Universally Composable Privacy Amplification from Causality Constraints

Lluís Masanes
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Parck, 08860 Castelldefels (Barcelona), Spain

(Received 27 July 2008; published 10 April 2009)

We consider schemes for secret key distribution which use as a resource correlations that violate Bell inequalities. We provide the first security proof for such schemes, according to the strongest notion of security, the so-called universally composable security. Our security proof does not rely on the validity of quantum mechanics, it solely relies on the impossibility of arbitrarily fast signaling between separate physical systems. This allows for secret communication in situations where the participants distrust their quantum devices.

DOI: 10.1103/PhysRevLett.102.140501 PACS numbers: 03.67.Dd, 03.65.Ud

In an experimental setup where a Bell inequality [1] is violated, one has the certainty that the outcomes of some local measurements are not determined beforehand. This limits the degree of correlation between such outcomes and other systems not involved in the experiment. It also limits the knowledge about these outcomes that a distant party can have. This fundamental piece of our understanding of physical reality can be exploited for implementing information-theoretic tasks. For instance, in this Letter we show that a secret key generated from the outcomes of Bell-violating measurements is secure. This reasoning is independent of quantum mechanics, the only key assumption is the impossibility of arbitrarily fast signaling between separate systems.

The first scheme for generating secret key from Bell-violating correlations was presented in [2], and was followed by others [3,4]. All these schemes where presented with partial security proofs. The results presented in this Letter, complemented with the ones in [5], provide a general security proof without assumptions (apart from no signaling) for all these schemes. We use the strongest security criterion, the so-called universally composable security [6], which warrants that key distribution is secure in any context. Our methods are very general, and can be adapted to other Bell-inequality-based key-distribution schemes.

No signaling.—Consider two parties, Alice and Bob, each having a physical system which can be measured with different observables. Let $a(b)$ be the outcome when Alice (Bob)'s system is measured with one of the observables parametrized by $x(y)$, with joint conditional probability distribution denoted by $P_{a,b|x,y}$. We say that $P_{a,b|x,y}$ is a nonsignaling distribution if the marginals depend only on their corresponding observables, that is $P_{a|x,y} = P_{a|x}$ and $P_{b|x,y} = P_{b|y}$ for all a, b, x, y [7]. It is clear that if one of these conditions is not satisfied, then arbitrarily fast signaling is possible.

Nonlocality.—The distributions that can be written as

$$P_{a,b|x,y} = \sum_{\lambda} P_{\lambda} P_{a|x,\lambda} P_{b|y,\lambda} \tag{1}$$

are called local, and satisfy all Bell inequalities [7]. In the binary case ($a, b, x, y \in \{0, 1\}$) all Bell inequalities are equivalent to the Clauser-Horne-Shimony-Holt (CHSH) inequality [8]. For what follows, it is convenient to write the CHSH inequality as $\langle \mathrm{CHSH}|P_{a,b|x,y}\rangle \geq \sqrt{2}$, where the vector

$$|\mathrm{CHSH}\rangle = \frac{1}{4\sqrt{2}} \begin{pmatrix} 1 & 5 & & 1 & 5 \\ 5 & 1 & & 5 & 1 \\ & & & & \\ 1 & 5 & & 5 & 1 \\ 5 & 1 & & 1 & 5 \end{pmatrix} \tag{2}$$

contains the coefficients of the inequality, and the vector

$$|P_{a,b|x,y}\rangle = \begin{pmatrix} P_{0,0|0,0} & P_{0,1|0,0} & & P_{0,0|0,1} & P_{0,1|0,1} \\ P_{1,0|0,0} & P_{1,1|0,0} & & P_{1,0|0,1} & P_{1,1|0,1} \\ & & & & \\ P_{0,0|1,0} & P_{0,1|1,0} & & P_{0,0|1,1} & P_{0,1|1,1} \\ P_{1,0|1,0} & P_{1,1|1,0} & & P_{1,0|1,1} & P_{1,1|1,1} \end{pmatrix} \tag{3}$$

contains the probabilities for all experimental settings. (We arrange the components of these vectors in a matrix for the sake of clarity.) Notice that in this form, the lower the quantity $\langle \mathrm{CHSH}|P_{a,b|x,y}\rangle$ the larger the violation. The distribution attaining maximal violation ($\langle \mathrm{CHSH}|P_{a,b|x,y}\rangle = 1/\sqrt{2}$) is the so-called PR box [9], which can be considered the maximally nonlocal (nonsignaling) distribution. The correlations generated by measuring quantum systems are constrained by Cirel'son's bound $\langle \mathrm{CHSH}|P_{a,b|x,y}\rangle \geq 2^{-1/2}3 - 1 \approx 1.121$ [10].

Privacy amplification.—Privacy amplification (PA) is the procedure by which a partially secret N_r-bit string $\mathbf{a}$ (the *raw key*) is transformed into a highly secret N_s-bit string $\mathbf{k}$ (the *secret key*) [11]. Usually, the secret key is shorter than the raw key ($N_s < N_r$), which is the price for the gain in privacy. The function implementing this transformation $h(\mathbf{a}) = \mathbf{k}$ is called *hash function*. It is usually the case that the hash function has to be generated randomly after the raw key $\mathbf{a}$ has been obtained, but in our scheme, h is fixed from the beginning and known to everybody, including the eavesdropper (Eve). An *ideal secret key* is a uniformly distributed random variable $\mathbf{k}$ which is uncorrelated with the rest of the universe (Eve). The information held by Eve is encoded in the state of a physical system, which can be measured with one of many different observables, parametrized by z. If $P_{e|z}$ is the distribution for the outcomes when this system is measured with the observable z, then the distribution of an *ideal secret key* is $P^{\mathrm{ideal}}_{\mathbf{k},e|z} = 2^{-N_s} P_{e|z}$. Usually, the *real secret key* generated by PA is not guaranteed to be an *ideal secret key*, $P_{\mathbf{k},e|z} \neq 2^{-N_s} P_{e|z}$.

In general, PA constitutes a subroutine within cryptographic protocols, which use a secret key as an ingredient (an example being the encryption of messages). It is desirable that the result obtained when any of these protocols is fed with the *real secret key*, is the same as if fed with an *ideal secret key*, with arbitrarily high probability. If this is the case, then we say that PA is universally composable, because it is secure in any context. Clearly, this happens if the *real* and *ideal* secret keys are indistinguishable.

The most general strategy for distinguishing the bipartite states $P_{\mathbf{k},e|z}$ (the real key) and $2^{-N_s} P_{e|z}$ (the ideal key) consists of performing joint measurements on the key and Eve's system. The no-signaling formalism alone does not say anything about joint measurements. However, the key is a classical system which can be observed without disturbing the global state. Therefore, the most general strategy is to read $\mathbf{k}$ and chose an observable z depending on its value. It is well known that the probability of guessing correctly with the optimal strategy is

$$p_{\mathrm{correct}} = \frac{1}{2} + \frac{1}{4} \sum_{\mathbf{k}} \max_{z} \sum_{e} |P_{\mathbf{k},e|z} - 2^{-N_s} P_{e|z}|. \quad (4)$$

Notice that the maximization on z depends on $\mathbf{k}$. When (4) is close to $1/2$, the optimal strategy for distinguishing the real from the ideal key is as good as a random guess—this is the security condition that we consider.

In *key distribution* from Bell-violating correlations, Alice has N systems, Bob has N systems and, without loss of generality, Eve has one "big" system, jointly distributed according to an arbitrary (unknown) $P_{\mathbf{a},\mathbf{b},e|\mathbf{x},\mathbf{y},z}$. (Bold symbols correspond to bit-string variables.) It is usually assumed that this is a $(2N+1)$-partite nonsignaling distribution [5] (i.e., the marginals only depend on their corresponding observables), however, we are able to proceed with a weaker assumption. If the secret key is a function of Alice's string $\mathbf{k} = h(\mathbf{a})$, then Bob's N systems can be considered as a single "big" system, that is, no signaling among Bob's systems is not required in our proof. We refer to this assumption as "$(N+2)$-partite no signaling." According to [12], the even weaker assumption of 3-partite no signaling (where Alice's N systems are also considered as single one) is insufficient to warrant security. Of these N pairs of systems, $N_r (N_r < N)$ are used for generating the raw key, and the rest are used to estimate how much nonlocality is shared by Alice and Bob [5]. In the large-N limit, N_r is equal to N up to terms sublinear in N—this is denoted by $N_r \approx N$.

The following result establishes the security of Alice's key $\mathbf{k} = h(\mathbf{a})$ when $\mathbf{a}$ is generated by measuring N_r of Alice's systems with the observable $x = 0$. Of course, it is necessary that the correlations shared by Alice and Bob $P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}$ have a sufficiently small value of $\langle \mathrm{CHSH}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle$, or in other words, are sufficiently nonlocal. However, the goal of key distribution is that both Alice and Bob hold the secret key $\mathbf{k}$. Later we address this problem.

Main result.—For almost all functions $h\colon \{0,1\}^{N_r} \rightarrow \{0,1\}^{N_s}$ and any (N_r+2)-partite nonsignaling distribution $P_{\mathbf{a},\mathbf{b},e|\mathbf{x},\mathbf{y},z}$, the random variable $\mathbf{k} = h(\mathbf{a})$ satisfies

$$\sum_{\mathbf{k}} \max_{z} \sum_{e} |P_{\mathbf{k},e|\mathbf{x}=\mathbf{0},z} - 2^{-N_s} P_{e|z}| \leq \sqrt{2}^{N_s + \sqrt{N_r}} \langle \mathrm{CHSH}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle, \quad (5)$$

where $\mathbf{0}$ is the zero vector.

Here and in the rest of the Letter we say that "almost all functions have a particular property" if when randomly picking a function h with uniform distribution over all functions $h\colon \{0,1\}^{N_r} \rightarrow \{0,1\}^{N_s}$ then the probability that h does not have that particular property is lower than $2\exp(5N_r - 2^{\sqrt{N_r}}/4)$. The above result is also true for any $\mathbf{x} \neq \mathbf{0}$, but for simplicity we consider only the case $\mathbf{x} = \mathbf{0}$, which is sufficient for key distribution.

When the given correlations $P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}$ are generated by measuring quantum systems Cirel'son's bound implies $\langle \mathrm{CHSH}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle > 1$, which prevents the right-hand side of (5) to be small. Hence, this simple scheme does not work with quantum correlations. This problem is solved by the Barrett-Hardy-Kent (BHK) protocol, which yields large secure secret keys. The BHK protocol is analyzed below. Now, we proceed to prove the main result, and start by stating two lemmas, the first is shown in [5,13] and the second is shown below.

Lemma 1.—For any (N_r+1)-partite nonsignaling distribution $P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}$ we have $P_{\mathbf{a}|\mathbf{x}=\mathbf{0}} = \langle \Gamma_{\mathbf{a}} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle$, where $|\Gamma_{\mathbf{a}}\rangle = |\gamma_{a_1}\rangle \otimes \cdots \otimes |\gamma_{a_{N_r}}\rangle$ and

$$|\gamma_0\rangle = \frac{1}{8} \begin{pmatrix} 1 & -3 & 1 & 5 \\ 5 & 1 & -3 & 1 \\ 1 & -3 & 5 & 1 \\ 5 & 1 & 1 & -3 \end{pmatrix},$$

$$|\gamma_1\rangle = \frac{1}{8} \begin{pmatrix} 1 & 5 & 1 & -3 \\ -3 & 1 & 5 & 1 \\ 1 & 5 & -3 & 1 \\ -3 & 1 & 1 & 5 \end{pmatrix}.$$

Lemma 2.—For any given function $h\colon \{0,1\}^{N_r} \rightarrow \{0,1\}^{N_s}$ and any $\mathbf{k} \in \{0,1\}^{N_s}$, define $\mathcal{A}_{\mathbf{k}} = h^{-1}(\mathbf{k})$ and $|\Gamma_{\mathcal{A}_{\mathbf{k}}}\rangle = \sum_{\mathbf{a} \in \mathcal{A}_{\mathbf{k}}} |\Gamma_{\mathbf{a}}\rangle$. Almost all functions h satisfy

$$|2^{N_s} |\Gamma_{\mathcal{A}_{\mathbf{k}}}\rangle - 4^{-N_r} |1's\rangle| \preceq \sqrt{2}^{N_s + \sqrt{N_r}} |\mathrm{CHSH}\rangle^{\otimes N_r}, \quad (6)$$

for all $\mathbf{k}$, where the symbol $|\cdot|$ denotes entrywise absolute value, the symbol $\preceq$ denotes entrywise less or equal than, and $|1's\rangle \in \mathbb{R}^{16^{N_r}}$ has all entries equal to one.

Proof of the main result.—Let h be any of the functions which satisfies (6), and for each $\mathbf{k}$, let $|\Gamma_{\mathcal{A}_\mathbf{k}}\rangle$ be the vector defined in Lemma 2. Using $P_{\mathbf{k}|\mathbf{x}=\mathbf{0}} = \langle \Gamma_{\mathcal{A}_\mathbf{k}} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle$, the convexity of the absolute-value function, the inequality (6), and the fact that the marginal for $\mathbf{a}$, $\mathbf{b}$ cannot depend on z, we have

$$\begin{aligned}\sum_{\mathbf{k}} \max_z \sum_e P_{e|z} |P_{\mathbf{k}|\mathbf{x}=\mathbf{0},e,z} - 2^{-N_s}| \\ \leq \sum_{\mathbf{k}} \max_z \sum_e P_{e|z} |\langle \Gamma_{\mathcal{A}_\mathbf{k}}| - 2^{-N_s - 2N_r}\langle 1's||| P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y},e,z}\rangle \\ = \sqrt{2}^{N_s + \sqrt{N_r}} \langle \mathrm{CHSH}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle, \qquad (7)\end{aligned}$$

which is precisely (5). □

Proof of Lemma 2.—Within this proof, the entries of any vector $|\Phi\rangle \in \mathbb{R}^{16^{N_r}}$ are labeled as $\Phi(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y})$. Also, for any pair of bit-strings $\mathbf{x}$, $\mathbf{y}$: (i) the string $\mathbf{x} \cdot \mathbf{y}$ is the bitwise product, (ii) the string $\mathbf{x} \oplus \mathbf{y}$ is the bitwise XOR, and (iii) the integer $\|\mathbf{x}\|$ is the number of ones in $\mathbf{x}$. Using this notation we can write the entries of the vector $|\mathrm{CHSH}\rangle^{\otimes N_r}$ as $\mathrm{CHSH}^{\otimes N_r}(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y}) = 2^{-5N_r/2} 5^{\|\mathbf{a}\oplus\mathbf{b}\oplus\mathbf{x}\cdot\mathbf{y}\|}$. Next we prove inequality (6) for a given $\mathbf{k}$ and a given entry $(\mathbf{a}_0, \mathbf{b}_0, \mathbf{x}_0, \mathbf{y}_0)$. Let $V_\mathbf{a} = 1$ if the string $\mathbf{a}$ belongs to $\mathcal{A}_\mathbf{k}$, and $V_\mathbf{a} = 0$ otherwise. If we pick a random function h with uniform distribution over the set of all functions, then the random variables $V_\mathbf{a}$ are independent and distributed according to $\mathrm{Prob}\{V_\mathbf{a} = 1\} = 2^{-N_s}$, for all $\mathbf{a}$. Let $\mu_\mathbf{a} = \Gamma_\mathbf{a}(\mathbf{a}_0, \mathbf{b}_0, \mathbf{x}_0, \mathbf{y}_0)$, $M = \|\mathbf{a}_0 \oplus \mathbf{b}_0 \oplus \mathbf{x}_0 \cdot \mathbf{y}_0\|$, and note that $|\mu_\mathbf{a}| \leq 5^M 8^{-N_r}$ for all $\mathbf{a}$. For any J and $\beta \geq 0$ the exponential Chebyshev inequality [14] gives

$$\mathrm{Prob}\left\{\sum_\mathbf{a} \mu_\mathbf{a} V_\mathbf{a} \geq J\right\} \leq \exp\left[2^{-N_s} \sum_\mathbf{a} (\beta\mu_\mathbf{a} + \beta^2 \mu_\mathbf{a}^2) - \beta J\right]$$

provided that $|\beta 5^M 8^{-N_r}| \leq 1$. Using $\sum_\mathbf{a} \mu_\mathbf{a} = 4^{-N_r}$, $\sum_\mathbf{a} \mu_\mathbf{a}^2 \leq 2^{-5N_r} 5^{2M}$, and substituting $J = 2^{-N_s - 2N_r} + 2^{(\sqrt{N_r} - N_r - N_s)/2} 4^{-N_r} 5^M$, $\beta = 2^{(\sqrt{N_r} + N_r + N_s)/2} 4^{N_r} 5^{-M}$ we obtain

$$\begin{aligned}\mathrm{Prob}\left\{\sum_\mathbf{a} \mu_\mathbf{a} V_\mathbf{a} \geq 2^{-N_s - 2N_r} + 2^{(\sqrt{N_r} - N_r - N_s)/2} 4^{-N_r} 5^M\right\} \\ \leq e^{-2^{\sqrt{N_r}}/4}.\end{aligned}$$

The expression obtained when replacing "≥" with "≤" above, can be derived in a similar way. Then, with probability $2e^{-2^{\sqrt{N_r}}/4}$ we have

$$\begin{aligned}|2^{N_s} \Gamma_{\mathcal{A}_\mathbf{k}}(\mathbf{a}_0, \mathbf{b}_0, \mathbf{x}_0, \mathbf{y}_0) - 4^{-N_r}| \\ \leq \sqrt{2}^{N_s + \sqrt{N_r}} \mathrm{CHSH}^{\otimes N_r}(\mathbf{a}_0, \mathbf{b}_0, \mathbf{x}_0, \mathbf{y}_0). \qquad (8)\end{aligned}$$

However, we want this to hold for all $\mathbf{k}$ and all entries $(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y})$. The number of different values of $\mathbf{k}$ is 2^{N_s}, and the number of different entries is 16^{N_r}, then the probability of (6) is lower than $2\exp(5N_r - 2^{\sqrt{N_r}}/4)$. □

Error correction and public communication.—It is usually the case that the given distribution $P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}$ does not provide perfect correlations between $\mathbf{a}$ and $\mathbf{b}$. Hence, if $\mathbf{a}$ is the raw key, Bob has to correct the errors in $\mathbf{b}$ before applying the hash function h. This can be done by Alice publishing some information about $\mathbf{a}$, and Bob using it for correcting his errors. This is a standard procedure in quantum key distribution, which is detailed in [5] or [15]. Other procedures within the key-distribution protocol may also require public communication. Let the N_c-bit string $\mathbf{c}$ be all the information about $\mathbf{a}$ that Alice has published during the protocol. Because $\mathbf{c}$ is a function of $\mathbf{a}$, we can still use the main result (5) in this new setting if we let both, $\mathbf{k}$ and $\mathbf{c}$, to be the outcomes of the function h: $\{0,1\}^{N_r} \to \{0,1\}^{N_c} \times \{0,1\}^{N_s}$. However, $\mathbf{k}$ and $\mathbf{c}$ play different roles: $\mathbf{k}$ is the secret key and $\mathbf{c}$ is part of the information owned by Eve. Hence, the extension of the security condition (5) to the present setting is

$$\begin{aligned}\sum_{\mathbf{k},\mathbf{c}} \max_z \sum_e |P_{\mathbf{k},\mathbf{c},e|z} - 2^{-N_s} P_{\mathbf{c},e|z}| \\ \leq 2\sqrt{2}^{N_c + N_s + \sqrt{N_r}} \langle \mathrm{CHSH}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle, \qquad (9)\end{aligned}$$

where here and in the rest, the conditioning on $\mathbf{x} = \mathbf{0}$ is implicit. This inequality is obtained by taking (5) and using the triangular inequality with the third distribution $2^{-N_c - N_s} P_{e|z}$. The secret key is secure if the right-hand side of (9) can be made arbitrarily small (as N_r grows). This happens when the length of the final key is

$$N_s \approx \log_2[\langle \mathrm{CHSH}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle^{-2}] - N_c, \qquad (10)$$

up to sublinear terms.

Parameter estimation.—In the unconditional-security scenario, the honest parties are given N pairs of systems in a completely unknown global distribution. To perform a key-distribution protocol, and, in particular, to set the numbers N_s and N_c, they need to bound some quantities, as for instance $\langle \mathrm{CHSH}|^{\otimes N} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle$. In order to do so, they invest some of the given pairs to obtain information about the distribution $P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}$ of the N_r remaining pairs. More precisely, they compute the bounds for N_s, N_c for another distribution $P'_{\mathbf{a},\mathbf{b},e|\mathbf{x},\mathbf{y},z}$, which is warranted to be close to the real (unknown) one ($\sum_{\mathbf{a},\mathbf{b},e} |P'_{\mathbf{a},\mathbf{b},e|\mathbf{x},\mathbf{y},z} - P_{\mathbf{a},\mathbf{b},e|\mathbf{x},\mathbf{y},z}| \leq \epsilon$ for all $\mathbf{x}$, $\mathbf{y}$). This is explained with full detail in [5]. It is shown in [13] that

$$\begin{aligned}\sum_{\mathbf{k},\mathbf{c}} \max_z \sum_e |P_{\mathbf{k},\mathbf{c},e|z} - 2^{-N_s} P_{e,\mathbf{c}|z}| \\ \leq 2\sqrt{2}^{N_s + N_c + \sqrt{N_r}} \langle \mathrm{CHSH}|^{\otimes N_r} | P'_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}}\rangle + 2\epsilon, \qquad (11)\end{aligned}$$

which provides the security bound for the real (unknown) distribution in terms of properties of any ϵ-close primed distribution.

The BHK protocol.—The BHK protocol introduced in [2] and analyzed in [4,5] gives a rate of one secret bit per singlet ($|00\rangle + |11\rangle$). It is remarkable that this protocol, where the adversary is only constrained by no signaling, gives the same rate as if the adversary is constrained by no signaling plus quantum mechanics. The essential difference of the BHK protocol is to measure each system with $m \geq 2$ observables, $x \in \{1, \ldots m\}$. In this case, instead of the CHSH, we use the Braunstein-Caves Bell inequality [16], which can be expressed as $\langle \mathrm{BC} | P_{a,b|x,y} \rangle \geq \sqrt{2}$, with

$$|\mathrm{BC}\rangle = \frac{1}{2\sqrt{2}m} \begin{pmatrix} 1 & \alpha & 1 & \alpha & & & & \\ \alpha & 1 & \alpha & 1 & & & & \\ & & 1 & \alpha & \ddots & & & \\ & & \alpha & 1 & & & & \\ & & & & \ddots & & 1 & \alpha \\ & & & & & & \alpha & 1 \\ \alpha & 1 & & & & & 1 & \alpha \\ 1 & \alpha & & & & & \alpha & 1 \end{pmatrix}, \tag{12}$$

where $\alpha = 2m + 1$, and the empty entries represent zeroes. Notice that for $m = 2$ this is equivalent to the CHSH inequality (2). Following the same methods as above, one can prove inequalities analogous to (5), (9), (11), and obtain a key rate as in (10) but with the Braunstein-Caves Bell inequality

$$N_s \approx \log_2[\langle \mathrm{BC}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}} \rangle^{-2}] - N_c. \tag{13}$$

This rate formula can be improved by modifying $|\mathrm{BC}\rangle$ in the following way: take the expression (12) and substitute α by $\sqrt{1 + 4m^2}$. The security of this rate will be proven somewhere else.

If Alice and Bob share singlets or something close to it, in the estimation process they measure them with all the observables corresponding to points in the equator of the block sphere (see [2,4,5] for details), the generated correlations have $\langle \mathrm{BC}|^{\otimes N_r} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}} \rangle \approx 1/\sqrt{2}$, for large m. The raw keys $\mathbf{a}$, $\mathbf{b}$ are generated by measuring all systems with the same observable $x = 0$, then $\mathbf{a} = \mathbf{b}$ and $N_c \approx 0$. Formula (13) tells that the secret key rate is *one secret bit per singlet*: $N_s \approx N_r$. This rate cannot be improved because it is also the optimal rate achievable against a much weaker (quantum) adversary.

Conclusions.—We show, for the first time, that key distribution from Bell-violating correlations is secure according to the strongest notion of security, the so-called universally composable security. This provides the possibility of implementing secure cryptographic protocols with untrusted quantum devices [3]. In this model, Alice and Bob have to trust some of their apparatuses (classical computers and the random number generator), but can distrust the devices for preparing and measuring the quantum systems sent through the channel. The efficiency rate is slightly lower than the one obtained in standard quantum key distribution, where trusting the quantum devices is necessary.

Interestingly, in our scheme, Bell-inequality violation plays the same role as the min entropy [15] does in standard quantum key distribution. Specifically, Eqs. (5) and (10) have a quantum counterpart, obtained with the exchange

$$\log_2[\langle \mathrm{CHSH}|^{\otimes N} | P_{\mathbf{a},\mathbf{b}|\mathbf{x},\mathbf{y}} \rangle^{-2}] \leftrightarrow H_{\min}(\mathbf{a}|e). \tag{14}$$

A novelty of our scheme is that randomness extraction, or equivalently PA, can be performed with a constant hash function. This contrasts with previous methods for extracting randomness (two-universal hashing [11], extractors, etc.), which need random functions.

We acknowledge Caixa Manresa for useful discussions and appreciate support from the Spanish MEC (FIS2005-04627, FIS2007-60182, Consolider QOIT), and the EU-IP programme SCALA.

[1] J. S. Bell, Physics **1**, 195 (1964).
[2] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[3] A. Acin, N. Gisin, and Ll. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
[4] A. Acin, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006).
[5] Ll. Masanes, R. Renner, A. Winter, J. Barrett, and M. Christandl, arXiv:quant-ph/0606049.
[6] R. Canetti, in *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science 2001* (IEEE Computer Society, Washington, DC, 2001), pp. 136–146.
[7] Ll. Masanes, A. Acín, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).
[8] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[9] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[10] B. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[11] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[12] E. Hänggi, R. Renner, and S. Wolf (to be published).
[13] Ll. Masanes, arXiv:0807.2158.
[14] A. Shiryaev, *Probability* (Springer-Verlag, New York, 1996), 2nd ed.
[15] R. Renner, Ph.D. thesis, ETH Zurich, Diss. ETH No. 16242, 2005. Also available in arXiv:quant-ph/0512258.
[16] S. Braunstein and C. Caves, Ann. Phys. (N.Y.) **202**, 22 (1990).