nature COMMUNICATIONS

ARTICLE

Received 6 Oct 2010 | Accepted 16 Feb 2011 | Published 15 Mar 2011

DOI:10.1038/ncomms1244

Secure device-independent quantum key distribution with causally independent measurement devices

Lluís Masanes[1], Stefano Pironio[2] & Antonio Acín[1,3]

Device-independent quantum key distribution (QKD) aims to provide key distribution schemes, the security of which is based on the laws of quantum physics, but which does not require any assumptions about the internal working of the devices used in the protocol. This strong form of security is possible only when using correlations that violate a Bell inequality. Here, we provide a general security proof for a large class of protocols in a model in which the raw key is generated by independent measurements. This independence condition may be justifiable in several implementations and is necessarily satisfied when the raw key is generated by *N* separate pairs of devices. Our work shows that device-independent QKD is possible with key rates comparable to those of standard schemes.

[1] ICFO-Institut de Ciències Fotòniques, Castelldefels, E-08860 Barcelona, Spain. [2] Laboratoire d'Infomation Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium. [3] ICREA-Institució Catalana de Recerca i Estudis Avançats, E-08010 Barcelona, Spain. Correspondence and requests for materials should be addressed to A.A. (email: antonio.acin@icfo.es).

A central problem in cryptography is the distribution among distant users of secret keys that can be used, for example, for the secure encryption of messages. This task is impossible in classical cryptography unless assumptions are made on the computational power of the eavesdropper. Quantum key distribution (QKD), on the other hand, offers security against adversaries with unbounded computing power[1].

The ultimate level of security provided by QKD was made possible, thanks to a change of paradigm. Although in classical cryptography security relies on the hardness of certain mathematical problems, in QKD it relies on the fundamental laws of quantum physics. A side effect of this change of paradigm, however, is that although the security of classical cryptography is based on the mathematical properties of the key itself—how the key was actually generated in practice being, in principle, irrelevant to the security of the scheme—in QKD, the security crucially depends on the physical properties of the key generation process, for example, on the fact that the key was produced by measuring the polarization of a single photon along well-defined directions. But then, how can one asses the level of security provided by a real-life implementation of QKD, which will inevitably differ in inconspicuous ways from the idealized, theoretical description[2]? Errors in the encoding of the signals of Alice[3], for instance, or features of the detectors not taken into account in the theoretical analysis[4] can be exploited to break the security of real-life QKD schemes.

Device-independent QKD (DIQKD)[5] aims at closing the gap between theoretical analyses and practical realizations of QKD by designing protocols whose security does not require a detailed characterization of the devices used to generate the secret key (such as, for example, the dimension of the Hilbert space of the quantum signals or the type of measurements performed on them)[5–8]. This stronger form of cryptography is possible if it is based on the observation of a Bell-inequality violation, which guarantees that the data produced by the quantum devices possess some amount of secrecy, independently of how exactly these data were generated[9,10]. In some sense, DIQKD combines the advantage of classical and quantum cryptography: security against unbounded adversaries based on the law of quantum physics, but which does not rely on the physical details of the generation process. A fully device-independent demonstration of QKD, however, still represents, at present, an experimental challenge[11].

In this work, we provide a general formalism for proving the security of DIQKD protocols. This is done in terms of the strongest notion of security, universally composable security, according to which the secret key generated by the protocol is indistinguishable from an ideal secret key[12]. Our approach can be applied to protocols based on arbitrary Bell inequalities and is valid against the most general attacks available to an eavesdropper. The DIQKD model that we consider, however, is partly restricted as it supposes that the measurement processes generating the different bits of the raw key are causally independent of each other (though they could be arbitrarily correlated). This independence condition is necessarily satisfied in a physical realization in which the N bits of the raw key are generated by N separate pairs of devices used in parallel. Our analysis therefore shows that secure fully DIQKD is, in principle, possible. Note that our measurement independence condition and the level of security provided here is equivalent to the one considered in refs 13–16. The difference with respect to refs 14–16 is that our proof does not rely only on the no-signalling principle but also on the validity of the quantum formalism. This results in much better key rates, comparable to those of standard QKD.

Results

General structure of a DIQKD protocol. Let us start by presenting the class of protocols that we consider here, which are the variations of Ekert's QKD protocol[9,17]. 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 $x_i = x_{\mathrm{raw}}$ and $y_i = y_{\mathrm{raw}}$ and the corresponding outputs $\mathbf{a} = (a_1, \ldots a_N)$ and $\mathbf{b} = (b_1, \ldots b_N)$ 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 $N_{\mathrm{est}} \approx \sqrt{N}$), the inputs x and y are chosen uniformly at random. From these N_{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 $q(ab|xy)$:

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

where g_{abxy} are the coefficients defining the Bell inequality and g_{loc} is its local bound. A particular example of a Bell inequality is the Clauser–Horne–Shimony–Holt (CHSH) inequality[18]

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

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_{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 k by applying a two-universal random function to $\mathbf{a}$ and $\mathbf{b}'$, respectively[19].

The DIQKD model. In the DIQKD approach, we do not assume that the devices behave according to predetermined specifications. For instance, the state emitted by the source of particles may be modified by the eavesdropper, or the implementation of the measuring devices may be imperfect. To analyse the security of a DIQKD protocol, we must therefore first specify how we model the N pairs of systems used to generate the raw key.

These N pairs of systems are eventually all measured using the inputs $x = x_{\mathrm{raw}}$ and $y = y_{\mathrm{raw}}$, but as they were initially selected at random and each of them could have been part of the N_{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 previous probability to obtain outcomes $\mathbf{a}$ and $\mathbf{b}$ if measurements $\mathbf{x} = (x_1, \ldots x_N)$ and $\mathbf{y} = (y_1, \ldots y_N)$ are made on these N pairs. This unknown probability distribution characterizes the initial system at the beginning of the protocol.

In the theoretical model that we consider here, we view the N bits of the raw key as arising from N commuting measurements on a joint quantum system ρ_{AB}. That is, we suppose that the probabilities $P(\mathbf{ab}|\mathbf{xy})$ can be written as

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

where A_i $(a_i|x_i)$ are operators describing the measurements made by Alice on her ith system if she select input x_i (they thus satisfy A_i

$(a_i|x_i)\geq 0$ and $\Sigma_{a_i} A_i(a_i \mid x_i) = 1$), where, similarly, B_i $(b_i|y_i)$ are operators describing the measurements made by Bob, and where these measurement operators satisfy the commutation relations

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

and

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

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 DIQKD 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 DIQKD model considered here. 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.

In the extreme adversarial scenario wherein the provider of the devices is not trusted (for example, 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 in which 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, in which 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 ρ^i_{AB} denotes the state of the system before measurement i, the non-normalized 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 $\tilde{A}_i^\dagger(a_i \mid x_i)\tilde{B}_i^\dagger(b_i \mid y_i)\rho^i_{AB}\tilde{A}_i(a_i \mid x_i)\tilde{B}_i(b_i \mid y_i)$ where $\tilde{A}_i(a \mid x)$ and $\tilde{B}_i(b_i \mid x_i)$ are generalized measurement operators describing Alice's and Bob's measurements and satisfying $\Sigma_a \tilde{A}_i(a \mid x)\tilde{A}_i^\dagger(a \mid x) = \Sigma_b \tilde{B}_i(b \mid y)\tilde{B}_i^\dagger(b \mid y) = I$. In such a model, the probabilities $P(\mathbf{ab}|\mathbf{xy})$ are then given by

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

where ρ_{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 $A_i(a \mid x) = \tilde{A}_i(a \mid x)\tilde{A}_i^\dagger(a \mid x)$ and $B_i(b \mid y) = \tilde{B}_i(b \mid y)\tilde{B}_i^\dagger(b \mid y)$.

Security proof. We now establish a bound on the secret-key rate that can be achieved against an unrestricted eavesdropper Eve for a QKD protocol satisfying the description (3), (4), (5). The information available to Eve can be represented by a quantum system that is correlated with the systems of Alice and Bob. We denote by $\rho_{AB\mathcal{E}}$ the corresponding $(2N+1)$-partite state, with $\mathrm{tr}_{\mathcal{E}}\rho_{AB\mathcal{E}} = \rho_{AB}$. 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

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

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 k obtained by processing the raw key $\mathbf{a}$ with an error-correcting protocol and a two-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 ref. 20 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[20], defined by

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

where $P(a,b) = 1/N\ \Sigma_{i=1}^{N}\Sigma_{a_i,b_i}P(a_i = a, b_i = b)$ 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 $H_{\min}(\mathbf{a}|E)$. We show in the following how to put a bound on this quantity as a function of the estimated Bell violation g. This bound is independent of which type of quantum systems and measurements are used by Alice and Bob, implying that our security proof is device independent.

Intuitively, we want to understand how the observed Bell violation limits the predictability of Alice's outcomes $\mathbf{a}$. We start by considering the simpler case of one pair of systems ($N=1$) uncorrelated to the adversary and characterized by the joint probabilities

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

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[21]. This guessing probability is equal to

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

as 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, whereas lower values for $P_{\mathrm{guess}}(a)$ imply less predictability.

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

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

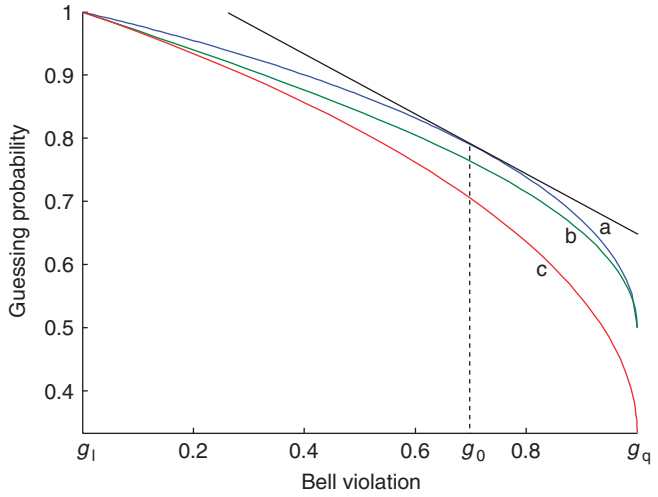

Figure 1 | Guessing probability versus Bell violation. The figure shows the guessing probability $P_{\text{guess (a)}}$ versus the Bell violation g_{exp} for (a) the CHSH inequality, (b) the chained inequality with $n=3$ inputs[26] and (c) the Collins–Gisin–Linden–Massar–Popescu (CGLMP) inequality with $d=3$ outputs[30]. Note that the symmetry of these inequalities implies that the bounds on the guessing probabilities are the same for any inputs x_{raw} entering into their definition. The horizontal scale represents the relative violation ranging from the local bound g_{loc} to the maximal quantum bound g_q. The CHSH curve is given by the function (12), the chained and CGLMP inequalities curves have been obtained by solving the problem (14) using the SDP relaxations introduced in refs 23 and 24. These last two curves upper-bound the optimal values by at most $O(10^{-4})$. The solid line represents a linearization of the form (15) of the CHSH function around a point g_0.

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). In the case of the CHSH inequality, for instance, the following (tight) bound holds (Methods, see also ref. 22)

$$P_{\text{guess}}(a) \leq \frac{1}{2}+\frac{1}{2}\sqrt{2-\frac{g_{\text{exp}}^2}{4}}, \tag{12}$$

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

More generally, let

$$P_{\text{guess}}(a) \leq f(g_{\text{exp}}), \tag{13}$$

be a bound between the guessing probability and the Bell violation, where f is a concave and monotically decreasing function. Such a bound can always be obtained using the semidefinite programming (SDP) method introduced in refs 23 and 24. Indeed, the maximal value of the guessing probability $P_{\text{guess}}(a)$ for a given value of the Bell expectation g_{exp} corresponds to the solution of the following optimization problem

$$\begin{aligned} \max_{\rho,A,B} \quad & \text{tr}[\rho A(a\,|\,x_{\text{raw}})] \\ \text{subject to} \quad & \text{tr}[\rho G]=g_{\text{exp}}, \end{aligned} \tag{14}$$

where the maximum is taken over all quantum states ρ and measurement operators $A(a|x)$ and $B(b|y)$. Following refs 23 and 24, one can introduce a hierarchy of SDP relaxations of the problem (14). The solution to any of these SDP relaxations yields an upper-bound to the optimal solution of (14) and thus a bound of the form (13), as illustrated on Figure 1 for different Bell inequalities. The resulting function f is then always concave and monotonically decreasing, as follows from the convex nature of the problem (14) and of its associated SDP relaxations. Note that relaxations higher in the hierarchy necessitate more computational resources but yield better upper-bounds. In the asymptotic limit, one has the guarantee that these upper-bounds will converge to the exact maximum of (14), though usually a few steps in the hierarchy already give the optimal bound (this is the case for instance for the CHSH inequality).

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

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

valid for all a, g_0, and any set of measurements $A(a|x)$ and $B(b|y)$. A proof of the bound (13) for the CHSH inequality based on such operator inequalities is given in Methods. In general, the validity of any linear operator inequality of the form (17) can be established, independently of the Hilbert space dimension, using the dual formulation[25] of the SDP techniques introduced in refs 23 and 24.

We now move to the case of N pairs of systems described by (3) and (7) and evaluate the probability with which Eve can correctly guess the raw key $\mathbf{a}$ by measuring her side information $\mathcal{E}$. Suppose thus that Eve performs some measurement z on her system $\mathcal{E}$ and obtains an outcome e. Let $P(\mathbf{a}|\mathbf{x}_{\text{raw}}, ez)$ denote the probability distribution of $\mathbf{a}$ conditioned on Eve's information. On average, her probability to correctly guess $\mathbf{a}$ is given by $\Sigma_e P(e\,|\,z)\max_{\mathbf{a}} P(\mathbf{a}\,|\,\mathbf{x}_{\text{raw}},ez)$, and her optimal correct-guessing probability (optimized over all measurements z) is[21]:

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

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

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

Consider the following N-partite Bell operator

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

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

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

To show this, write $A'_i=A_i(a_i\,|\,x_{\text{raw}})$ and $G'_i=\mu(g_0)1+\nu(g_0)G_i$. We thus want to establish that $\Pi_{i=1}^N G'_i-\Pi_{i=1}^N A'_i \geq 0$. 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 $\Pi_{i=1}^N G'_i-\Pi_{i=1}^N A'_i=\Pi_{i=1}^N(Z_i+A'_i)-\Pi_{i=1}^N A'_i=\Pi_{i=1}^N Z_i+Z_1\Pi_{i=2}^N A'_i+\ldots+\Pi_{i=1}^{N-1}A'_i Z_n$. Inequality (21) then follows

from the fact that each term in this sum is positive as it is the product of operators that are positive and, according to (5), commuting.

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

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

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

Note now that the quantity $\text{tr}[\rho_{\text{AB}} \mathbf{G}(g_0)]$ 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 ref. 15, 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 ref. 15 implies that the inequality

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

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 ref. 21 that the (quantum) min-entropy $H_{\text{min}}(\mathbf{a}|\mathcal{E})$ of a state of the form (7) is given by

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

which implies the asymptotic secret-key rate

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

This bound on the secret-key rate constitutes the main result of our work. As mentioned previously, the second term $H(a|b)$ is standard and quantifies the amount of communication needed for the error-correcting phase. The non-trivial part of our bound corresponds to the first term, which quantifies the knowledge of Eve and thus the amount of privacy amplification needed to make her information arbitrarily small.

Key rate of specific protocols. We now illustrate the above formalism on two DIQKD protocols, based, respectively, on the chained inequality[17,26] for $n=2$ and $n=3$ inputs. This inequality reads

$$g_c = \sum_{a,b} \sum_{x=0}^{n-1} \sum_{y=x-1}^{x} (-1)^{a+b+\delta(y)} q(ab\,|\,xy) \leq 2, \tag{27}$$

where a, $b \in \{0,1\}$ and x, $y \in \{0,1,\ldots n-1\}$; the $\delta(y)=1$ when $y=-1$ and zero otherwise. Note that for $n=2$, the chained inequality reduces to the CHSH inequality.

In both protocols, the observed correlations $P(\boldsymbol{ab}|\boldsymbol{xy})$ are obtained by measuring a two-qubit maximally entangled state $|\phi\rangle = |00\rangle + |11\rangle$ along n possible directions for Alice and $n+1$ for Bob. The inputs $x_{\text{raw}} = n-1$ and $y_{\text{raw}} = n$ correspond to measurements in the computational basis $\{|0\rangle, |1\rangle\}$ and are used to generate the raw key. The chained inequality violation is estimated using the inputs x, $y \in \{0,\ldots,n-1\}$ and the corresponding measurement directions are setup to obtain the maximal violation of the chained inequality given by $2\sqrt{2}$ and $3\sqrt{3}$ for the cases $n=2$ and $n=3$, respectively. For the sake of illustration, let us assume that the effect of the noise in the protocol amounts to the distribution of an entangled state $v|\phi\rangle\langle\phi| + (1-v)1/4$ of visibility v. The conditional Shannon entropy $H(a|b)$ is then equal to $h[(1-v)/2]$, where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy, and the observed Bell violations are equal to $g = 2\sqrt{2}v$ and $g = 3\sqrt{3}v$. For the CHSH inequality, we then obtain using (12) and (26) the key rate

$$R \geq 1 - \log_2 \left[1 + \sqrt{2 - 2v^2} \right] - h[(1-v)/2]. \tag{28}$$

The value of the visibility such that this bound is equal to zero corresponds to a quantum-bit-error rate of 5%. The key rate for the chained inequality for $n=3$ is plotted in Figure 2, based on the SDP bound of Figure 1. The critical visibility corresponds to a quantum-bit-error rate of 7.5%, comparable to those obtained for standard QKD. Numerical evidence suggests that the chained inequalities for a larger number of settings, $n>3$, provide worse lower bounds on the key rate.

Discussion

We have shown how to compute a bound on the key rate of a large class of DIQKD protocols (it is easy to see that our security proof can also be adapted to cover the less efficient protocols introduced in refs 7 and 27, or protocols with pre-processing of the raw key[17]). Our approach is based on a fundamental relation between the amount by which two quantum systems violate a Bell inequality and the unpredictability of their local measurement outcomes, as illustrated in Figure 1. A similar relation has been used in the context of device-independent randomness generation[22].

Compared with the security proof given in refs 5, 8 and 13, which is restricted to protocols based on the CHSH inequality[18], our approach is completely general and can be applied to protocols based on arbitrary Bell inequalities. This is particularly interesting from a practical point of view. As shown in Figure 2, using inequalities other than CHSH may lead to better key rates in the presence of noise. It could also be very useful to improve the resistance of DIQDK protocols to photon detection inefficiencies[11], as relevant improvements over CHSH can be obtained in realistic situations[28].

To derive our security proof, we have used the fact that the behaviour of N uses of the quantum devices is represented by probabilities of the form (3) with measurement operators satisfying the commutation relations (5). These commutation relations can be satisfied in a physical realization in which N pairs of separated and non-interacting devices are used to generate the N symbols of the raw key. If necessary, these commutation relations can be enforced by shielding the devices in such a way that no communication between them occurs during the measurement process. Note that if the provider of the quantum apparatuses is untrusted, shielding of the devices is anyway required to guarantee that they do not send unwanted information to the adversary. Admittedly, a realization requiring N different devices for the generation of N raw-key symbols is impractical. Our results nevertheless show that secure fully device-independent QDK with key rates comparable to those of traditional QKD is in principle possible.

In a more realistic implementation, the raw key is generated by repeatedly performing measurements on a single pair of devices. In such a sequential implementation, the description provided by equations (3) and (5) corresponds to the assumption that the functioning of the measuring devices does not depend on an internal memory storing the quantum states and measurement results obtained at previous steps. Although it would be desirable to extend our security proof to cover such possible memory effects, it may be reasonable to expect our no-memory condition to be satisfied in a variety of practical setups. After all, this no-memory condition is assumed in standard QKD, in which the description of the devices

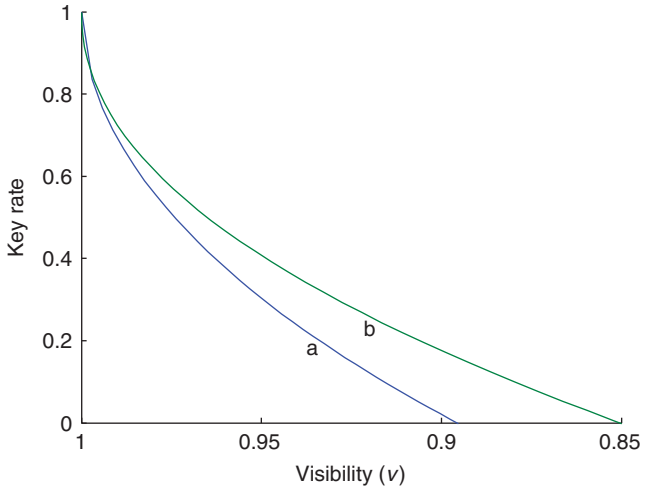

Figure 2 | Key rate versus visibility. The figure shows the key rate as a function of the visibility for (a) the CHSH inequality and (b) the chained inequality with three inputs. The key rate is given by the formula (26) where the function f is given by (12) for the CHSH inequality and has been obtained by solving the problem (14) using the SDP relaxations introduced in refs. 23, 24 for the chained inequality (see Fig. 1). Interestingly for the particular type of noise illustrated here, the chained inequality leads to better key rate than CHSH.

fits in the formalism of equations (3)–(5). But although we make here no assumptions at all on the measurement operators A_i $(a_i|x_i)$, B_i $(b_i|y_i)$ (nor on the Hilbert spaces on which they are defined), in standard QKD one assumes that these measuring operators have a fixed and known value, which is identical for all i—an idealized assumption difficult to verify in practise. From this perspective, the DIQKD model considered here clearly represents a relaxation of standard QKD, and thus can only be more secure.

Note that the no-memory assumption allows for devices whose behaviour may vary with time (as implied by the dependence of A_i $(a_i|x_i)$ on the subindex i), it only excludes, for example, that the response of the devices at step j depends on the particular measurement input at step $j-k$. Such kind of memory effects can arguably be excluded if no explicit memory has been introduced in the devices or if an 'initialization' procedure is performed before every measurement, based on an estimation of the apparatus memory characteristics. It may thus be legitimate to assume for particular implementations that no imperfections, failures or implementation weaknesses would create detrimental memory effects (even though imperfections could be exploited in other ways by an eavesdropper). From this perspective, our work contributes to narrow the gap between theoretical security proofs and practical realizations of QKD.

While this manuscript was in preparation, closely related results to those presented here were independently obtained[29].

Methods

Guessing probability versus CHSH inequality violation. In this section, we show how a tight bound on the guessing probability (10) can be derived from the CHSH inequality. Let $P(a,b|x,y)$ with $a, b, x, y \in \{0,1\}$ be a quantum distribution of the form

$$P(ab|xy) = \mathrm{tr}[\rho A(a|x) B(b|y)] \tag{29}$$

and let $g = \Sigma_{a,b,x,y} (-1)^{a+b+xy} P(ab|xy)$ be the corresponding CHSH expectation. We establish here that

$$P(a|x) \leq \frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{g^2}{4}} \tag{30}$$

for all $a, x \in \{0,1\}$, which implies inequality (12) of the main text. We consider only the case $a=0$ and $x=0$ (the argument applies by symmetry to the other cases as well).

Let $G = \Sigma_{a,b,x,y} (-1)^{a+b+xy} A(a|X) B(b|y)$. Following the discussion after equation (15) in the main text, inequality (30) is equivalent for $g_0 \in [2, 2\sqrt{2}]$ to the series of operator inequalities

$$A(0|0) \leq \frac{1}{2} + \frac{1}{\sqrt{2 - \frac{g_0^2}{4}}} - \frac{g_0}{8\sqrt{2 - \frac{g_0^2}{4}}} G, \tag{31}$$

since $f'(g) = -g/\left(8\sqrt{2 - g^2/4}\right)$. By increasing the dimension of the Hilbert space, we can always take the measurement operators $A(a|x)$ and $B(b|y)$ to be projection operators. Define then operators $A_x = A(a=0|x) - A(a=1|x)$ and $B_y = B(b=0|y) - B(b=1|y)$. It is easily verified that these new operators are hermitian and satisfy $A_x^2 = 1$ and $B_y^2 = 1$. In term of these operators, we can rewrite inequality (31) as

$$\frac{1}{2} + \frac{1}{2} A_0 \leq \frac{1}{2} + \frac{1}{\sqrt{2 - \frac{g_0^2}{4}}} - \frac{g_0}{8\sqrt{2 - \frac{g_0^2}{4}}} G, \tag{32}$$

where $G = A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1$ We now prove this operator inequality. For this, let $\alpha = 1/(\sqrt{8 - g_0^2})$, $\gamma_1 = \sqrt{\alpha}/4$, $\gamma_2 = -g_0\sqrt{\alpha}/8$, $\gamma_3 = g_0/(16\sqrt{\alpha})$, $\gamma_4 = 1/(8\sqrt{\alpha})$ and $\gamma_5 = (1 - g_0^2/4)\sqrt{\alpha}/4$, and define the following four operators

$$\begin{aligned}
O_1 &= -2\gamma_1 A_2 - \gamma_2(B_1 - B_2) + \gamma_3(A_2B_1 + A_2B_2) \\
O_2 &= -2\gamma_2 - 2\gamma_3 A_1 + \gamma_4(B_1 + B_2) \\
&\quad -\gamma_1(A_1B_1 + A_1B_2) + \gamma_5(A_2B_1 - A_2B_2) \\
O_3 &= -\gamma_4(B_1 - B_2) + \gamma_1(A_1B_1 - A_1B_2) \\
&\quad -\gamma_5(A_2B_1 + A_2B_2) \\
O_4 &= 2\gamma_4 - 2\gamma_5 A_1 + \gamma_2(B_1 + B_2) - \gamma_3(A_2B_1 - A_2B_2),
\end{aligned}$$

Using the fact that $A_x^2 = 1$, $B_y^2 = 1$, and $[A_x, B_y] = 0$, the following algebraic idendity is easily verified

$$\sum_i O_i^\dagger O_i = -\frac{1}{2} A_0 \otimes 1 + \frac{1}{\sqrt{2 - \frac{g_0^2}{4}}} - \frac{g_0}{8\sqrt{2 - \frac{g_0^2}{4}}} G. \tag{33}$$

Note now that as the left hand side is a sum of square, it is necessarily positive semidefinite, that is, $\Sigma_i O_i^\dagger O_i \geq 0$, which immediately implies (32). Note that we have established inequality (30) only for $g_0 \in [2, 2\sqrt{2}[$. The bound for $g_0 = 2\sqrt{2}$ follows from the fact that the function $f(g)$ corresponding to the right-hand side of (30) is concave and monotonically decreasing and hence $f(2\sqrt{2}) \leq \lim_{\varepsilon \to 0} f(2\sqrt{2} - \varepsilon) = 1/2$.

Finally, we show that inequality (30) is optimal, that is, that there exists quantum states and operators that saturate the inequality. Consider the two-qubit state $\cos\theta|00\rangle + \sin\theta|11\rangle$, and the measurement operators $A_0 = \sigma_z \otimes 1$, $A_1 = \sigma_x \otimes 1$, $B_0 = 1 \otimes \cos\phi\sigma_z + \sin\phi\sigma_x$ and $B_1 = 1 \otimes \cos\phi\sigma_z - \sin\phi\sigma_x$, where $\tan\phi = \sin 2\theta$ and $2\sqrt{1 + \sin^2(2\theta)} = g$. It is straightforward to see that the corresponding quantum probabilities $P(\boldsymbol{ab}|\boldsymbol{xy})$ saturate the inequality (30) for all values of $g \in [2, 2\sqrt{2}]$.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India 175–179 (1984).
2. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation 286405250problems arXiv:0906.4547.
3. Xu, F., Qi, B. & Lo, H.- K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution 286404887system. *New J. Phys.* **12,** 113026 (2010)arXiv:1005.2376.
4. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4,** 686–689 (2010).
5. Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S. & Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
6. Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Inform. Comput.* **4,** 273–286 (2004).
7. Acín, A., Gisin, N. & Masanes, L.l. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97,** 120405 (2006).
8. Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S. & Scarani, V. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11,** 045021 (2009).
9. Ekert, A. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).

10. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
11. Gisin, N., Pironio, S. & Sangouard, N. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.* **105,** 070501 (2010).
12. Canetti, R. Universally composable security: a new paradigm for cryptographic protocols. *Proc. 42nd IEEE Symp. Found. Comput. Sci. (FOCS)* 136–145 (2001).
13. McKague, M. *Quantum Information Processing with Adversarial Devices*. PhD thesis, University of Waterloo, Canada, arXiv:1006.2352.
14. Masanes, L.l. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.* **102,** 140501 (2009).
15. Masanes, Ll., Renner, R., Christandl, M., Winter, A. & Barrett, J. Unconditional security of key distribution from causality 286405294constraints arXiv:quant-ph/0606049.
16. Hänggi, E., Renner, R. & Wolf, S. Quantum cryptography based solely on Bell's 286218786theorem. *EUROCRYPT* 216–234 (2010).
17. Acín, A., Massar, S. & Pironio, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.* **8,** 126 (2006).
18. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880–884 (1969).
19. Carter, J. L. & Wegman, M. N. Universal classes of hash functions. *J. Comput. Sys. Sci.* **18,** 143–154 (1979).
20. Csiszár, I. & Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **24,** 339–348 (1978).
21. Koenig, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55** (2009).
22. Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D. N. & Maunz, P. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021 (2010).
23. Navascues, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98,** 010401 (2007).
24. Navascues, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **11,** 045021 (2009).
25. Pironio, S., Navascues, M. & Acín, A. Convergent relaxations of polynomial optimization problems with non-commuting variables. *SIAM J. Optim.* **20,** 2157–2180 (2010).
26. Braunstein, S. L. & Caves, C. M. Wringing out better Bell inequalities. *Ann. Phys.* **202,** 22–56 (1990).
27. Horodecki, K. *et al.* Contextuality offers device-independent security arXiv:1006.0468.
28. Vertesi, T., Pironio, S. & Brunner, N. Closing the detection loophole in Bell experiments using qudits. *Phys. Rev. Lett.* **104,** 060401 (2010).
29. Hänggi, E. & Renner, R. Device-independent quantum key distribution with commuting measurements arXiv:1009.1833.
30. Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88,** 040404 (2002).

Acknowledgments

This work is supported by the Spanish MEC/MINCIN projects QTIT (FIS2007-60182) and QOIT (Consolider Ingenio 2010), EU Integrated Project Q-Essence and ERC Starting Grant PERCENT, Caixa Manresa, Generalitat de Catalunya and the Brussels-Capital region through a BB2B grant.

Author contributions

L.M., S.P. and A.A. equally contributed to the ideas underlying this work, the calculations, and the writing of the article.

Additional information

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Masanes, L. *et al.* Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* 2:238 doi: 10.1038/ncomms1244 (2011).