Limits of privacy amplification against nonsignaling memory attacks

Rotem Arnon-Friedman and Amnon Ta-Shma
The Blavatnik School of Computer Science, Tel-Aviv University, Tel-Aviv, Israel
(Received 7 November 2012; published 27 December 2012)

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 nonsignaling 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 nonsignaling system, which allow past subsystems to signal future subsystems (using the device's memory for example), superpolynomial privacy amplification by any hashing is impossible. This is of great relevance when considering practical device-independent key-distribution protocols which assume a superquantum adversary.

DOI: 10.1103/PhysRevA.86.062333 PACS number(s): 03.67.Dd

I. INTRODUCTION

A. 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 Bennett-Brassard 1984 (BB84) protocol [1], one should be able to fully characterize 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 characterization 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 nonlocal 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 Clauser-Horne-Shimony-Holt (CHSH) inequality [6] or other more general chained Bell inequities [7,8], and if Alice and Bob enforce a nonsignaling condition between them in order to make sure that these correlations are indeed nonlocal, 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 nonsignaling adversaries.

When considering a nonsignaling adversary the only thing which limits the adversary is the nonsignaling principle. That is, the adversary has superquantum power; however, if Alice and Bob enforce some local nonsignaling 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 spacelike-separated way. For example, if Alice and Bob perform their measurements in a spacelike-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 subsystems, 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 information leaks from one system to another. Such a harsh constraint, which we call the full nonsignaling 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 nonsignaling 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 protocol.[1] However, this protocol, like the BHK protocol, cannot tolerate any reasonable amount of noise.

B. 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

[1]If 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 nonlocal 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.

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 $X_1,X_2,\ldots,X_n$, 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 function[2] $f:\{0,1\}^n \to \{0,1\}^{|K|}$ (for $|K| < n$) to $X_1,X_2,\ldots,X_n$ 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 nonsignaling adversary is possible if we assume that Alice's and Bob's systems fulfill the full nonsignaling conditions [10,11], PA is also possible in this setting. However, it was already proven in [13] that PA is impossible if we impose nonsignaling conditions only between Alice and Bob,[3] i.e., Alice and Bob cannot signal each other, while signaling 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 nonsignaling assumption between Alice and Bob, within the system of the parties signaling 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 nonsignaling conditions, are defined formally in Definition 2.

In contrast to the full nonsignaling conditions, the time-ordered nonsignaling 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 signaling 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 signaling is possible only in the forward direction of time. In fact, these are the nonsignaling 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 nonsignaling conditions. If Alice's and Bob's devices have memory then information from past measurements can be available for future measurements, i.e., signaling is possible from the past to the future but not the other way around.

In this paper we ask the following question. Under the assumption of a time-ordered nonsignaling system, is privacy amplification against nonsignaling adversaries possible? We give an example for a system which fulfils all the time-ordered nonsignaling conditions, and in which superpolynomial 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 nonsignaling system, superpolynomial 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 $\Omega(\frac{1}{n})$.

Although this proves that superpolynomial PA is impossible under these conditions, it 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.

II. PRELIMINARIES

A. Chained Bell inequalities

For two correlated random variables X,U we denote the conditional probability distribution of X given U by $P_{X|U}(x|u) = \text{Prob}(X = x|U = u)$. 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 nonlocal correlations under measurements [15]. We consider the following Bell-type experiments. Alice and Bob share a bipartite system $P_{XY|UV}$ where $U \in \{0,2,\ldots,2N-2\}$ and $V \in \{1,3,\ldots,2N-1\}$. We define a set of allowed input pairs for Alice and Bob to be $G_N = \{(u,v)|u \in U, v \in V, |u-v| = 1\} \bigcup \{(0,2N-1)\}$. 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]

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

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

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

[3]In contrast to the QKD problem, when considering the PA problem the only goal of Bob is to establish nonlocal correlations with Alice.

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

$$I_N^\star = 2N\sin^2\frac{\pi}{4N} < \frac{\pi^2}{8N}. \tag{2}$$

This implies that $I_N^\star$ 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 types of system 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.

B. Nonsignaling 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 spacelike-separated regions or by shielding their systems.

Definition 1 (nonsignaling 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 signaling 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 signaling 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 signaling.

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

Definition 2 (time-ordered nonsignaling system). For any $i \in \{2,\ldots,n\}$, denote the set $\{1,\ldots,i-1\}$ by I_1 and the set $\{i,\ldots,n\}$ by I_2, and for $i = 1$, $I_1 = \phi$ 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 nonsignaling system (does not allow for signaling from the future to the past) if for any $i \in [n]$,

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

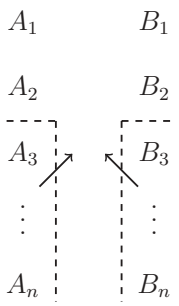

FIG. 1. Time-ordered nonsignaling condition for $i = 3$. Signaling is impossible in the direction of the straight arrow.

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

C. Nonsignaling adversaries

When modeling a nonsignaling adversary, the question in mind is as follows: given a system $P_{XY|UV}$ shared by Alice and Bob, for which some arbitrary nonsignaling conditions hold, which extensions to a system $P_{XYZ|UVW}$, including the adversary Eve, are possible? The only principle which limits Eve is the nonsignaling 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 fulfill all of the nonsignaling conditions that $P_{XY|UV}$ fulfills, and in addition $P_{XYZ|UVW}$ cannot allow signaling between Alice and Bob together and Eve.

We adopt here the model given in [10,13,17] of nonsignaling 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 fulfills a certain set of

[4]However, 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 nonlocal correlations.

nonsignaling conditions $\mathcal{C}$, is a family of pairs $(p^z, P^z_{XY|UV})$, where

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

(2) for all z, $P^z_{XY|UV}$ is a system that fulfills $\mathcal{C}$;

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

In our scenario the goal of the adversary is to gain information about $f(X)$, for some function[5] $f : \{0,1\}^n \to \{0,1\}$. 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 1. (Lemma 3.7 in [17].) For the case $K = f(X)$, where $f : \{0,1\}^n \to \{0,1\}$, $U = u$, $V = v$, and where the strategy w is defined by the partition $\{(p^z, P^z_{XY|UV})\}_{z\in\{0,1\}}$ such that $\text{Prob}[K = 0|Z = 0] \geqslant \frac{1}{2}$, the distance from uniform of $f(X)$ given the strategy w is

$$\begin{aligned} &d(K|Z(w)) \\ &\quad = p^{z=0}\left(\text{Prob}[K = 0|Z = 0] - \text{Prob}[K = 1|Z = 0]\right) \\ &\qquad - \tfrac{1}{2}\left(\text{Prob}[K = 0] - \text{Prob}[K = 1]\right). \end{aligned}$$

III. 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 nonsignaling 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 Eq. (2). We denote the system of each entangled pair by $P_{X_iY_i|U_iV_i}$ for $i \in [n]$ and the whole system by $P_{XY|UV} = \prod_{i\in[n]} P_{X_iY_i|U_iV_i}$.

Let $f : \{0,1\}^n \to \{0,1\}$ 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 two parts, $P^0_{XY|UV}$ and $P^1_{XY|UV}$, each occurring with probability $\frac{1}{2}$ and $P_{XY|UV} = \frac{1}{2}P^0_{XY|UV} + \frac{1}{2}P^1_{XY|UV}$. In our partition $P^0_{XY|UV}$ is biased towards $f(x) = 0$ and $P^1_{XY|UV}$ 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 $P^0_{XY|UV}$.

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

$$\begin{aligned} &\underset{x_{i+1,\ldots,n}}{\text{Prob}}\left[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n}) = 0\right] \\ &\quad > \underset{x_{i+1,\ldots,n}}{\text{Prob}}\left[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n}) = 0\right]. \end{aligned}$$

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

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

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

We denote the biased system by $P^{z_i=\sigma}_{X_iY_i|U_iV_i}$ for $\sigma \in \{0,1\}$. The biased system is given in Appendix A.

Therefore, in our adversarial strategy, if the value of the ith bit x_i, given the prefix $x_{1,\ldots,i-1}$, has enough influence over the outcome of f (we will soon define how much is enough), although the suffix is unknown, then the ith system is being biased by $c(I^\star_N)$. Note that for any prefix $x_{1,\ldots,i-1}$ a different system $P_{X_iY_i|U_iV_i}$ should be biased.

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

$$\begin{aligned} \Delta_i(x_{1,\ldots,i-1}) \equiv \Big|&\underset{x_{i+1,\ldots,n}}{\text{Prob}}\left[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n}) = 0\right] \\ &- \underset{x_{i+1,\ldots,n}}{\text{Prob}}\left[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n}) = 0\right]\Big|. \end{aligned}$$

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

Definition 4 (pivotal index[7]*).* Given $f : \{0,1\}^n \to \{0,1\}$, for any x, the pivotal index $i(x) \in [n]$ is the smallest index such that $\Delta_{i(x)}(x_{1,\ldots,i-1}) \geqslant \frac{2}{3n}$.

Consider for example the function presented in Fig. 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 $x_1x_2 = 10$ and $x_1x_2 = 11$ the pivotal index is $i(x) = 3$.

Luckily, for every function $f : \{0,1\}^n \to \{0,1\}$ for which $|\text{Prob}_x[f(x) = 0] - \text{Prob}_x[f(x) = 1]| \leqslant \frac{1}{3}$ and every $x \in \{0,1\}^n$ there exists such a pivotal index $i(x)$ for which $\Delta_{i(x)}(x_{1,\ldots,i-1}) \geqslant \frac{2}{3n}$ and therefore for every x there exists

[5] It 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.

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

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

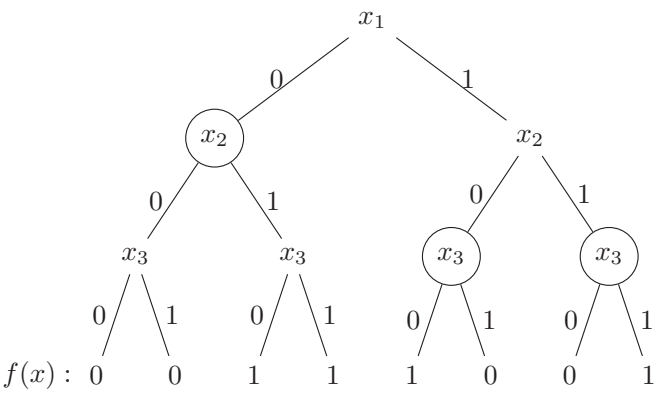

FIG. 2. Binary tree with pivotal nodes. The pivotal nodes are marked with circles.

some bit $x_{i(x)}$ which can give non-negligible information to Eve about the final output.

Lemma 3. Let $f:\{0,1\}^n \to \{0,1\}$ be an almost balanced function, i.e., $|\mathrm{Prob}_x[f(x)=0] - \mathrm{Prob}_x[f(x)=1]| \leqslant \frac{1}{3}$. Then for any x there exists a pivotal index $i(x)$ such that $\Delta_{i(x)}(x_{1,\ldots,i-1}) \geqslant \frac{2}{3n}$.

Lemma 3 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 $c(I_N^\star)$ towards 0 if $\mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n}) = 0] > \mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n}) = 0]$ and towards 1 otherwise. The system $P^0_{XY|UV}$ which results from such a strategy is given in Eq. (C1) 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 ith system by $c(I_N^\star)$ towards 0 if $\mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n}) = 0] < \mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n}) = 0]$ 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 $P^0_{XY|UV}$ is indeed time-ordered nonsignaling. 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 signaling 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 $c(I_N^\star)$. However, the advantage Eve gets from this shift in the probabilities is only $c(I_N^\star)\Delta_{i(x)}(x_{1,\ldots,i-1})$ since the pivotal bit does not determine $f(x)$ exactly.[8] Moreover, since $P^0_{XY|UV}$ and $P^1_{XY|UV}$ 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 $|\mathrm{Prob}_x[f(x)=0] - \mathrm{Prob}_x[f(x)=1]| > \frac{1}{3}$ Eve can just guess the value of the function with a constant success probability of at least $\frac{2}{3}$. Therefore these kinds of functions do not bother us. Altogether we get the following theorem.

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

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

A. Concluding remarks and open questions

In this paper we showed that when considering systems which can signal only forward in time and nonsignaling adversaries, then superpolynomial 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

R.A.-F. thanks Roger Colbeck for helpful comments. Both authors acknowledge support from the FP7 FET–Open Project QCS.

APPENDIX A: PROOF OF LEMMA 2

We now prove the following lemma:

Lemma 4. For any $i \in [n]$, the system $P_{X_iY_i|U_iV_i}$, for which $I_N(P_{X_iY_i|U_iV_i}) = I_N^\star$, can be biased towards 0 (or 1) by $c(I_N^\star) = \frac{I_N^\star}{2N}$.

Proof. In order to prove this we define the system $P^{z_i=0}_{X_iY_i|U_iV_i}$ which is biased towards 0 by $c(I_N^\star)$. We do so by shifting

[8] When 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 $\pi(p_2 - p_1)$. In our case, $p_2 - p_1$ is exactly $\Delta_{i(x)}(x_{1,\ldots,i-1})$ in our case.

[9] Remember 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 $I_N^\star$.

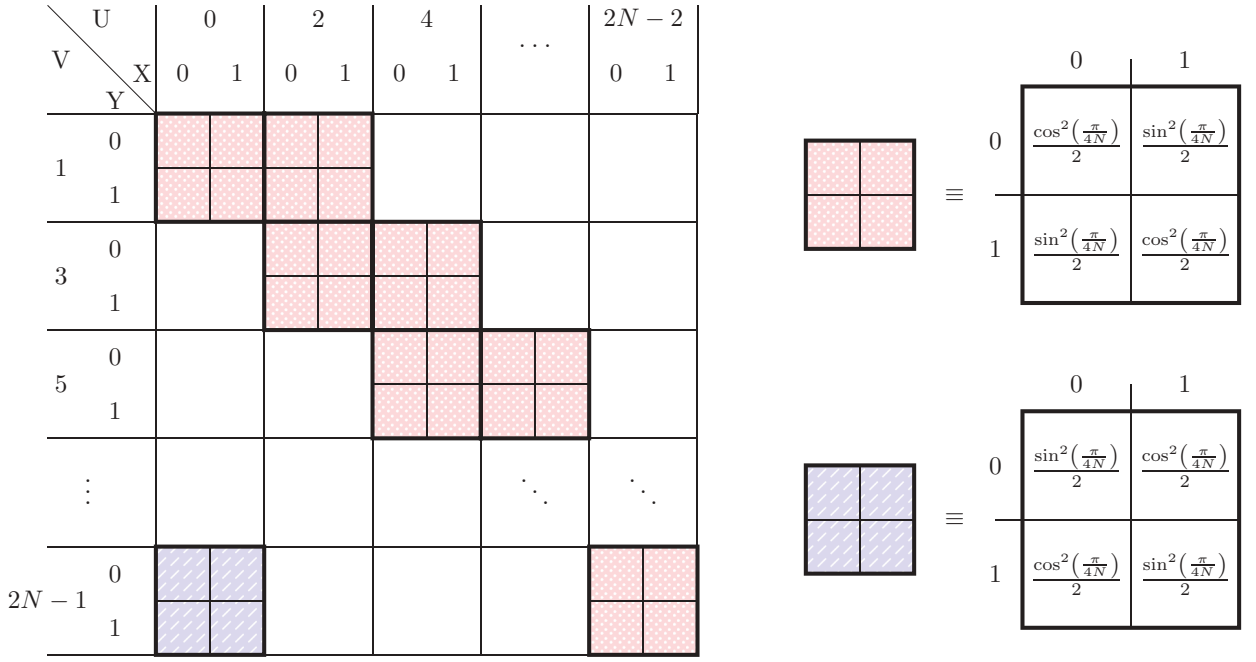

FIG. 3. (Color online) The unbiased system $P_{X_iY_i|U_iV_i}$ for which $I_N^\star = 2N\sin^2\frac{\pi}{4N}$. The empty squares in the figure are not relevant for the correlations and therefore are not considered in cryptographic protocols.

probabilities around in the original unbiased system $P_{X_iY_i|U_iV_i}$. The original system $P_{X_iY_i|U_iV_i}$, as in Fig. 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 $\theta = \frac{\pi U}{2N}, U \in \{0,2,\ldots,2N-2\}$ and for Bob $\theta = \frac{\pi V}{2N}$, $V \in \{1,3,\ldots,2N-1\}$.

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 $\sin^2(\frac{\pi}{4N})$. We do so by shifting in every row probability of $\frac{1}{2}\sin^2(\frac{\pi}{4N})$ out from the cell with $x_i = 1$ and into the cell with $x_i = 0$, as indicated in Fig. 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 $c(I_N^\star) = \frac{1}{2N} I_N^\star$.

Note that by shifting probabilities in this way we do not change the correlations of the system, i.e., $I_N(P^{z_i=0}_{X_iY_i|U_iV_i}) = I_N^\star$.

The system $P^{z_i=1}_{X_iY_i|U_iV_i}$, 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 $\frac{1}{2}P^{z_i=0}_{X_iY_i|U_iV_i} + \frac{1}{2}P^{z_i=1}_{X_iY_i|U_iV_i} = P_{X_iY_i|U_iV_i}$. ■

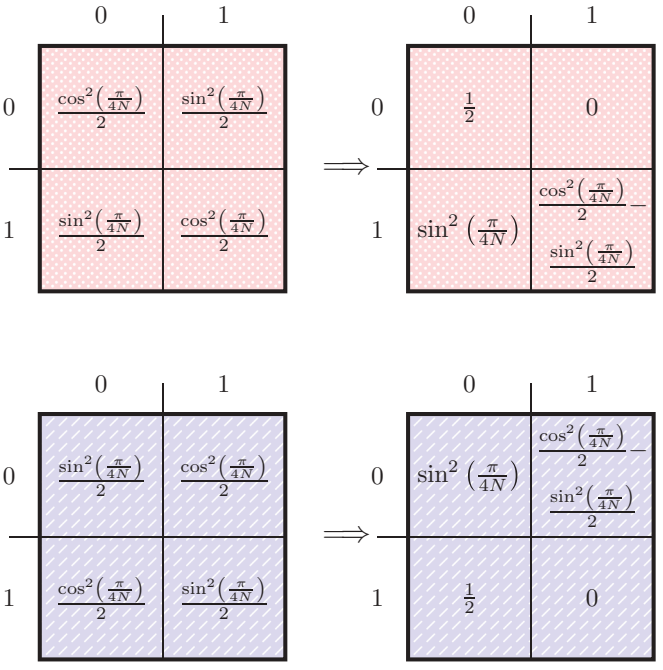

FIG. 4. (Color online) The biased system $P^{z_i=0}_{X_iY_i|U_iV_i}$. Here are the same squares of Fig. 3 after the probability shift.

APPENDIX B: PROOF OF LEMMA 3

For convenience we rewrite Lemma 3 here again.

Lemma 5. Let $f : \{0,1\}^n \to \{0,1\}$ be an almost balanced function for which $|\mathrm{Prob}_x[f(x)=0] - \mathrm{Prob}_x[f(x)=1]| \leqslant \frac{1}{3}$. Then for any x there exists a pivotal index $i(x)$ such that $\Delta_{i(x)}(x_{1,\ldots,i-1}) \geqslant \frac{2}{3n}$, where

$$\Delta_i(x_{1,\ldots,i-1}) \equiv \Big|\Pr_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n}) = 0] - \Pr_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n}) = 0]\Big|.$$

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

$$\pi^0(x_{1,\ldots,i-1}) = \tfrac{1}{2}\left[\pi^0(x_{1,\ldots,i-1}0) + \pi^0(x_{1,\ldots,i-1}1)\right],$$
$$\pi^0(\phi) \geqslant \tfrac{1}{3},$$
$$\pi^0(x_{1,\ldots,n}) \in \{0,1\}.$$

Assume without loss of generality that $\pi^0(x_{1,\ldots,n}) = 0$ [the proof is symmetric for the case $\pi^0(x_{1,\ldots,n}) = 1$].

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

$$\tfrac{1}{3}\leqslant|\pi^0(\phi)-\pi^0(x_{1,\ldots,n})|\leqslant n\zeta$$

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

$$\begin{aligned}\pi^0(x_{1,\ldots,j-1})&=\tfrac{1}{2}[\pi^0(x_{1,\ldots,j-1}0)+\pi^0(x_{1,\ldots,j-1}1)]\\&=\tfrac{1}{2}[\pi^0(x_{1,\ldots,j-1}x_j)+\pi^0(x_{1,\ldots,j-1}\overline{x_j})],\end{aligned}$$

we get that $\pi^0(x_{1,\ldots,j-1}\overline{x_j})\geqslant\pi^0(x_{1,\ldots,j-1}x_j)+\frac{2}{3n}$ and therefore for any x there exists an index $i(x)=j$ for which $\Delta_{i(x)}(x_{1,\ldots,i-1})\geqslant\frac{2}{3n}$. ■

APPENDIX C: FORMAL DEFINITION OF THE STRATEGY

As explained in the main text, Eve's strategy is to use a partition $\{(\frac{1}{2},P^z_{XY|UV})\}_{z\in\{0,1\}}$ for which $P_{XY|UV}=\frac{1}{2}P^0_{XY|UV}+\frac{1}{2}P^1_{XY|UV}$. The systems $P^0_{XY|UV}$ and $P^1_{XY|UV}$ 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 $P^{z_i=0}_{X_iY_i|U_iV_i}$ and $P^{z_i=1}_{X_iY_i|U_iV_i}$ be the biased systems as defined in Appendix A. The system $P^0_{XY|UV}$ is then formally defined by

$$P^0_{XY|UV}(x,y|u,v)=\prod_{j=1}^{i(x)-1}P_{X_jY_j|U_jV_j}(x_j,y_j|u_j,v_j)P^{z_i=\sigma}_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(x_{i(x)},y_{i(x)}|u_{i(x)},v_{i(x)})\prod_{j=i(x)+1}^{n}P_{X_jY_j|U_jV_j}(x_j,y_j|u_j,v_j),\tag{C1}$$

where $i(x)$ is the pivotal index of x as in Definition 4 and

$$\sigma=\begin{cases}0, & \mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n})=0]>\mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n})=0],\\1 & \text{otherwise.}\end{cases}$$

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 $\Delta_{i(x)}(x_{1,\ldots,i-1})\geqslant\frac{2}{3n}$, $\mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}0x_{i+1,\ldots,n})=0]$ never equals $\mathrm{Prob}_{x_{i+1,\ldots,n}}[f(x_{1,\ldots,i-1}1x_{i+1,\ldots,n})=0]$.

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

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

Lemma 6. The system $P^0_{XY|UV}$ is a probability distribution. That is,

(1) for all x,y,u,v, $P^0_{XY|UV}(x,y|u,v)\geqslant 0$,

(2) the system is normalized: for all u,v, $\sum_{x,y}P^0_{XY|UV}(x,y|u,v)=1$.

Proof. Each of the multiplicands in Eq. (C1) is non-negative and therefore for all x,y,u,v it also holds that $P^0_{XY|UV}(x,y|u,v)\geqslant 0$. Furthermore, since

$$\begin{aligned}&P^{z_i=\sigma}_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(x_{i(x)},y_{i(x)}|u_{i(x)},v_{i(x)})+P^{z_i=\sigma}_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(\overline{x_{i(x)}},y_{i(x)}|u_{i(x)},v_{i(x)})\\&\quad=P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(x_{i(x)},y_{i(x)}|u_{i(x)},v_{i(x)})+P_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(\overline{x_{i(x)}},y_{i(x)}|u_{i(x)},v_{i(x)})\end{aligned}\tag{C2}$$

(cf. Fig. 4) we also have

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

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

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

■

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

Lemma 7. $P_{XY|UV}=\frac{1}{2}P^0_{XY|UV}+\frac{1}{2}P^1_{XY|UV}$.

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 $P^{z_i=\sigma}_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}(x_{i(x)},y_{i(x)}|u_{i(x)},v_{i(x)})$.

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

■

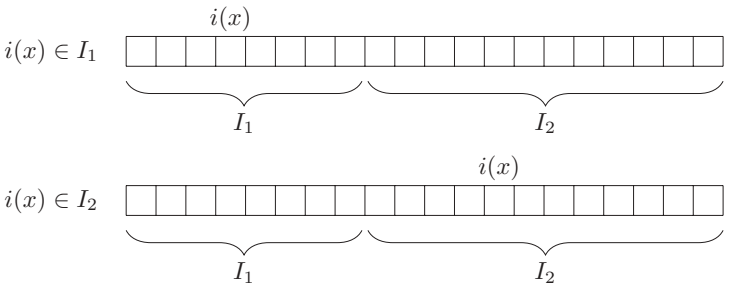

FIG. 5. Two possible cases: $i(x) \in I_1$ or $i(x) \in I_2$.

We have only left to show that the system $P^0_{XY|UV}$ is a time-ordered nonsignaling system.

Lemma 8. The system $P^0_{XY|UV}$ is time-ordered nonsignaling as in Definition 2.

Proof. For the conditions on Bob's side of the system we first note the following. In the system $P^{z_i=\sigma}_{X_{i(x)}Y_{i(x)}|U_{i(x)}V_{i(x)}}$ we shift probabilities only within the same row. Moreover, we shift the probability in the exact same way on identical rows (cf. Fig. 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 nonsignaling 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 nonsignaling 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

$$\forall\, x_{I_1}, y, u_{I_1}, u_{I_2}, u'_{I_2}, v, \quad \sum_{x_{I_2}} P^0\big(x_{I_1}, x_{I_2}, y \big| u_{I_1}, u_{I_2}, v\big) = \sum_{x_{I_2}} P^0(x_{I_1}, x_{I_2}, y | u_{I_1}, u'_{I_2}, v). \tag{C3}$$

For any x_{I_1} there are two possible cases as indicated in Fig. 5; the pivotal index $i(x)$ is either in I_1 or in I_2. We show that in both cases the time-ordered nonsignaling 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

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

and $x' = x'_1, \ldots, x'_n$. 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

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

and therefore Eq. (C3) holds as well.

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

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

where the third equality is due to Eq. (C2). Now since the unbiased system P fulfills all nonsignaling conditions, and in particular it is also time-ordered nonsignaling, 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

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

Therefore for both cases Eq. (C3) holds and the system $P^0_{XY|UV}$ is time-ordered nonsignaling. The same proof holds for $P^1_{XY|UV}$ as well. ■

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE Computer Society Press, Los Alamitos, CA, 1984), p. 175.

[2] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[3] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, 1998* (IEEE, New York, 1998), pp. 503–509.

[4] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[5] A. Acin, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[7] S. L. Braunstein and C. M. Caves, Ann. Phys. (NY) **202**, 22 (1990).

[8] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006).

[9] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[10] E. Hänggi, R. Renner, and S. Wolf, EUROCRYPT **2010**, 216 (2010).

[11] L. Masanes, Phys. Rev. Lett. **102**, 140501 (2009).

[12] J. Barrett, R. Colbeck, and A. Kent, arXiv:1209.0435.

[13] E. Hänggi, R. Renner, and S. Wolf, arXiv:0906.4760.

[14] R. Arnon Friedman, E. Hänggi, and A. Ta-Shma, arXiv:1205.3736.

[15] J. S. Bell, Physics (Long Island City, NY) **1**, 195 (1964).

[16] V. Scarani and C. Kurtsiefer, arXiv:0906.4547.

[17] E. Hänggi, Ph.D. thesis, ETH Zurich, 2010, arXiv:1012.3878.