Bounds on Information and the Security of Quantum Cryptography

Eli Biham[1] and Tal Mor[2]
[1]*Computer Science Department, Technion, Haifa 32000, Israel*
[2]*Physics Department, Technion, Haifa 32000, Israel*

(Received 12 November 1996; revised manuscript received 18 July 1997)

In this paper we use properties of quantum mixed states to find bounds on various measures of their distinguishability. These bounds are used for analyzing strong *joint* attacks against quantum key distribution which use quantum probes, quantum memories, and quantum gates to attack *directly* the final key. We present a wide class of joint attacks, and we prove security against them. [S0031-9007(97)04463-3]

PACS numbers: 89.70.+c, 02.50.–r, 03.65.Bz, 89.80.+h

Various types of measures of information which can be obtained from quantum states (which are also measures of distinguishability of the quantum states) are useful for the analysis of the security of quantum cryptography. In many cases upper bounds on the information suffice. Moreover, when the exact calculation is unknown, there are no alternatives. In this paper we present new types of bounds on such measures and we use these bounds to prove security against a large class of attacks on quantum key distribution. These bounds are very simple and general, and they can be found useful for other tasks in quantum information and computation.

Quantum cryptography [1] suggests an *information secure* key distribution. It is based on the fact that nonorthogonal quantum states cannot be cloned, and any attempt to obtain information regarding these states necessarily disturbs them and induces noise. For instance, in the four-state scheme [1] the sender (Alice) and the receiver (Bob) use two conjugate bases and, in each basis two orthogonal states represent "0" and "1"; if the eavesdropper (Eve) measures a particle in one basis she randomizes its state if it was prepared in the other. In principle, the legitimate users of a quantum key distribution scheme should quit the protocol if they notice a noise. However, in real protocols, the channels and devices are not perfect, and some errors are inevitable. As long as the rate of errors p_e is small, the errors must be accepted and corrected by the legitimate users. As a result, Eve can obtain some information on the transmitted data, if she induces less errors than allowed (e.g., by eavesdropping on a small portion of the transmitted particles). Furthermore, she can obtain more information using the error-correction data transmitted via a classical channel. To overcome these problems, privacy amplification techniques [2], which reduce Eve's information on the final key, were suggested. The simplest privacy amplification technique uses the parity bit of a long string as the secret bit (where the parity is zero if the string contains an even number of 1's or else it is one). Privacy amplification and error correction are required even in the ideal case of an error-free channel (e.g., Eve could eavesdrop on one bit and be left unnoticed).

The objective of quantum cryptography is to provide protocols that are secure against an adversary equipped with *any* technology allowed by the rules of quantum mechanics. It is rather clear that the known schemes are secure against restricted attacks where only a portion of the bits are attacked, and against restricted attacks in which all bits are attacked, but each bit is attacked on line [2].

The security of the known schemes against sophisticated *joint* attacks, which use quantum probes, quantum memories, quantum gates, and delayed measurements to attack *directly* the final key, was not analyzed in early works. Recently, the security against joint attacks was analyzed using several different approaches. It is established only for a particular case [3,4], or under restricting conditions such as error-free channel [5] or perfect devices [6]. Recently, the approach of [5] was used to claim for proving the ultimate security [7], but there is as yet no general consensus in the scientific community regarding the correctness of this proof.

An important hint that privacy amplification might still be effective against attacks on the final key (in a realistic scenario) was provided by Bennett, Mor, and Smolin (BMS) [3]: Suppose that Eve obtains a binary string of n bits where each bit is presented by nonorthogonal polarization states, $\psi_0 = \binom{\cos\alpha}{\sin\alpha}$ or $\psi_1 = \binom{\cos\alpha}{-\sin\alpha}$, with *small* angle 2α between them (which is 4α when using "spin" notations as we do in the following). The work of [3] calculates the optimal information on parity bits obtained by unrestricted measurements. It shows that the optimal coherent measurement (which is much better than the optimal individual measurement) yields $I_M(n,\alpha) \approx c\binom{2k}{k}\alpha^{2k}$ (with $n = 2k$ and $c = 1$ for even n, and $n = 2k - 1$ and $c = 1/\ln 2$ for odd n), which is (still) exponentially small with the length of the string [3]. This result (henceforth, the BMS result) suggests that privacy amplification is effective also when Eve uses coherent measurements.

In real protocols, Eve does not obtain one of two states with a small angle between them, but she can probe the states sent from Alice to Bob using any technique she likes. Biham and Mor [4] presented a restricted class of joint attacks, called *collective attacks,* which can use the BMS method and result: (a) Eve attaches a *separate, uncorrelated* probe to each transmitted particle using a translucent attack; (b) Eve keeps the probes in a quantum memory till receiving all classical data including error-correction code and privacy amplification data; (c) Eve performs the optimal measurement on her probes in order to learn the optimal information on the final key. The italicized constraints on the probes distinguish the collective attacks from more general joint attacks, and enable analyzing the attacks in terms of the density matrices which Eve obtains.

The term translucent attack [8] stands for choosing a probe in a known pure state and applying a known unitary transformation to the transmitted particle and the probe together.

Let us define *qubit-symmetric* collective attacks in which the same translucent attack is applied to each transmitted particle, and *state-symmetric* collective attacks in which the attack is symmetric to any of the allowed quantum states of each particle. In the current paper we concentrate on attacks which fulfill both symmetries. Such attacks induce the same probability of error to each transmitted bit. They must be weak, or else they would induce a nonacceptable error rate. Thus, the possible states of Eve's probe cannot differ much.

In an explicit example of such an attack [4] Alice and Bob use the two-state scheme of Bennett [9] (with pure spin states with angle 4θ between them). Eve uses, in the first step of the collective attack, the (weak) translucent attack without entanglement [8], which leaves each probe in one of two pure states, ψ_0 or ψ_1, with small angle 4α between them. After an error-estimation step, Alice and Bob have an n-bit string. Alice and Bob choose the parity bit of that (full n-bit) string to be their secret bit, and Alice sends to Bob some parities of substrings as the error-correction data. In [4] we calculated Eve's density matrices for the parity bit (for this particular attack) while taking into account the error-correction data she has [10]. Then, we found Eve's best strategy for measuring the probes and her optimal mutual information on the parity bit (for short codes). For Hamming codes, H_r (of any length), it was shown based on a conjecture [see Eq. (5) in [4]] that

$$I(n,\alpha) \leq C(n)\,(2\alpha)^{(n+1)/2}, \tag{1}$$

with $C(n) = \frac{2}{\ln 2\sqrt{\pi}}\sqrt{(n+1)}$. Recently we improved the results of [4], verifying the conjecture numerically for $n \leq 31$ bits in case of Hamming codes. Furthermore, we proved a slightly modified version of the conjecture which provides a similar bound with an additional factor of 1.39. We are still working on proving Eq. (1) without the undesired modification, but even if this factor remains, it does not affect the value of our results.

Unfortunately, Eq. (1) applies only to collective attacks in which the translucent attack leaves Eve's probes in pure states, while most possible translucent attacks on the two-state scheme [9], and any attack on the four-state scheme [1], leave Eve's probes in mixed states.

The first goal of this Letter is to present new types of bounds on information which can be obtained from two quantum states. This is done based on the observation that *mixing* cannot improve distinguishability of quantum states. The second goal of this Letter is to apply these bounds, together with Eq. (1) as the upper bound, to the case where Eve's probes are in mixed states of certain types (restricting Eve to do only symmetric collective attacks and to use two-dimensional probes). The main achievement of using these new bounds is an upper bound on Eve's information when attacking the four-state scheme using the *optimal attack* of that type.

For two mixed states ρ_p in any dimension suppose that we can choose a state χ_n, and two states Φ_p such that

$$\begin{aligned} \rho_0 &= m\Phi_0 + (1-m)\chi_n\,, \\ \rho_1 &= m\Phi_1 + (1-m)\chi_n\,. \end{aligned} \tag{2}$$

Definition.—Let I(state 1; state 2) be some (positive) measure for the optimal distinguishability of two states, so that *any operation done on them* cannot lead to a distinguishability better (larger) than I.

From the above definition it is clear that any such measure I(state 1; state 2) for optimal distinguishability cannot be improved when the states are mixed with another (known) state. Thus, from the construction of (2), it is clear that the two mixed states ρ_p are not more distinguishable than the two (possibly pure) states Φ_p.

Theorem.—$I(\Phi_0;\Phi_1) \geq I(\rho_0;\rho_1)$.

Proof.—Suppose the contrary $I(\Phi_0;\Phi_1) < I(\rho_0;\rho_1)$. Then, when one receives Φ_p he can mix them with some χ_n and derive a better distinguishability than $I(\Phi_0;\Phi_1)$, in contradiction to the definition of $I(\Phi_0;\Phi_1)$.

We can choose any measure of an optimal information carried by these systems to describe the distinguishability. Very complicated types of information can be extracted from such systems, as for example, the optimal information on the parity of an n-bit string of encoded using quantum states [3,4]. In the case [4] where parities of substrings are given, a solution exists only for pure states with small angles (1) and we can now use it as an upper bound.

Any state (density matrix) in two-dimensional Hilbert space can be written as $\rho = \frac{\hat{I}+r\cdot\hat{\sigma}}{2}$ so that

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix},$$

with $r=(x,y,z)$ being a vector in $\mathcal{R}^3$, $\hat{\sigma}=(\hat{\sigma}_x,\hat{\sigma}_y,\hat{\sigma}_z)$ the Pauli matrices, and $\hat{I}$ the unit matrix. In this spin notation, each state is represented by the corresponding vector r. For pure states (Φ) the radius is $|r|=1$, and for mixed states $|r|<1$. Suppose that χ and ζ are two density matrices, represented by r_χ and r_ζ, respectively. It is possible to construct the density matrix $\rho = m\zeta + (1-m)\chi$ from the two matrices (where $0 \leq m \leq 1$), and the geometric representation of such a density matrix $\rho = \frac{\hat{I}+r_\rho\cdot\hat{\sigma}}{2}$ is $r_\rho = mr_\zeta + (1-m)r_\chi$.

Let us concentrate on mixed states with equal determinants which can always be written as

$$\rho_p = \frac{1}{2}\begin{pmatrix} 1+z & \pm x \\ \pm x & 1-z \end{pmatrix},$$

where the plus sign is for $p = 0$ and the minus for $p = 1$. Let ρ_{cms} be the completely mixed state $\rho_{\mathrm{cms}} = \frac{1}{2}\hat{I}$. Also let $\rho_\downarrow$ be the pure state of spin down in the z direction. Two cases of Eq. (2) are useful for our purpose: (a) $\rho_p = m\Phi_p + (1-m)\rho_{\mathrm{cms}}$, where the pure states Φ_p have the same angle as ρ_p [see Fig. 1(a)]; (b) $\rho_p = m\Phi_p + (1-m)\rho_\downarrow$, where Φ_p (which are uniquely determined) are shown in Fig. 1(b). The first type of bound is useful if ρ_p have a small angle 4α between them (which satisfies $\tan 2\alpha = x/z$), so that the angle 4β between the pure states satisfies $\beta = \alpha$, hence is also small. The second type of bound is useful when the "distance" $2x$ between the two possible mixed states is small (while α might be large). In this case x is small and z positive; hence the resulting angle 4β between the two pure states is small (following $\tan\beta = \tan 2\delta = \frac{x}{z+1} \leq x$). Thus, in both cases the angle between the two pure states is small so that $I(n,\beta)$ [Eq. (1) with an angle β] provides an upper bound on Eve's information on the final key.

For example, let Eve's probe be in an initial state $\binom{1}{0}$. She performs a unitary transformation $U\binom{1}{0}|\phi\rangle$ (with $|\phi\rangle$ Alice's state), where

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & c_\gamma & -s_\gamma & 0 \\ 0 & s_\gamma & c_\gamma & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad (3)$$

with $c_\gamma = \cos\gamma$ and $s_\gamma = \sin\gamma$. Note that, with $\gamma = \pi/2$, this transformation swaps the particle and the probe. Eve chooses a small angle γ so that the attack is a *weak swap*. Let Alice's possible initial states be $|\phi_p\rangle = \binom{\cos\theta}{\pm\sin\theta}$ in the two-state scheme, and $|\phi_m\rangle = \frac{1}{\sqrt{2}}\binom{1}{i^m}$ (with $m = 0,\ldots,3$) in the four-state scheme. The corresponding final states are

$$|\Psi_p\rangle = \begin{pmatrix} \cos\theta \\ \pm\sin\theta c_\gamma \\ \pm\sin\theta s_\gamma \\ 0 \end{pmatrix}; \quad |\Psi_m\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i^m c_\gamma \\ i^m s_\gamma \\ 0 \end{pmatrix}, \qquad (4)$$

respectively. Bob's reduced density matrices (RDM's) are calculated from $|\Psi\rangle\langle\Psi|$ by tracing out Eve's particle. This operation is usually denoted by $\rho_B = \mathrm{Tr}_E[|\Psi\rangle\langle\Psi|]$, where the full formula is given by Eq. (5.19) in [11] ($\rho_{nm} = \sum_{\mu\nu}\rho_{n\nu,m\mu}\delta_{\mu\nu} = \sum_\mu \rho_{n\mu,m\mu}$). We denote this operation by $\rho_B = \mathrm{Tr}_E[(|\Psi\rangle\langle\Psi|)\hat{I}]$, where $\hat{I}$ is the two-dimensional unit matrix $\delta_{\mu\nu}$. From Bob's matrices we find the error rate, that is, the probability p_e that he receives a wrong bit value. Calculating Eve's density matrix is sometimes trickier as we see later on.

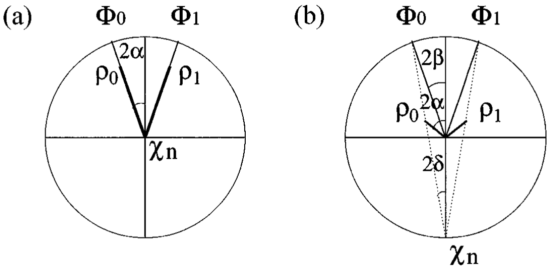

FIG. 1. Two ways of constructing the two density matrices ρ_p from two pure states Φ_p and a third state χ_n common to both density matrices. (a) $\chi_n = \rho_{\mathrm{cms}}$, the completely mixed state. (b) $\chi_n = \downarrow_z$, the "down z" pure spin state.

In the case of the four-state scheme Bob measures his particle in one of the bases x (corresponding to $m = 0,2$) or y ($m = 1,3$). Suppose that Alice and Bob use the x basis; Bob's RDM's are

$$\rho_B = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}(s_\gamma)^2 & \pm\frac{1}{2}c_\gamma \\ \pm\frac{1}{2}c_\gamma & \frac{1}{2} - \frac{1}{2}(s_\gamma)^2 \end{pmatrix},$$

leading to an error rate $p_e = \sin^2(\gamma/2)$ which is the probability that he identifies $|\phi_2\rangle$ when $|\phi_0\rangle$ is sent. Eve has the same knowledge of the basis; hence her RDM's are

$$\rho_E = \begin{pmatrix} \frac{1}{2} + \frac{1}{2}(c_\gamma)^2 & \pm\frac{1}{2}s_\gamma \\ \pm\frac{1}{2}s_\gamma & \frac{1}{2} - \frac{1}{2}(c_\gamma)^2 \end{pmatrix},$$

so that $x = s_\gamma$, $z = (c_\gamma)^2$, and the relevant angles are $2\beta = 2\alpha = (\tan)^{-1}(s_\gamma/c_\gamma^2)$ (using the first type of bounds). For a small angle γ we get $p_e \approx \gamma^2/4 + O(\gamma^4)$, $\beta \approx \gamma/2 + O(\gamma^3)$, and thus $p_e \approx \beta^2 + O(\beta^4)$. The information is thus bounded by $I(n,p_e) < C(n)\,(4p_e)^{(n+1)/4}$ to be exponentially small [using Eq. (1)].

We shall now prove security against any collective symmetric attack against the four-state scheme as long as Eve uses two-dimensional probes in the first step of the collective attack. We recently noticed that the one-particle mutual information $I_{\mathrm{ind}} = 1 + q_e\log_2 q_e + (1-q_e)\log_2(1-q_e)$ (where $q_e = 1/2 - s_\gamma/2$ is Eve's error probability), which Eve obtains using our gate, is equal to the information obtained by the optimal one-particle attack found in [12]. Thus, our attack maximizes Eve's information on a single particle for a given error rate p_e. As a result our gate also provides the maximal distance on the Poincaré sphere and it is $2x = 2s_\gamma$. Any other gate, and in particular the *unknown gate* which provides the optimal collective symmetric attack, leads to a distance $d \leq 2s_\gamma$. Now, the second type of bounds assures us that the angle 2δ of any attack is smaller than (or equal to) $\tan^{-1} s_\gamma$ (obtained when the distance d is drawn on the x axis). Finally, $\beta \leq \tan^{-1} s_\gamma$, and for small angle γ we get $\beta \leq \gamma + O(\gamma^3)$, $p_e \approx \beta^2/4 + O(\beta^4)$, and the optimal possible information obtained using two-dimensional probes and the symmetric collective attack is bounded by $I(n,p_e) < C(n)\,(16p_e)^{(n+1)/4}$.

In the case of the two-state scheme Bob's RDM's are

$$\rho_B = \begin{pmatrix} (c_\theta)^2 + (s_\theta)^2(s_\gamma)^2 & \pm c_\theta s_\theta c_\gamma \\ \pm c_\theta s_\theta c_\gamma & (s_\theta)^2(c_\gamma)^2 \end{pmatrix}.$$

Bob chooses one of two possible measurements with equal probability. In one case Bob measures the received state to distinguish ϕ_0 from its orthogonal state ϕ_0' and finds a conclusive result 1 whenever he gets ϕ_0'. (In the other case, the conclusive result 0 is obtained by replacing 0 and 1 in the above.) The error rate is the probability of identifying ϕ_p' when ϕ_p is sent, and it is $p_e = (s_\theta)^2(c_\theta)^2[1 - c_\gamma]^2 + (s_\theta)^4(s_\gamma)^2$.

To obtain Eve's density matrices in the two-state scheme one must take into account all the information she possibly has. If one ignores the classical information and calculates the standard RDM's (as in [13]), then the result is of significant importance to quantum information, while it is less relevant to quantum cryptography. Recall that Bob keeps only particles identified conclusively (as either ϕ_0' or ϕ_1'); Bob informs Alice—and thus Eve—which they are, and, as a result, Eve knows that Bob received either ϕ_0' or ϕ_1' in his measurement, and not ϕ_0 or ϕ_1. This fact influences her density matrices, and these are not given anymore by the simple tracing formula $\rho_E = \mathrm{Tr}_B[(|\Psi\rangle\langle\Psi|)\hat{I}]$. In general, *information dependent* RDM's are obtained by replacing $\hat{I}$ by any other positive operator $\hat{A}$ (as the operators which appear in generalized measurements): $\rho_E = \mathrm{Tr}_B[(|\Psi\rangle\langle\Psi|)\hat{A}]$, up to normalization. In our case $\rho_E = \mathrm{Tr}_B[(|\Psi\rangle\langle\Psi|)\,(\frac{1}{2}|\phi_0'\rangle\langle\phi_0'| + \frac{1}{2}|\phi_1'\rangle\langle\phi_1'|)]$, where the halves result from the probability that Bob chooses one measurement or the other. This tracing technique leads to

$$\rho_E = \begin{pmatrix} (s_\theta)^2(c_\theta)^2 + (s_\theta)^2(c_\theta)^2(c_\gamma)^2 & \pm c_\theta(s_\theta)^3 s_\gamma \\ \pm c_\theta(s_\theta)^3 s_\gamma & (s_\theta)^4(s_\gamma)^2 \end{pmatrix}.$$

After normalization we get $x = 2 s_\gamma c_\theta (s_\theta)^3/\mathrm{Tr}\rho_E$ and $z = \frac{1+z}{2} - \frac{1-z}{2} = \{(c_\theta)^2(s_\theta)^2[1 + (c_\gamma)^2] - (s_\theta)^4(s_\gamma)^2\}/\mathrm{Tr}\rho_E$. The relevant angles are $2\beta = 2\alpha = \tan^{-1}(x/z)$. For small angle γ we get $p_e \approx s_\theta^4\gamma^2 + O(\gamma^4)$, $2\beta \approx (s_\theta/c_\theta)\gamma + O(\gamma^3)$. Finally we get $p_e \approx (s_\theta)^2(c_\theta)^2(2\beta)^2 + O(\beta^4)$ from which we find $I(p_e, n) \le C(n) \times (p_e/(s_\theta c_\theta))^{(n+1)/4}$.

Once the optimal gate for individual attack shall be used, the same approach, as previously used for the four-state scheme, can also be used to bound Eve's information obtained on the two-state scheme (using any two-dimensional probes, symmetric collective attack).

In this Letter we presented a new type of bounds and use these bounds to obtain certain security proofs for quantum key distribution. Such bounds (or their generalizations) can have other uses in quantum information theory, whenever mixed states are used.

More general collective attacks can use nonsymmetric translucent attacks and/or can use probes in higher dimensions, in the first step of the collective attack. Our method, and generalizations of it might enable proving security against many such cases, and we are currently investigating these ideas.

A more crucial issue is the possibility of finding stronger joint attacks which are not collective. The argument which is the basis for approaching the security problem through the collective attack is as follows: by the time Eve holds the transmitted particles she has no knowledge of the error correction and privacy amplification techniques to be used by Alice and Bob. Also, she does not know which particles will be discarded in the error estimation stage, and the basis used for the relevant bits. Thus, we conjecture that she cannot gain information by searching or by creating correlations between the transmitted particles; she better keep one separate probe for each particle, and perform the measurements after obtaining the missing information as is done in the collective attacks. It seems that any attempt of searching for such coherent correlations at the first step of the attack induces error, while it cannot improve much Eve's information. It could improve her information much if she could guess correctly the required correlations and the bases for the relevant bits, but the probability of a successful guess is exponentially small.

Unfortunately, proving this intuitive argument is yet an open problem.

It is a pleasure for us to thank Asher Peres, William Wootters, and Gilles Brassard for helpful discussions. The gate we use here was also considered by them.

[1] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[3] C.H. Bennett, T. Mor, and J. Smolin, Phys. Rev. A **54**, 2675 (1996).

[4] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[5] A. Yao, in *Proceedings of the 27th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1995), pp. 67.

[6] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).

[7] D. Mayers, in *Advances in Cryptology: Proceedings of Crypto'96,* Lecture Notes in Computer Science Vol. 1109 (Springer-Verlag, Berlin, 1996), p. 343.

[8] A.K. Ekert, B. Huttner, G.M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

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

[10] This calculation was done with the help of D. Mayers (private communication).

[11] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, 1993).

[12] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997). See Eq. (65).

[13] C.A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).