Security of Device-Independent Quantum Key Distribution Protocols

Chirag Dhara[1], Lluis Masanes[1], Stefano Pironio[2], and Antonio Acín[1,3](✉)

[1] ICFO–Institut de Ciències Fotòniques, Castelldefels, 08860 Barcelona, Spain
[2] Laboratoire d'Infomation Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium
[3] ICREA–Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain
antonio.acin@icfo.es

Abstract. Device-independent cryptography represent the strongest form of physical security: it is based on general physical laws and does not require any detailed knowledge or control of the physical devices used in the protocol. We discuss a general security proof valid for a large class of device-independent quantum key distribution protocols. The proof relies on the validity of Quantum Theory and requires that the events generating the raw key are causally disconnected. We then apply the proof to the chained Bell inequalities and compute the corresponding secret-key rates.

1 Introduction

Quantum Key Distribution (QKD), and more generally Quantum Cryptography, implied a change of paradigm in security. Before the conception of QKD in 1984 [1], most cryptographic applications based their security on reasonable assumptions on the eavesdropper's computational power plus unproven assumptions on the computational complexity of some problems. In QKD, however, security is mainly based on a physically motivated assumption: the honest parties, Alice and Bob, and the eavesdropper, Eve, are constrained by the laws of quantum physics. Still, this is not the only assumption needed for security proofs of QKD. First of all, the honest parties should have a good physical characterization and control of the devices used in the protocol. Moreover, the security proof also requires a pair of minimal assumptions essential to make the cryptographic scenario meaningful: no information leaks Alice and Bob's laboratories, and the honest parties have a source of trusted randomness and trusted devices to process and store the information generated during the protocol execution.

The main goal of Device-Independent Quantum Key Distribution (DIQKD) [2–4] is to design protocols whose security proof requires no detailed knowledge of the physical devices used for generating correlations. That is, apart from unavoidable assumptions on the security of the honest parties' locations and the reliability of the devices they use for information processing, which in a way are inherent to the very definition of the cryptographic scenario, only the general validity of quantum theory is needed for security. In this scenario, the only

D. Bacon et al. (Eds.): TQC 2011, LNCS 6745, pp. 13–22, 2014.
DOI: 10.1007/978-3-642-54429-3_2, © Springer-Verlag Berlin Heidelberg 2014

possible security certificate is the one proposed by Ekert [5], see also [2,6]: the observation of a Bell inequality violation. There are three main motivations to consider the device-independent scenario. First, from a purely theoretical point of view, DIQKD involves fewer assumptions and, thus, implies a stronger security. More generally, identifying the minimal set of physical assumptions needed for secure key distribution is a fundamental problem in cryptography. Second, from an applied point of view, the implementation of DIQKD schemes is more robust to imperfections since their security proof is independent of the devices' details. However, it requires a long-distance detection-loophole-free Bell inequality violation, which at present is an experimental challenge (see however [7]). Finally, DIQKD, as the works on self testing techniques [8,9], opens Quantum Cryptography to the unreliable, yet non-adversarial, provider scenario, as any device compatible with the protocol requirements is secure.

In this work we discuss a general formalism to prove the security of DIQKD protocols [10] (see also [11]). The security proof is completely general and can be applied to any protocol associated to a Bell inequality. The key element in the construction is a bound on the min-entropy of the raw key from the estimated Bell inequality violation. Compared to previous approaches [12], the proof exploits the constraints imposed by quantum theory, which significantly increases the efficiency of the protocols. For instance, when applied to the protocol of Ref. [3], based on the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [13], security can be guaranteed up to a quantum-bit error rate (QBER) of approximately 5 %.

The security proof, however, needs a requirement which limits its applicability from a practical point of view: all the events generating the raw-key symbols must be causally disconnected. There are different possibilities to meet this requirement. First, one can relax the device-independent character of the protocol and assume that the measuring apparatuses have no internal memory. Of course, the no-memory assumption is present in any of the security proofs for standard QKD [1]. The requirement can also be fulfilled in a device-independent manner if the honest parties have access to separated devices. For instance, if all raw-key symbols are defined by space-like separated events, special relativity warrants their causal independence. However, space-like separation is not necessarily required for the generation of the raw-key symbols. It is sufficient that the parties are able to shield each of these devices and prevent any unwanted information exchange among them when generating the raw-key symbols. This assumption is similar to the one that the honest parties are capable of preventing information leakage from their laboratories, without which the the cryptographic scenario would not make sense.

2 Bell Inequalities and DIQKD Protocols

The class of protocols we consider are variations of Ekert's QKD protocol [5,14]. Alice and Bob share a quantum channel that distributes entangled states and they both have a quantum apparatus to measure their incoming particles. These apparatuses take an input (the measurement setting) and produce an output (the measurement outcome). We label the inputs and outputs x and a for Alice, and y and b for Bob, and assume that they take a finite set of possible values.

The first step of the protocol consists in measuring the pairs of quantum systems distributed to Alice and Bob. In most of the cases (say N), the inputs are set to fixed values $x_i = x_{\rm raw}$ and $y_i = y_{\rm raw}$ and the corresponding outputs $\mathbf{a} = (a_1, \dots a_N)$ and $\mathbf{b} = (b_1, \dots b_N)$ constitute the two versions of the raw key. In the remaining systems, which represent a small random subset of all measured pairs (of size say $N_{\rm est} \approx \sqrt{N}$), the inputs x, y are chosen uniformly at random. From these $N_{\rm est}$ pairs, Alice and Bob determine the relative frequencies $q(ab|xy)$ with which the outputs a and b are obtained when using inputs x and y. These relative frequencies quantify the degree of non-local correlations between Alice and Bob's system through the violation of the Bell inequality associated to the DIQKD protocol. This Bell inequality is defined by a linear function g of the input-output correlations $q(ab|xy)$:

$$g = \sum_{a,b,x,y} g_{abxy} q(ab|xy) \le g_{\rm loc}, \tag{1}$$

where g_{abxy} are the coefficients defining the Bell inequality and $g_{\rm loc}$ is its local bound. A particular example of a Bell inequality is the CHSH inequality [13]

$$g_{\rm chsh} = \sum_{a,b,x,y} (-1)^{a+b+xy} q(ab|xy) \le 2, \tag{2}$$

where $a, b, x, y \in \{0, 1\}$.

After this initial "measure and estimate" phase, the rest of the protocol is similar to any other QKD protocol. Alice publishes an $N_{\rm pub}$-bit message about $\mathbf{a}$, which is used by Bob to correct his errors $\mathbf{b} \to \mathbf{b}'$, such that $\mathbf{b}' = \mathbf{a}$ with arbitrarily high probability. Alice and Bob then generate their final secret key $\mathbf{k}$ by applying a 2-universal random function to $\mathbf{a}$ and $\mathbf{b}'$, respectively [15].

3 Generation of the Raw-Key Symbols

In the DIQDK approach, we do not assume that the devices behave according to predetermined specifications. Yet, we must first specify how we model the N pairs of systems used to generate the raw key. These N pairs are eventually all measured using the inputs $x = x_{\rm raw}$ and $y = y_{\rm raw}$, but since they where initially selected at random and each of them could have been part of the $N_{\rm est}$ pairs used to estimate the Bell violation, we must also consider what would have happened for any other inputs x and y. Let therefore $P(\mathbf{ab}|\mathbf{xy})$ denote the prior probability to obtain outcomes $\mathbf{a}$ and $\mathbf{b}$ if measurements $\mathbf{x} = (x_1, \dots, x_N)$ and $\mathbf{y} = (y_1, \dots, y_N)$ are made on these N pairs. This unknown probability distribution characterizes the initial system at the beginning of the protocol.

In the theoretical model needed for the security proof of Ref. [10], the N bits of the raw key are viewed as arising from N *commuting* measurements on a joint quantum system $\rho_{\mathcal{AB}}$. That is, the probabilities $P(\mathbf{ab}|\mathbf{xy})$ can be written as

$$P(\mathbf{ab}|\mathbf{xy}) = \mathrm{tr}[\rho_{\mathcal{AB}} \prod_{i=1}^{N} A_i(a_i|x_i) B_i(b_i|y_i)], \tag{3}$$

where $A_i(a_i|x_i)$ are operators describing the measurements performed by Alice on her ith system if she select input x_i (they thus satisfy $A_i(a_i|x_i) \geq 0$ and $\sum_{a_i} A_i(a_i|x_i) = \mathbb{1}$), where, similarly, $B_i(b_i|y_i)$ are operators describing the measurements by Bob, and where these measurement operators satisfy the commutation relations

$$[A_i(a|x), B_j(b|y)] = 0 \tag{4}$$

and

$$[A_i(a|x), A_j(a'|x')] = [B_i(b|y), B_j(b'|y')] = 0 \tag{5}$$

for all i, j and a, a', b, b', x, x'. Apart from the conditions (4) and (5), the state ρ_{AB} and the operators $A_i(a_i|x_i)$ and $B_i(b_i|y_i)$ are arbitrary and unspecified. The only constraint on them is that they should return measurement probabilities (3) compatible with the statistics of the N_{est} randomly selected pairs, characterized by the observed Bell-inequality violation g.

In quantum theory, measurement operators that commute represent compatible measurements that do not influence each other and which can be performed independently of each other. The commutation relations (4) between the operators $A_i(a_i|x_i)$ describing Alice's measurement devices and the operators $B_i(b_i|y_i)$ describing Bob's measurement devices are thus a necessary part of any DIQDK model; security cannot be guaranteed without them.

The commutation relations (5) between the operators $A_i(a_i|x_i)$ *within* Alice's location, and the commutation relations between the operators $B_i(b_i|y_i)$ *within* Bob's location, represent, on the other hand, additional constraints specific to the model discussed here. As already mentioned these commutation relations are satisfied in an implementation in which the N bits of the raw key are generated by N separate and non-interacting pairs of devices used in parallel. Let's elaborate more on this point.

In the extreme adversarial scenario where the provider of the devices is not trusted (e.g., if the provider is the eavesdropper itself), this independence condition can be guaranteed by shielding the N devices in such a way that no communication between them occurs during the measurement process. One could also consider a setup where the measurements performed by the N devices define space-like separated events. However, even in a space-like separated configuration, the ability to shield the devices is required if the provider of the devices is untrusted, as we cannot guarantee through other means that the devices do not send directly unwanted information to the adversary. But, then, the ability to shield the devices is already sufficient by itself to guarantee (5).

In a more practical implementation where the raw key is generated by repeatedly performing measurements in sequence on a *single* pair of devices, the commutation relation (5) expresses the condition that the functioning of the devices should not depend on any internal memory storing the quantum states and measurement results obtained in previous rounds. In the most general DIQKD model, the quantum devices could possess a quantum memory such that the state of the system after the ith measurement is passed to the successive round $i+1$ (this state could also contain classical information about the measurement inputs and outputs of step i). If $\rho^i_{\mathcal{AB}}$ denotes the state of the system before measurement i, the unormalised state passed to round $i+1$ in the event that Alice and Bob use inputs x_i and y_i and obtain outputs a_i and b_i would then be $\tilde{A}_i^\dagger(a_i|x_i)\tilde{B}_i^\dagger(b_i|y_i)\rho^i_{\mathcal{AB}}\tilde{A}_i(a_i|x_i)\tilde{B}_i(b_i|y_i)$ where $\tilde{A}_i(a|x)$ and $\tilde{B}_i(b_i|x_i)$ are generalized measurement operators describing Alice's and Bob's measurements and satisfying $\sum_a \tilde{A}_i(a|x)\tilde{A}_i^\dagger(a|x) = \sum_b \tilde{B}_i(b|y)\tilde{B}_i^\dagger(b|y) = I$. In such a model, the probabilities $P(\mathbf{ab}|\mathbf{xy})$ are then given by

$$P(\mathbf{ab}|\mathbf{xy}) = \mathrm{tr}[\prod_{i=N}^{1} \tilde{A}_i^\dagger(a_i|x_i)\tilde{B}_i^\dagger(b_i|y_i) \times \rho_{\mathcal{AB}} \prod_{i=1}^{N} \tilde{A}_i(a_i|x_i)\tilde{B}_i(b_i|y_i)], \qquad (6)$$

where $\rho_{\mathcal{AB}}$ denotes the initial state at the beginning of the protocol, and the order in the products is relevant. Imposing commutation relations between all operators pertaining to different rounds corresponds to neglect the causal order in (6) due to memory effects. We then recover a model of the form (3) by defining $A_i(a|x) = \tilde{A}_i(a|x)\tilde{A}_i^\dagger(a|x)$ and $B_i(b|y) = \tilde{B}_i(b|y)\tilde{B}_i^\dagger(b|y)$.

4 Security Proof

We are now in position to review the bound on the secret key rate derived in [10]. This bound can be achieved against an unrestricted eavesdropper Eve for any QKD protocol satisfying the description (3), (4) and (5). The information available to Eve can be represented by a quantum system that is correlated with the Alice and Bob's systems. We denote by $\rho_{\mathcal{ABE}}$ the corresponding $(2N+1)$-partite state, with $\mathrm{tr}_{\mathcal{E}}\, \rho_{\mathcal{ABE}} = \rho_{\mathcal{AB}}$. This state describes the $2N+1$ systems at the beginning of the protocol. After the N systems of Alice have been measured, the joint state of Alice and Eve is described by the classical-quantum state

$$\rho_{\mathcal{AE}} = \sum_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}_{\mathrm{raw}})|\mathbf{a}\rangle\langle\mathbf{a}| \otimes \rho_{\mathcal{E}|\mathbf{a}}, \qquad (7)$$

where $\rho_{\mathcal{E}|\mathbf{a}}$ is the reduced state of Eve conditioned on Alice having observed the outcomes $\mathbf{a}$.

The length of the secret key $\mathbf{k}$ obtained by processing the raw key $\mathbf{a}$ with an error correcting protocol and a 2-universal random function is, up to terms of order $\sqrt{N}$, lower bounded by $H_{\min}(\mathbf{a}|\mathcal{E}) - N_{\mathrm{pub}}$, where $H_{\min}(\mathbf{a}|\mathcal{E})$ is the min-entropy of $\mathbf{a}$ conditioned on Eve's information for the state (7) and N_{pub} is the length of the message published by Alice in the error-correcting phase. It is shown in [16] that the length of the public message necessary for correcting Bob's errors is $N_{\mathrm{pub}} = NH(a|b)$, up to terms of order $\sqrt{N}$. The quantity $H(a|b)$ is the conditional Shannon entropy [16], defined by

$$H(a|b) = \sum_{a,b} -P(a,b)\log_2 P(a|b), \qquad (8)$$

where $P(a,b) = 1/N \sum_{i=1}^{N} \sum_{a_i,b_i} P(a_i = a, b_i = b)$ is the average probability with witch the pair of outcomes a and b are observed. Computing the key rate of the DIQKD protocol, thus essentially amounts to determine the min-entropy $H_{\min}(\mathbf{a}|E)$. A bound on this quantity can be derived as a function of the estimated Bell violation g.

Consider first the simpler case of one pair of systems ($N = 1$) uncorrelated to the adversary and characterized by the joint probabilities

$$P(ab|xy) = \mathrm{tr}[\rho\, A(a|x)B(b|y)]. \tag{9}$$

If $P(a|x_{\mathrm{raw}}) < 1$ for all a, then the outcome of the measurement x_{raw} cannot be perfectly predicted. The degree of unpredictability of a can be quantified by the probability to correctly guess a [17]. This guessing probability is equal to

$$P_{\mathrm{guess}}(a) = \max_{a} P(a|x_{\mathrm{raw}}), \tag{10}$$

since the best guess that one can make about a is to output the most probable outcome. If $P_{\mathrm{guess}}(a) = 1$ then the outcome of the measurement x_{raw} can be predicted with certainty, while lower values for $P_{\mathrm{guess}}(a)$ imply less predictability.

Let $g_{\mathrm{exp}} = \sum_{abxy} g_{abxy} P(ab|xy) = \mathrm{tr}[\rho\, G]$ denote the expected quantum violation of the Bell inequality (1) for the pair of systems described by (9), where

$$G = \sum_{a,b,x,y} g_{abxy} A(a|x)B(b|y), \tag{11}$$

is the Bell operator associated to the inequality g and to the measurements $A(a|x)$ and $B(b|y)$. Independently of the precise form of the state ρ and of the measurement operators $A(a|x)$ and $B(b|y)$, the value of the Bell expectation g_{exp} imposes a constraint on the guessing probability (10). Formally, this constraint can be expressed as a bound of the form

$$P_{\mathrm{guess}}(a) \le f(g_{\mathrm{exp}}), \tag{12}$$

satisfied by all quantum distributions (9). The optimal point-wise values $f(g_0)$ (for any g_0) correspond to the solution of the following maximization problem

$$\begin{aligned} \max_{\rho,A,B} \quad & \mathrm{tr}[\rho\, A(a|x_{\mathrm{raw}})] \\ \text{subject to } & \mathrm{tr}[\rho\, G] = g_0, \end{aligned} \tag{13}$$

which can be solved (or upper-bounded) using the semidefinite programming (SDP) relaxations introduced in [18]. The resulting functions f (and in particular the optimal one) are then always concave and monotonically decreasing, as follows from the convex nature of the problem (13) and of its associated SDP relaxations. In the case of the CHSH inequality, the optimal function f is [10, 19]

$$f_{\mathrm{chsh}}(g) = \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{g^2}{4}}, \tag{14}$$

for any of the two possible values $x_{\mathrm{raw}} = 0$ or 1 entering in the CHSH definition (2).

As the function f is concave, it can be upper-bounded by its linearization around any point g_0

$$f(g) \leq \mu(g_0) + \nu(g_0)g, \tag{15}$$

where $\mu(g_0) = f(g_0) - f'(g_0)g_0$, $\nu(g_0) = f'(g_0)$. From concavity, it also follows that

$$f(g) = \min_{g_0} \left[\mu(g_0) + \nu(g_0)g\right]. \tag{16}$$

The bound (12) is thus equivalent to the family of inequalities $P(a|x_{\mathrm{raw}}) \leq \mu(g_0) + \nu(g_0), g_{\mathrm{exp}}$ for all a and g_0. Since these inequalities are satisfied by any quantum distribution (9), and thus in particular by any state ρ, they are equivalent to the operator inequalities

$$A(a|x_{\mathrm{raw}}) \leq \mu(g_0)\mathbb{1} + \nu(g_0)G, \tag{17}$$

valid for all a, g_0, and any set of measurements $A(a|x)$ and $B(b|y)$.

Moving to the case of N pairs of systems described by (3) and (7), the probability with which Eve can correctly guess the raw key $\mathbf{a}$ by measuring her side information $\mathcal{E}$ can be computed as follows. Suppose thus that Eve performs some measurement z on her system $\mathcal{E}$ and obtains an outcome e. Let $P(\mathbf{a}|\mathbf{x}_{\mathrm{raw}}, ez)$ denote the probability distribution of $\mathbf{a}$ conditioned on Eve's information. On average, her probability to correctly guess $\mathbf{a}$ is given by $\sum_e P(e|z) \max_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}_{\mathrm{raw}}, ez)$, and her optimal correct-guessing probability (optimized over all measurements z) is [17]:

$$P_{\mathrm{guess}}(\mathbf{a}|\mathcal{E}) = \max_z \sum_e P(e|z) \max_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}_{\mathrm{raw}}, ez). \tag{18}$$

Denote by $\rho_{\mathcal{AB}|ez}$ the $2N$-partite state prepared when Eve measures z and obtains the outcome e (with $\rho_{\mathcal{AB}} = \sum_e P(e|z)\rho_{\mathcal{AB}|ez}$), and write $\mathbf{A}(\mathbf{a}|\mathbf{x}_{\mathrm{raw}}) = \prod_{i=1}^N A_i(a_i|x_{\mathrm{raw}})$, so that

$$P(\mathbf{a}|\mathbf{x}_{\mathrm{raw}}, ez) = \mathrm{tr}\left[\rho_{\mathcal{AB}|ez}\mathbf{A}(\mathbf{a}|\mathbf{x}_{\mathrm{raw}})\right]. \tag{19}$$

Consider the following N-partite Bell operator

$$\mathbf{G}(g_0) = \prod_{i=1}^{N} [\mu(g_0)\mathbb{1} + \nu(g_0)G_i], \tag{20}$$

where $G_i = \sum_{a,b,x,y} g_{abxy} A_i(a_i|x_i)B_i(b_i|y_i)$. The single-copy operator inequality (17) implies that for all $\mathbf{a}$ and g_0

$$\mathbf{A}(\mathbf{a}|\mathbf{x}_{\mathrm{raw}}) \leq \mathbf{G}(g_0). \tag{21}$$

To show this, write $A'_i = A_i(a_i|x_{\mathrm{raw}})$ and $G'_i = \mu(g_0)\mathbb{1} + \nu(g_0)G_i$. We thus want to establish that $\prod_{i=1}^N G'_i - \prod_{i=1}^N A'_i \geq 0$. Inequality (17) implies that for all i,

$0 \leq A_i' \leq G_i'$. Defining $Z_i = G_i' - A_i' \geq 0$, note then that $\prod_{i=1}^N G_i' - \prod_{i=1}^N A_i' = \prod_{i=1}^N (Z_i + A_i') - \prod_{i=1}^N A_i' = \prod_{i=1}^N Z_i + Z_1 \prod_{i=2}^N A_i' + \cdots + \prod_{i=1}^{N-1} A_i' Z_n$. Inequality (21) then follows from the fact that each term in this sum is positive since it is the product of operators that are positive and, according to (5), commuting.

Using inequality (21) in (18), we find

$$\begin{aligned} P_{\text{guess}}(\mathbf{a}|\mathcal{E}) &= \max_z \sum_e P(e|z) \max_{\mathbf{a}} \operatorname{tr}\left[\rho_{\mathcal{AB}|ez} A(\mathbf{a}|\mathbf{x}_{\text{raw}})\right] \\ &\leq \max_z \sum_e P(e|z) \min_{g_0} \operatorname{tr}\left[\rho_{\mathcal{AB}|ez} \mathbf{G}(g_0)\right], \\ &\leq \min_{g_0} \operatorname{tr}\left[\rho_{\mathcal{AB}}\, \mathbf{G}(g_0)\right] \end{aligned} \tag{22}$$

where to deduce the first inequality we used, in addition to (21), the positivity of $\rho_{\mathcal{AB}|ez}$.

Note now that the quantity $\operatorname{tr}[\rho_{\mathcal{AB}}, \mathbf{G}(g_0)]$ is a function of the marginal distributions $P(\mathbf{ab}|\mathbf{xy})$ of Alice and Bob only and does not involve directly the system of Eve. It is shown in [17], that Alice and Bob can estimate (with high probability) this quantity from the Bell violation g observed on the randomly-chosen N_{est} pairs. More precisely, Lemma 5 from reference [17] implies that the inequality

$$\operatorname{tr}[\rho_{\mathcal{AB}}, \mathbf{G}(g_0)] \leq \left[\mu(g_0) + \nu(g_0) g_{\text{est}} + N_{\text{est}}^{-1/4}\right]^N \tag{23}$$

holds except with probability exponentially small in N_{est}. This, (22), and (16) imply that

$$P_{\text{guess}}(\mathbf{a}|\mathcal{E}) \leq \left[f(g^{\text{est}}) + N_{\text{est}}^{-1/4}\right]^N. \tag{24}$$

Finally, it is shown in [17] that the (quantum) min-entropy $H_{\min}(\mathbf{a}|\mathcal{E})$ of a state of the form (7) is given by

$$H_{\min}(\mathbf{a}|\mathcal{E}) = -\log_2 P_{\text{guess}}(\mathbf{a}|\mathcal{E}), \tag{25}$$

which implies the asymptotic secret key rate

$$R \geq -\log_2 f(g_{\text{est}}) - H(a|b). \tag{26}$$

As announced, the bound applies to any Bell inequality and the corresponding DIQKD protocol.

5 Key Rates for the Chained Bell Inequality

As an illustration of the formalism, we explicitly compute the secret-key rates for the chained Bell inequalities of Ref. [20]. These inequalities were initially introduced in the scenario in which Alice and Bob perform M measurements of two outcomes. Later, they were generalized to an arbitrary number of outcomes [21], but we don't consider this generalization here.

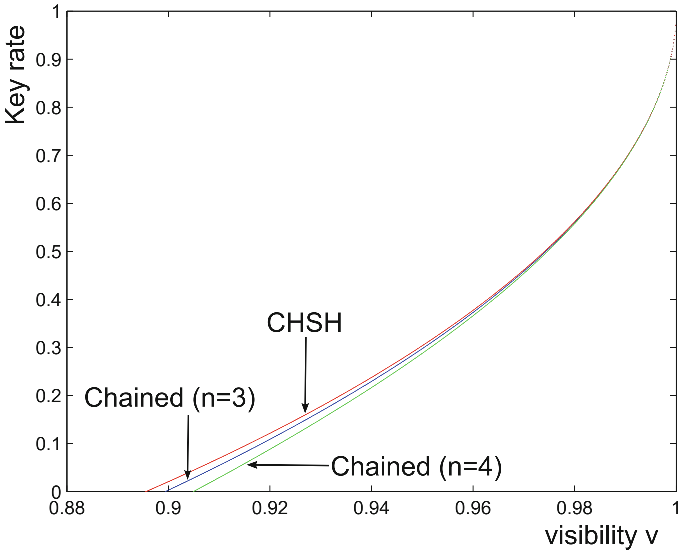

Fig. 1. Key rates for the chained Bell inequalities for 2, 3 and 4 measurements. The critical visibility such that the lower bound on the key rate is zero is approximately of 0.9. Increasing the number of settings up to 4 worsens this critical visibility.

The chained inequalities for two measurement outcomes read as follows. The two outcomes of each measurement by Alice (Bob) are labeled by $A_i = \pm 1$ ($B_i = \pm 1$), with $i = 1, \ldots, M$. Then, for any local model one has

$$\sum_{i=1}^{M} \langle A_i B_i \rangle + \sum_{i=1}^{M-1} \langle B_i A_{i+1} \rangle - \langle B_M A_1 \rangle \leq 2(M-1), \tag{27}$$

where $\langle X \rangle$ stands for the expectation value of the random variable X. The case $M = 2$ corresponds to the standard CHSH inequality.

In Fig. 2 we depict the lower bound on the secret-key rates (26) for DIQKD protocols based on the chained inequalities for $M = 2, 3, 4$. These rates have been computed for the probability distribution resulting from applying the optimal measurements for the maximal quantum violation of the chained inequality on a mixture of a two-qubit maximally entangled state $|\Phi^+\rangle$ and white noise, that is,

$$\rho_{AB} = v|\Phi^+\rangle\langle\Phi^+| + (1-v)\mathbb{1}/4, \tag{28}$$

where v is often known as the visibility. It is important to recall that, while the rate is computed for a concrete set of states and measurements, the security analysis is fully device independent (up to the requirement that measurement outcomes are causally disconnected). Each value of the visibility defines a value for the error rate between Alice and Bob, $\epsilon_{AB} = (1+v)/2$, which specifies the amount of bits needed for error correction. The violation of the chained Bell inequality is just the maximal quantum violation multiplied by the visibility v. Putting the two things together, one derives the rates given in Fig. 1. The obtained critical values of the visibility such that the key rate is provably strictly positive, are of approximately 0.9. They are then comparable to those of standard QKD, which are around 0.78.

Acknowledgements. This work is supported by the Spanish MINCIN though projects FIS2007-60182 and FIS2010-14830, CHIST-ERA DIQIP, EU Project QCS and an ERC Starting Grant PERCENT, CatalunyaCaixa.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, p. 175 (1984)
2. Acín, A., Gisin, N.: Ll. Masanes. Phys. Rev. Lett. **97**, 120405 (2006)
3. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., Scarani, V.: Phys. Rev. Lett. **98**, 230501 (2007)
4. Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., Scarani, V.: New J. Phys. **11**, 045021 (2009)
5. Ekert, A.: Phys. Rev. Lett. **67**, 661 (1991)
6. Barrett, J., Hardy, L., Kent, A.: Phys. Rev. Lett. **95**, 010503 (2005)
7. Gisin, N., Pironio, S., Sangouard, N.: Phys. Rev. Lett. **105**, 070501 (2010)
8. Mayers, D., Yao, A.: Quantum Inf. Comput. **4**, 273 (2004)
9. Magniez, F., Mayers, D., Mosca, M., Ollivier, H.: Self-testing of quantum circuits. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4051, pp. 72–83. Springer, Heidelberg (2006)
10. Masanes, L., Pironio, S., Acín, A.: Nat. Comm. **2**, 238 (2011)
11. Hanggi, E., Renner, R.: arXiv:1009.1833
12. Ll. Masanes, Phys. Rev. Lett. **102**, 140501 (2009)
13. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Phys. Rev. Lett. **23**, 880 (1969)
14. Acín, A., Massar, S., Pironio, S.: New J. Phys. **8**, 126 (2006)
15. Carter, J.L., Wegman, M.N.: J. Comput. Syst. Sci. **18**, 143–154 (1979)
16. Csiszár, I., Kröner, J.: IEEE Trans. Inf. Theor. **24**, 339 (1978)
17. Koenig, R., Renner, R., Schaffner, C.: IEEE Trans. Inf. Theor. **55**, 9 (2009)
18. Navascues, M., Pironio, S., Acín, A.: Phys. Rev. Lett. **98**, 010401 (2007)
19. Pironio, S., Acín, A., Massar, S., Maunz, A., Olmschenk, S., Hayes, D., Luo, L., Manning, T.A., Monroe, C.: arXiv:0911.3427
20. Braunstein, S.L., Caves, C.M.: Ann. Phys. **202**, 22 (1990)
21. Barret, J., Kent, A., Pironio, S.: Phys. Rev. Lett. **97**, 170409 (2006)