Eur. Phys. J. D **37**, 441–450 (2006)
DOI: 10.1140/epjd/e2005-00314-3

THE EUROPEAN PHYSICAL JOURNAL D

Provable entanglement and information cost for qubit-based quantum key-distribution protocols

G.M. Nikolopoulos[a], A. Khalique, and G. Alber

Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany

Received 26 July 2005
Published online 22 November 2005 –

Abstract. Provable entanglement has been shown to be a necessary precondition for unconditionally secure key generation in the context of quantum cryptographic protocols. We estimate the maximal threshold disturbance up to which the two legitimate users can prove the presence of quantum correlations in their data, in the context of the four- and six-state quantum key-distribution protocols, under the assumption of coherent attacks. Moreover, we investigate the conditions under which an eavesdropper can saturate these bounds, by means of incoherent and two-qubit coherent attacks. A direct connection between entanglement distillation and classical advantage distillation is also presented.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication

1 Introduction

Quantum key-distribution (QKD) protocols exploit quantum correlations in order to establish a secret key between two legitimate users (Alice and Bob). In a typical quantum cryptographic scheme, after the transmission stage Alice and Bob must process their raw key, in order to end up with identical random keys about which an adversary (Eve) has negligible information. In principle, classical as well as quantum algorithms (distillation protocols) can be used for this post-processing [1–10]. In any case, it is necessary for Alice and Bob to estimate the error rate in their sifted key, for the purpose of detecting the presence of Eve on the channel.

An important quantity for any QKD protocol is the threshold disturbance i.e., the maximal disturbance or *quantum bit error rate* (QBER) which can be tolerated by Alice and Bob for being capable of producing a secret key. This threshold disturbance quantifies the robustness of the QKD scheme under consideration against a specific eavesdropping strategy, and depends on the algorithm that Alice and Bob are using for post-processing their raw key. Up to date, the robustness of the four-state (BB84) [11] and the six-state [12] QKD protocols has been mainly discussed on the basis of the so-called Csiszár-Körner criterion [6] and/or incoherent attacks, and various bounds have been obtained [13–21]. Moreover, it is also known that a necessary precondition for unconditionally secure QKD is that the correlations established between Alice and Bob during the state distribution cannot be explained in the framework of separable states (*provable entanglement*) [22,23]. Clearly, the threshold disturbance up to which this precondition is satisfied under the assumption of general coherent (joint) attacks, quantifies the ultimate robustness bound of a particular QKD protocol.

In a recent paper [24], we proved that for QKD protocols using two mutually unbiased bases, this threshold disturbance for provable entanglement (robustness bound) scales with the dimension d of the information carriers as $(d-1)/2d$. Thus for the BB84 QKD protocol ($d = 2$) [11], Alice and Bob always share provable entanglement for estimated disturbances below 1/4. Extending our studies, in this paper it is shown that the corresponding threshold disturbance for entanglement distillation in the context of the six-state QKD protocol [12] is 1/3.

Our studies show that even the most powerful eavesdropping attacks are not able to disentangle the two legitimate users for estimated disturbances below these borders. In other words, Eve is not able to decrease the robustness of the protocols. The natural question arises, however, is whether and at which cost these disentanglement thresholds can be attained in the framework of eavesdropping attacks that maximize Eve's properties (information gain and/or probability of success in guessing). In this paper we address this open question in the context of incoherent as well as two-qubit coherent attacks. In particular, we present evidence that in the limit of many pairs, coherent attacks might be able to disentangle the two honest parties at the lowest threshold disturbance while simultaneously maximizing Eve's probability of success in guessing correctly the transmitted signal.

This paper is organized as follows: in Section 2 we briefly describe the prepare-and-measure as well as the associated entanglement-based versions of the BB84 and the six-state QKD protocols. The corresponding threshold

[a] e-mail: nikolg@physik.tu-darmstadt.de

disturbances for provable entanglement (robustness bounds) are derived in Section 3, while in Section 4 we investigate the cost at which an eavesdropper can saturate these bounds. A link between entanglement distillation and classical advantage distillation protocols is discussed in Section 5.

2 Basic facts about BB84 and six-state protocols

For the sake of completeness, in this section we briefly summarize basic facts about the two qubit-based QKD protocols especially in connection with their verification-test stage.

2.1 Prepare-and-measure schemes

In the prepare-and-measure BB84 protocol [11], Alice sends a sequence of qubits to Bob each of which is randomly prepared in one of the basis states $\{|0\rangle, |1\rangle\}$ or $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ which are eigenstates of two maximally conjugated physical variables, namely the two Pauli spin operators $\mathcal{Z}$ and $\mathcal{X}$. The eigenstates of $\mathcal{Z}$, i.e. $\{|0\rangle, |1\rangle\}$, and of $\mathcal{X}$, i.e. $\{|\bar{0}\rangle, |\bar{1}\rangle\}$, are related by the Hadamard transformation

$$\mathcal{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1}$$

i.e. $|\bar{i}\rangle = \sum_j \mathcal{H}_{ij} |j\rangle$ $(i, j \in \{0, 1\})$. In the computational basis $\{|0\rangle, |1\rangle\}$, the Pauli spin operators are represented by the matrices

$$\mathcal{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathcal{Y} = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \mathcal{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2}$$

Bob measures the received qubits randomly in one of the two bases. After the transmission stage, Alice and Bob apply a random permutation of their data and publicly discuss the bases chosen, discarding all the bits where they have selected different bases. Subsequently, they randomly select a number of the bits from the remaining random key (sifted key) and determine their *error probability* or QBER. If, as a result of a noisy quantum channel or of an eavesdropper, the estimated QBER is too high the protocol is aborted. Otherwise, Alice and Bob perform error correction and privacy amplification with one- or two-way classical communication, in order to obtain a smaller number of secret and perfectly correlated random bits [1–5].

The six-state prepare-and-measure scheme is quite similar to the BB84 (four-state) scheme [12]. More precisely, Alice and Bob use at random three bases namely, the two bases used in the BB84 plus an additional one $\{|\bar{\bar{0}}\rangle, |\bar{\bar{1}}\rangle\}$ which corresponds to the $\mathcal{Y}$ Pauli operator. In analogy to BB84, the three bases are related (up to a global phase) via the transformation

$$\mathcal{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -\mathrm{i} \\ 1 & \mathrm{i} \end{pmatrix}, \tag{3}$$

i.e. $|\bar{i}\rangle = \sum_j \mathcal{T}_{ij} |j\rangle$ and $|\bar{\bar{i}}\rangle = \sum_j \mathcal{T}_{ij}^2 |j\rangle$ with $i, j \in \{0, 1\}$.

2.2 Entanglement-based schemes

It has been shown that, from the point of view of an arbitrarily powerful eavesdropper, each one of these two prepare-and-measure schemes is equivalent to an entanglement-based QKD protocol [25–31]. These latter forms of the protocols offer advantages, in particular with respect to questions concerning their unconditional security, and work as follows: Alice prepares each of, say $2n$, entangled-qubit pairs in a particular Bell state [32], say $|\Psi^-\rangle \equiv (|0_\mathrm{A}1_\mathrm{B}\rangle - |1_\mathrm{A}0_\mathrm{B}\rangle)/\sqrt{2}$ (where the subscripts A, B refer to Alice and Bob, respectively). This state is invariant under any unitary transformation of the form $\mathcal{U}_A \otimes \mathcal{U}_B$. Alice keeps half of each pair and submits the other half to Bob after having applied a random unitary transformation chosen either from the set $\{\mathbf{1}, \mathcal{H}\}$ (two-basis protocol) or from the set $\{\mathbf{1}, \mathcal{T}, \mathcal{T}^2\}$ (three-basis protocol).

At the end of the transmission stage, Alice announces publicly the transformations she applied on the transmitted qubits and Bob reverses all of them. At this stage, in an ideal scenario Alice and Bob would share $2n$ pairs in the state $|\Psi^-\rangle^{\otimes 2n}$. Due to channel noise and the presence of a possible eavesdropper, however, at the end of the transmission stage all the $2n$ entangled-qubit pairs will be corrupted. In fact, they will be entangled among themselves as well as with Eve's probe. Thus, the next step for Alice and Bob is to estimate the number of singlets among the $2n$ shared pairs (alternatively to estimate the fraction of pairs which are in error). To this end, they apply a verification test which proceeds as follows: firstly, Alice and Bob permute randomly all the pairs, distributing thus any influence of the channel noise and the eavesdropper equally among all the pairs [4,27]. Afterwards, they randomly select a number (say n_c) of the pairs as check pairs, they measure each one of them *separately* along a common basis and they publicly compare their outcomes. The influence of channel noise or of an eavesdropper is thus quantified by the average estimated QBER of the check pairs while, assuming that the check pairs constitute a fair sample [33], the estimated QBER applies also to the remaining, yet unmeasured, $2n - n_\mathrm{c}$ pairs.

After the verification test all the check pairs are dismissed and, if the QBER is too high the protocol is aborted. Otherwise, Alice and Bob apply an appropriate entanglement purification protocol (EPP) with classical one- or two-way communication [8,9] on the remaining $2n - n_\mathrm{c}$ pairs, in order to distill a smaller number of almost pure entangled-qubit pairs. Finally, measuring these almost perfectly entangled-qubit pairs in a common basis, Alice and Bob obtain a secret random key, about which an adversary has negligible information.

2.3 Verification test and confidence level

In closing this introductory part of the paper let us recall some known basic facts about the verification test which are necessary for the subsequent discussion. The reasons for which such a classical random sampling

procedure applies to a quantum scenario have been thoroughly discussed in the literature [4,26–31]. Briefly, the *commuting-observables* idea allows us to reduce any quantum eavesdropping attack (even a joint one) to a classical probabilistic cheating strategy, for which classical probability theory can be safely applied [26,29]. Furthermore, Eve does not know in advance which pairs will be used for quality checks and which pairs will contribute to the final key. Thus she is not able to treat them differently and the check pairs constitute a fair [33] classical random sample of all the pairs [4,26,27]. By invoking the verification test therefore the two legitimate users can be confident that (with high probability) the estimated error rate is also the error rate they would have measured if they were able to perform a Bell measurement projecting their pairs onto a $2n$-pair Bell basis [26,29,30]. The confidence level is determined by classical random sampling theory [34]. In particular, the conditional probability that the verification test is passed given that Alice and Bob underestimate the error rate in their pairs is exponentially small in the sample-size $n_{\rm c}$ (i.e., $\sim 2^{-n_{\rm c}}$) [26,29]. In other words the probability that Eve cheats successfully can be made arbitrarily small by choosing a sufficiently large sample.

3 Provable entanglement and threshold disturbances

According to a recent observation, a *necessary precondition* for secret key distillation is that the correlations established between Alice and Bob during the state distribution cannot be explained by a separable state [22,23]. Throughout this work, we consider that Alice and Bob focus on the sifted key during the post-processing (i.e., they discard immediately all the polarization data for which they have used different bases) and that they treat each pair independently. Thus, according to the aforementioned precondition, given a particular value of the estimated QBER (observable), the task of Alice and Bob is to infer whether they share provable entanglement or not. Thereby, entanglement is considered to be provable if Alice's and Bob's correlations cannot be explained by a separable state within the framework of the protocols (including post-processing) and observables under consideration.

Recently [24], for the same post-processing, we estimated the threshold disturbance for provable entanglement in the context of two-basis qudit-based QKD protocols under the assumption of joint eavesdropping attacks. In particular, we showed that for estimated disturbances below $(d-1)/2d$ (where d is the size of the information carriers), Alice and Bob can be confident that they share provable entanglement with probability exponentially close to one (see Sect. 2.3). In this section, for the sake of completeness, we briefly recapitulate the main steps of our proof adapted to the BB84 scheme. Subsequently, along the same lines, we estimate the corresponding threshold disturbance for the six-state QKD scheme. For the sake of consistency, we will adopt the entanglement-based versions of the protocols. We would like to stress, however, that the estimated threshold disturbances characterize both versions of the protocols.

3.1 BB84 protocol

Given the unitarity and hermiticity of $\mathcal{H}$, the average disturbance (average error probability per qubit pair), that Alice and Bob estimate during the verification test is given by [4,24,27]

$$D = \frac{1}{2n_{\rm c}} \sum_{b=0,1} \sum_{j_i;i=1}^{n_{\rm c}} {\rm Tr}_{A,B}\Big\{ \left[\mathcal{H}_{AB}^{b}\ \mathcal{P}\ \mathcal{H}_{AB}^{b}\right]_{j_i}\ \rho_{AB}\Big\}, \quad (4)$$

with the projector [35]

$$\mathcal{P}_{j_i} = \sum_{l=0,1} |l_A, l_B\rangle\langle l_A, l_B| = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|\,, \quad (5)$$

and $\mathcal{H}_{AB}^{b} \equiv \mathcal{H}_{A}^{b} \otimes \mathcal{H}_{B}^{b}$. The last equality in (5) indicates that the verification test is nothing more than a quality-check test of the fidelity of the $2n$ pairs with respect to the ideal state $|\Psi^-\rangle^{\otimes 2n}$ [4,26–31]. The state ρ_{AB} in equation (4) denotes the reduced density operator of Alice and Bob for all $2n$ pairs while the index j_i indicates that the corresponding physical observable refers to the j_ith randomly selected qubit pair. The powers of the Hadamard transformations $\mathcal{H}^b$, with $b \in \{0,1\}$, reflect the fact that the errors in the sifted key originate from measurements in both complementary bases which have been selected randomly by Alice and Bob with equal probabilities.

As we mentioned in Section 2.3 one of the crucial cornerstones for the unconditional security of the protocol is that Eve does not know in advance which pairs will be used for quality checks and which pairs will contribute to the final key. Thus she is not able to treat them differently and the check pairs constitute a classical random sample of all the pairs [4,26–28]. To ensure such a homogenization, Alice and Bob permute all of their pairs randomly before the verification stage. In view of this homogenization, the eavesdropping attack (although a joint one) becomes symmetric on all the pairs [4,27] i.e., $\rho_{AB}^{(1)} = \rho_{AB}^{(2)} = \cdots = \rho_{AB}^{(2n)}$. Here, the reduced density operator of Alice's and Bob' s kth pair is denoted by $\rho_{AB}^{(k)} = {\rm Tr}_{AB}^{(\not k)}(\rho_{AB})$ and ${\rm Tr}_{AB}^{(\not k)}$ indicates the tracing (averaging) procedure over all the qubit pairs except the kth one. Accordingly, the average estimated disturbance (4) reads [24]

$$D = \frac{1}{2}\sum_{b=0}^{1} {\rm Tr}_{A,B}^{(j_1)}\Big\{ \left[(\mathcal{H}_{A}^{b} \otimes \mathcal{H}_{B}^{b})\ \mathcal{P}\ (\mathcal{H}_{A}^{b} \otimes \mathcal{H}_{B}^{b})\right]_{j_1} \rho_{AB}^{(j_1)}\Big\} \quad (6)$$

where ${\rm Tr}_{A,B}^{(j_1)}$ denotes the tracing procedure over the j_1th qubit pair of Alice and Bob. So, an arbitrary eavesdropping attack which gives rise to a particular reduced single-pair state $\rho_{AB}^{(j_1)}$ is indistinguishable, from the point of view

of the estimated average disturbance, from a corresponding collective (individual) attack which results in a decorrelated $2n$-pair state of the form $\bigotimes_{j=1}^{2n} \rho_{AB}^{(j)}$.

Our purpose now is to estimate the threshold disturbance $D_{\rm th}$ such that for any estimated $D < D_{\rm th}$ Alice and Bob can be confident that their correlations cannot have emerged from a separable state. To this end let us explore the symmetries underlying the observable under consideration i.e., the estimated average QBER. According to equations (6) and (5), D is invariant under the transformations

$$(l, b) \to (l \oplus_2 1, b), \quad (l, b) \to (l, b \oplus_2 1), \tag{7}$$

where $\oplus_2$ denotes addition modulo 2. This invariance implies that the reduced density operators $\rho_{AB}^{(j_1)}$ and

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{8} \sum_{g \in \mathcal{G}_1, h \in \mathcal{G}_2} U(h) U(g) \rho_{AB}^{(j_1)} U(g)^\dagger U(h)^\dagger \tag{8}$$

give rise to the same observed value of the QBER [24]. The unitary and hermitian operators appearing in equation (8) form unitary representations of two discrete Abelian groups $\mathcal{G}_1 = \{g_1, g_2, g_3, g_4\}$ and $\mathcal{G}_2 = \{h_1, h_2\}$, and are given by

$$\begin{aligned} U(g_1) &= \mathcal{X}_A \otimes \mathcal{X}_B, \quad & U(g_2) &= \mathcal{Z}_A \otimes \mathcal{Z}_B, \\ U(g_3) &= -\mathcal{Y}_A \otimes \mathcal{Y}_B, \quad & U(g_4) &= \mathbf{1}_A \otimes \mathbf{1}_B, \end{aligned} \tag{9}$$

and

$$U(h_1) = \mathcal{H}_A \otimes \mathcal{H}_B, \quad U(h_2) = \mathbf{1}_A \otimes \mathbf{1}_B. \tag{10}$$

Moreover, invariance of the average QBER under the symmetry transformations of equation (7) induces invariance of $\tilde{\rho}_{AB}^{(j_1)}$ under both discrete Abelian groups $\mathcal{G}_1$ and $\mathcal{G}_2$.

The key point is now that $\rho_{AB}^{(j_1)}$ and $\tilde{\rho}_{AB}^{(j_1)}$ differ by local unitary operations and convex summation. Thus the density operator $\rho_{AB}^{(j_1)}$ is entangled if $\tilde{\rho}_{AB}^{(j_1)}$ is entangled. Our main problem of determining the values of the QBER for which Alice and Bob share provable entanglement can be reduced therefore to the estimation of the values of D for which the most general two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ (which is invariant under both Abelian discrete groups) is entangled.

The hermitian operators $U(g_1)$ and $U(g_2)$ of the group $\mathcal{G}_1$ constitute already a *complete set of commuting operators* in the Hilbert space of two qubits and the corresponding eigenstates are the Bell states [32]. Thus, the most general two-qubit state which is invariant under the Abelian group $\mathcal{G}_1$ is given by

$$\begin{aligned} \tilde{\rho}_{AB}^{(j_1)} = {} & \lambda_{00} |\Phi^+\rangle\langle\Phi^+| + \lambda_{10} |\Phi^-\rangle\langle\Phi^-| \\ & + \lambda_{01} |\Psi^+\rangle\langle\Psi^+| + \lambda_{11} |\Psi^-\rangle\langle\Psi^-|, \end{aligned} \tag{11}$$

with $\lambda_{\alpha\beta} \geq 0$ and

$$\sum_{\alpha,\beta \in \{0,1\}} \lambda_{\alpha\beta} = 1, \tag{12}$$

while additional invariance under the discrete group $\mathcal{G}_2$ implies that

$$\lambda_{01} = \lambda_{10}. \tag{13}$$

Thus, the state (11) with the constraint (13) is the most general two-qubit state invariant under the Abelian groups $\mathcal{G}_1$ and $\mathcal{G}_2$.

For later convenience let us rewrite the state $\tilde{\rho}_{AB}^{(j_1)}$ in the computational basis, i.e.

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{2} \begin{pmatrix} D & 0 & 0 & G \\ 0 & F & H & 0 \\ 0 & H & F & 0 \\ G & 0 & 0 & D \end{pmatrix}, \tag{14}$$

with $F = 1 - D$ denoting the so-called fidelity, i.e. the total probability for Bob to receive the submitted signal undisturbed. Furthermore, the remaining parameters are given by

$$\begin{aligned} D &= \lambda_{00} + \lambda_{10}, \quad & F &= \lambda_{01} + \lambda_{11}, \\ G &= \lambda_{00} - \lambda_{10}, \quad & H &= \lambda_{01} - \lambda_{11}, \end{aligned} \tag{15}$$

with D denoting the disturbance (QBER). In general, the parameters G and H can be expressed in terms of the overlaps between different states of Eve's probe and are thus intimately connected to the eavesdropping strategy. The key point for the subsequent discussion, is that for the estimation of the threshold disturbance it is not required to know the explicit form of the "macroscopic" parameters G and H and their detailed dependences on Eve's attack. More precisely, using equations (15), the constraints (12) and (13) read

$$F + D = 1 \tag{16}$$

$$F + H = D - G \tag{17}$$

respectively, while non-negativity of the eigenvalues $\lambda_{\alpha\beta}$ implies

$$D \geq |G|, \tag{18}$$

$$F \geq |H|. \tag{19}$$

The possible values of the estimated disturbance for which $\tilde{\rho}_{AB}^{(j_1)}$ is entangled can be estimated by means of the fully-entangled fraction (see [24]) or the Peres-Horodecki criterion [36]. Using the latter, we have that $\tilde{\rho}_{AB}^{(j_1)}$ is separable *if and only if* the inequalities

$$D \geq |H|, \tag{20}$$

$$F \geq |G|, \tag{21}$$

are satisfied. As depicted in Figure 1, these last inequalities combined with inequalities (18, 19) and equations (16, 17) imply that the symmetrized state $\tilde{\rho}_{AB}^{(j_1)}$ is entangled if and only if the estimated QBER is below 1/4 or above 3/4. Given, however, that the states $\tilde{\rho}_{AB}^{(j_1)}$ and

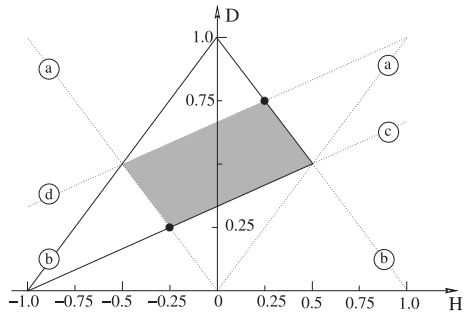

Fig. 1. BB84 protocol: region of the independent parameters D(QBER) and H for which the two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ is separable (shaded region). The various constraints that these parameters satisfy are indicated by straight dotted lines. Specifically, (a) equation (20); (b) equation (19); (c) equations (18) and (16, 17); (d) equations (21) and (16, 17). The protocol operates in the region which is defined by the solid lines.

$\rho_{AB}^{(j_1)}$ are related via local operations and convex summation, the original single-pair state $\rho_{AB}^{(j_1)}$ must also be entangled in the same regime of parameters. Moreover, the probability that the QBER has been underestimated during the verification test is exponentially small in n_c (see Sect. 2.3 and related references). Hence we may conclude that, whenever Alice and Bob detect an average QBER below 1/4 (or above 3/4), they can be confident that they share entanglement with probability exponentially close to one ($\sim 1 - 2^{-n_c}$), and their correlations cannot have originated from a separable state. The necessary precondition for secret-key distillation is therefore fulfilled for estimated disturbances within these intervals.

On the contrary, for $1/4 \leq D \leq 3/4$ we have that $\tilde{\rho}_{AB}^{(j_1)}$ is separable. Of course, this does not necessarily imply that $\rho_{AB}^{(j_1)}$ is also separable. But it does indicate that in this regime of parameters, Alice's and Bob's correlations within the framework of the BB84 protocol can be explained by a separable state, namely by $\tilde{\rho}_{AB}^{(j_1)}$. So, according to [22,23], this implies that Alice and Bob cannot extract a secret key and must abort the protocol. From now on we focus on the regime of practical interest ($F \geq D$), where the lowest possible threshold disturbance ($D_{\rm th} = 1/4$) is attained for $G = H = -1/4$.

3.2 Six-state protocol

The threshold disturbances for the six-state protocol can be determined in the same way. In this case, however, all three bases are used with the same probabilities and thus the average estimated disturbance (QBER) reads

$$D = \frac{1}{3}\sum_{b=0}^{2} \mathrm{Tr}_{A,B}^{(j_1)} \left\{ \left[\left(\mathcal{T}_A^b \otimes \mathcal{T}_B^b \right) \mathcal{P} \left(\mathcal{T}_A^{b\dagger} \otimes \mathcal{T}_B^{b\dagger} \right) \right]_{j_1} \rho_{AB}^{(j_1)} \right\} \tag{22}$$

where the unitary (but not hermitian) transformation $\mathcal{T}$ is defined in equation (3).

In analogy to the BB84 protocol, exploiting the symmetries underlying equation (22) one finds that D is invariant under the transformations

$$(l,b) \to (l \oplus_2 1, b), \quad (l,b) \to (l, b \oplus_3 1), \quad (l,b) \to (l, b \oplus_3 2), \tag{23}$$

with $\oplus_3$ denoting addition modulo 3. Furthermore, the invariance of D under the transformations (23) implies that the reduced density operators $\rho_{AB}^{(j_1)}$ and

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{12} \sum_{g \in \mathcal{G}_1, t \in \mathcal{G}_3} U(t) U(g) \rho_{AB}^{(j_1)} U(g)^\dagger U(t)^\dagger \tag{24}$$

yield the same average QBER. This latter state is invariant under the discrete Abelian groups $\mathcal{G}_1$ [with elements given in Eq. (9)] and $\mathcal{G}_3 = \{t_1, t_2, t_3\}$ with elements

$$U(t_1) = \mathcal{T}_A \otimes \mathcal{T}_B, \quad U(t_2) = \mathcal{T}_A^2 \otimes \mathcal{T}_B^2, \quad U(t_3) = \mathbf{1}_A \otimes \mathbf{1}_B. \tag{25}$$

The most general two-qubit state invariant under the Abelian groups $\mathcal{G}_1$ and $\mathcal{G}_3$ is now of the form (11), with

$$\lambda_{00} = \lambda_{10} = \lambda_{01}. \tag{26}$$

Thus, in the computational basis $\tilde{\rho}_{AB}^{(j_1)}$ is given by (14) with

$$D = 2\lambda_{00}, \quad F = \lambda_{11} + \lambda_{00}, \quad G = 0, \quad H = \lambda_{00} - \lambda_{11}. \tag{27}$$

Accordingly, condition (17) now reads

$$F + H = D, \tag{28}$$

while non-negativity of the eigenvalues $\lambda_{\alpha\beta}$ implies inequality (19) only. Finally, applying the Peres-Horodecki criterion one finds that $\tilde{\rho}_{AB}^{(j_1)}$ is separable *if and only if* inequality (20) is satisfied.

As a consequence of equations (16, 28) and $G = 0$, there is only one macroscopic independent parameter in our problem, say H, while combining inequalities (19) and (20) with equations (16) and (28) we obtain that the reduced density operator $\tilde{\rho}_{AB}^{(j_1)}$ is separable *iff* $1/3 \leq D \leq 2/3$ (Fig. 2). That is, no matter how powerful the eavesdropper is, Alice and Bob share always provable entanglement for estimated disturbances smaller than 1/3. The lowest disentanglement border for the six-state scheme ($D_{\rm th} = 1/3$) is attained for $H = -1/3$. It is also worth noting that, in contrast to BB84, in the six-state protocol there is only one disentanglement threshold since for $D > 2/3$ the protocol is not valid.

As expected, the bound for the six-state protocol is higher than the one for the BB84 protocol. In fact, as a consequence of the high symmetry of the six-state protocol, the disentanglement area of the BB84 scheme (shaded region in Fig. 1) shrinks to a line in Figure 2 (thick line). As will be seen later on, this "degeneracy" affects significantly the options of a potential eavesdropper in the framework of the six-state protocol, increasing thus the robustness of the protocol.

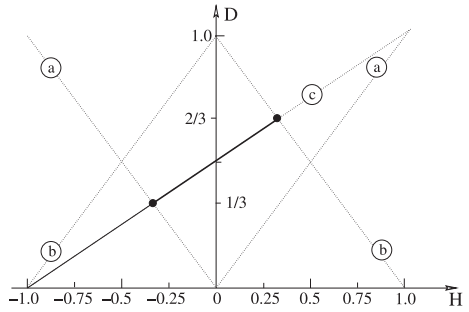

Fig. 2. Six-state protocol: region of the parameters D(QBER) and H for which the two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ is separable (thick solid line). The various constraints that these parameters satisfy are indicated by straight dotted lines. Specifically, (a) equation (20); (b) equation (19); (c) equations (16) and (28). The protocol operates along the solid lines.

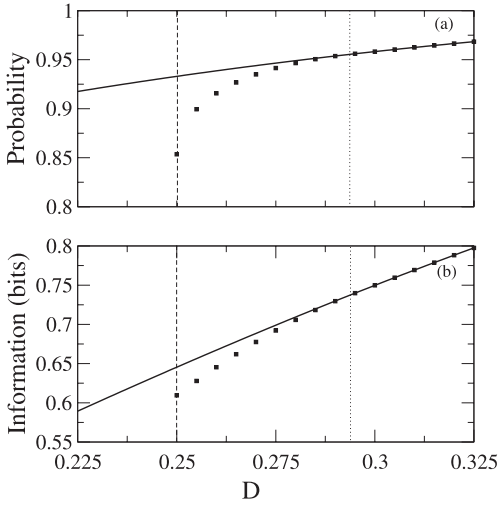

Fig. 3. BB84 protocol — Incoherent attacks: (a) Eve's probability of guessing correctly the transmitted message as a function of disturbance D. The solid line corresponds to an attack that maximizes Eve's probability of success in guessing, while each square denotes the corresponding probability for an attack which in addition, disentangles Alice and Bob at the specific disturbance. (b) As in (a) but for Eve's information gain. The vertical dotted lines correspond to the solid curves, and denote the disturbance $D^{(1)} \approx 30\%$ up to which Alice and Bob share an entangled state. The vertical dashed lines denote the lowest disentanglement threshold disturbance $D_{\rm th} = 1/4$ which can be attained in the context of general coherent attacks and intercept-resend strategies.

4 The price of disentanglement

In QKD issues, Eve's attack is usually optimized by maximizing her Shannon information (or the probability of her guessing correctly Alice's bit-string) conditioned on a fixed disturbance. Given, however, that the unconditional security of the BB84 and six-state cryptographic schemes is beyond doubt, Eve might be willing to reduce the robustness of the protocols to the lowest possible level while simultaneously maximizing any of her properties [19]. Thus, what remains to be clarified now is the cost at which Eve can saturate the lowest disentanglement threshold $D_{\rm th}$, in terms of her information gain and probability of correct guessing. To this end, we have to consider in detail the eavesdropping attack on the BB84 and the six-state protocols.

Such an investigation, however, is practically feasible only in the context of attacks on a few qubits. As the number of attacked qubit-pairs increases the complete treatment of the problem becomes intractable due to the large number of independent parameters involved. In this section we will focus on incoherent and two-qubit coherent attacks. The disentanglement of Alice and Bob in the framework of incoherent attacks has been extensively studied in the literature [17–21]. In most of these studies, however, Eve's attack is by default optimized to provide her with the maximal Shannon information. On the contrary, here we give Eve all the flexibility to adjust her parameters in order to break entanglement between Alice and Bob and simultaneously maximize her properties. Finally, for the two QKD protocols under consideration, we are not aware of any related previous work on disentanglement in the context of coherent attacks.

4.1 BB84 protocol

4.1.1 Incoherent attacks

Incoherent attacks belong to the class of the so-called single-qubit or individual attacks, where Eve manipulates each transmitted qubit individually. To this end, she attaches a single probe (initially prepared in e.g. state $|0_E\rangle$) to each transmitted qubit and lets the combined system undergo a unitary transformation of the form [13,37,38]

$$|0_B\rangle \otimes |0_E\rangle \rightarrow \sqrt{F}\,|0_B\rangle \otimes |\phi_0\rangle + \sqrt{D}\,|1_B\rangle \otimes |\theta_0\rangle,$$
$$|1_B\rangle \otimes |0_E\rangle \rightarrow \sqrt{F}\,|1_B\rangle \otimes |\phi_1\rangle + \sqrt{D}\,|0_B\rangle \otimes |\theta_1\rangle, \quad (29)$$

with F and D being the fidelity and disturbance respectively, while $|\phi_j\rangle$ and $|\theta_j\rangle$ are normalized states of Eve's probe when Bob receives the transmitted qubit undisturbed (probability F) and disturbed (probability D), respectively. Applying unitarity and symmetry conditions on this transformation one finds that the states $|\phi_j\rangle$ are orthogonal to the states $|\theta_j\rangle$ ($j \in \{0,1\}$), while the overlaps $\langle\phi_0|\phi_1\rangle$ and $\langle\theta_0|\theta_1\rangle$ are real-valued [13,37,38]. Thus, an incoherent attack can be described by the four parameters satisfying equations (16–19) with $H = -F\langle\phi_0|\phi_1\rangle$ and $G = -D\langle\theta_0|\theta_1\rangle$. In other words, there are only two independent parameters and by fixing one of them, say D, one is able to determine any property of the attack. In Figure 3, we present Eve's optimal information gain and probability of success in guessing the transmitted qubit correctly as functions of the disturbance (solid line). The optimization is performed in the usual way, i.e. for a fixed disturbance D, Eve's mutual information with Alice is maximized [13,38]. It is also known that such an optimized strategy disentangles the qubits of Alice and Bob

at $D^{(1)} \approx 30\%$ (vertical dotted line) [17], which is well above $D_{\rm th} = 25\%$. Thus, the natural question arises is whether, under the assumption of incoherent attacks, Eve can saturate the lowest possible disentanglement border $D_{\rm th}$ and if yes, at which cost of information loss.

To answer this question, for a fixed disturbance D, we calculated numerically all the possible values of G and H which are consistent with the constraints (16–19) and which yield a separable state of Alice and Bob. In general, at any given disturbance there is more than one combination of values of G and H which fulfill all these constraints. For each of these combinations, we calculated Eve's information gain and her probability of correct guessing [13,38]. The results presented as squares in Figure 3, refer to those combinations of parameters which, not only disentangle the two honest parties for a particular disturbance D, but which simultaneously maximize Eve's property as well. Clearly, for disturbances close to $D_{\rm th}$, the two strategies are not equivalent since they yield substantially different results. In other words, an optimal incoherent attack that maximizes Eve's information gain is certainly not the one which achieves the lowest possible robustness bound. Furthermore, our simulations show that saturation of $D_{\rm th} = 1/4$ is feasible at the cost of $\sim$4% less information gain of Eve or equivalently at the cost of $\sim$7.44% less probability of success in guessing.

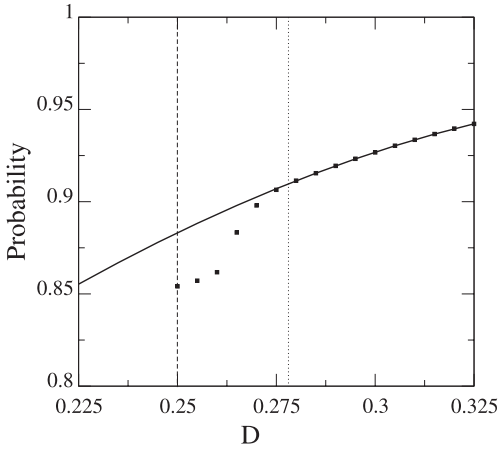

Fig. 4. BB84 protocol — Two-qubit coherent attacks: Eve's probability of guessing correctly a two-bit transmitted message as a function of disturbance D. The solid line corresponds to an attack that maximizes Eve's probability of success in guessing only, while each square denotes the corresponding probability for an attack that, in addition, disentangles Alice and Bob at the specified disturbance. The vertical dotted line corresponds to the solid curve, and denotes the disturbance $D^{(2)} \approx 28\%$ up to which Alice and Bob share an entangled state. The vertical dashed line denotes the lowest possible disentanglement threshold disturbance $D_{\rm th} = 1/4$ that can be attained in the context of general coherent attacks and intercept-resend strategies.

4.1.2 Two-qubit coherent attacks

In a two-qubit coherent attack, Eve attaches one probe to two of the qubits sent by Alice. Let $|m_B\rangle$ with $m \in \{0, 1, 2, 3\}$, be the message sent from Alice to Bob in binary notation. The combined system then undergoes a unitary transformation of the form [38]

$$\begin{pmatrix} |0_B\rangle \\ |1_B\rangle \\ |2_B\rangle \\ |3_B\rangle \end{pmatrix} \otimes |0_E\rangle \rightarrow \mathcal{E} \otimes \begin{pmatrix} |0_B\rangle \\ |1_B\rangle \\ |2_B\rangle \\ |3_B\rangle \end{pmatrix}, \qquad (30)$$

where $\mathcal{E}$ is a 4×4 matrix which contains normalized states in the Hilbert space of Eve's probe

$$\mathcal{E} \equiv \begin{pmatrix} \sqrt{\alpha}\,|\phi_0\rangle & \sqrt{\beta}\,|\theta_0\rangle & \sqrt{\beta}\,|\omega_0\rangle & \sqrt{\gamma}\,|\chi_0\rangle \\ \sqrt{\beta}\,|\theta_1\rangle & \sqrt{\alpha}\,|\phi_1\rangle & \sqrt{\gamma}\,|\chi_1\rangle & \sqrt{\beta}\,|\omega_1\rangle \\ \sqrt{\beta}\,|\omega_2\rangle & \sqrt{\gamma}\,|\chi_2\rangle & \sqrt{\alpha}\,|\phi_2\rangle & \sqrt{\beta}\,|\theta_2\rangle \\ \sqrt{\gamma}\,|\chi_3\rangle & \sqrt{\beta}\,|\omega_3\rangle & \sqrt{\beta}\,|\theta_3\rangle & \sqrt{\alpha}\,|\phi_3\rangle \end{pmatrix}.$$

The states ϕ_j, θ_j, ω_j and χ_j denote Eve's probe states in cases in which Bob receives all the transmitted qubits undisturbed, one qubit disturbed or both transmitted qubits disturbed.

Applying unitarity and symmetry conditions on equation (30), the problem can be formulated in terms of the following four mutually orthogonal subspaces [38]

$$S_\phi = \{\phi_0, \phi_1, \phi_2, \phi_3\}, \qquad S_\chi = \{\chi_0, \chi_1, \chi_2, \chi_3\},$$
$$S_\theta = \{\theta_0, \theta_1, \theta_2, \theta_3\}, \qquad S_\omega = \{\omega_0, \omega_1, \omega_2, \omega_3\},$$

while all the overlaps between the various states within each of these subspaces are real-valued. Thus, Eve is able to infer with certainty whether Bob has received both qubits undisturbed (S_ϕ), one qubit disturbed ($S_{\theta,\omega}$) or both qubits disturbed (S_χ). These events occur with probabilities α, 2β and γ, respectively. It can be shown that a general coherent two-qubit attack can be described in terms of five independent parameters [38]. The average reduced density matrix for Alice and Bob is then of the form (14), with $F = \alpha + \beta$, $D = \beta + \gamma$, $H = -(\alpha\langle\phi_0|\phi_1\rangle + \beta\langle\theta_0|\theta_2\rangle)$, $G = -(\gamma\langle\chi_0|\chi_1\rangle + \beta\langle\theta_0|\theta_1\rangle)$, satisfying the constraints (16–19).

Compared to an incoherent attack, a two-qubit coherent attack can improve the probability that Eve guesses correctly the whole two-bit message sent by Alice to Bob [38]. Eve's optimal probability of success in guessing is plotted in Figure 4 (solid line), as a function of disturbance D. This curve has been obtained by maximizing Eve's probability of success in guessing conditioned on a fixed disturbance D. For such an optimal attack, we found numerically that Alice and Bob share entanglement up to disturbances of the order of $D^{(2)} \approx 28\%$ (dotted vertical line). This is in contrast to the bound $D^{(1)} \approx 30\%$ attained in an optimal incoherent attack. Furthermore, we also found that Eve is able to saturate the lowest possible robustness bound (dashed vertical line), at the cost of $\sim$3% less probability of success in guessing. This loss of Eve's probability in guessing is substantially smaller than the corresponding loss for incoherent attacks ($\sim$7.44%). Thus, it could be argued that a two-qubit coherent attack which is optimized with respect to the probability

of guessing only, is very close to an optimal coherent attack which also disentangles Alice and Bob at $D_{\rm th} = 1/4$. The reason is basically that in a two-qubit coherent attack each one of the two independent macroscopic parameters G and H can be expressed in terms of two different overlaps whereas in incoherent attacks the corresponding dependences involve a single overlap only. In a coherent attack Eve has therefore more possibilities enabling her to push the disentanglement border towards the lowest possible value, while simultaneously maximizing her probability of guessing correctly the transmitted message.

4.2 Six-state protocol

So far, we have considered incoherent and coherent attacks in the context of the BB84 protocol where Eve's attack is determined by a set of two macroscopic parameters (G, H). These two independent parameters give a considerable flexibility to Eve since at a given disturbance there exists a variety of physically allowed attacks. This fact is also reflected in Figure 1 where, for a specific disturbance, Alice and Bob can be disentangled for different values of H (and therefore of G).

In the highly symmetric six-state protocol, however, the situation is much simpler. In fact, the high symmetry of the protocol reduces significantly the options of an eavesdropper since there is only one independent macroscopic parameter in our problem, namely H. Moreover, the analysis of the attacks under consideration becomes rather straightforward [39]. In particular, for incoherent attacks $G = -D\langle\theta_0|\theta_1\rangle = 0$ which indicates that Eve has full information about the disturbed qubits received by Bob. However, as depicted in Figure 2, at a given value of D there is a unique value of H consistent with the laws of quantum mechanics. It is determined by equations (16) and (28) [line (c) in Fig. 2]. Similarly, for the two qubit coherent attack we have $\langle\chi_0|\chi_1\rangle = \langle\theta_0|\theta_1\rangle = 0$ and thus $G = 0$, whereas $H = -(\alpha\langle\phi_0|\phi_1\rangle + \beta\langle\theta_0|\theta_2\rangle) = -(\alpha - \gamma) = 2D - 1$. As a result, for both incoherent and two-qubit coherent attacks, the physically allowed attack is the one that maximizes Eve's probability of guessing and simultaneously disentangles Alice and Bob at a given disturbance. It is sufficient for Eve therefore to optimize her attack with respect to her probability of correct guessing in order to disentangle Alice and Bob at the lowest possible disturbance.

5 Entanglement and intrinsic information

So far, we have discussed for both the four- and six-state protocols the maximal disturbance up to which Alice and Bob share entanglement. Clearly, this bound indicates that in principle secret-key generation is feasible by means of a quantum purification protocol. In this section we show that, at least in the context of incoherent attacks, a two-way classical protocol, the so-called advantage distillation protocol, exists which can tolerate precisely the same amount of disturbance as a quantum purification protocol.

To this end, we adopt Maurer's model for classical key agreement by public discussion from common information [3]. Briefly, in this classical scenario, Alice, Bob and Eve, have access to *independent* realizations of random variables X, Y and Z, respectively, jointly distributed according to P_{XYZ}. Furthermore, the two honest parties are connected by a noiseless and authentic (but otherwise insecure) channel. In the context of this model, Maurer and Wolf have shown that a useful upper bound for the secret-key rate $S(X;Y||Z)$ is the so-called intrinsic information $I(X;Y \downarrow Z)$ which is defined as

$$I(X;Y \downarrow Z) = \min_{Z \to \bar{Z}} \{I(X:Y|Z)\},$$

where $I(X:Y|Z)$ is the mutual information between the variables X and Y conditioned on Eve's variable Z, while the minimization runs over all the possible maps $Z \to \bar{Z}$ [40].

For our purposes, we can link this classical scenario to a quantum one. More precisely, the joint distribution P_{XYZ} can be thought of as arising from measurements performed on a quantum state $|\Psi_{\rm ABE}\rangle$ shared between Alice, Bob and Eve. We have, however, to focus on incoherent attacks where Eve interacts individually with each qubit and performs any measurements before reconciliation. Thus, at the end of such an attack the three parties share independent realizations of the random variables X, Y and Z. Accordingly, the resulting mixed state after tracing out Eve's degrees of freedom is of the form (14) where $H = -F\langle\phi_0|\phi_1\rangle$ and $G = -D\langle\theta_0|\theta_1\rangle$. It turns out [18] that the random variables X and Y are symmetric bits whose probability of being different is given by $\mathrm{Prob}[X \neq Y] = D$ whereas Eve's random variable consists of two bits Z_1 and Z_2. The first bit $Z_1 = X \oplus_2 Z$ shows whether Bob has received the transmitted qubit disturbed ($Z_1 = 1$) or undisturbed ($Z_1 = 0$). The probability that the second bit Z_2 indicates correctly the value of the bit Y is given by

$$\mathrm{Prob}[Z_2 = Y] = \delta = \frac{1 + \sqrt{1 - \langle\phi_0|\phi_1\rangle^2}}{2}. \qquad (31)$$

As has been shown by Gisin and Wolf [18], for the scenario under consideration secret key agreement is always possible *iff* the following condition holds

$$\frac{D}{1-D} < 2\sqrt{(1-\delta)\delta}. \qquad (32)$$

More precisely, one can show that if the above condition is not satisfied, the intrinsic information vanishes whereas, in any other case there exists a classical protocol that can provide Alice and Bob with identical keys about which Eve has negligible information. Such a protocol, for instance is the so-called advantage distillation protocol which is described in detail elsewhere [3].

In our case now, considering that Eve has adjusted the parameters in her attack to disentangle Alice and Bob at

the lowest possible disturbance, equation (31) yields for the two protocols

$$\delta = \begin{cases} \dfrac{3+2\sqrt{2}}{6} & \text{BB84 protocol} \\ \dfrac{2+\sqrt{3}}{4} & \text{six-state protocol.} \end{cases}$$

Using these values of δ in equation (32) one then obtains bounds that are precisely the same with the threshold disturbances for provable entanglement we derived in Section 3. In other words we have shown that, as long as Alice and Bob are entangled, a classical advantage distillation protocol is capable of providing them with a secret key, provided Eve restricts herself to individual attacks only (see also [20,21] for similar results).

This result is a manifestation of the link between quantum and secret correlations in both four- and six-state QKD protocols [22,23]. For the time being, the validity of this equivalence between classical and quantum distillation protocols is restricted to individual attacks only. Investigations of tomographic QKD protocols have shown, however, that such an equivalence is invalid for coherent attacks [41].

6 Concluding remarks

We have discussed provable entanglement in the framework of the BB84 and the six-state QKD protocols under the assumption of coherent (joint) attacks. In particular, we have shown that the threshold disturbances for provable entanglement are 1/4 and 1/3 for the four- and six-state QKD protocols, respectively. Perhaps surprisingly, these borders coincide with the disentanglement borders associated with the standard intercept-resend strategy [42,43]. Here we have shown, however, that even the most powerful eavesdropping attacks (which are only limited by the fundamental laws of quantum theory), are not able to push these disentanglement borders to lower disturbances. In other words, for the two protocols under consideration, any eavesdropping attack which disentangles Alice and Bob gives rise to QBERs above 1/4 (BB84) and 1/3 (six-state). Hence, for estimated disturbances below these borders the two honest parties can be confident (with probability exponentially close to one) that their quantum correlations cannot be described in the context of separable states and can be explored therefore for the extraction of a secret key.

In particular, for the entanglement-based versions of the protocols such a secure key can be obtained after applying an EPP which purifies the qubit pairs shared between Alice and Bob. Nevertheless, for the prepare-and-measure forms of the protocols the situation is more involved. To the best of our knowledge, the highest tolerable error rates that have been reported so far in the context of the prepare-and-measure BB84 and six-state schemes are close to 20% and 27%, respectively [4,5]. These best records are well below the corresponding threshold disturbances we obtained in this work. Thus, an interesting open problem is the development of prepare-and-measure protocols which bridge the remaining gap and are capable of generating a provably secure key up to 25% and 33.3% bit error rates. In view of the fundamental role of entanglement in secret key distribution such a development appears to be plausible. For this purpose, however, construction of new appropriate EPPs with two-way classical communication, which are consistent with the prepare-and-measure schemes, is of vital importance.

Furthermore, we have investigated the cost of information loss at which an eavesdropper can saturate these bounds in the context of symmetric incoherent and two-qubit coherent attacks. We have found that for the highly symmetric six-state scheme, there is always a unique eavesdropping attack which disentangles Alice and Bob at a fixed disturbance (above 1/3) and simultaneously maximizes Eve's information gain and/or probability of guessing. For the BB84 protocol, however, the situation is substantially different. Specifically, an attack which maximizes any of Eve's properties (information gain or probability of success in guessing) is not necessarily also the one that yields the lowest possible robustness bound. In fact, if Eve aims at reducing the robustness of the BB84 protocol she has to accept less information gain and probability of correct guessing. Nevertheless, our simulations show that for a two-qubit coherent attack this cost is substantially smaller than the cost for an incoherent attack. We conjecture therefore that, for coherent attacks on a larger number of qubits, the strategy that maximizes Eve's probability of success in guessing, is also the one that defines the lowest possible disentanglement threshold.

In closing, it should be stressed that the bounds we have obtained throughout this work depend on the post-processing that Alice and Bob apply. In particular, they rely on the complete omission of any polarization data from the raw key that involve different bases for Alice and Bob as well as on the individual manipulation of each pair of (qu)bits during the post-processing. In other words only one observable is estimated, namely the disturbance or QBER. If some of these conditions are changed, also the threshold disturbances may change. In this context it was demonstrated recently that with the help of entanglement witnesses which are constructed from the data of the raw key, the detection of quantum correlations between Alice and Bob is feasible even for QBERs above the bounds we have obtained here [22].

Stimulating discussions with Nicolas Gisin and Norbert Lütkenhaus are gratefully acknowledged. This work is supported by the EU within the IP SECOQC.

References

1. G. Brassard, L. Salvail, in *Advances in Cryptology — EUROCRYPT'93 Proceedings, Lecture Notes in Computer Science*, edited by T. Helleseth (Springer Verlag, New York, 1994), Vol. 765, p. 410
2. C.H. Bennett, G. Brassard, C. Crepeau, U.M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995)

3. U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993)
4. D. Gottesman, H.K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003)
5. H.F. Chau, Phys. Rev. A **66**, 060302 (2002)
6. I. Csiszár, J. Körner, IEEE Trans. Inf. Theory **IT-24**, 339 (1978)
7. G. Brassard, L. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994)
8. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996)
9. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wooters, Phys. Rev. A **54**, 3824 (1996)
10. C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wooters, Phys. Rev. Lett. **76**, 722 (1996)
11. C.H. Bennett, G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175
12. D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998)
13. C.A. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, A. Peres, Phys. Rev. A **56**, 1163 (1997)
14. D. Bruß, C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002)
15. N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002)
16. M. Bourennane, A. Karlsson, G. Björk, N. Gisin, N.J. Cerf, J. Phys. A **35**, 10065 (2002)
17. N. Gisin, S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999)
18. N. Gisin, S. Wolf, in *Proceedings CRYPTO 2000 Lecture Notes in Computer Science* (Springer Verlag, Heidelberg), Vol. 1880, p. 482
19. A. Acín, N. Gisin, V. Scarani, Quant. Info. Comp. **3**, 563 (2003)
20. A. Acín, L. Masanes, N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003)
21. D. Bruß et al., Phys. Rev. Lett. **91**, 097901 (2003)
22. M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2003); M. Curty, O. Gühne, M. Lewenstein, N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005)
23. A. Acín, N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005)
24. G.M. Nikolopoulos, G. Alber, Phys. Rev. A **72**, 032320 (2005); see also `arXiv:quant-ph/0507221`
25. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
26. H.K. Lo, H.F. Chau, Science **283**, 2050 (1999)
27. P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000)
28. H.K. Lo, Quant. Info. Comput. **2**, 81 (2001)
29. H.K. Lo, H.F. Chau, M. Ardehali, J. Cryptology **18**, 133 (2005); see also `arXiv:quant-ph/0011056`
30. D. Gottesman, J. Preskill, Phys. Rev. A **63**, 022309 (2001)
31. H.K. Lo, J. Phys. A **34**, 6957 (2001)
32. The Bell states, $|\Phi^{\pm}\rangle \equiv (|0_{\rm A}0_{\rm B}\rangle \pm |1_{\rm A}1_{\rm B}\rangle)/\sqrt{2}$ and $|\Psi^{\pm}\rangle \equiv (|0_{\rm A}1_{\rm B}\rangle \pm |1_{\rm A}0_{\rm B}\rangle)/\sqrt{2}$, form an orthonormal basis in the two-qubit Hilbert space
33. In general, a logarithmic scaling of the size of the random sample with the length of Alice's and Bob's key, seems to be sufficient for security issues. See reference [29] for a rigorous proof
34. S.K. Thompson, *Sampling* (John Wiley & Sons, New York, 2002); W.G. Cochran, *Sampling Techniques* (John Wiley & Sons, New York, 1997)
35. Note that in the absence of noise and eavesdropping each pair of qubits shared between Alice and Bob is in the Bell state $|\Psi^{-}\rangle$ [32]. Thus, in this ideal scenario, Alice and Bob obtain perfectly anticorrelated measurement results whenever they perform their measurements along the same basis
36. A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **223**, 1 (1996)
37. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
38. I. Cirac, N. Gisin, Phys. Lett. A **229**, 1 (1997)
39. H. Bechmann-Pasquinucci, N. Gisin, Phys. Rev. A **59**, 4238 (1999)
40. U. Maurer, S. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999)
41. D. Kaszlikowski et al., e-print `arXiv:quant-ph/0312172`
42. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptology **5**, 3 (1992)
43. A. Ekert, B. Huttner, J. Mod. Opt. **41**, 2455 (1994)