UNIVERSITÉ DE GENÈVE

Archive ouverte UNIGE

https://archive-ouverte.unige.ch

Article scientifique Article 2005 Published version Open Access

This is the published version of the publication, made available in accordance with the publisher's policy.

Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication

Kraus, Barbara; Gisin, Nicolas; Renner, R.

How to cite

KRAUS, Barbara, GISIN, Nicolas, RENNER, R. Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication. In: Physical review letters, 2005, vol. 95, n° 8. doi: 10.1103/PhysRevLett.95.080501

This publication URL: https://archive-ouverte.unige.ch/unige:36762

Publication DOI: 10.1103/PhysRevLett.95.080501

© This document is protected by copyright. Please refer to copyright holder(s) for terms of use.

Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication

B. Kraus,[1] N. Gisin,[1] and R. Renner[2]

[1]*Group of Applied Physics, University of Geneva, CH-Geneve, Switzerland*
[2]*Computer Science Department, ETH-Zürich, Switzerland*

(Received 6 February 2005; published 15 August 2005)

We investigate a general class of quantum key distribution (QKD) protocols using one-way classical communication. We show that full security can be proven by considering only collective attacks. We derive computable lower and upper bounds on the secret-key rate of those QKD protocols involving only entropies of two-qubit density operators. As an illustration of our results, we determine new bounds for the Bennett-Brassard 1984, the 6-state, and the Bennett 1992 protocols. We show that in all these cases the first classical processing that the legitimate partners should apply consists in adding noise.

DOI: 10.1103/PhysRevLett.95.080501 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum cryptography, the art of exploiting quantum physics to defeat any possible eavesdropper, has rapidly grown over the past decade from the level of a nice idea into an entire branch of physics [1]. Indeed, the first commercial equipment are already offered [2].

A generic quantum key distribution (QKD) protocol can be divided into two parts: (I) distribution of quantum information and measurement, and (II) a classical part consisting in parameter estimation (PE) and classical post-processing (CPP). To implement the quantum part of the protocol, the two legitimate persons, Alice (A) and Bob (B), agree on some encoding or decoding procedure [3]. We denote by $S_0 = \{|\phi_j^0\rangle\}_{j\in J}$ and $S_1 = \{|\phi_j^1\rangle\}_{j\in J}$, where $J = \{1, \ldots, m\}$, the sets of states used to encode the bit values 0 and 1, respectively. First, A sends n qubits prepared at random in the state $|\phi_{j_1}^{i_1}\rangle \otimes \cdots \otimes |\phi_{j_n}^{i_n}\rangle \equiv |\phi_{\mathbf{j}}^{\mathbf{i}}\rangle$ to B [4]. The adversary, Eve (E), interacts now with all the qubits sent by A. She applies a unitary transformation (since she is restricted to the laws of quantum mechanics) to all those qubits and an ancilla in the state $|0\rangle$. The state of E and B is then given by $|\Phi_{\mathbf{j}}^{\mathbf{i}}\rangle_{BE} \equiv \mathcal{U}_{BE}|\phi_{\mathbf{j}}^{\mathbf{i}}\rangle_B|0\rangle_E$. Next, B applies some filtering operation, which might be unitary as in the case of the Bennett-Brassard 1984 (BB84) or the 6-state protocol, and measures his qubits in the z basis. A and B compare publicly which encoding or decoding operation they used and keep only those pairs of qubits where they were compatible (sifting). The state describing E's system is $|\Phi_{\mathbf{j}}^{\mathbf{i},\mathbf{k}}\rangle_E \equiv \langle\mathbf{k}|B_{\mathbf{j}}U_{BE}|\phi_{\mathbf{j}}^{\mathbf{i}}\rangle_B|0\rangle_E$, where we denoted by B the filtering operation used by B and by $\mathbf{k}$ his z-measurement outcome [5]. A and B now compare publicly some of their measurement outcomes to estimate the quantum bit error rate (QBER).

The security of the protocol relies on the fact that E, trying to gain information about the bit values, introduces some errors due to the laws of quantum mechanics. However, any realistic channel used by A and B is noisy, i.e., QBER > 0. In order to ensure that the protocol is secure, one must assume that all the noise (estimated by A and B) is due to an unlimited eavesdropping attack, a coherent attack [6,7]. A and B know how to counter such an adversary: they apply a CPP, consisting in error correction (EC) and privacy amplification (PA). This general principle leaves a central question open: How much error can be tolerated in order to be able to distill a secret key? This is precisely what we concentrate on in this Letter.

Many security proofs are based on the following observations [8–11]. Instead of preparing a system and then sending it to B, A can equivalently prepare B's system at a distance by using an entangled state (entanglement-based scheme [12]) [13]. If A and B could distill their state to singlets, their systems cannot be entangled to E. The essential feature of the distillation can be carried out processing only classical data, leading to perfectly correlated data.

We present here a different kind of security proof, which is not based on entanglement distillation and that applies to a general class of QKD protocols including the BB84, the 6-state, and the Bennett 1992 (B92) protocols [14–16]. First of all, we determine the state shared by A and B (using the entanglement-based scheme) after a general eavesdropping attack. Then we analyze the classical part of the protocol, i.e., PE and CPP, for the case of one-way communication. We present a new formula for the secret-key length. Then we derive a lower bound on the secret-key rate involving only entropies of two-qubit density operators. We also present an upper bound on the secret-key rate. At the end we illustrate our results by determining new values for the lower bounds on the secret-key rate for the protocols mentioned above. These new bounds are generally stronger than those achievable with entanglement-based security proofs.

To study the entanglement-based scheme, we use the same notation as before and define the encoding operators $A_j = |0\rangle\langle(\phi_j^0)^*| + |1\rangle\langle(\phi_j^1)^*|$ and the decoding operators $B_j = |0\rangle\langle\hat{\phi}_j^1| + |1\rangle\langle\hat{\phi}_j^0|$, where $|\hat{\phi}_j^i\rangle$ denotes the orthogonal state to $|\phi_j^i\rangle$ and $|(\phi_j^i)^*\rangle$ denotes the complex conjugate of $|\phi_j^i\rangle$ in the computational basis for $i = 0, 1$ and $j \in J$. Note that those operators are not necessarily unitary, e.g.,

© 2005 The American Physical Society

for the B92 protocol. After applying one of those encoding or decoding operations, A and B measure in the z basis, associating with the outcome the bit values 0 or 1. Using the facts that $A^T \otimes \mathbb{1}|\Phi^+\rangle = \mathbb{1} \otimes A|\Phi^+\rangle$ for any operator A and $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ and that the operators applied on A's systems commute with the operator applied by E, it is easy to verify that $|\Phi_{\mathbf{j}}^{\mathbf{i},\mathbf{k}}\rangle_E = {}_A\langle\mathbf{i}|_B\langle\mathbf{k}|\Phi_{\mathbf{j}}\rangle_{ABE}$, where $|\Phi_{\mathbf{j}}\rangle_{ABE} = A_{\mathbf{j}} \otimes B_{\mathbf{j}} U_{BE}|\Phi^+\rangle_{AB}^{\otimes n}|0\rangle_E$.

To account for all the different realizations ($\mathbf{j}$), we introduce a new system R_1 and define the state $|\chi_0\rangle_{ABER} = \Sigma_{\mathbf{j}} \frac{1}{\sqrt{p_{\mathbf{j}}}}|\Phi_{\mathbf{j}}\rangle_{ABE}|\mathbf{j}\rangle_{R_1}$, with p_j determined by the probability with which A and B decide to keep the systems in case they used the operators $A_{\mathbf{j}}, B_{\mathbf{j}}$. Now, first of all, R_1 measures and obtains the outcome $\mathbf{j}$. The state shared by A, B, and E is then $|\Phi_{\mathbf{j}}\rangle_{ABE}$.

Let us now introduce an equivalent protocol where A and B additionally apply the following operations [17]: (I) A and B both apply the same unitary transformation $U_{\mathbf{1}'}$ chosen for each qubit at random among $U_1 = \mathbb{1}$, $U_2 = \sigma_z$, with the Pauli operator σ_z. The state describing E's system is then, up to a global phase, equivalent to $|\Phi_{\mathbf{j}}^{\mathbf{i},\mathbf{k}}\rangle_E$. (II) A and B can decide to flip their bit values (both at the same time). We combine the first two possible operations. The operator O_{l_i} denotes a unitary operator of the form $U_{l_i'}V_{l_i''}$, for $l_i', l_i'' \in \{1, 2\}$, and $V_1 = \mathbb{1}$, $V_2 = \sigma_x$. Since we assume that both apply the same operation, they need to coordinate their actions via classical communication. This exchanged classical information is denoted by $\boldsymbol{l}$. (III) A and B are also free to permute their bits, i.e., qubits before the measurement in the z basis. Obviously, they have to use the same permutation operator, $P_{\mathbf{m}}$. The classical information that has to be exchanged is denoted by $\mathbf{m}$.

We introduce now two random number generators, R_2 and R_3, which account, respectively, for the operators, $O_{\boldsymbol{l}}$ and $P_{\mathbf{m}}$. The state describing all the systems is $|\chi\rangle_{ABER_1R_2R_3} = \Sigma_{\mathbf{j},\boldsymbol{l},\mathbf{m}} \frac{1}{\sqrt{p_{\mathbf{j}}}}|\Phi_{\mathbf{j},\mathbf{l},\mathbf{m}}\rangle_{ABE}|\mathbf{j}\rangle_{R_1}|\boldsymbol{l}\rangle_{R_2}|\mathbf{m}\rangle_{R_3}$, with $|\Phi_{\mathbf{j},\boldsymbol{l},\mathbf{m}}\rangle_{ABE} = P\mathbf{m}O_lA_j \otimes P\mathbf{m}O_lB_{\mathbf{j}}U_{BE}|\Phi^+\rangle_{AB}^{\otimes n}|0\rangle_E$, the state shared by A, B, and E for the particular realization $(\mathbf{j}, \boldsymbol{l}, \mathbf{m})$.

Let us now relax the assumptions about E. We provide E with all the systems R_1, R_2, R_3. Since she can measure the R systems ending up in the same situation as before [E knows the classical information $(\mathbf{j}, \boldsymbol{l}, \mathbf{m})$], we clearly provide her with at least as much power as she had before. The state A and B share is given by the partial trace of the state $|\chi\rangle_{ABER_1R_2R_3}$ over E, R_1, R_2, R_3. We find $\rho_{AB}^n = \mathcal{P}_S\{\mathcal{D}_2^{\otimes n}[\mathcal{D}_1^{\otimes n}(\rho_{AB}^0)]\}$, where the normalized state $\rho_{AB}^0 = \mathrm{tr}_E(P_{|\psi_0\rangle})$ with $|\psi_0\rangle = U_{BE}|\Phi^+\rangle_{AB}^{\otimes n}|0\rangle_E$. Here, and in the following, we use the notation $P_{|\Phi\rangle} = |\Phi\rangle\langle\Phi|$ for any state $|\Phi\rangle$. $\mathcal{P}_S$ denotes the completely positive map (CPM) symmetrizing the state with respect to all qubit pairs. The CPM $\mathcal{D}_1$ is entirely defined by the protocol and is given by $\mathcal{D}_1(\rho) = \Sigma_{\mathbf{j}} \frac{1}{p_{\mathbf{j}}} A_{\mathbf{j}} \otimes B_{\mathbf{j}}(\rho)A_{\mathbf{j}}^\dagger \otimes B_{\mathbf{j}}^\dagger$. $\mathcal{D}_2$ is independent of the protocol, and is defined as $\mathcal{D}_2(\rho) = \Sigma_l O_l \otimes O_l(\rho)O_l^\dagger \otimes O_l^\dagger$, i.e., the depolarization map transforming any two-qubit state into a Bell-diagonal state. This implies that the density operator A and B share, before their measurement in the z basis, has for any protocol the simple form

$$\rho_{AB}^n = \sum \lambda_{n_1,n_2,n_3,n_4} \mathcal{P}_S(P_{|\Phi_1\rangle}^{\otimes n_1} \otimes P_{|\Phi_2\rangle}^{\otimes n_2} \otimes P_{|\Phi_3\rangle}^{\otimes n_3} \otimes P_{|\Phi_4\rangle}^{\otimes n_4}). \quad (1)$$

Here, the sum is performed such that $n_4 = n - n_1 - n_2 - n_3$, with $n_i \geq 0$. The states $|\Phi_{1/2}\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$ and $|\Phi_{3/4}\rangle = 1/\sqrt{2}(|10\rangle \pm |01\rangle)$ denote the Bell basis. Note that this state is separable with respect to the different qubit pairs. Note further that this result Eq. (1) is independent of the CPP; thus, it can also be used in order to investigate any protocol employing two-way CPP.

Let us summarize this part of the Letter. Let ρ_{AB} be a density operator, which is measured by A and B in a certain basis (say, the z basis). Assume that E has a purification of ρ_{AB}; i.e., the state describing A's, B's, and E's system is $|\Psi\rangle_{ABE}$ such that $\rho_{AB} = \mathrm{tr}_E(P_{|\Psi_{ABE}\rangle})$, for some state $|\Psi_{ABE}\rangle$. We call an operator ρ_{AB}' *in the measurement basis reducible* to ρ_{AB} if (1) ρ_{AB}' leads to the same measurement statistics for the measurement of A and B as ρ_{AB}, and (2) providing E with a purification of the state ρ_{AB}' can only increase her power (compared to the case where A and B share the state ρ_{AB} and E has a purification of this state). Any state of the form $\rho_{AB}' = \Sigma_i p_i O_i \otimes \mathbb{1}\rho_{AB}O_i^\dagger \otimes \mathbb{1}$, with $p_i \geq 0$, $\Sigma_i p_i = 1$ and unitary operators O_i diagonal in the measurement basis, i.e., $O_i|j\rangle = \lambda_i^j|j\rangle$, with $|\lambda_i^j|^2 = 1$, leads to the same measurement statistics, i.e., $|i, j\rangle \times \langle i, j|\rho_{AB}'|i, j\rangle\langle i, j| = |i, j\rangle\langle i, j|\rho_{AB}|i, j\rangle\langle i, j|$, $\forall\ i, j$. Obviously, the same holds for operators acting on B's system [see, for instance, the unitary operators presented in (I)]. We have shown above that these operators are reducible to ρ_{AB}. Thus, if the measurement basis is known, we can choose any of those reducible operators. If, furthermore, A and B symmetrize their qubit pairs by the operations that commute with the measurement, like the ones described in (II) and (III), then the state describing their qubits has the form of Eq. (1). Providing E then with a purification of this state might only increase her power.

In order to analyze the classical part of the protocol, we partially use some of the information-theoretic arguments [18,19], which have first been proposed in [20] in order to analyze the security of a large class of QKD protocols [21]. We assume that A (B) hold strings X^n (Y^n), obtained by measuring a given state ρ_{AB}^n, Eq. (1).

Let us consider the CPP consisting of three steps. The protocol is one-way, i.e., only communication from, say A to B, is needed. (I) *Preprocessing:* Using her bit string X^n, A computes two strings U^n and V^n, according to given conditional probability distributions $P_{U|X}$ and $P_{V|U}$, respectively. She keeps U^n and sends V^n to B. (II) *Information reconciliation:* A computes error correcting information W from U^n and sends W to B. Using his information, Y^n and W, B computes a guess $\hat{U}^n$ for U^n.

(III) *Privacy amplification:* A randomly chooses a function F from a family of two-universal hash functions and sends a description of F to B. Then A and B compute their keys, $S_A = F(U^n)$ and $S_B = F(\hat{U}^n)$, respectively.

Let us introduce some notation before analyzing this protocol. We describe the classical information of A and B as well as the quantum information of E by a tripartite density operator ρ_{XYE} of the form $\rho_{XYE}^n = \Sigma_{x,y} P_{X^nY^n}(x, y) P_{|x\rangle} \otimes P_{|y\rangle} \otimes \rho_E^{x,y}$ where $\{|x\rangle\}_x$ and $\{|y\rangle\}_y$ are families of orthonormal vectors and where $\rho_E^{x,y}$ is the quantum state of E given that A's and B's values are x and y, respectively. Similarly, $\rho_{S_AS_BE'}$ describes the classical key pair (S_A, S_B) together with the adversary's information $\rho_{E'}$ after the protocol execution. We say that (S_A, S_B) is ε *secure* if $\mathrm{tr}|\rho_{S_AS_BE'} - \Sigma_{s\in} P_{|s\rangle} \otimes P_{|s\rangle} \otimes \rho_{E'}| \leq \varepsilon$. Note that this definition leads to the so-called *universally composable* security, which implies that the key can safely be used in *any* arbitrary context [18].

To determine the number ℓ_n^ε of ε-secure key bits that can be generated by the above protocol, we use the following recent results: (I) The amount of key that can be extracted from a string U^n is given by the uncertainty of the adversary about U^n, measured in terms of the so-called *smooth Rényi entropy,* $S_2^{\varepsilon'}$, $S_0^{\varepsilon'}$ [18], as introduced in [22]. (II) The amount of information B needs to correct his errors, using optimal error correction, is given by his uncertainty about A's string (again measured in terms of the smooth Rényi entropy). Combining those results we find for the number of ε-secure bits [23],

$$\ell_n^\varepsilon \approx \sup_{V^n \leftarrow U^n \leftarrow X^n} [S_2^{\varepsilon'}(\rho_{UEV}^n) - S_0^{\varepsilon'}(\rho_{EV}^n) - H_0^{\varepsilon'}(U^n|Y^nV^n)],$$

where "$\approx$" means that equality holds up to some small term independent of n and ε' is a function of ε that vanishes as ε tends to zero. In this formula, ρ_{UEV}^n is the density operator describing the string U^n together with the adversary's knowledge [24]. The supremum is taken over all preprocessing applied by A.

We show now how a lower bound on the secret rate, $r: = \lim_{n\to\infty}(\ell_n^\varepsilon/n)$, can be determined considering only two-qubit density operators. To this aim, we first of all fix some preprocessing by A. We assume that it is bitwise; i.e., for each bit value X_i she computes U_i and V_i [25]. At the end we take the supremum with respect to all those preprocessings.

Because of the symmetry (with respect to the qubit pairs) of the state ρ_{AB}^n we can assume, without loss of generality, that the first $n_{\mathrm{p.e.}}$ qubits are used for the PE and the rest, n_{data}, are used to generate the key. Choosing $n_{\mathrm{p.e}}$ sufficiently large guarantees that the data qubits contain the same amount of error as estimated in the PE phase. Since the only free parameters of ρ_{AB}^n are its eigenvalues $\lambda_{n_1,n_2,n_3,n_4}$ the outcome of the PE implies very strong conditions on them [Eq. (1)]. In fact, conditioned on this outcome, the data qubits can be described by some state $\rho_{|Q}^n$, where $Q = (n_1, n_2, n_3, n_4)/n$ is the frequency distribution (depending on the PE outcome) of a Bell measurement. The state $\rho_{|Q}^n$ has similar properties as the product state $\sigma_Q^{\otimes n}$, where σ_Q is a two-qubit Bell-diagonal state with eigenvalues Q. Because of this similarity, one can show that the smooth Rényi entropies of those states are the same. Finally, using the fact that the smooth Rényi entropy of a product state is asymptotically equal to the von Neumann entropy [22], we obtain the following lower bound on the secret rate [23]:

$$r \geq \sup_{\substack{U\leftarrow X\\ V\leftarrow U}} \inf_{\sigma_{AB}\in\Gamma_{\mathrm{QBER}}} [S(U|VE) - H(U|YV)]. \tag{2}$$

In this formula, $S(U|VE)$ denotes the von Neumann entropy of U conditioned on V and E, i.e., $S(U|VE) := S(\sigma_{UVE}) - S(\sigma_{VE})$. The state σ_{UVE} is obtained from σ_{AB} by taking a purification σ_{ABE} of the Bell-diagonal state $\mathcal{D}_2[\mathcal{D}_1(\sigma_{AB})]$, i.e., Eq. (1) for $n = 1$, and applying the measurement of A followed by the classical channels $U \leftarrow X$ and $V \leftarrow U$. Similarly, Y is the outcome of B's measurement applied to the second subsystem of σ_{ABE}. The set Γ_{QBER} contains all two-qubit states, σ, for which the protocol computes a secret key when starting with the state $\sigma^{\otimes n}$, where σ is any state that A and B might share after a collective attack by E. Thus, in order to prove full security for this class of QKD protocols one has to consider only collective attacks. Note that, in order to compute a lower bound, V can be discarded. *A priori,* one might think that also the preprocessing $X \longrightarrow U$ could not be of any help, since the only choice A has is to flip each bit value with some probability, i.e., to introduce noise. However, this noise differs clearly from the channel's noise. Although it diminishes A's mutual information with B, it may more severely penalize E.

In order to derive this bound, we assume that Eve has a purification of the state σ, which is always possible as long as the encoding or decoding operators (A_j, B_j) are unitary. This implies that, for instance, for the BB84 and the 6-state protocols, coherent attacks are not more powerful than collective attacks [26].

Because of the fact that the states $\mathcal{D}_2[\mathcal{D}_1(\Gamma_{\mathrm{QBER}})]$ are measured in the z basis, we have $\lambda_1 = 1 - Q - \lambda_2$, $\lambda_4 = Q - \lambda_3$, where $Q = \mathrm{QBER}$, denotes the averaged error (with respect to the errors occurring in the different bases). The considered protocol, i.e., the map $\mathcal{D}_1$, implies then additional conditions on the λ's. Using similar ideas, one can derive the same bound as in Eq. (2), but with σ_{ABE} being the purification $\mathcal{D}_2(\sigma_{AB})$. Γ_{QBER} could then be defined as the set of two-qubit density operators leading to the same error in the different bases [23].

Using techniques from quantum information theory, one can show that if the supremum on the right-hand side of Eq. (2) is also taken over any quantum state ρ_{UV} computed from X, then it is also an upper bound for the rate r, i.e., $r \leq \min_\rho \sup_{V\leftarrow U\leftarrow X}[S(\rho_{UEV}) - S(\rho_{EV}) - H(U|VY)]$, where the minimum is taken over all states $\rho = \rho_{ABE}$ that can be generated by an attack of E [27].

Let us now illustrate our result for several protocols. For the BB84 protocol the encoding or decoding operators are $A_1 = B_1 = V_x$ and $A_2 = B_2 = \mathbb{1}$, where V_x is the Hadamard transformation. It is easy to verify that $\mathcal{D}_2[\mathcal{D}_1(\rho_0)] = (1 - Q - \lambda_1)P_{|\Phi^+\rangle} + \lambda_1 P_{|\Phi^-\rangle} + \lambda_1 P_{|\Psi^+\rangle} + (Q - \lambda_1)P_{|\Psi^-\rangle}$ with $0 \leq \lambda_1 \leq Q$ for any state ρ_0. We find for the optimal values $\lambda_1 = Q - Q^2$ and $q \rightarrow 0.5$, the probability for A to flip the bit value, that the secret-key rate is positive for all $Q \leq 0.124$. Without the preprocessing by A, we would obtain the well-known bound 0.110 [8,20]. For the upper bound we obtain the known result that the protocol is not secure if the QBER is higher than 0.146 [28]. For the 6-state protocol we find that the secret-key rate is positive as long as $Q < 0.141$ (known result 0.127 [9]). On the other hand, the protocol is insecure for all $Q \geq 0.162$. For the B92 protocol we find a positive rate as long as $\delta \leq 0.027$ (known result $\delta \leq 0.024$ [10,20]), where δ characterizes the depolarization of a channel introducing the same amount of noise.

Before we conclude, let us note that if we would restrict E to individual attacks [6], Eq. (2) would be, apart from the preprocessing, equivalent to the bound widely studied and sometimes called Csiszár and Körner bound. Also in this simplified case the preprocessing turns out to be important. For instance, for the 6-state protocol numerical optimization shows that for all nonzero QBERs it is always advantageous for A to first add some noise to her data, before the EC and PA.

To conclude, we studied the security of a class of QKD protocols, including BB84, 6-state, and B92 protocols, among many others. We presented a new security proof not based on entanglement distillation for all those protocols using one-way CPP. We show that in order to prove full security one has only to consider collective attacks. We derived a computable lower bound on the secret-key rate involving only entropies of two-qubit density operators. It is shown that A should add noise before the EC and PA phases. The state A and B share before the EC and PA is then separable, which might prevent an entanglement-based proof of security to work there. We illustrated our results by presenting new bounds on all the protocols mentioned above.

N. G. and B. K. thank the Swiss NCCR "Quantum photonics" and the European IST project SECOQC.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] http://www.idquantique.com; http://www.magiqtech.com.

[3] We consider here only qubits; however, a generalization to higher-dimensional systems is straightforward.

[4] A bold letter, $\boldsymbol{l}$, denotes the vector $(l_1, \ldots, l_n)$. A vector as a superscript always denotes associated bit values, whereas a vector as a subscript denotes the used encoding.

[5] U_{BE} might no longer be unitary here since we consider the state after the sifting; however, this will not change the following arguments.

[6] We distinguish between (I) Individual attacks: $U_{BE} = U_1^{\otimes n}$ and independent measurement of auxiliary systems right after E knows $\mathbf{j}$; (II) Collective attacks: $U_{BE} = U_1^{\otimes n}$ and collective measurement at the very end of the protocol, including the CPP; (III) Coherent attacks: general unitary and measurement at the very end of the protocol.

[7] E might be able to replace the channel with an ideal channel. However, it is reasonable to assume that the detector noise is not under E's control. Thus, we consider here only the situation of a noisy channel.

[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[9] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).

[10] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[11] On the other hand, the security proofs presented in D. Mayers, *Advances in Cryptology—CRYPTO 1996*, Lecture Notes in Computer Science Vol. 1109 (Springer, New York, 1996), p. 343 and E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the 32nd Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 2000), p. 715, are based on information-theoretic methods.

[12] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[13] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[14] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer Systems and Signal Processing* (IEEE, New York, 1984), p. 175.

[15] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[16] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[17] By "equivalent" we mean that we do not change the quantum part of the protocol and the information of A, B, and E is not changed.

[18] R. Renner and R. König, in *Proceedings of Theory of Cryptography Conference 2005*, Lecture Notes in Computer Science Vol. 3378 (Springer, New York, 2005).

[19] R. König, M. Maurer, and R. Renner, quant-ph/0305154.

[20] M. Christandl, R. Renner, and A. Ekert, quant-ph/0402131).

[21] The proof technique introduced in [20] is based on the result of [19] and the fact that the rank of a purification of A's and B's system can be bounded.

[22] R. Renner and S. Wolf, in *Proceedings of ASIACRYPT 2005*, Lecture Notes in Computer Science (Springer-Verlag, New York, 2005), p. 233.

[23] For details see R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[24] Since V^n is sent from A to B over an insecure channel, E might know these values as well.

[25] Note that a bitwise processing might not be optimal; however, a generalization to a multibit preprocessing is straightforward.

[26] Note that if we would consider a multibit preprocessing, then also the states in the generalized expression of Eq. (2) would be higher dimensional.

[27] A similar upper bound has been presented in I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[28] Ch. Fuchs, R. B. Griffiths, Ch. Sh. Niu, A. Peres, and N. Gisin, Phys. Rev. A **56**, 1163 (1997).