can be justified physically by shielding the systems or by performing the measurements in a space-like separated way.

Definition 2.2.3. (Non-signalling between Alice and Bob). A $2n$-party conditional probability distribution $P_{XY|UV}$ over $X, Y, U, V \in \{0,1\}^n$ does not allow for signalling from Alice to Bob if

$$\forall y, u, u', v \quad \sum_x P_{XY|UV}(x,y|u,v) = \sum_x P_{XY|UV}(x,y|u',v)$$

and does not allow for signalling from Bob to Alice if

$$\forall x, v, v', u \quad \sum_y P_{XY|UV}(x,y|u,v) = \sum_y P_{XY|UV}(x,y|u,v').$$

On top of the assumption that Alice and Bob cannot signal to each other, we can now add different types of non-signalling conditions. In a more mathematical way, we can think about it as follows. The full non-signalling conditions are a set of linear equations as in Definition 2.2.1 and Lemma 2.2.2. We

---

[1]If we will not ensure this condition, say by making sure that they are in space-like separated regions or by shielding their systems, the measured Bell violation will have no meaning and any protocol based on some kind of non locality will fail

can assume that all of these equations hold (this is the full non-signalling scenario) or we can use just a subset (which does not span the whole set) of these equations.

One type of systems which are physically interesting are the systems which can only signal forward in time (messages cannot be sent to the past). This can be easily achieved by measuring several quantum systems one after another, and therefore these are the non-signalling conditions that one "gets for free" when performing an experiment of QKD. For example, an entanglement-based protocol in which Alice and Bob receive entangled photons and measure them one after another using the same apparatus will lead to the conditions of Definition 2.2.4. If the apparatus has memory signalling is possible from A_i to A_{i+1} for example. However, signals cannot go outside from Alice's laboratory to Bob's laboratory. Formally, we use the following definition for backward non-signalling systems.

Definition 2.2.4. (Backward non-signalling system). For any $i \in \{2, ..., n-1\}$ denote the set $\{1, ..., i-1\}$ by I_1 and the set $\{i, ..., n\}$ by I_2. A $2n$-party conditional probability distribution $P_{XY|UV}$ over $X, Y, U, V \in \{0,1\}^n$ is a backward non-signalling system (does not allow for signalling backward in time) if for any $i \in [n]$,

$$\forall x_{I_1}, y, u_{I_1}, u_{I_2}, u'_{I_2}, v \quad \sum_{x_{I_2}} P_{XY|UV}(x_{I_1}, x_{I_2}, y | u_{I_1}, u_{I_2}, v) = \sum_{x_{I_2}} P_{XY|UV}(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v)$$

$$\forall x, y_{I_1}, u, v_{I_1}, v_{I_2}, v'_{I_2} \quad \sum_{y_{I_2}} P_{XY|UV}(x, y_{I_1}, y_{I_2} | u, v_{I_1}, v_{I_2}) = \sum_{y_{I_2}} P_{XY|UV}(x, y_{I_1}, y_{I_2} | u, v_{I_1}, v'_{I_2}).$$

In order to understand why these are the conditions that we choose to call "backward non-signalling" note that in these conditions Alice's (and analogously Bob's) systems A_{I_2} cannot signal not only to A_{I_1}, but even to A_{I_1} and all of Bob's systems together. I.e., A_{I_2} cannot change the statistics of A_{I_1} and B, even if they are collaborating with one another. Another way to see why these conditions make sense, is to consider a scenario in which Bob, for example, performs all of his measurements first. This of course should not change the results of the experiment since Alice and Bob are separated and cannot send signals to each other. Therefore when Alice performs her measurements on the systems A_{I_2}, her outcomes cannot impact the statistics of both A_{I_1} and B together.

In this letter we consider a different set of conditions, which does not allow for most types of signalling to the past.

Definition 2.2.5. (Almost backward non-signalling system). For any $i \in \{2, ..., n-1\}$ denote the set $\{1, ..., i-1\}$ by I_1 and the set $\{i, ..., n\}$ by I_2. A $2n$-party conditional probability distribution $P_{XY|UV}$
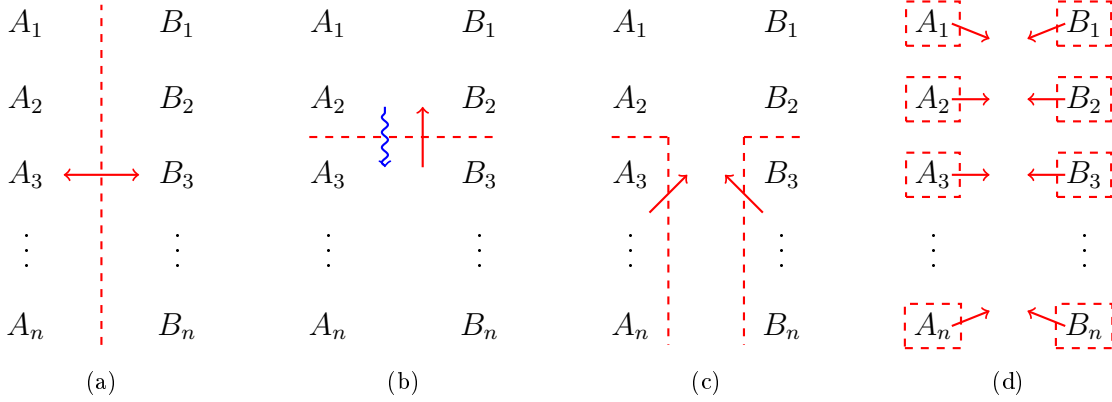
Figure 2.2.1: Different non-signalling conditions: signalling is impossible in the direction of the straight red arrow. (a) Non-signalling between Alice and Bob. (b) The conditions of Definition 2.2.5, almost backward non-signalling conditions, for $i = 3$. Note that signalling may be possible in the direction of the curly blue arrow. (c) The conditions of Definition 2.2.4, backward non-signalling conditions, for $i = 3$. (d) Full non-signalling conditions. The conditions we consider are the combination of (a) and (b).

over $X, Y, U, V \in \{0,1\}^n$ is an almost backward non-signalling system if for any $i \in [n]$,

$$\forall x_{I_1}, y_{I_1}, u_{I_1}, u_{I_2}, u'_{I_2}, v_{I_1}, v_{I_2}, v'_{I_2}$$
$$\sum_{x_{I_2}, y_{I_2}} P_{XY|UV}(x_{I_1}, x_{I_2}, y_{I_1}, y_{I_2} | u_{I_1}, u_{I_2}, v_{I_1}, v_{I_2}) = \sum_{x_{I_2}, y_{I_2}} P_{XY|UV}(x_{I_1}, x_{I_2}, y_{I_1}, y_{I_2} | u_{I_1}, u'_{I_2}, v_{I_1}, v'_{I_2}).$$

Figure 2.2.1 visualizes the difference between all of these non-signalling conditions.

The difference between the conditions of Definition 2.2.4 and Definition 2.2.5 is that when assuming the conditions of an almost backward non-signalling system signalling is not forbidden from A_i to B_i and A_j together for any i and $j < i$. I.e., if A_i wants to signal to some system in the past, A_j, B_i has to cooperate with A_j. To see this consider the following system for example. Alice and Bob share a system $P_{XY|UV}$ for $X, Y, U, V \in \{0,1\}^2$. We define the system such that each of the outputs is a perfectly random bit and independent of any input, except for X_1, which is equal to $Y_2 \oplus U_2$. Obviously, the outputs on Bob's side look completely random and independent of any input, i.e., the system is non-signalling from Alice to Bob. Now note that whenever we do not have access to Y_2, X_1 also looks like a perfectly random bit and independent of the input. Therefore, the system is also non-signalling from Bob to Alice, and almost backward non-signalling. However, the conditions of Definition 2.2.4 does not hold, since the input U_2 can be perfectly known from X_1 and Y_2 (i.e. A_2 can signal A_1 and B_2 together).

10

For every system $P_{XY|UV}$ which fulfills some arbitrary non-signalling conditions we can define marginal systems and extensions to the system in the following way.

Definition 2.2.6. (Marginal system). A system $P_{X|U}$ is called a marginal system of the system $P_{XZ|UW}$ if $\forall x, u, w \quad P_{X|U}(x|u) = \sum_z P_{XZ|UW}(x, z|u, w)$.

Note that for the marginal system $P_{X|U}$ of $P_{XZ|UW}$ to be defined properly, all we need is a non-signalling condition between the parties holding $X(U)$ and the parties holding $Z(W)$.

Definition 2.2.7. (Extension system). A system $P_{XZ|UW}$ is called an extension to the system $P_{X|U}$, which fulfills some arbitrary set of non-signalling conditions $\mathcal{C}$, if:

1. $P_{XZ|UW}$ does not allow for signalling between the parties holding $X(U)$ and the parties holding $Z(W)$.

2. The marginal system of $P_{XZ|UW}$ is $P_{X|U}$.

3. For any z the system $P_{X|U}^{Z=z}$ fulfills the same non-signalling conditions $\mathcal{C}$.

Note that for every system $P_{X|U}$ there are many different extensions. Next, in an analogous way to the definition of a classical-quantum state, $\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x$, we would like to define a classical-non-signalling system.

Definition 2.2.8. (Classical - non-signalling system). A classical - non-signalling (c-n.s.) system is a system $P_{XZ|UW}$ such that $|U| = 1$.

We can think about it as a system in which some of the parties cannot choose or change the input on their side of the system. When it is clear from the context which side of the system is classical and which side is not we drop the index which indicates the trivial choice for U and just write $P_{XZ|W}$. Notice that for a general system with some U, after choosing an input $u_i \in U$ we get the c-n.s. system $P_{XZ|U=u_i,W}$.

2.3 Distance measures

In general, the distance between any two systems $P_{X|U}$ and $Q_{X|U}$ can be measured by introducing another entity - the distinguisher. Suppose $P_{X|U}$ and $Q_{X|U}$ are two known systems. The distinguisher gets one of these systems, S, and has to guess which system he was given. In the case of our non-signalling systems, the distinguisher can choose which measurements to make (which inputs to insert to the system) and to see all the outputs. He then outputs a bit B with his guess. The distinguishing advantage between systems $P_{X|U}$ and $Q_{X|U}$ is the maximum guessing advantage the best distinguisher can have.

Definition 2.3.1. (Distinguishing advantage). The distinguishing advantage between two systems $P_{X|U}$ and $Q_{X|U}$ is

$$\delta(P_{X|U}, Q_{X|U}) = \max_{D} [P(B = 1 | S = P_{X|U}) - P(B = 1 | S = Q_{X|U})]$$

where the maximum is over all distinguishers D, S is the system which is given to the distinguisher and B is its output bit. Two systems $P_{X|U}$ and $Q_{X|U}$ are called ϵ-indistinguishable if $\delta(P_{X|U}, Q_{X|U}) \leq \epsilon$.

If the distinguisher is given an n-party system for $n > 1$ he can choose not only the n inputs but also the order in which he will insert them. The distinguisher can be adaptive, i.e., after choosing an input and seeing an output he can base his later decisions for the following inputs on the results seen so far. Therefore the maximization in this case will be on the order of the measurements and their values.

If the distinguisher is asked to distinguish between two c-n.s. systems we can equivalently write the distinguishing advantage as in the following lemma.

Lemma 2.3.2. *(Distinguishing advantage between two c-n.s. systems). The distinguishing advantage between two c-n.s systems $P_{KZ|W}$ and $Q_{KZ|W}$ is*

$$\delta(P_{KZ|W}, Q_{KZ|W}) = \sum_{k} \max_{w} \sum_{z} \left| P_{KZ|W=w}(k,z) - Q_{KZ|W=w}(k,z) \right|.$$

Proof. In order to distinguish between two c-n.s. systems, $P_{KZ|W}$ and $Q_{KZ|W}$, the distinguisher has only one input to choose, W. In addition, because the distinguisher has no choice for the input of the classical part, the distinguishing advantage can only increase if the distinguisher will first read the classical part of the system and then choose W according to the value of K. Therefore, for two

c-n.s. systems, the best strategy will be to read K and then to choose the best W, as indicated in the expression above.

$\square$

The distance (in norm 1) between two systems is defined to be half of the distinguishing advantage between these systems.

Definition 2.3.3. (Distance between two c-n.s. systems). The distance between two c-n.s systems $P_{KZ|W}$ and $Q_{KZ|W}$ in norm 1 is

$$\left| P_{KZ|W} - Q_{KZ|W} \right|_1 \equiv \frac{1}{2} \sum_k \max_w \sum_z \left| P_{KZ|W=w}(k,z) - Q_{KZ|W=w}(k,z) \right|.$$

In a cryptographic setting, we mostly consider the distance between the real system in which the key is being calculated from the output of the system held by the parties, and an ideal system. The ideal system in our case is a system in which the key is uniformly distributed and independent of the adversary's system. For a c-n.s. system $P_{KZ|W}$ where K is over $\{0,1\}^n$, let U_n denote the uniform distribution over $\{0,1\}^n$ and let $P_{Z|W}$ be the marginal system held by the adversary. The distance from uniform is a defined as follows.

Definition 2.3.4. (Distance from uniform). The distance from uniform of the c-n.s. system $P_{KZ|W}$ is
$$d(K|Z(W)) \equiv \left| P_{KZ|W} - U_n \times P_{Z|W} \right|_1$$
where the system $U_n \times P_{Z|W}$ is defined such that $U_n \times P_{Z|W}(k,z|w) = U_n(k) \cdot P_{Z|W}(z|w)$.

In the following sections we consider the distance from uniform given a specific input (measurement) of the adversary, $W = w$. In this case, according to Definition 2.3.4, we get

$$
\begin{aligned}
d(K|Z(w)) &= \frac{1}{2} \sum_{k,z} \left| P_{KZ|W=w}(k,z) - U_n(k) \cdot P_{Z|W=w}(z) \right| = \\
&= \frac{1}{2} \sum_{k,z} P_{Z|W=w}(z) \left| P_{K|Z=z}(k) - \frac{1}{n} \right|.
\end{aligned}
\tag{2.3.1}
$$

2.4   Modeling non-signalling adversaries

When modeling a non-signalling adversary, the question in mind is: given a system $P_{XY|UV}$ shared by Alice and Bob, for which some arbitrary non-signalling conditions hold, which extensions to a system $P_{XYZ|UVW}$, including the adversary Eve, are possible? The only principle which limits Eve is the non-signalling principle, which means that the conditional system $P_{XY|UV}^{Z=z}$, for any $z \in Z$, must fulfill all of the non-signalling conditions that $P_{XY|UV}$ fulfills, and in addition $P_{XYZ|UVW}$ does not allow signalling between Alice and Bob together and Eve. Since any non-signalling assumptions about the system of Alice and Bob are ensured physically (by shielding the systems for example), they must still hold even if Eve's output z is given to some other party. Therefore the conditional system $P_{XY|UV}^{Z=z}$ must also fulfill all the non-signalling conditions of $P_{XY|UV}$, which justifies our assumptions about the power of the adversary in this setting.

$$U \longrightarrow \boxed{P_{XYZ|UVW}} \longleftarrow V$$
$$X \longleftarrow \qquad \longrightarrow Y$$
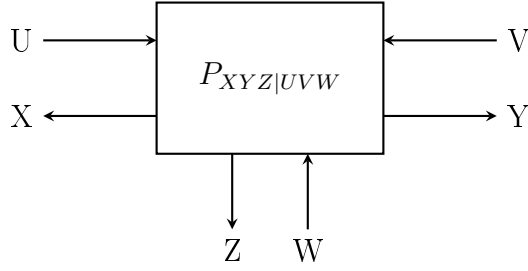$$Z \quad W$$

Figure 2.4.1: A three-partite system

We adopt here the model given in [11, 10, 12] of non-signalling adversaries. We reduce the scenario in which Alice, Bob and Eve share a system $P_{XYZ|UVW}$ to the scenario considering only Alice and Bob in the following way. Because Eve cannot signal to Alice and Bob (even together) by her choice of input, we must have, for all x, y, u, v, w, w',

$$\sum_z P_{XYZ|UVW}(x, y, z|u, v, w) = \sum_z P_{XYZ|UVW}(x, y, z|u, v, w') = P_{XY|UV}(x, y|u, v).$$

Moreover, as said before, since any non-signalling condition must still hold even if Eve's output z is given to some other party, the system conditioned on Eve's outcome, $P_{XY|UV}^{Z=z}$, must also fulfill all the non-signalling conditions of $P_{XY|UV}$. We can therefore see Eve's input as a choice of a convex decomposition of Alice's and Bob's system and her output as indicating one part of this decomposition. Formally,

Definition 2.4.1. (Partition of the system). A partition of a given multipartite system $P_{XY|UV}$, which fulfills a certain set of non-signalling conditions $\mathcal{C}$, is a family of pairs $(p^z, P_{XY|UV}^z)$, where:

14

1. p^z is a classical distribution (i.e. for all z $p^z \geq 0$ and $\sum_z p^z = 1$).

2. For all z, $P^z_{XY|UV}$ is a system that fulfills $\mathcal{C}$.

3. $P_{XY|UV} = \sum_z p^z \cdot P^z_{XY|UV}$.

We can use the same proof as in Lemma 2 and 3 in [12] to prove that this is indeed a legitimate model, i.e., that the set of all partitions covers exactly all the possible strategies of a non-signalling adversary in our case.

It is further proven in [11] that for showing an impossibility result, we can assume that Eve's information Z is a binary random variable:

Lemma 2.4.2. *(Lemma 5 in [11]). If $(p^{z=0}, P^{z=0}_{XY|UV})$ is an element of a partition with m elements, then it is also possible to define a new partition with only two elements, in which one of the elements is $(p^{z=0}, P^{z=0}_{XY|UV})$.*

Moreover, it is not necessary to determine both parts of the partition $((p^{z=0}, P^{z=0}_{XY|UV})$ and $(p^{z=1}, P^{z=1}_{XY|UV}))$ explicitly. Instead, a condition on the system given outcome $z = 0$ is given, which will make sure that there exists a second part, complementing it to a partition:

Lemma 2.4.3. *(Lemma 6 in [11]). Given a non-signalling distribution $P_{XY|UV}$, there exists a partition with element $(p^{z=0}, P^{z=0}_{XY|UV})$ if and only if for all inputs and outputs x, y, u, v it holds that $p^{z=0} \cdot P^{z=0}_{XY|UV}(x, y|u, v) \leq P_{XY|UV}(x, y|u, v)$.*

For the formal proofs of these lemmas, note that since the non-signalling conditions are linear the same proofs as in Lemma 5 and Lemma 6 in [11] will hold here as well, no matter which non-signalling conditions are imposed for $P_{XY|UV}$.

Defining a partition is equivalent to choosing a measurement $W = w$, therefore, we can also write the distance from uniform of a key, as in Equation (2.3.1), using the partition itself. Since we will only need to consider the case where Alice and Bob try to output one secret bit, we can further simplify the expression, as in the following lemma.

Lemma 2.4.4. *(Lemma 5.1 in [10]). For the case $K = f(X)$, where $f : \{0,1\}^{|X|} \to \{0,1\}$, $U = u$,*

$V = v$, and where the strategy $W = w$ is defined by the partition $\left\{ \left(p^{z_w}, P^{z_w}_{XY|UV} \right) \right\}_{z_w \in \{0,1\}}$,

$$d\left(K|Z(w)\right) = \frac{1}{2} \sum_{z_w} p^{z_w} \cdot \left| \sum_{x,y} (-1)^{f(x)} P^{z_w}_{XY|UV}(x,y|u,v) \right|.$$

For a proof see Lemma 5.1 in [10].

Chapter 3

The Non-signalling Assumptions

3.1 The basic assumptions

It was proven in [12] (Lemma 5) that any unbiased PR-box with error $\varepsilon < 0.25$ holds some secrecy. With the goal of amplifying the privacy of the secret in mind, Alice and Bob now share n such systems. The underlying system of Alice and Bob that we consider is a product of n independent PR-boxes with errors (Definition 1.2.3), as seen from Alice's and Bob's point of view. This is stated formally in the following definition:

Definition 3.1.1. (Product system). A product system of n copies of PR-boxes with error ε is the system $P_{XY|UV} = \prod_{i \in [n]} P_{X_i Y_i | U_i V_i}$, where for each i, the system $P_{X_i Y_i | U_i V_i}$ is an unbiased PR-box with error ε as in Definition 1.2.3.

In addition, as explained in Section 2.2, in order for any system to be useful, we will always make sure that Alice and Bob cannot signal to each other (otherwise any non-local violation will not have any meaning - it could have also been achieved by signalling between the systems). Mathematically, this means that for any outcome z of any adversary, Alice and Bob cannot signal to each other using the system $P_{XY|UV}^z$. I.e., $P_{XY|UV}^z$ fulfills the conditions of Definition 2.2.3.

On top of this assumption we can now add more non-signalling assumptions of different types. For example, in [12], [15] and [16] it was proven that if we assume full non-signalling conditions then privacy amplification is possible. On the contrary, in [11] it was proven that if we do not add more non-signalling assumption (and use only the assumption that Alice and Bob cannot signal to each other) then privacy amplification is impossible. An interesting question is therefore, what happens in the middle? Is privacy amplification possible when we use some additional assumptions but not all of

them?

The goal of this letter is to consider the conditions of almost backward non-signalling systems, given in Definition 2.2.5. We will do so by considering a larger set of equations, defined formally in Section 3.2.

3.2 Our additional assumptions

Consider the following system.

Definition 3.2.1. Alice and Bob and Eve share a system $P_{XYZ|UVW}$ such that:

1. The marginal system of Alice and Bob $P_{XY|UV}$ is a product system as in Definition 3.1.1.

2. For any z, $P^z_{XY|UV}$ fulfills the conditions of Definition 2.2.3 (Alice and Bob cannot signal each other).

3. For all $i \in [n]$ and for any z

$$\forall x_{\bar{i}}, y_{\bar{i}}, u_i, u'_i, u_{\bar{i}}, v \qquad \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u, v) = \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u', v)$$

$$\forall x_{\bar{i}}, y_{\bar{i}}, u, v_i, v'_i, v_{\bar{i}} \qquad \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u, v) = \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u, v').$$

Note that the set of these conditions is equivalent to

$$\forall x_{\bar{i}}, y_{\bar{i}}, u_i, u'_i, u_{\bar{i}}, v_i, v'_i, v_{\bar{i}} \qquad \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u, v) = \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u', v'). \tag{3.2.1}$$

To see this first note that the conditions of Definition 3.2.1 are a special case of Equation (3.2.1). For the second direction: $\forall x_{\bar{i}}, y_{\bar{i}}, u_i, u'_i, u_{\bar{i}}, v_i, v'_i, v_{\bar{i}}$,

$$\sum_{x_i, y_i} P^z_{XY|UV}(x, y|u, v) = \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u', v) = \sum_{x_i, y_i} P^z_{XY|UV}(x, y|u', v').$$

Therefore, the equations of Definition 3.2.1 mean that for all i, parties A_i and B_i together cannot signal the other parties (See Figure 3.2.1).

Adding these assumptions to the the non-signalling assumption between Alice and Bob (Definition 2.2.3) does not imply the full non-signalling conditions. To see this consider the following example.
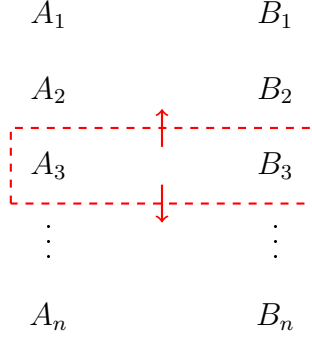
18

$$\begin{array}{cc} A_1 & B_1 \\[1em] A_2 & B_2 \\[1em] A_3 & B_3 \\[1em] \vdots & \vdots \\[1em] A_n & B_n \end{array}$$

Figure 3.2.1: The n.s. conditions of Definition 3.2.1 for $i = 3$

Alice and Bob share a system $P_{XY|UV}$ such that $X, Y, U, V \in \{0, 1\}^2$. We define the system such that each of the outputs is a perfectly random bit and independent of any input, except for X_2, which is equal to $Y_1 \oplus U_1$. The outputs on Bob's side look completely random and independent of any input, i.e., the system is non-signalling from Alice to Bob. Now note that whenever we do not have access to Y_1, then X_2 also looks like a perfectly random bit and independent of the input. Therefore, the system is also non-signalling from Bob to Alice, and the conditions of Definition 3.2.1 hold as well. However, this system is not fully non-signalling, since the input U_1 can be perfectly known from X_2 and Y_1 (i.e. A_1 can signal A_2 and B_1 together).

Adding this set of equations as assumptions means to add a lot more assumptions about the system (on top of the basic system described before). Intuitively, such a system is close to being a fully non-signalling system. We will prove that even in this case, Theorem 15 in [11] still holds and privacy amplification is impossible:

Theorem 3.2.2. *There exists a system as in Definition 3.2.1 such that for any hash function f, there exists a partition w for which the distance from uniform of $f(X)$ given w is at least $c(\varepsilon)$, i.e., $d(f(X)|Z(w)) \geq c(\varepsilon)$, where $c(\varepsilon)$ is some constant which depends only on the error of a single box, ε (as in Definition 3.1.1).*

Note that although our set of equations might seem unusual, proving an impossibility result for this set implies the same impossibility result for all sets of linear equations that are determined by it. The set of equations of an almost backward non-signalling system, as in Definition 2.2.5, is one interesting example of such a set.

Lemma 3.2.3. *The almost backward non-signalling conditions, as in Definition 2.2.5, are implied by the non-signalling conditions of Definition 3.2.1.*

Proof. Consider the set of equations in Definition 2.2.5. We will now prove them using the equations in Definition 3.2.1, this will imply that if the assumptions of Definition 3.2.1 hold then so do the assumption of almost backward non-signalling.

For every $i \in [n]$ we can write

$$
\sum_{x_{I_2}, y_{I_2}} P_{XY|UV}(x, y | u_{I_1}, u_{I_2}, v_{I_1}, v_{I_2}) = \sum_{\substack{x_{I_2/\{i\}} \\ y_{I_2/\{i\}}}} \sum_{x_i \\ y_i} P_{XY|UV}(x, y | u_{I_1}, u_i, u_{I_2/\{i\}}, v_{I_1}, v_i, v_{I_2/\{i\}})
$$

$$
= \sum_{\substack{x_{I_2/\{i\}} \\ y_{I_2/\{i\}}}} \sum_{x_i \\ y_i} P_{XY|UV}(x, y | u_{I_1}, u_i', u_{I_2/\{i\}}, v_{I_1}, v_i', v_{I_2/\{i\}})
$$

$$
= \sum_{\substack{x_{I_2/\{i+1\}} \\ y_{I_2/\{i+1\}}}} \sum_{x_{i+1} \\ y_{i+1}} P_{XY|UV}(x, y | u_{I_1}, u_i', u_{i+1}, u_{I_2/\{i,i+1\}}, v_{I_1}, v_i', v_{i+1}, v_{I_2/\{i,i+1\}})
$$

$$
= \sum_{\substack{x_{I_2/\{i+1\}} \\ y_{I_2/\{i+1\}}}} \sum_{x_{i+1} \\ y_{i+1}} P_{XY|UV}(x, y | u_{I_1}, u'_{\{i,i+1\}}, u_{I_2/\{i,i+1\}}, v_{I_1}, v'_{\{i,i+1\}}, v_{I_2/\{i,i+1\}})
$$

$$
= \dots = \sum_{x_{I_2}, y_{I_2}} P_{XY|UV}(x, y | u_{I_1}, u'_{I_2}, v_{I_1}, v'_{I_2}). \qquad \square
$$

Combining Lemma 3.2.3 together with Theorem 3.2.2 implies the following.

Corollary 3.2.4. *There exists an almost backward non-signalling system as in Definition 2.2.5 such that for any hash function f, there exists a partition w for which the distance from uniform of $f(X)$ given w is at least $c(\varepsilon)$, i.e., $d(f(X)|Z(w)) \geq c(\varepsilon)$, where $c(\varepsilon)$ is some constant which depends only on the error of a single box, ε (as in Definition 3.1.1).*

Another interesting example is the set of equations which includes non-signalling conditions between all of Alice's systems alone and non-signalling conditions between all of Bob's systems alone, together with the condition of non-signalling between Alice and Bob.

Definition 3.2.5. An n-party conditional probability distribution $P_{XY|UV}$ over $X, Y, U, V \in \{0,1\}^n$ is completely non-signalling on Alice's side and completely non-signalling on Bob's side, if for any $i \in [n]$,

$$\forall x_{\bar{i}}, u_i, u_i', u_{\bar{i}} \quad \sum_{x_i} P_{X|U}(x_i, x_{\bar{i}}|u_i, u_{\bar{i}}) = \sum_{x_i} P_{X|U}(x_i, x_{\bar{i}}|u_i', u_{\bar{i}})$$

$$\forall y_{\bar{i}}, v_i, v_i', v_{\bar{i}} \quad \sum_{y_i} P_{Y|V}(y_i, y_{\bar{i}}|v_i, v_{\bar{i}}) = \sum_{y_i} P_{Y|V}(y_i, y_{\bar{i}}|v_i', v_{\bar{i}})$$

where $P_{X|U}$ is the marginal system of $P_{XY|UV}$, held by Alice, and $P_{Y|V}$ is the marginal system of $P_{XY|UV}$, held by Bob.

Lemma 3.2.6. *The non-signalling conditions of Definition 3.2.5 are implied by the non-signalling conditions of Definition 3.2.1.*

Proof. We show that this is true for Alice's side. The proof for Bob's side is analogous. First, for any $i \in [n]$, we can write the equation

$$\forall x_{\bar{i}}, u_i, u_i', u_{\bar{i}} \qquad \sum_{x_i} P_{X|U}(x_i, x_{\bar{i}}|u_i, u_{\bar{i}}) = \sum_{x_i} P_{X|U}(x_i, x_{\bar{i}}|u_i', u_{\bar{i}})$$

using the original system $P_{XY|UV}$ and the definition of a marginal system:

$$\forall x_{\bar{i}}, u_i, u_i', u_{\bar{i}}, v \qquad \sum_{x_i, y} P_{XY|UV}(x, y|u_i, u_{\bar{i}}, v) = \sum_{x_i, y} P_{XY|UV}(x, y|u_i', u_{\bar{i}}, v).$$

Now, as in the proof of Lemma 3.2.3,

$$\sum_{x_i, y} P_{XY|UV}(x, y|u_i, u_{\bar{i}}, v) = \sum_{y/\{y_i\}} \sum_{x_i, y_i} P_{XY|UV}(x, y|u_i, u_{\bar{i}}, v)$$

$$= \sum_{y/\{y_i\}} \sum_{x_i, y_i} P_{XY|UV}(x, y|u_i', u_{\bar{i}}, v)$$

$$= \sum_{x_i, y} P_{XY|UV}(x, y|u_i', u_{\bar{i}}, v). \qquad \square$$

Combining Lemma 3.2.6 together with Theorem 3.2.2 implies the following.

Corollary 3.2.7. *There exists a system as in Definition 3.2.5 such that for any hash function f, there exists a partition w for which the distance from uniform of $f(X)$ given w is at least $c(\varepsilon)$, i.e., $d(f(X)|Z(w)) \geq c(\varepsilon)$, where $c(\varepsilon)$ is some constant which depends only on the error of a single box, ε (as in Definition 3.1.1).*

Chapter 4

Privacy Amplification Against Non-signalling Adversaries

4.1 The impossibility of privacy amplification under the basic non-signalling assumptions

We use here the same adversarial strategy as presented in [11] and therefore repeat it here shortly for completeness. For intuitive explanations and complete formal proofs please see [11].

As explained before, Alice's and Bob's goal is to create a highly secure key using a system, $P_{XY|UV}$, shared by both of them. Eve's goal is to get some information about the key. It is therefore natural to model this situation in the following way: Alice, Bob and Eve share together a system $P_{XYZ|UVW}$, an extension of the system $P_{XY|UV}$ held by Alice and Bob, which fulfills some known non-signalling conditions. Each party can perform measurements on it's part of the system (i.e., insert input and read the outputs of their interfaces of the system), communicate using a public authenticated channel, Alice then applies some public hash function f to the outcome she holds and in the end Alice should hold a key, $K = f(X)$, which is ϵ-indistinguishable from an ideal, uniformly distributed key, even conditioned on Eve's information. I.e., $d(K|Z(W)) \le \epsilon$.

The distance from uniform of the key k is lower-bounded by the distance from uniform of a single bit of the key, and therefore, for an impossibility result, it is enough to assume that f outputs just one bit. Note that since the adversarial strategy can be chosen after all public communication is over, it can also depend on a random seed for the hash function. Therefore it is enough to consider deterministic functions in this case.

We consider a partition with only two outputs, $z = 0$ and $z = 1$, each occurring with probability $\frac{1}{2}$, such that given $z = 0$, $f(X)$ is maximally biased towards 0. According to Lemma 2.4.3 it is enough

to explicitly construct the conditional system given measurement outcome $z = 0$. In order to do so we start from the unbiased system as seen by Alice and Bob and "shift around" probabilities such that $f(X)$ is maximally biased towards 0 and the marginal system remains valid. By valid me mean that:

1. All entries must remain probabilities between 0 and 1.

2. The normalization of the probability distribution must remain.

3. The non-signalling condition between Alice and Bob must be satisfied.

4. There must exist a second measurement outcome $z = 1$ occurring with probability $\frac{1}{2}$, and such that the conditional system, given outcome $z = 1$, is also a valid probability distribution. This second system must be able to compensate for the shifts in probabilities. According to Lemma 2.4.3 this means that the entry in every cell must be smaller or equal twice the original entry.

The system $P^{z=0}_{XY|UV}$ which describes this strategy is defined formally in the following way. For simplicity we will drop the subscript of $P_{XY|UV}(x, y|u, v)$ and write only $P(x, y|u, v)$. We use the same notations as in [11, 10] and define the following groups, for all u, v:

$$
\begin{aligned}
y_< &= \left\{ y \ \middle| \ \sum_{x|f(x)=0} P(x, y|u, v) < \sum_{x|f(x)=1} P(x, y|u, v) \right\} \\
y_> &= \left\{ y \ \middle| \ \sum_{x|f(x)=0} P(x, y|u, v) > \sum_{x|f(x)=1} P(x, y|u, v) \right\} \\
x_0 &= \left\{ x \ \middle| \ f(x) = 0 \right\} \\
x_1 &= \left\{ x \ \middle| \ f(x) = 1 \right\}
\end{aligned}
$$

and a factor $c(x, y|u, v)$ as:

$$
\begin{aligned}
\forall x &\in x_0, y \in y_< & c(x, y|u, v) &= 2 \\
\forall x &\in x_1, y \in y_< & c(x, y|u, v) &= \frac{\sum_{x'} (-1)^{(f(x')+1)} P(x', y|u, v)}{\sum_{x'|f(x')=1} P(x', y|u, v)} \\
\forall x &\in x_0, y \in y_> & c(x, y|u, v) &= \frac{\sum_{x'} P(x', y|u, v)}{\sum_{x'|f(x')=0} P(x', y|u, v)} \\
\forall x &\in x_1, y \in y_> & c(x, y|u, v) &= 0
\end{aligned}
$$

24

The system $P^{z=0}$ is then defined as $P^{z=0}(x,y|u,v) = c(x,y|u,v) \cdot P(x,y|u,v)$.

Intuitively, this definition of the strategy means that for each u,v and within each row, Eve shifts as much probability as possible out from the cells $P(x,y|u,v)$ for which $f(x) = 1$ and into the cells $P(x',y|u,v)$ for which $f(x') = 0$ (she wants $P^{z=0}$ to be biased towards 0). The factor $c(x,y|u,v)$ is defined in such a way that as much probability as possible is being shifted, while still keeping the system $P^{z=0}$ a valid element of a partition.

Although Eve shifts probabilities for each u,v separately, $P^{z=0}$ will still fulfill the required non-signalling conditions, which connect the inputs u,v to other inputs u',v'; this is due to the high symmetry in the original marginal box of Alice and Bob (Definition 3.1.1). For example, it is easy to see that since Eve only shifts probabilities within the same row (i.e. cells with the same value of y) Bob cannot signal to Alice using $P^{z=0}$; the sum of the probabilities in one row stays the same as it was in P, and since P did not allow for signalling from Bob to Alice, so do $P^{z=0}$. The other non-signalling conditions follow from a bit more complex symmetries.

It was proven in [11] that for this strategy[1] $d(K|Z(w)) \leq \frac{-1+\sqrt{1+64\varepsilon^2}}{32\varepsilon}$.

4.2 Proof of the theorem - a more general impossibility result

In order to prove Theorem 3.2.2 we will just prove that the adversarial strategy presented in [11] still works. Formally, this means that we need to prove that the element $\left(p^{z=0} = \frac{1}{2}, P^{z=0}(x,y|u,v)\right)$ in the partition is still valid, even when we add the assumptions of Definition 3.2.1, and that $d(K|Z(w))$ is high. Since we do not change the strategy, the same bound on $d(K|Z(w))$ still holds. Moreover, it was already proven in [11] that $P^{z=0}(x,y|u,v)$ does not allow signalling between Alice and Bob, therefore we only need to prove that our additional non-signalling assumptions of Definition 3.2.1 hold in the system $P^{z=0}(x,y|u,v)$, i.e., the system satisfies our assumptions even conditioned on Eve's result. draw,

The first three lemmas deal with the impossibility of signalling from Alice's side and the next three lemmas deal with Bob's side. All the lemmas use the high symmetry of the marginal box (Definition 3.1.1). What these lemmas show is that most of this symmetry still exists in $P^{z=0}$, because we only shift probabilities within the same row.

We use the following notation; for all $i \in [n]$ let $u^{i'}$ be $u^{i'} = u_1...u_{i-1}, \overline{u_i}, u_{i+1}...u_n$ (i.e., only the i'th bit is flipped) and the same for $x^{i'}$, $y^{i'}$ and $v^{i'}$.

Lemma 4.2.1. *For all $i \in [n]$ and for all x,y,u,v such that $v_i = 1$, $P(x,y^{i'}|u,v) = P(x,y|u^{i'},v)$.*

---

[1]Actually, this strategy is being used only when Alice is using an hash function which does not allow Bob to generate a bit from his output of the system Y, which is highly correlated with the key. If Alice uses a function which does allow Bob to get an highly correlated key, then this function has to be biased and therefore Eve can just use the trivial strategy of doing nothing. For more details please see [11].

Proof. For every single box , $P_{X_iY_i|U_iV_i}(x_i, y_i|u_i, v_i) = P_{X_iY_i|U_iV_i}(\overline{x_i}, \overline{y_i}|u_i, v_i)$. Therefore it also holds that $P(x, y|u, v) = P(x^{i'}, y^{i'}|u, v)$. Moreover,

$$
\begin{aligned}
P(x, y|u^{i'}, v) &= \left(\frac{1}{2} - \frac{\varepsilon}{2}\right)^{\sum_l 1 \oplus x_l \oplus y_l \oplus u_l^{i'} \cdot v_l} \cdot \left(\frac{\varepsilon}{2}\right)^{\sum_l x_l \oplus y_l \oplus u_l^{i'} \cdot v_l} = \\
&= \left(\frac{1}{2} - \frac{\varepsilon}{2}\right)^{\sum_l 1 \oplus x_l^{i'} \oplus y_l \oplus u_l \cdot v_l} \cdot \left(\frac{\varepsilon}{2}\right)^{\sum_l x_l^{i'} \oplus y_l \oplus u_l \cdot v_l} = \\
&= P(x^{i'}, y|u, v)
\end{aligned}
$$

Combining these two properties together, we get $P(x, y|u^{i'}, v) = P(x^{i'}, y|u, v) = P(x, y^{i'}|u, v)$.

$\square$

Lemma 4.2.2. *For all $i \in [n]$ and for all x,y,u,v such that $v_i = 1$, $c(x, y^{i'}|u, v) = c(x, y|u^{i'}, v)$. I.e., the cells $P(x, y^{i'}|u, v)$ and $P(x, y|u^{i'}, v)$ are from the same type $(x_0/x_1, y_>/y_<)$.*

Proof. First, it is clear that if $P(x, y^{i'}|u, v)$ was a x_0 (x_1) cell, so is $P(x, y|u^{i'}, v)$ because this only depends on x.

Now note that Lemma 4.2.1 is correct for every x, therefore the entire row $P(\bullet, y^{i'}|u, v)$ is equivalent to the row $P(\bullet, y|u^{i'}, v)$. This means that if we change $y^{i'}$ to y and u to $u^{i'}$ together, we will get the same row, and therefore if $P(x, y^{i'}|u, v)$ was a $y_<$ ($y_>$) cell, so is $P(x, y|u^{i'}, v)$. All together we get $c(x, y^{i'}|u, v) = c(x, y|u^{i'}, v)$.

$\square$

The properties of the marginal system $P_{XY|UV}$ which are being used in Lemma 4.2.1 and Lemma 4.2.2 can be easily seen, for example, in Table 4.1 and Table 4.2. For simplicity we consider a product of only 2 systems. When changing Alice's input from $u = 11$ to $u = 10$ while $v = 11$, the rows interchange as Lemma 4.2.1 suggests.

	x / y	00	01	10	11
		$u = 11$			
$v = 111$	00	$\left(\frac{\varepsilon}{2}\right)^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\left(\frac{1-\varepsilon}{2}\right)^2$
	01	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\left(\frac{\varepsilon}{2}\right)^2$	$\left(\frac{1-\varepsilon}{2}\right)^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$
	10	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\left(\frac{1-\varepsilon}{2}\right)^2$	$\left(\frac{\varepsilon}{2}\right)^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$
	11	$\left(\frac{1-\varepsilon}{2}\right)^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\left(\frac{\varepsilon}{2}\right)^2$

Table 4.1: $P_{XY|UV}$ for two systems ($n = 2$), for $u = 11$, $v = 11$

		$u = 10$			
	x	00	01	10	11
y					
	00	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$(\frac{\varepsilon}{2})^2$	$(\frac{1-\varepsilon}{2})^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$
$v = 111$	01	$(\frac{\varepsilon}{2})^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$(\frac{1-\varepsilon}{2})^2$
	10	$(\frac{1-\varepsilon}{2})^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$(\frac{\varepsilon}{2})^2$
	11	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$	$(\frac{1-\varepsilon}{2})^2$	$(\frac{\varepsilon}{2})^2$	$\frac{\varepsilon}{2} \cdot \frac{1-\varepsilon}{2}$

Table 4.2: $P_{XY|UV}$ for two systems ($n = 2$), for $u = 10$, $v = 11$

Lemma 4.2.3. *In the conditional system* $P^{z=0}$ *, for any* $i \in [n]$

$$\forall x_{\bar{i}}, y_{\bar{i}}, u_i, u_{\bar{i}}, v \qquad \sum_{x_i, y_i} P^{z=0}(x, y | u, v) = \sum_{x_i, y_i} P^{z=0}(x, y | u^{i'}, v).$$

Proof. First note that for any u and v such that $v_i = 0$ the probability distribution $P_{XY|U=u,V=v}$ is identical to $P_{XY|U=u^{i'},V=v}$ (because of the properties of a single box, see Figure 1.2.3). Therefore Eve will shift the probabilities in these two systems in the same way, which implies that $P^{z=0}_{XY|U=u,V=v}$ is identical to $P^{z=0}_{XY|U=u^{i'},V=v}$, and in particular, any non-signalling conditions will hold in this case.

Assume $v_i = 1$. We will prove something a bit stronger than needed. We prove that for all $x, y_{\bar{i}}, u_i, u_{\bar{i}}, v, \sum_{y_i} P^{z=0}(x, y | u, v) = \sum_{y_i} P^{z=0}(x, y | u^{i'}, v)$. This in particular implies that $\sum_{x_i, y_i} P^{z=0}(x, y | u, v) = \sum_{x_i, y_i} P^{z=0}(x, y | u^{i'}, v)$ also holds.

$$\sum_{y_i} P^{z=0}(x, y | u^{i'}, v) = \sum_{y_i} c(x, y | u^{i'}, v) \cdot P(x, y | u^{i'}, v)$$
$$= \sum_{y_i} c(x, y^{i'} | u, v) \cdot P(x, y^{i'} | u, v)$$
$$= \sum_{y_i} P^{z=0}(x, y^{i'} | u, v)$$
$$= \sum_{y_i} P^{z=0}(x, y | u, v).$$

The first and third equalities are by the definition of $P^{z=0}$, the second equality is due to Lemma 4.2.1 and Lemma 4.2.2 and the last equality is due the fact that the sum is over y_i.

$\square$

Lemma 4.2.4. *For all* $i \in [n]$ *and for all* x,y,u,v, $P(x, y^{i'} | u, v) = P(x, y | u, v^{i'})$.

Proof.

$$P(x,y|u,v^{i'}) = \left(\frac{1}{2}-\frac{\varepsilon}{2}\right)^{\sum_l 1 \oplus x_l \oplus y_l \oplus u_l \cdot v_l^{i'}} \cdot \left(\frac{\varepsilon}{2}\right)^{\sum_l x_l \oplus y_l \oplus u_l \cdot v_l^{i'}} =$$

$$= \left(\frac{1}{2}-\frac{\varepsilon}{2}\right)^{\sum_l 1 \oplus x_l \oplus y_l^{i'} \oplus u_l \cdot v_l} \cdot \left(\frac{\varepsilon}{2}\right)^{\sum_l x_l \oplus y_l^{i'} \oplus u_l \cdot v_l} =$$

$$= P(x,y^{i'}|u,v). \qquad \square$$

Lemma 4.2.5. *For all $i \in [n]$ and for all x,y,u,v such that $v_i = 1$, $c(x,y^{i'}|u,v) = c(x,y|u,v^{i'})$. I.e., the cells $P(x,y^{i'}|u,v)$ and $P(x,y|u,v^{i'})$ are from the same type $(x_0/x_1, y_>/y_<)$.*

Proof. As in Lemma 4.2.2, it is clear that if $P(x,y^{i'}|u,v)$ was a x_0 (x_1) cell, so is $P(x,y|u,v^{i'})$ because this only depends on x.

Lemma 4.2.4 is correct for every x, therefore the entire row $P(\bullet,y^{i'}|u,v)$ is equivalent to the row $P(\bullet,y|u,v^{i'})$ and therefore if $P(x,y^{i'}|u,v)$ was a $y_<$ ($y_>$) cell, so is $P(x,y|u,v^{i'})$. All together we get $c(x,y^{i'}|u,v) = c(x,y|u,v^{i'})$. $\qquad \square$

Lemma 4.2.6. *In the conditional system $P^{z=0}$, for any $i \in [n]$*

$$\forall x_{\bar{i}}, y_{\bar{i}}, u, v_i, v_{\bar{i}} \qquad \sum_{x_i,y_i} P^{z=0}(x,y|u,v) = \sum_{x_i,y_i} P^{z=0}(x,y|u,v^{i'}).$$

Proof. In an analogous way to the proof of Lemma 4.2.3, if $u_i = 0$ the proof is trivial. Assume $u_i = 1$.

We prove that for all $x,y_{\bar{i}},u,v_i,v_{\bar{i}}$, $\sum_{y_i} P^{z=0}(x,y|u,v) = \sum_{y_i} P^{z=0}(x,y|u,v^{i'})$. This in particular implies that $\sum_{x_i,y_i} P^{z=0}(x,y|u,v) = \sum_{x_i,y_i} P^{z=0}(x,y|u,v^{i'})$ also holds.

$$\sum_{y_i} P^{z=0}(x,y|u,v^{i'}) = \sum_{y_i} c(x,y|u,v^{i'}) \cdot P(x,y|u,v^{i'}) =$$

$$= \sum_{y_i} c(x,y^{i'}|u,v) \cdot P(x,y^{i'}|u,v) =$$

$$= \sum_{y_i} P^{z=0}(x,y^{i'}|u,v) =$$

$$= \sum_{y_i} P^{z=0}(x,y|u,v). \qquad \square$$

28

Note that the only difference between the full non-signalling conditions and what we have proved here is that in Lemma 4.2.3 we have to keep the summation over y_i. Moreover, it is interesting to see that at least on Bob's side, the "full" non-signalling conditions also hold in $P^{z=0}$. Since Eve's strategy is defined to work on each row separately, the symmetry on Bob's side does not break at all.

Lemmas 4.2.3 and 4.2.6 together prove that the assumption of Definition 3.2.1 holds even conditioned on Eve's result. Adding this to the rest of the proof of [11] proves Theorem 3.2.2.

Chapter 5

Concluding Remarks and Open Questions

In this letter we proved that privacy amplification is impossible even if we add a lot more non-signalling conditions over the assumptions of [11]. This also implies that privacy amplification is impossible under the assumptions of an almost backward non-signalling system. An interesting question which arises from our theorem is whether the non-signalling conditions in which the backward non-signalling systems and the almost backward non-signalling system differs are the ones which give Eve the tremendous power which makes privacy amplification impossible. If yes, then it might be the case that privacy amplification is possible in the relevant setting of backward non-signalling systems. On the other hand, if the answer to this question is no, then privacy amplification is also impossible for backward non-signalling systems. If this is indeed the case then it seems that the security proof for any practical QKD protocol will have to be based on quantum physics somehow, and not on the non-signalling postulate alone.

Another interesting question is whether we can extend our result to the case where Alice and Bob use a more interactive protocol to amplify the secrecy of their key; instead of just applying some hash function only on Alice's output X and get a key $K = f(X)$, maybe they can use Bob's output Y as well and create a key $K = g(X, Y)$.

Bibliography

[1] B. Podolsky A. Einstein and N. Rosen. Can quantum-mechanical description of physcial reality be considered complete? *Physical Review*, 47:777–780, 1935.

[2] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):10503, 2005.

[3] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[4] C.H. Bennett, G. Brassard, and J.M. Robert. Privacy amplification through public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[5] C.H. Bennett, G. Brassard, and J.M. Robert. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6, Part 2):1915–1923, 1995.

[6] B.S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[7] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[8] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *Arxiv preprint arXiv:0912.5514*, 2009.

[9] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. De Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. *STOC*, page 516–525, 2007.

[10] E. Hänggi. Device-independent quantum key distribution. PhD thesis, ETH Zurich. *Arxiv preprint arXiv:1012.3878*, 2010.

[11] E. Hänggi, R. Renner, and S. Wolf. The impossibility of non-signaling privacy amplification. http://arxiv.org/abs/0906.4760.

[12] E. Hänggi, R. Renner, and S. Wolf. Quantum cryptography based solely on Bell's theorem. *Arxiv preprint arXiv:0911.4171*, 2009.

[13] R. König, U. Maurer, and R. Renner. On the power of quantum memory.

[14] L. Masanes. Personal communication, 2009.

[15] L. Masanes. Universally composable privacy amplification from causality constraints. *Physical Review Letters*, 102(14):140501, 2009.

[16] L. Masanes, S. Pironio, and A. Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2:238, 2011.

[17] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pages 503–509. IEEE, 1998.

[18] N. Nisan and A. Ta-Shma. Extracting randomness: A survey and new constructions. *Journal of Computer and System Sciences*, 58(1):148–173, 1999.

[19] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11:045021, 2009.

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

[21] R. Shaltiel. An introduction to randomness extractors. *Automata, Languages and Programming*, pages 21–41, 2011.