

Limits of privacy amplification against non-signalling memory attacks

Rotem Arnon-Friedman and Amnon Ta-Shma

The Blavatnik School of Computer Science, Tel-Aviv University, Israel

January 1, 2013

Abstract

The task of privacy amplification, in which Alice holds some partially secret information with respect to an adversary Eve and wishes to distill it until it is completely secret, is known to be solvable almost optimally in both the classical and quantum worlds. Unfortunately, when considering an adversary who is limited only by non-signalling constraints such a statement cannot be made in general. We here consider systems which violate the chained Bell inequality and prove that under the natural assumptions of a time-ordered non-signalling system, which allow past subsystems to signal future subsystems (using the device's memory for example), super-polynomial privacy amplification by any hashing is impossible. This is of great relevance when considering practical device independent key distribution protocols which assume a super-quantum adversary.

1 Introduction

Device independent key distribution

Key distribution is the task of creating a shared secret string, called the key, between two parties. In contrast to classical key distribution protocols, which base their security on the computational power of the adversary, quantum key distribution (QKD) protocols are resilient against quantum adversaries with unbounded computational power. However, in order to apply traditional QKD security proofs, such as security proofs for the BB84 protocol [1], one should be able to fully characterise the devices on which the protocol is being executed. Failing to do so can introduce security flaws which can be exploited by the adversary [2]. Unfortunately, giving a full characterisation of quantum devices is usually an impractical task.

Due to this difficulty, in the past few years there has been a growing interest in device independent QKD (DIQKD). In DIQKD protocols [3, 4] we assume that the system on which the protocol is being executed was made and given to the honest parties Alice and Bob by a malicious adversary Eve. We therefore ought to consider the system, which we know nothing about, as a black box, and the security proof cannot be based on the internal functioning of the device.

How can this be done? As was first shown in [5], security proofs for DIQKD can be based on observed non-local correlations between Alice and Bob, i.e., on the correlations of the outputs they get from their systems. If the correlations they observe violate some Bell inequality, such as the CHSH inequality [6] or other more

general chained Bell inequities [7, 8], and if Alice and Bob enforce a non-signalling condition between them in order to make sure that these correlations are indeed non-local, then they can be sure that some secrecy is available to them [8].

The first DIQKD protocol which was proven secure was a protocol by Barret, Hardy and Kent (BHK) [9]. Although this protocol cannot tolerate a reasonable amount of noise, it showed that the task of DIQKD is in principle possible. Moreover, the BHK protocol security proof applies not only against quantum adversaries, but also against non-signalling adversaries.

When considering a non-signalling adversary the only thing which limits the adversary is the non-signalling principle. That is, the adversary has super-quantum power; however, if Alice and Bob enforce some local non-signalling constraints then these cannot be broken by the adversary. Such constraints can be enforced by shielding and isolating the devices or by placing them in a space-like separated way. For example, if Alice and Bob perform their measurements in a space-like separated way, then according to relativity theory, Alice cannot use her system in order to signal Bob and vice-versa.

After the BHK protocol, several other DIQKD protocols, such as [10, 11], have been proven secure, but all using an impractical assumption; in order to guarantee security each subsystem used in the protocol must be isolated from all other subsystem, such that they cannot signal each other. For example, if Alice gets n systems from Eve, each producing one bit, she must isolate each of these systems, in order to make sure that no informa-

tion leaks from one system to another. Such an harsh constraint, which we call the full non-signalling constraint, eliminates the possibility of devices with memory.

Recently a new protocol, which does not share this drawback, was proven secure [12]. The sole assumption about the non-signalling constraints of the system in this protocol is that Alice, Bob and Eve cannot signal each other using the system, which is a minimal requirement from any cryptographic protocol¹. However, this protocol, like the BHK protocol, cannot tolerate any reasonable amount of noise.

Privacy amplification

In this paper we consider a simpler problem, called privacy amplification (PA). In the PA problem Alice holds some information which is only partially secret with respect to an adversary, Eve. Alice’s goal is to distill her information, to a shorter string, which is completely (or almost completely) secret. Note that in the PA problem we only want Alice to have a secret key with respect to the adversary, while in QKD we also want Bob to hold the same key as Alice. Therefore PA is easier than QKD.

In order to understand what exactly is the PA problem, consider the following scenario. Assume that Alice has a system, a black box, which produces for her a partially secret bit or a string, X . By saying that X is partially secret we mean that there is some entropy in X conditioned on Eve’s knowledge about X . One would hope that by letting Alice use several such systems, which will produce several partially secret bits X_1, X_2, \dots, X_n , she will have enough entropy in order to produce a more secret bit or a string, K , out of them, or in other words, she will be able to amplify the privacy of her key. The idea behind the PA protocols is to apply some hash function² $f : \{0, 1\}^n \rightarrow \{0, 1\}^{|K|}$ (for $|K| < n$) to X_1, X_2, \dots, X_n in order to receive a shorter, but more secret, bit string K . The amount of secrecy is usually measured by the distance of the actual system of Alice and Eve from an ideal system, in which K is uniformly distributed and uncorrelated to Eve’s system. This will be defined formally in the following section.

Since QKD in the presence of a non-signalling adversary is possible if we assume that Alice’s and Bob’s systems fulfil the full non-signalling conditions [10, 11], PA is also possible in this setting. However, it was already proven in [13] that PA is impossible if we impose non-signalling conditions only between Alice and Bob,³ i.e., Alice and Bob cannot signal each other, while signalling within their systems is possible. Recently, the

impossibility result of [13] was extended to an even more general case [14].

A more realistic assumption to consider is that in addition to the non-signalling assumption between Alice and Bob, within the system of the parties signalling is possible only from the past to the future and not the other way around. These are natural assumptions when considering a protocol in which Alice and Bob each use just one device with memory. In that case, the inputs and outputs of past measurements (which were saved in the memory of the device) can affect the outputs of future measurements. Such conditions, which we call time-ordered non-signalling conditions, are defined formally in Definition 2.

In contrast to the full non-signalling conditions, the time-ordered non-signalling conditions are easy to ensure. Alice and Bob can both shield their entire system (as has to be done anyhow in order to make sure that no information leaks straight to the adversary) and therefore signalling will be impossible between them. Moreover, when running the protocol, they will perform their measurements in a sequential manner; the first system will be measured in the beginning, then the second one and so on. This will make sure (as long as we believe that messages cannot be sent from the future to the past) that signalling is possible only in the forward direction of time. In fact, 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 device will lead to the time-ordered non-signalling conditions. If Alice’s and Bob’s devices have memory then information from past measurements can be available for future measurements, i.e., signalling is possible from the past to the future but not the other way around.

In this paper we ask the following question. Under the assumptions of time-ordered non-signalling system, is privacy amplification against non-signalling adversaries possible? We give an example for a system which fulfils all the time-ordered non-signalling conditions, and in which super-polynomial PA is impossible. More precisely, we prove that for protocols which are based on a violation of chained Bell inequalities, under the assumption of a time-ordered non-signalling system, super-polynomial PA is impossible by any hashing. That is, when using n black boxes, each producing a partially secret bit, the adversary can always get a great amount of information about the hashing result; at least as high as $\Omega\left(\frac{1}{n}\right)$.

Although this proves that super-polynomial PA is

¹If Alice’s system can signal Eve’s system then Alice’s secret can leak to Eve completely. If Alice’s system can signal Bob’s system, then the correlations they observe are not necessarily non-local and could have been produced by a deterministic system. This implies that Eve can get all the information that Alice and Bob have as well.

²The hash function might also take a random seed of size m as an additional input; in that case $f : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^{|K|}$.

³In contrast to the QKD problem, when considering the PA problem the only goal of Bob is to establish non-local correlations with Alice.

impossible under these conditions, this is still a partial answer to our question for two reasons. First, there might still be some other system, in which the secrecy is based on a different Bell inequality, for which exponential PA is possible. Second, in this paper we show that, independently of which hash function Alice is using, Eve can bias the key by at least $\Omega(\frac{1}{n})$; but can we find a specific hash function for which she cannot do any better than this? That is, is this result tight? Therefore, the question of whether (linear) privacy amplification is at all possible remains open.

2 Preliminaries

Chained Bell inequalities

For two correlated random variables X, U 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 distribution $P_{XY|UV}$, where U and X are usually Alice's input and output respectively, while V and Y are Bob's input and output. When considering a tripartite system which includes Eve, $P_{XYZ|UVW}$, Eve's input and output are W and Z .

Bell proved that entangled quantum states can display non-local correlations under measurements [15]. We consider the following Bell-type experiments. Alice and Bob share a bipartite system $P_{XY|UV}$ where $U \in \{0, 2, \dots, 2N-2\}$ and $V \in \{1, 3, \dots, 2N-1\}$. We define a set of allowed input pairs for Alice and Bob to be $G_N = \{(u, v)|u \in U, v \in V, |u - v| = 1\} \cup \{(0, 2N-1)\}$. For each measurement of Alice U , and each measurement of Bob V , there are two possible outcomes, 0 or 1. That is, $X, Y \in \{0, 1\}$. The relevant Bell inequality then reads [7, 8]

$$I_N = P(X = Y|U = 0, V = 2N - 1) + \sum_{\substack{u, v \\ |u - v| = 1}} P(X \neq Y|U = u, V = v) \geq 1. \quad (1)$$

This implies that correlations which satisfy $I_N < 1$ are non-local and cannot be described by shared randomness of the parties. For $N = 2$ this inequality is the CHSH inequality [6].

For the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, if Alice's measurements are in the basis $\{\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle\}$ for $\theta = \frac{\pi U}{2N}$ and Bob's measurements are in the same basis but for $\theta = \frac{\pi V}{2N}$ then the correlations they get satisfy

$$I_N^* = 2N \sin^2 \frac{\pi}{4N} < \frac{\pi^2}{8N}. \quad (2)$$

This implies that I_N^* can be made arbitrarily small for sufficiently large N .⁴

In our proof we will assume that the systems violate the chained Bell inequality. This is of course not the only possible choice for QKD protocols, although it is the most common one. Moreover, note that since for these type of systems PA is impossible, we cannot treat in general any system which produces some secrecy as a black box and therefore PA in general is impossible.

Non-signalling systems

Denote Alice's and Bob's system by $P_{XY|UV}$. A minimal requirement needed for any useful system is that Alice cannot signal to Bob using the system and vice versa, otherwise, the measured Bell violation will have no meaning. This can be ensured by placing Alice and Bob in space-like separated regions or by shielding their systems.

Definition 1. (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

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

This definition implies that Bob (Alice) cannot infer from his (her) part of the system which input was given by Alice (Bob). The marginal system each of them sees is the same for all inputs of the other party and therefore the system $P_{XY|UV}$ cannot be used for signalling.

In this paper we consider the conditions that we call time-ordered non-signalling conditions.

⁴However, as N gets larger it becomes difficult to close the detection loophole [16] in the performed experiments, which is essential for any protocol that is based on non-local correlations.

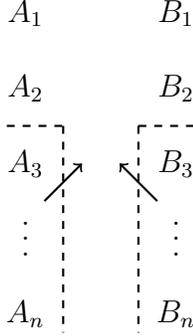


Figure 1: Time-ordered non-signalling condition for $i = 3$. Signalling is impossible in the direction of the straight arrow.

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

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

Figure 1 illustrates these conditions. Note that the conditions of Definition 1 follow from these conditions.

Non-signalling adversaries

When modelling a non-signalling adversary, the question in mind is as follows: 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 for any of her measurements w , the conditional system $P_{XY|UV}^{Z(w)=z}$, for any $z \in Z$, must fulfil all of the non-signalling conditions that $P_{XY|UV}$ fulfils, and in addition $P_{XYZ|UVW}$ cannot allow signalling between Alice and Bob together and Eve.

⁵It is enough to consider the case where Alice wants to create just one secret bit. An impossibility result for one bit implies an impossibility result for several bits.

We adopt here the model given in [10, 13, 17] of non-signalling adversaries. 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' ,

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

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, we can define every strategy of Eve as a partition of Alice's and Bob's system in the following way.

Definition 3. (Partition of the system). A partition of a given multipartite system $P_{XY|UV}$, which fulfils a certain set of non-signalling conditions \mathcal{C} , is a family of pairs $(p^z, P_{XY|UV}^z)$, where:

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 , $P_{XY|UV}^z$ is a system that fulfils \mathcal{C} .
3. $P_{XY|UV} = \sum_z p^z P_{XY|UV}^z$.

In our scenario the goal of the adversary is to gain information about $f(X)$, for some function⁵ $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Note that since the adversarial strategy can be chosen after all public communication between Alice and Bob is done any additional random seed cannot help Alice and Bob. Therefore it is enough to consider deterministic functions in this case.

In order to quantify how good a strategy w is, i.e., how much information Eve gains about $f(X)$ by using w , we use the variational distance between the real system and the ideal system, in which $f(X)$ is uniformly distributed and independent of the adversary's system.

Lemma 4. (Lemma 3.7 in [17]). For the case $K = f(X)$, where $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $U = u$, $V = v$, and where the strategy w is defined by the partition $\left\{ (p^z, P_{XY|UV}^z) \right\}_{z \in \{0,1\}}$ such that $\Pr[K = 0 | Z = 0] \geq \frac{1}{2}$, the distance from uniform of $f(X)$ given the strategy w is

$$\begin{aligned} d(K|Z(w)) = \\ p^{z=0} \cdot (\Pr[K = 0 | Z = 0] - \Pr[K = 1 | Z = 0]) \\ - \frac{1}{2} (\Pr[K = 0] - \Pr[K = 1]). \end{aligned}$$

3 Main result

In order to show an impossibility result we give a concrete adversarial strategy against any almost balanced hash functions. Eve will create a time-ordered non-signalling system between Alice, Bob and herself, such that when she inputs the hash function f which was chosen by Alice on her side of the system, the output will be a guess at $f(x)$. We prove that this guess is correct with probability of at least $\frac{1}{2} + \frac{c}{n}$, where c is some constant and n is the number of systems shared by Alice and Bob. Against functions which are not almost balanced Eve can just use a trivial strategy and guess the value of the function without using her part of the system at all.

As noted before, in order to prove an impossibility result it is enough to prove it for a specific system. We assume that when the adversary is not present, Alice and Bob share n independent maximally entangled states and perform the measurements which achieve the violation of Equation (2). We denote the system of each entangled pair by $P_{X_i Y_i | U_i V_i}$ for $i \in [n]$ and the whole system by $P_{XY|UV} = \prod_{i \in [n]} P_{X_i Y_i | U_i V_i}$.

Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be an almost balanced function. Showing a strategy is giving a partition of Alice's and Bob's system, as in Definition 3. Our partition will have 2 parts, $P_{XY|UV}^0$ and $P_{XY|UV}^1$, each occurring with probability $\frac{1}{2}$ and $P_{XY|UV} = \frac{1}{2}P_{XY|UV}^0 + \frac{1}{2}P_{XY|UV}^1$. In our partition $P_{XY|UV}^0$ is biased towards $f(x) = 0$ and $P_{XY|UV}^1$ towards $f(x) = 1$. That is., if Eve gets an outcome of $z = 0$ (1) when measuring her part of the system she knows that Alice's output x is more likely to be a preimage of 0 (1) according to f .

In this section we explain the idea and the intuition behind the adversarial strategy and the main principles of the proof. For the formal proof and technical details please see Appendix C. We start by describing how Eve can bias the system towards $f(x) = 0$, i.e., what is $P_{XY|UV}^0$.

Assume for the moment that for some given prefix of x , $x_{1\dots i-1}$, and function f we have

$$\Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}0x_{i+1\dots n}) = 0] > \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}1x_{i+1\dots n}) = 0].$$

This implies that, for this specific prefix $x_{1\dots i-1}$, if Eve can guess the i 'th bit x_i then she can also guess the output bit of f . Therefore Eve can definitely benefit from biasing the i 'th bit towards 0.

Can the i 'th subsystem be biased without changing the correlations Alice and Bob observe? The following lemma answers this question.

Lemma 5. For any $i \in [n]$, the system $P_{X_i Y_i | U_i V_i}$, for which $I_N(P_{X_i Y_i | U_i V_i}) = I_N^*$, can be biased towards 0 (or 1) by $c(I_N^*) = \frac{I_N^*}{2N}$.

We denote the biased system by $P_{X_i Y_i | U_i V_i}^{z_i = \sigma}$ for $\sigma \in \{0, 1\}$. The biased system is given in Appendix A.

Therefore, in our adversarial strategy, if the value of the i 'th bit x_i , given the prefix $x_{1\dots i-1}$, has enough influence over the outcome of f (we will soon define how much is enough), although the suffix is unknown, then the i 'th system is being biased by $c(I_N^*)$. Note that for any prefix $x_{1\dots i-1}$ a different system $P_{X_i Y_i | U_i V_i}$ should be biased.

Next we say how Eve determines which subsystem $P_{X_i Y_i | U_i V_i}$ to bias for every x . For every function f , index $i \in [n]$ and prefix $x_{1\dots i-1}$ define

$$\Delta_i(x_{1\dots i-1}) \equiv \left| \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}0x_{i+1\dots n}) = 0] - \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}1x_{i+1\dots n}) = 0] \right|.$$

$\Delta_i(x_{1\dots i-1})$ quantifies how much influence the i 'th bit has over f given the prefix $x_{1\dots i-1}$ ⁶. For every x , Eve will bias the subsystem with the pivotal index, as we now define.

Definition 6. (Pivotal index⁷). Given $f : \{0, 1\}^n \rightarrow \{0, 1\}$, for any x , the pivotal index $i(x) \in [n]$ is the smallest index such that $\Delta_{i(x)}(x_{1\dots i-1}) \geq \frac{2}{3n}$.

Consider for example the function presented in Figure 2. The pivotal indices are marked in the binary tree of the function by a circle. For strings x with prefix $x_1 = 0$ the pivotal index is $i(x) = 2$, while for strings with prefixes $x_1 x_2 = 10$ and $x_1 x_2 = 11$ the pivotal index is $i(x) = 3$.

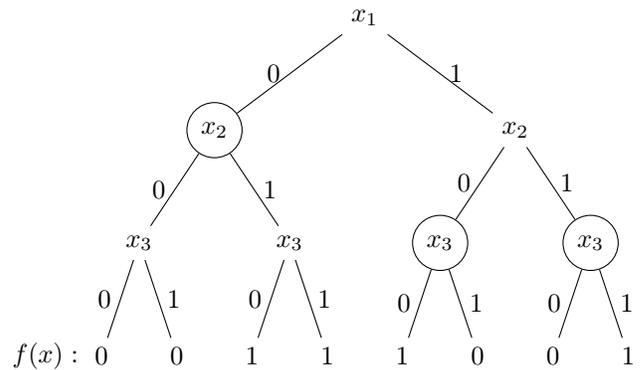


Figure 2: Binary tree with pivotal nodes. The pivotal nodes are marked with circles.

Luckily, for every function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ for which $|\Pr_x [f(x) = 0] - \Pr_x [f(x) = 1]| \leq \frac{1}{3}$ and ev-

⁶Note that the influence towards $f(x) = 0$ and $f(x) = 1$ is the same.

⁷The terms 'pivotal' and 'influence' are taken from the field of Boolean function analysis.

ery $x \in \{0, 1\}^n$ there exists such a pivotal index $i(x)$ for which $\Delta_{i(x)}(x_{1\dots i-1}) \geq \frac{2}{3n}$ and therefore for every x there exists some bit, $x_{i(x)}$, which can give non-negligible information to Eve about the final output.

Lemma 7. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be an almost balanced function, i.e. $|\Pr_x[f(x) = 0] - \Pr_x[f(x) = 1]| \leq \frac{1}{3}$. Then for any x there exists a pivotal index $i(x)$ such that $\Delta_{i(x)}(x_{1\dots i-1}) \geq \frac{2}{3n}$.*

Lemma 7 is proven in Appendix B. Putting everything together, Eve's strategy is as follows. For every x the $i(x)$ 'th subsystem, where $i(x)$ is the pivotal index of x , is biased. It is biased by $c(I_N^*)$ towards 0 if $\Pr_{x_{i+1\dots n}}[f(x_{1\dots i-1}0x_{i+1\dots n}) = 0] > \Pr_{x_{i+1\dots n}}[f(x_{1\dots i-1}1x_{i+1\dots n}) = 0]$ and towards 1 otherwise. The system $P_{XY|UV}^0$ which results from such a strategy is given in Equation (3) in Appendix C.

The strategy for biasing the system towards $f(x) = 1$ is symmetric to the strategy we described for $f(x) = 0$. The only difference is that Eve will bias the i 'th system by $c(I_N^*)$ towards 0 if $\Pr_{x_{i+1\dots n}}[f(x_{1\dots i-1}0x_{i+1\dots n}) = 0] < \Pr_{x_{i+1\dots n}}[f(x_{1\dots i-1}1x_{i+1\dots n}) = 0]$ and towards 1 otherwise, and not the other way around. The fact that these two symmetric systems put together a legal partition, as in Definition 3, is proven in Appendix C.

Since Eve biases a different subsystem $P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}$ for every x , it is not clear that the system $P_{XY|UV}^0$ is indeed time-ordered non-signalling. The key idea for proving such a thing is that for every x , the location of the pivotal index $i(x)$ depends only on the prefix of x until this index exactly. Intuitively, in our case this corresponds to the fact that signalling is possible from past measurements to future measurements, or in other words, the fact that in any given time the prefix of x can be saved in Alice's device. This is proven formally in Appendix C.

How much information does this strategy give Eve? For every x the $i(x)$ 'th subsystem is biased by $c(I_N^*)$. However, the advantage Eve gets from this shift in the probabilities is only $c(I_N^*) \cdot \Delta_{i(x)}(x_{1\dots i-1})$ since the pivotal bit does not determine $f(x)$ exactly⁸. Moreover, since $P_{XY|UV}^0$ and $P_{XY|UV}^1$ are symmetric and both occur with the same probability $\frac{1}{2}$ they both contribute the same amount of knowledge to Eve.

As mentioned before, for any function for which

$|\Pr_x[f(x) = 0] - \Pr_x[f(x) = 1]| > \frac{1}{3}$ Eve can just guess the value of the function with a constant success probability of at least $\frac{2}{3}$. Therefore these kind of functions do not bother us. Altogether we get the following theorem.

Theorem 8. *There exists a time-ordered non-signalling system $P_{XY|UV}$ as in Definition 2 such that for any hash function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ there exists a strategy w , for which the distance from uniform of $f(x)$ given w is at least $c(I_N^*) \cdot \frac{2}{3n}$, i.e., $d(f(x)|Z(w)) \geq c(I_N^*) \cdot \frac{2}{3n} \in \Omega(\frac{1}{n})$ where $I_N(P_{XY|UV}) = I_N^*$ and $c(I_N^*) = \frac{I_N^*}{2N}$.⁹*

Proof. If $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is an almost balanced function as in Lemma 7 then w is the strategy described above, for which $d(f(x)|Z(w)) \geq c(I_N^*) \cdot \frac{2}{3n}$. Otherwise, the strategy is to guess $f(x)$. For this trivial strategy we have $d(f(x)|Z(w)) \geq \frac{2}{3} - \frac{1}{2} \geq c(I_N^*) \cdot \frac{2}{3n}$. \square

Concluding remarks and open questions

In this paper we showed that when considering systems which can signal only forward in time and non-signalling adversaries, then super-polynomial privacy amplification by any hash function is impossible. For protocols which are based on the violation of the chained Bell inequalities, we presented a specific adversarial strategy which uses the memory of the device in order to gain information about the value of the function.

It is not yet clear whether our result is tight. We showed that, independently of which hash function Alice is using, Eve can bias the key by at least $\Omega(\frac{1}{n})$. For some bad choices of hash functions Eve can get even more information than $\Omega(\frac{1}{n})$ by using the same strategy. For example, if the chosen hash function is the XOR, then by using the exact same strategy, but with a different analysis, Eve can bias the final key bit by a constant. When using the Majority function this strategy can only give her $\Omega(\frac{1}{\sqrt{n}})$ bias. Is this the best Eve can do? Can we find a specific hash function for which she cannot do any better than this? The question whether linear privacy amplification is possible or not therefore remains open.

Acknowledgments: Rotem Arnon-Friedman thanks Roger Colbeck for helpful comments. Both authors acknowledge support from the FP7 FET-Open Project QCS.

⁸When we shift some probability π around from a cell which has probability p_1 to result in $f(x) = 0$ (over the suffix) to a cell which has probability p_2 to result in $f(x) = 0$ the advantage we get from shifting π is $\pi \cdot (p_2 - p_1)$. In our case, $p_2 - p_1$ is exactly $\Delta_{i(x)}(x_{1\dots i-1})$ in our case.

⁹Remember that n is the number of systems while N is the number of possible measurements for each system. For any given protocol N is constant and therefore so also is I_N^* .

References

- [1] C.H. Bennett, G. Brassard, et al. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.
- [2] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2:349, 2011.
- [3] 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.
- [4] 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.
- [5] A. Acin, N. Gisin, and L. Masanes. From Bell’s theorem to secure quantum key distribution. *Physical review letters*, 97(12):120405, 2006.
- [6] 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.
- [7] S.L. Braunstein and C.M. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202(1):22–56, 1990.
- [8] J. Barrett, A. Kent, and S. Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, 97:170409, Oct 2006.
- [9] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):10503, 2005.
- [10] E. Hänggi, R. Renner, and S. Wolf. Quantum cryptography based solely on Bell’s theorem. *Arxiv preprint arXiv:0911.4171*, 2009.
- [11] L. Masanes. Universally composable privacy amplification from causality constraints. *Physical Review Letters*, 102(14):140501, 2009.
- [12] J. Barrett, R. Colbeck, and A. Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Arxiv preprint arXiv:1209.0435*, 2012.
- [13] E. Hänggi, R. Renner, and S. Wolf. The impossibility of non-signaling privacy amplification. <http://arxiv.org/abs/0906.4760>.
- [14] R. Arnon Friedman, E. Hänggi, and A. Ta-Shma. Towards the impossibility of non-signalling privacy amplification from time-like ordering constraints. *Arxiv preprint quant-ph/1205.3736*, 2012.
- [15] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.
- [16] V. Scarani and C. Kurtsiefer. The black paper of quantum cryptography: real implementation problems. *Arxiv preprint arXiv:0906.4547*, 2009.
- [17] E. Hänggi. Device-independent quantum key distribution. PhD thesis, ETH Zurich. *Arxiv preprint arXiv:1012.3878*, 2010.

Appendices

A Proof of Lemma 5

We now prove the following lemma:

Lemma. *For any $i \in [n]$, the system $P_{X_i Y_i | U_i V_i}$, for which $I_N(P_{X_i Y_i | U_i V_i}) = I_N^*$, can be biased towards 0 (or 1) by $c(I_N^*) = \frac{I_N^*}{2N}$.*

Proof. In order to prove this we define the system $P_{X_i Y_i | U_i V_i}^{z_i=0}$ which is biased towards 0 by $c(I_N^*)$. We do so by shifting probabilities around in the original unbiased system $P_{X_i Y_i | U_i V_i}$. The original system $P_{X_i Y_i | U_i V_i}$, as in Figure 3, describes the measurements statistics of the maximally entangled state $|\Phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the basis $\{\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle\}$, where for Alice $\theta = \frac{\pi U}{2N}$, $U \in \{0, 2, \dots, 2N - 2\}$ and for Bob $\theta = \frac{\pi V}{2N}$, $V \in \{1, 3, \dots, 2N - 1\}$.

In order to bias this system towards 0 we shift probabilities within each individual square in the figure, such that each square will be biased toward 0 by $\sin^2\left(\frac{\pi}{4N}\right)$. We do so by shifting in every row probability of $\frac{1}{2}\sin^2\left(\frac{\pi}{4N}\right)$

out from the cell with $x_i = 1$ and into the cell with $x_i = 0$, as indicated in Figure 4. Each square corresponds to a different measurement made by Alice and Bob, and therefore for every measurement the bias is the same and equivalent to $c(I_N^*) = \frac{1}{2N} \cdot I_N^*$.

Note that by shifting probabilities in this way we do not change the correlations of the system, i.e., $I_N \left(P_{X_i Y_i | U_i V_i}^{z_i=0} \right) = I_N^*$.

The system $P_{X_i Y_i | U_i V_i}^{z_i=1}$, which is biased towards 1, is symmetric. That is, we shift the same amount of probability but in the opposite direction (from $x_i = 0$ to $x_i = 1$). This also implies that $\frac{1}{2} P_{X_i Y_i | U_i V_i}^{z_i=0} + \frac{1}{2} P_{X_i Y_i | U_i V_i}^{z_i=1} = P_{X_i Y_i | U_i V_i}$. \square

B Proof of Lemma 7

For convenience we rewrite Lemma 7 here again.

Lemma. *Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be an almost balanced function for which $|\Pr_x[f(x) = 0] - \Pr_x[f(x) = 1]| \leq \frac{1}{3}$. Then for any x there exists a pivotal index $i(x)$ such that $\Delta_{i(x)}(x_{1\dots i-1}) \geq \frac{2}{3n}$, where*

$$\Delta_i(x_{1\dots i-1}) \equiv \left| \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1} 0 x_{i+1\dots n}) = 0] - \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1} 1 x_{i+1\dots n}) = 0] \right|.$$

Proof. Let $\pi^0(x_{1\dots i-1}) = \Pr_{x_{i\dots n}} [f(x) = 0]$ where $x = x_{1\dots i-1} x_{i\dots n}$ and note the following properties:

$$\begin{aligned} \pi^0(x_{1\dots i-1}) &= \frac{1}{2} [\pi^0(x_{1\dots i-1} 0) + \pi^0(x_{1\dots i-1} 1)] \\ \pi^0(\phi) &\geq \frac{1}{3} \\ \pi^0(x_{1\dots n}) &\in \{0, 1\}. \end{aligned}$$

Assume w.l.o.g $\pi^0(x_{1\dots n}) = 0$ (the proof is symmetric for the case $\pi^0(x_{1\dots n}) = 1$).

Let $\max_{i \in [n]} |\pi^0(x_{1\dots i}) - \pi^0(x_{1\dots i-1})| \leq \zeta$. This implies the following:

$$\frac{1}{3} \leq \left| \pi^0(\phi) - \pi^0(x_{1\dots n}) \right| \leq n \cdot \zeta$$

and therefore $\zeta \geq \frac{1}{3n}$. I.e., there exists $j \in [n]$ such that $|\pi^0(x_{1\dots j}) - \pi^0(x_{1\dots j-1})| \geq \frac{1}{3n}$ and since we assumed $\pi^0(x_{1\dots n}) = 0$ we can farther write $\pi^0(x_{1\dots j-1}) \geq \pi^0(x_{1\dots j}) + \frac{1}{3n}$. Moreover, since

$$\begin{aligned} \pi^0(x_{1\dots j-1}) &= \frac{1}{2} [\pi^0(x_{1\dots j-1} 0) + \pi^0(x_{1\dots j-1} 1)] \\ &= \frac{1}{2} [\pi^0(x_{1\dots j-1} x_j) + \pi^0(x_{1\dots j-1} \bar{x}_j)] \end{aligned}$$

we get that $\pi^0(x_{1\dots j-1} \bar{x}_j) \geq \pi^0(x_{1\dots j-1} x_j) + \frac{2}{3n}$ and therefore for any x there exists an index $i(x) = j$ for which $\Delta_{i(x)}(x_{1\dots i-1}) \geq \frac{2}{3n}$. \square

C Formal definition of the strategy

As explained in the main text, Eve's strategy is to use a partition $\left\{ \left(\frac{1}{2}, P_{XY|UV}^z \right) \right\}_{z \in \{0,1\}}$ for which $P_{XY|UV} = \frac{1}{2} P_{XY|UV}^0 + \frac{1}{2} P_{XY|UV}^1$. The systems $P_{XY|UV}^0$ and $P_{XY|UV}^1$ are obtained by biasing one individual subsystem $P_{X_i(x) Y_i(x) | U_i(x) V_i(x)}$ for each x . For any $i \in [n]$ let $P_{X_i Y_i | U_i V_i}^{z_i=0}$ and $P_{X_i Y_i | U_i V_i}^{z_i=1}$ be the biased systems as defined in Appendix A. The system $P_{XY|UV}^0$ is then formally defined by

$$P_{XY|UV}^0(x, y | u, v) = \prod_{j=1}^{i(x)-1} P_{X_j Y_j | U_j V_j}(x_j, y_j | u_j, v_j) \cdot P_{X_{i(x)} Y_{i(x)} | U_{i(x)} V_{i(x)}}^{z_i=\sigma}(x_{i(x)}, y_{i(x)} | u_{i(x)}, v_{i(x)}) \cdot \prod_{j=i(x)+1}^n P_{X_j Y_j | U_j V_j}(x_j, y_j | u_j, v_j) \quad (3)$$

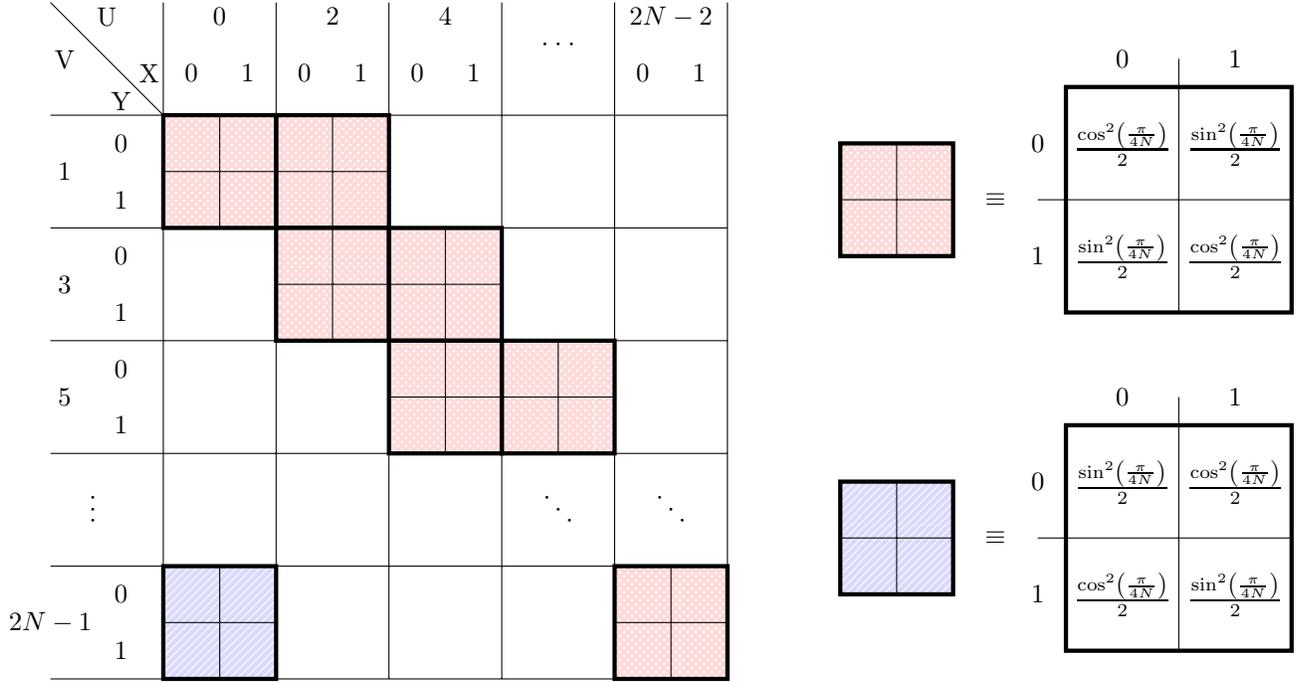


Figure 3: The unbiased system $P_{X_i Y_i | U_i V_i}$ for which $I_N^* = 2N \sin^2 \frac{\pi}{4N}$. The empty squares in the figure are not relevant for the correlations and therefore are not considered in cryptographic protocols.

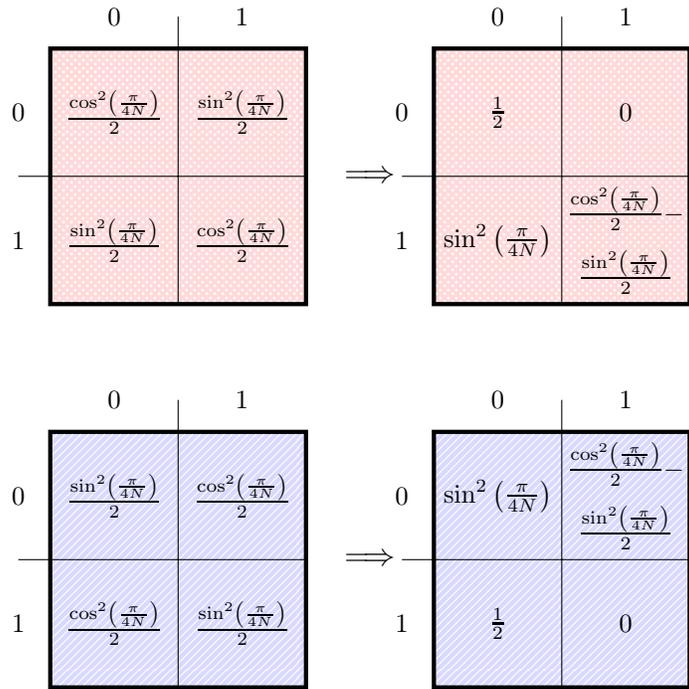


Figure 4: The biased system $P_{X_i Y_i | U_i V_i}^{z_i=0}$. Here are the same squares of Figure 3 after the probability shift.

where $i(x)$ is the pivotal index of x as in Definition 6 and

$$\sigma = \begin{cases} 0 & \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}0x_{i+1\dots n}) = 0] > \Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}1x_{i+1\dots n}) = 0] \\ 1 & \text{otherwise} \end{cases}.$$

That is, if $f(x)$ is more likely to result in $f(x) = 0$ if $x_{i(x)} = 0$ then Eve biases the $i(x)$ 'th system towards 0 and if not then towards 1. Note that since Eve manipulates the $i(x)$ 'th system only if $\Delta_{i(x)}(x_{1\dots i-1}) \geq \frac{2}{3n}$ $\Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}0x_{i+1\dots n}) = 0]$ never equals $\Pr_{x_{i+1\dots n}} [f(x_{1\dots i-1}1x_{i+1\dots n}) = 0]$.

The complementary system $P_{XY|UV}^1$ is defined in the exact same way but with $\bar{\sigma}$ instead of σ .

In order to prove the legality of the strategy we first prove that $P_{XY|UV}^0$ is a probability distribution.

Lemma. *The system $P_{XY|UV}^0$ is a probability distribution. That is,*

1. For all x, y, u, v $P_{XY|UV}^0(x, y|u, v) \geq 0$
2. The system is normalized. For all u, v , $\sum_{x, y} P_{XY|UV}^0(x, y|u, v) = 1$

Proof. Each of the multiplicands in Equation (3) is non-negative and therefore for all x, y, u, v it also holds that $P_{XY|UV}^0(x, y|u, v) \geq 0$. Farther more, since

$$P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}^{z_i=\sigma}(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)}) + P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}^{z_i=\bar{\sigma}}(\overline{x_{i(x)}}, y_{i(x)}|u_{i(x)}, v_{i(x)}) = P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)}) + P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(\overline{x_{i(x)}}, y_{i(x)}|u_{i(x)}, v_{i(x)}) \quad (4)$$

(cf. Figure 4) we also have

$$P_{XY|UV}^0(x, y|u, v) + P_{XY|UV}^0(x^{i(x)}, y|u, v) = P_{XY|UV}(x, y|u, v) + P_{XY|UV}(x^{i(x)}, y|u, v)$$

where $x^{i(x)}$ is the string x with the $i(x)$ 'th bit flipped, i.e., $x^{i(x)} = x_1\dots x_{i(x)-1}\bar{x}_{i(x)}x_{i(x)+1}\dots x_n$. This implies that

$$\sum_{x, y} P_{XY|UV}^0(x, y|u, v) = \sum_{x, y} P_{XY|UV}(x, y|u, v) = 1.$$

□

The same proof holds for $P_{XY|UV}^1$ as well. The fact that $P_{XY|UV}^0$ and $P_{XY|UV}^1$ are probability distributions is not enough. We also need to prove that they are complementary systems, i.e., $P_{XY|UV} = \frac{1}{2}P_{XY|UV}^0 + \frac{1}{2}P_{XY|UV}^1$.

Lemma. $P_{XY|UV} = \frac{1}{2}P_{XY|UV}^0 + \frac{1}{2}P_{XY|UV}^1$.

Proof. For simplicity we drop the subscript $XY|UV$ from all the systems. For example $P(x, y|u, v)$ should be understood as $P_{XY|UV}(x, y|u, v)$ while $P^{z_i=\sigma}(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)})$ should be understood as $P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}^{z_i=\sigma}(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)})$.

$$\begin{aligned} 2P(x, y|u, v) - P^0(x, y|u, v) &= 2\prod_{j=1}^n P(x_j, y_j|u_j, v_j) - P^0(x, y|u, v) \\ &= \prod_{\substack{j=1 \\ j \neq i(x)}}^n P(x_j, y_j|u_j, v_j) \cdot [2P(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)}) - P^{z_i=\sigma}(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)})] \\ &= \prod_{\substack{j=1 \\ j \neq i(x)}}^n P(x_j, y_j|u_j, v_j) \cdot P^{z_i=\bar{\sigma}}(x_{i(x)}, y_{i(x)}|u_{i(x)}, v_{i(x)}) \\ &= P^1(x, y|u, v). \end{aligned}$$

□

We have only left to show that the system $P_{XY|UV}^0$ is a time-ordered non-signalling system.

Lemma. *The system $P_{XY|UV}^0$ is time-ordered non-signalling as in Definition 2.*

Proof. For the conditions on Bob's side of the system we first note the following. In the system $P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}^{z_i=\sigma}$ we shift probabilities only within the same row. Moreover, we shift the probability in the exact same way on identical rows (cf. Figure 4: the first row in the upper boxes is identical to the second row in the lower boxes). It then follows from Lemmas 4.4, 4.5 and 4.6 in [14] that full non-signalling conditions hold for Bob's side (i.e., every subset of his systems cannot signal any other subset of systems). In particular, the time-ordered non-signalling conditions hold.

For simplicity we drop the subscript $XY|UV$ from all the systems as in the previous proof. We now want to prove that the conditions on Alice's side hold, i.e., that for any sets I_1, I_2 as in Definition 2

$$\forall x_{I_1}, y, u_{I_1}, u_{I_2}, u'_{I_2}, v \quad \sum_{x_{I_2}} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u_{I_2}, v) = \sum_{x_{I_2}} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v). \quad (5)$$

For any x_{I_1} there are two possible cases, as indicated in Figure 5; the pivotal index $i(x)$ is either in I_1 or in I_2 . We show that on both cases the time-ordered non-signalling conditions on Alice's side hold.

First assume that for the pivotal index $i(x) \in I_1$. For any u, u' and v , for any x let

$$x'_j = \begin{cases} \bar{x}_j & u_j \neq u'_j \wedge v_j = 2N - 1 \\ x_j & \text{otherwise} \end{cases}$$

and $x' = x'_1 \cdots x'_n$. Furthermore, note that for the unbiased system $P_{XY|UV}$ we have $P_{XY|UV}(x, y | u', v) = P_{XY|UV}(x', y | u, v)$. Since $i(x) \in I_1$ we have

$$\begin{aligned} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v) &= \prod_{j=1}^{i(x)-1} P(x_j, y_j | u_j, v_j) \cdot P^{z_i=\sigma}(x_{i(x)}, y_{i(x)} | u_{i(x)}, v_{i(x)}) \cdot \prod_{j=i(x)+1}^n P(x_j, y_j | u'_j, v_j) \\ &= \prod_{j=1}^{i(x)-1} P(x_j, y_j | u_j, v_j) \cdot P^{z_i=\sigma}(x_{i(x)}, y_{i(x)} | u_{i(x)}, v_{i(x)}) \cdot \prod_{j=i(x)+1}^n P(x'_j, y_j | u_j, v_j) \\ &= P^0(x_{I_1}, x'_{I_2}, y | u_{I_1}, u_{I_2}, v) \end{aligned}$$

and therefore Equation (5) holds as well.

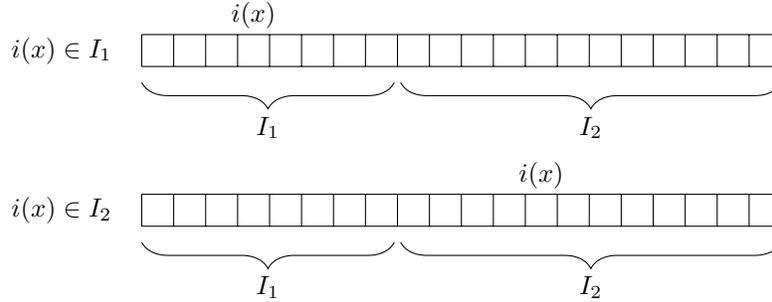


Figure 5: Two possible cases: $i(x) \in I_1$ or $i(x) \in I_2$

For the second case, assume that $i(x) \notin I_1$. $\forall x_{I_1}, y, u_{I_1}, u_{I_2}, u'_{I_2}, v$, denote by $u' = u_{I_1} u'_{I_2}$. Then

$$\begin{aligned}
\sum_{x_{I_2}} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v) &= \sum_{x_{I_2}} \prod_{j=1}^{i(x)-1} P(x_j, y_j | u'_j, v_j) \cdot P^{z_i=\sigma}(x_{i(x)}, y_{i(x)} | u'_{i(x)}, v_{i(x)}) \cdot \prod_{j=i(x)+1}^n P(x_j, y_j | u'_j, v_j) \\
&= \sum_{x_{I_2/i(x)}} \prod_{j=1}^{i(x)-1} P(x_j, y_j | u'_j, v_j) \cdot \\
&\quad \cdot \left[P^{z_i=\sigma}(x_{i(x)}, y_{i(x)} | u'_{i(x)}, v_{i(x)}) + P^{z_i=\sigma}(\overline{x_{i(x)}}, y_{i(x)} | u'_{i(x)}, v_{i(x)}) \right] \cdot \\
&\quad \cdot \prod_{j=i(x)+1}^n P(x_j, y_j | u'_j, v_j) \\
&= \sum_{x_{I_2/i(x)}} \prod_{j=1}^{i(x)-1} P(x_j, y_j | u'_j, v_j) \cdot \\
&\quad \cdot \left[P(x_{i(x)}, y_{i(x)} | u'_{i(x)}, v_{i(x)}) + P(\overline{x_{i(x)}}, y_{i(x)} | u'_{i(x)}, v_{i(x)}) \right] \cdot \\
&\quad \cdot \prod_{j=i(x)+1}^n P(x_j, y_j | u'_j, v_j) \\
&= \sum_{x_{I_2}} \prod_{j=1}^n P(x_j, y_j | u'_j, v_j) \\
&= \sum_{x_{I_2}} P(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v)
\end{aligned}$$

where the third equality is due to Equation (4). Now since the unbiased system P fulfils all non-signalling conditions, and in particular it is also time-ordered non-signalling, we have $\sum_{x_{I_2}} P(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v) = \sum_{x_{I_2}} P(x_{I_1}, x_{I_2}, y | u_{I_1}, u_{I_2}, v)$.

Adding everything together we get

$$\begin{aligned}
\sum_{x_{I_2}} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v) &= \sum_{x_{I_2}} P(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v) \\
&= \sum_{x_{I_2}} P(x_{I_1}, x_{I_2}, y | u_{I_1}, u_{I_2}, v) \\
&= \sum_{x_{I_2}} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u_{I_2}, v).
\end{aligned}$$

Therefore for both cases Equation (5) holds and the system $P_{XY|UV}^0$ is time-ordered non-signalling. \square

The same proof holds for $P_{XY|UV}^1$ as well.