PHYSICAL REVIEW A **73**, 012327 (2006)

Secrecy properties of quantum channels

A. Acín,[1] J. Bae,[1] E. Bagan,[2] M. Baig,[2] Ll. Masanes,[3,4] and R. Muñoz-Tapia[2]
[1]*ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[2]*Grup de Física Teòrica, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain*
[3]*Departament d'Estructura i Constituents de la Matèria, Univ. de Barcelona, 08028 Barcelona, Spain*
[4]*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
(Received 14 December 2004; published 20 January 2006)

We identify those properties of a quantum channel that are relevant for cryptography. We focus on general key distribution protocols that use prepare and measure schemes and the existing classical reconciliation techniques, as these are the protocols feasible with current technology. Given a channel, we derive an easily computable necessary condition of security for such protocols. In spite of its simplicity, this condition is shown to be tight for the Bennett-Brassard 1984 and six-state protocols. We show that the condition becomes also sufficient in the event of a so-called collective attack.

DOI: 10.1103/PhysRevA.73.012327 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Cryptography, the art of sending private information, has become inherent to our way of life. Concepts such as secure protocols, or secret key distribution are gradually becoming part of everyday language, as we gain awareness of an increasing number of transactions being encrypted to ensure confidentiality. Quantum cryptography [1], i.e., quantum key distribution (QKD) followed by one-time pad, enables two honest parties, Alice and Bob, to exchange private information by means of *provable-secure protocols*. The security is guaranteed by quantum-mechanical laws.

All known QKD protocols can be decomposed into the following three steps: First, Alice and Bob perform a tomographic analysis to obtain information about the quantum channel they share. This step is crucial because from the gathered information (e.g., from the error rate of the channel) the honest parties should conclude whether a given QKD protocol [e.g., Bennett-Brassard 1984 (BB84) [2] or six-state [3]] is viable or secure. Second, if the first step is successful, Alice and Bob use the QKD protocol to establish some correlations. Third, these correlations are transformed into a perfect secret key by means of distillation techniques, either classical or quantum. Concerning the first step, for each QKD protocol there is a specific set of relevant channel parameters, e.g., the critical quantum bit error rate (QBER), beyond which key distillation is impossible.

In this work, we identify and quantify the cryptographic properties of quantum channels *per se*, independently of any particular QKD protocol. This is meaningful by itself, but it has also a sharp practical edge, since in the real world the channel connecting Alice and Bob is fixed. Knowing its secrecy properties would enable them to choose the best suited protocol. Along this line, it is well known that any entanglement breaking channel, i.e., a channel that is useless for distributing entangled states, does not allow secure QKD [4]. It has also been shown in [5] that the mere presence of entanglement already guarantees some secrecy. Leaving these aside, little more is known about which channel properties are necessary and/or sufficient for secure QKD. Here we take a significant step in this direction.

The task is complex because there exists an infinite variety of QKD protocols. Here, we restrict our considerations to what we call *realistic* protocols in which (a) the parameter estimation and correlation distribution are made by prepare and measure techniques, i.e., Alice prepares states from a set of bases and Bob applies measurements chosen from another set of bases, and (b) standard reconciliation (key distillation) techniques, are employed. These techniques consist of two-way advantage distillation [6] followed by one-way error correction and privacy amplification. Note that most of the existing QKD protocols, such as BB84, six-state or Ekert's [7] fit into this category (see [8]). Likewise, most of the general security proofs, such as Shor-Preskill [9], apply to (b). Moreover, the word *realistic* suits these protocols well, as they are experimentally feasible; they do not require the use of entangled particles or quantum memories.

The article is structured as follows: first, we derive a simple, easily computable, necessary condition for the existence of a realistic and secure QKD protocol. If the channel connecting Alice and Bob does not meet this condition, there exists no prepare and measure protocol by which they can establish a secret key with the current distillation techniques (b). This follows from the analysis of a specific attack, where the eavesdropper, Eve, interacts individually and in the same way with each of the states sent by Alice, but can arbitrarily delay the measurement on her own state. These types of attacks are often called *collective* [10]. The attack studied here is similar to that in Ref. [11]. Then, we apply our general result to the BB84 and six-state protocols, deriving the critical QBER. The obtained values turn out to be tight for techniques (b), since they coincide with those derived by Chau in his general security proof [12]. Finally, we prove that our necessary security condition becomes also sufficient when Eve performs arbitrary collective attacks.

II. SECURITY CONDITION

To state precisely and prove our security condition, let us dive into the guts of a realistic QKD protocol. It proves convenient to present the problem in the completely equiva-

lent entanglement-based formulation, where Alice's state preparations are replaced by measurements [8]. For the sake of simplicity, and also because of its practical relevance, we restrict our present analysis to a qubit Pauli channel, but our techniques also apply to other channels of arbitrary dimension [13]. In a Pauli channel, the qubit either remains unchanged or is affected by a σ_x, σ_y, or σ_z rotation, with different probabilities. Therefore, we can assume that the Alice and Bob channel is characterized by an effective Bell diagonal state

$$\rho_{AB} = \lambda_1[\Phi^+] + \lambda_2[\Phi^-] + \lambda_3[\Psi^+] + \lambda_4[\Psi^-], \tag{1}$$

with $\lambda_i \geqslant 0$ and $\Sigma_i \lambda_i = 1$. Throughout this paper square brackets denote one-dimensional projectors (not necessarily normalized); e.g., $[\psi] = |\psi\rangle\langle\psi|$. We also use the standard convention: $|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$.

In step one, Alice and Bob estimate λ_i by means of channel tomography. It is important to stress here that, although Alice and Bob can effectively describe their data by means of a state (1), they cannot assume to share N independent realizations of this state (channel) because Eve may have introduced correlations among the copies. Without loss of generality, one can impose that

$$\lambda_1 = \max_i \lambda_i, \quad \lambda_2 = \min_i \lambda_i, \tag{2}$$

since any permutation of the coefficients λ_i in (1) can be achieved combining the following local unitaries:

$$T([\Phi^+] \leftrightarrow [\Phi^-]) = 2^{-1}(\mathbb{1} - i\sigma_z) \otimes (\mathbb{1} - i\sigma_z),$$

$$T([\Phi^-] \leftrightarrow [\Psi^+]) = 2^{-1}(\sigma_x + \sigma_z) \otimes (\sigma_x + \sigma_z),$$

$$T([\Psi^+] \leftrightarrow [\Psi^-]) = 2^{-1}(\mathbb{1} + i\sigma_z) \otimes (\mathbb{1} - i\sigma_z). \tag{3}$$

We can now state or main result: *the inequality*

$$(\lambda_1 - \lambda_2)^2 > (1 - \lambda_1 - \lambda_2)(\lambda_1 + \lambda_2) \tag{4}$$

is a necessary security condition for realistic QKD on a Pauli channel. The proof is given in the next lines, and follows from the analysis of a specific collective attack.

In step two, each honest party performs a local measurement on each of a large number of copies of the state they share, thus obtaining two lists of outcomes (bits): $\{A_i\}$ (Alice) and $\{B_i\}$ (Bob). We need to identify a pair of measurement bases whose secret correlations, implicit in each pair of outcomes (A_i, B_i), can be distilled into a secret key in the third step of the protocol.

Within the two-way scheme (b), introduced by Maurer [6], each of the honest parties transforms blocks of M bits into a single bit. By doing that, they map their initial lists of bits into shorter, more secret and correlated ones. To achieve this goal, Alice randomly chooses M bits from $\{A_i\}$, and Bob takes their M counterparts from $\{B_i\}$. Next, Alice generates a secret random bit s_A, computes the M numbers $X_i := (A_i + s_A) \bmod 2$, and sends

$$X_1, X_2, \ldots, X_M \tag{5}$$

through the insecure but authenticated public channel. Bob then adds bitwise (mod 2) this string to his list, $B_1, B_2, \ldots B_M$. If he obtains the same result s_B for the M sums, i.e., if $(B_i + X_i) \bmod 2 = s_B$ for $i = 1, 2, \ldots M$, he keeps the bit s_B and communicates its acceptance. Otherwise, the two parties reject the M bits. After this, Alice and Bob apply standard one-way error-correction and privacy amplification techniques to obtain the key.

A. Eve's attack

Since Eve's attack is collective, the three parties share N independent copies of a state $|\Psi_{ABE}\rangle$, where, see Eq. (1),

$$|\Psi_{ABE}\rangle = \sqrt{\lambda_1}|\Phi^+\rangle|1\rangle + \sqrt{\lambda_2}|\Phi^-\rangle|2\rangle + \sqrt{\lambda_3}|\Psi^+\rangle|3\rangle + \sqrt{\lambda_4}|\Psi^-\rangle|4\rangle. \tag{6}$$

That is, Eve has a large quantum system that is a purification of Alice and Bob's state, $\rho_{AB} = \mathrm{tr}_E[\Psi_{ABE}]$.

Let us start analyzing the situation in which Alice and Bob obtain their list of bits to be transformed into the secret key by measuring in the computational basis. After the measurement they are left with classical data, whereas Eve could still hold a quantum system. The correlations they share are described by the state (up to normalization)

$$\sum_x [x]_{AB} \otimes [\psi_x]_E, \tag{7}$$

where $x = 00, 01, 10, 11$, and

$$|\psi_{00/11}\rangle = \sqrt{\lambda_1}|1\rangle \pm \sqrt{\lambda_2}|2\rangle,$$

$$|\psi_{01/10}\rangle = \sqrt{\lambda_3}|3\rangle \pm \sqrt{\lambda_4}|4\rangle. \tag{8}$$

Notice that the above vectors are non-normalized. Next, Alice and Bob apply advantage distillation. Eve has then her M (four-dimensional) quantum systems as well as the information that the honest parties have exchanged through the public channel, i.e., the M-bit string (5). If she performs the unitary transformation

$$U_i = [1]_E + (-1)^{X_i}[2]_E + [3]_E + (-1)^{X_i}[4]_E \tag{9}$$

to her ith system ($i = 1, \ldots, M$), the tripartite state becomes, up to normalization,

$$\sum_x [x]_{AB} \otimes [\psi_x]_E^{\otimes M}. \tag{10}$$

After the transformation (9), the tripartite state (10) becomes completely uncorrelated to (5). The rest of the protocol is also independent of (5), so this information is no longer useful. Hence, state (10) summarizes all the correlations among Alice, Bob, and Eve before applying one-way reconciliation. Bob's error probability reads

$$\epsilon_B = \frac{(\lambda_3 + \lambda_4)^M}{(\lambda_1 + \lambda_2)^M + (\lambda_3 + \lambda_4)^M}. \tag{11}$$

Eve now performs the two-outcome measurement defined by

$$F_{\rm eq} = [1]_E + [2]_E, \quad F_{\rm dif} = [3]_E + [4]_E, \tag{12}$$

on each one of her M systems, where the subscript "eq" ("dif") refers to the outcome, A being equal to (different from) B. According to (10), all M measurements give the same outcome. Note that Eve knows in a deterministic way whether s_A and s_B coincide, which implies that her information on these variables is the same. If Eve obtains the outcome corresponding to $F_{\rm eq}$, the tripartite state becomes (up to normalization)

$$[00]_{AB} \otimes [\psi_{00}]_E^{\otimes M} + [11]_{AB} \otimes [\psi_{11}]_E^{\otimes M}. \tag{13}$$

In order to learn s_A, she must discriminate between the two pure states ψ_{00} and ψ_{11}. It was proved in [14] (see also [15]) that the minimum error probability she can achieve is

$$P^{\rm error} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - c^{2M}}, \tag{14}$$

where c is the overlap between the states. Applying this formula to (13), her error probability in guessing s_A reads

$$\epsilon_{\rm eq} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - \Lambda_{\rm eq}^{2M}}. \tag{15}$$

Similarly, if Eve obtains instead the outcome corresponding to $F_{\rm dif}$, the error probability $\epsilon_{\rm dif}$ is given by (15) with the substitution $\Lambda_{\rm eq} \to \Lambda_{\rm dif}$, where

$$\Lambda_{\rm eq} = \frac{|\lambda_1 - \lambda_2|}{\lambda_1 + \lambda_2}, \quad \Lambda_{\rm dif} = \frac{|\lambda_3 - \lambda_4|}{\lambda_3 + \lambda_4}. \tag{16}$$

At this point, Eve's information, denoted by E, consists of s_E (her guess for s_A) as well as the outcome of the measurement (12). Our goal is now to prove that the obtained probability distribution, $P(s_A, s_B, E)$, is nondistillable when (4) does not hold. We will do that by showing that Eve can always map P into a new probability distribution Q, which turns out to be nondistillable when (4) is false. Thus the same has to be true for P.

Without loss of generality, we assume that the flow of communication after advantage distillation goes from Alice to Bob. Eve proceeds as follows. From (2), it can be seen that $\Lambda_{\rm dif} \leqslant \Lambda_{\rm eq}$, which implies that $\epsilon_{\rm dif} \leqslant \epsilon_{\rm eq}$. When she obtains the outcome corresponding to $F_{\rm dif}$, she increases her error until $\epsilon_{\rm dif} = \epsilon_{\rm eq}$. She achieves this by changing the value of s_E with some probability. Then, she forgets the outcome of measurement (12). The obtained probability distribution, $Q(s_A, s_B, s_E)$, satisfies

$$Q(s_B, s_E | s_A) = Q(s_B | s_A) Q(s_E | s_A). \tag{17}$$

Additionally we know that $Q(s_B|s_A)$ and $Q(s_E|s_A)$ are binary symmetric channels with error probability ϵ_B in (11) and $\epsilon_{\rm eq}$ in (15), respectively. It is proved in [6] that in such situation the one-way key rate is $K_{\rightarrow} = h(\epsilon_{\rm eq}) - h(\epsilon_B)$, which is nonpositive if $\epsilon_{\rm eq} \leqslant \epsilon_B$. Let us finally prove that this inequality holds for all values of M if condition (4) is not satisfied. Define $z = \lambda_1 + \lambda_2$. The range of interest is $1/2 \leqslant z \leqslant 1$, since no secret key can be extracted from a separable state [4] and a Bell diagonal state is entangled *iff* $\lambda_1 > 1/2$. After some algebra, one can prove the inequality

$$\epsilon_{\rm eq} \leqslant \frac{1}{2} - \frac{1}{2}\sqrt{1 - \left(\frac{1-z}{z}\right)^M} \leqslant \frac{(1-z)^M}{z^M + (1-z)^M} = \epsilon_B, \tag{18}$$

where M is *any* positive integer. The first inequality follows from $(\lambda_1 - \lambda_2)^2/z^2 \leqslant (1-z)/z$, which is the negation of Eq. (4).

Note that the previous analysis has been made assuming that Alice and Bob measure in the z basis. However, the same techniques could be applied to measurements in any basis. We have performed an extensive numerical analysis that shows that the computational bases are optimal against the considered attack. Notice that in many cases, these measurements do not maximize the correlations between Alice and Bob, but they rather tend to *optimize their secret correlations*. Therefore no secret key can be established through a Pauli channel with any realistic protocol if condition (4) is not met. This concludes the proof.

It is important to remember here that although our analysis has been applied to the case of Pauli channels, it can be adapted to other situations [13]. Our condition (4) is in general stronger than the entanglement condition of [4], as it happens for Bell diagonal states. Indeed, our results suggest that it may be impossible in general to reach the entanglement limit by a prepare and measure protocol. Yet it is weaker because *stricto sensu* it only refers a subclass of realistic schemes. Nevertheless, these are the schemes feasible using the existing technology and reconciliation techniques.

B. Application to known protocols

Although the analysis we have presented here aims at characterizing quantum channels independently of QKD schemes, it can also be applied to the study of specific cryptographic protocols. In this case, no optimization over the bases is required, since they are fixed by the details of the protocol. Consider the BB84 and six-state protocols. A typical question in this context is to determine the critical QBER of the channel. Now, Alice and Bob characterize their channel by a single parameter: the error rate. As above, we restrict our analysis to the known reconciliation techniques (b). In the case of the six-state protocol, Eve can prepare N independent copies of the two-qubit Werner state

$$\rho_W = \lambda_1 [\Phi^+] + \frac{1-\lambda_1}{3}([\Phi^-] + [\Psi^+] + [\Phi^-]), \tag{19}$$

which has QBER$=2(1-\lambda_1)/3$. Condition (4) shows that a secure key extraction is not possible if the error rate satisfies QBER$\geqslant 0.2764$; see Fig. 1.

For BB84, Eve can prepare the state

$$\rho_{BB84} = \lambda_1 [\Phi^+] + \frac{1-\lambda_1}{2}([\Phi^-] + [\Psi^+]), \tag{20}$$

for which QBER$=(1-\lambda_1)/2$. The critical QBER is now 0.2. Remarkably enough, these figures coincide with those obtained by Chau in [12], where a general security proof for these protocols was given. Indeed, Chau's distillation protocol belongs to the family (b) considered here. The simple

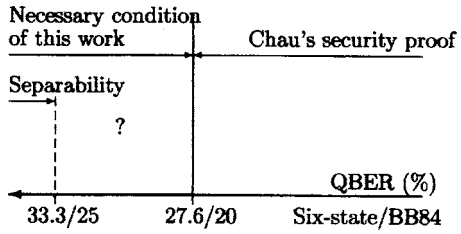

FIG. 1. Security bounds for six-state and BB84 protocols using classical advantage distillation followed by one-way error correction and privacy amplification. Our necessary condition coincides with the values derived by Chau for both protocols. It remains as an open question whether the entanglement limit can be reached.

attack we have presented above is therefore tight and proves that, unless so-far unknown two-way reconciliation techniques are employed [16], the critical QBER values we have obtained cannot be raised.

By completing this work, we learn that similar results on the tightness of Chau's proof have independently been obtained in [17].

C. General collective attacks

Given the simplicity of our attack, its tightness for the BB84 and six-state protocols is somehow surprising. Recall that Eve is assumed to (i) apply the same interaction to the states sent by Alice and (ii) measure right after advantage distillation, while she could have delayed her measurement until the end of the reconciliation protocol. Assumption (i) may be not as strong as it might seem: the recent results of [10] suggest that Eve may gain no advantage by introducing correlations among the pairs of systems shared by Alice and Bob (see also [18]). Assumption (ii) looks much more restrictive since after listening to the public communication between Alice and Bob during the whole reconciliation, Eve could in principle further optimize her measurement.

In view of this, it is relevant to see how condition (4) has to be modified in the case of general collective attacks, where assumption (ii) is dropped. In this case, Eve does not measure her state after advantage distillation, so Alice, Bob, and Eve share classical-classical-quantum correlations described by the state (10). It was proved in [19], that the secret key rate achievable with one-way communication ($K_{\rightarrow}$) when Alice holds a classical system satisfies

$$K_{\rightarrow} \geqslant I(A:B) - I(A:E). \tag{21}$$

In this equation $I(X:Y)=H(X)+H(Y)-H(X,Y)$, where $H(X)=-\mathrm{tr}(\rho_X \log_2 \rho_X)$, is the mutual information. After some algebra, the following equality for the state (10) can be obtained

$$I(A:B) - I(A:E) = 1 - h(\epsilon_B) - (1-\epsilon_B)h\left(\frac{1-\Lambda_{\mathrm{eq}}^M}{2}\right) - \epsilon_B h\left(\frac{1-\Lambda_{\mathrm{dif}}^M}{2}\right), \tag{22}$$

where $h(x)=-x\log_2 x-(1-x)\log_2(1-x)$. It can be checked that if (4) is satisfied, there exists a sufficiently large M such that the right-hand side of (21), i.e., Eq. (22), is positive. Thus, our necessary condition (4) for key distillation becomes sufficient for general collective attacks. That is, Eve gains no advantage by delaying her measurement until the end of the reconciliation.

III. CONCLUSIONS

We have analyzed quantum channels in terms of their secrecy properties. This approach is specially well suited to practical QKD: it enables Alice and Bob to devise protocols that *optimally* exploit the secret correlations present in the quantum channel they share. We have derived a simple and easily computable necessary condition for the existence of a secure prepare and measure protocol with the current distillation techniques. When applied to BB84 and the six-states protocol, this condition turns out to be tight. Moreover, it becomes sufficient in the case of general collective attacks.

ACKNOWLEDGMENTS

We thank G. M. Nikolopoulos for discussion. This work is supported by the Spanish Ministry of Science and Technology project BFM2002-02588, "Ramón y Cajal," 2002FI-00373 and 2004FI-00068 grants, by CIRIT project SGR-00185, by the U.K. Engineering and Physical Sciences Research Council (IRC QIP), and by QUPRODIS working group EEC IST-2001-38877.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2202).

[2] C. H. Bennett and G. Brassard, in *Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

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

[4] N. Gisin and S. Wolf, *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer-Verlag, Berlin, 2000), p. 482; M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[5] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).

[6] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

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

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

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

[10] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**,

080501 (2005).
[11] D. Kaszlikowski *et al.*, Phys. Rev. A **71**, 012309 (2005).
[12] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[13] Work in preparation.
[14] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[15] A. Acin *et al.*, Phys. Rev. A **71**, 032338 (2005).
[16] For Bell diagonal states, no improvement is obtained by introducing the preprocessing of [10]; see [13].
[17] K. S. Ranade and G. Alber, quant-ph/0510041.
[18] R. König and R. Renner, quant-ph/0410229.
[19] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).