Security of EPR-based quantum cryptography against incoherent symmetric attacks

2001 J. Phys. A: Math. Gen. 34 6913

(http://iopscience.iop.org/0305-4470/34/35/317)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 6913–6918 PII: S0305-4470(01)19299-1

Security of EPR-based quantum cryptography against incoherent symmetric attacks

Hitoshi Inamori, Luke Rallan and Vlatko Vedral

Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3Pu, UK

Received 21 November 2000
Published 24 August 2001
Online at stacks.iop.org/JPhysA/34/6913

Abstract

We investigate a new strategy for incoherent eavesdropping in Ekert's entanglement-based quantum key distribution protocol. We show that under certain assumptions of symmetry the effectiveness of this strategy reduces to that of the original single-qubit protocol of Bennett and Brassard.

PACS numbers: 03.67.Dd, 03.65.Ta, 03.67.−a

Quantum key distribution (QKD) employs quantum features such as the uncertainty principle and quantum correlations to provide for unconditionally secure communications [1]. In classical cryptography no mechanism is known for unconditionally secure key distribution. The importance of QKD protocols within cryptography is paramount as they allow for the practical implementation of unconditionally secure cryptographic algorithms such as the one-time pad [2].

A quantum cryptographic system can be thought to be constructed of two main parts: firstly the underlying quantum key distribution protocol securely establishes a common key between Alice and Bob, and secondly the message is simply encrypted with the established key and transmitted. Theoretical models for quantum key distribution protocols based on the uncertainty principle have been analysed by Bennett and Brassard (BB84) [3] and models based on quantum correlations have been proposed by Ekert (E91) [4]. A modified version of E91 that is closer to BB84 has been proposed by Bennett, Brassard and Mermin (BBM92) [5].

Eavesdropping can be considered as the interception of a transmission between Alice and Bob by an eavesdropper (Eve) and then the application of an appropriate measurement to extract information. Regardless of the difficulty of interception of the message, in principle any classical channel can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place. This is not so for quantum channels. Any measurement disturbs the transmitted state and hence can be detected by Alice and Bob. This leads to a trade-off between the amount of information that Eve can acquire about the transmission and the degree to which she disturbs it and hence can be detected [6].

In this paper we present an incoherent eavesdropping strategy for BBM92. The BBM92 protocol can be presented in five main stages:

- Entangled photons are distributed to Alice and Bob who measure them randomly choosing between two fixed measurement bases. This state is such that in the absence of noise or eavesdropping Alice and Bob's measurement results are the same if they choose the same basis.
- Alice and Bob communicate classically their choice of basis for all pairs and discard all measurement results where different bases were used.
- A subset of the remaining measurement results is publicly compared and used to determine the error rate (i.e. where Alice's and Bob's outcomes do not coincide). This error rate is assumed to be due to Eve.
- Finally, if the error rate is below a certain acceptable threshold, then the remaining undisclosed outcomes constitute the sifted keys. Otherwise, the outcomes are discarded and the whole process is repeated.
- The sifted keys may be partially corrupted and compromised. Alice and Bob perform error correction to reconcile the discrepancies between their sifted keys. The privacy amplification step returns from this partially compromised reconciled key a shorter string of bits called private key. This step should be devised so that Eve's knowledge about the private key is arbitrarily small.

The classical communications between Alice and Bob in the above protocol are assumed to be authenticated, i.e. Eve is able to read any classical message exchanged between Alice and Bob, but cannot modify it without being detected (if such modification is detected then the protocol is terminated).

In the following part of the paper, we consider the situation in which Alice and Bob use an interactive error-correction scheme that does not reveal any information about Alice's and Bob's sifted keys, except possibly the positions of the discrepancies. Such a correction can be obtained for instance by using the Cascade protocol proposed by Brassard and Salvail [7], in which the parity bits are encrypted using the one-time pad.

In our eavesdropping strategy we assume that Eve prepares both photons of the entangled pair before they are transmitted to Alice and Bob. We do not analyse the most general attack of this type, but instead focus on a simpler symmetric attack.

We adopt a conservative view in which Eve prepares a pair of photons in an arbitrary state, possibly entangled with other quantum systems. These auxiliary quantum systems are known as a probe. Without loss of generality [8], the initial joint state of the photon pair and the probe can be assumed to be a pure state $|\psi\rangle$ of the following form:

$$|\psi\rangle = \sum_{\alpha,\beta\in\{0,1\}} |\mathcal{E}_{\alpha,\beta}\rangle|\alpha\rangle_+|\beta\rangle_+ \tag{1}$$

where $\{|0\rangle_+, |1\rangle_+\}$ is a basis for the polarization state of a single photon. The states $|\alpha\rangle_+$ and $|\beta\rangle_+$ refer to Alice and Bob's respective photon states. The kets for Eve's probe $|\mathcal{E}_{\alpha,\beta}\rangle$ are not necessarily normalized or orthogonal. The only condition on these vectors is the overall normalization of $|\psi\rangle$, leading to

$$\sum_{\alpha,\beta\in\{0,1\}} \langle\mathcal{E}_{\alpha,\beta}|\mathcal{E}_{\alpha,\beta}\rangle = 1. \tag{2}$$

If we assume that Alice controls the EPR source, then the security of the above BBM92 scheme is equivalent to the security of BB84 protocol [5]. This is because Alice first generates an entangled pair locally, keeps one photon and sends the other to Bob. Therefore only one photon can be intercepted and measured by Eve which is thus analogous to BB84.

Notice that if Eve is limited only to eavesdropping on the quantum channel between the source and Bob, her eavesdropping can be described without loss of generality as an unitary interaction between Bob's photon and Eve's probe:

$$|F\rangle|0\rangle_+ \mapsto |F_{00}\rangle|0\rangle_+ + |F_{01}\rangle|1\rangle_+ \tag{3}$$

$$|F\rangle|1\rangle_+ \mapsto |F_{10}\rangle|0\rangle_+ + |F_{11}\rangle|1\rangle_+ \tag{4}$$

where $|F\rangle$ is the initial state of Eve's probe, and the $|F_{\alpha,\beta}\rangle$ are again not necessarily normalized or orthogonal, but obey the unitarity conditions:

$$\langle F_{00}|F_{00}\rangle + \langle F_{01}|F_{01}\rangle = 1 \tag{5}$$

$$\langle F_{10}|F_{10}\rangle + \langle F_{11}|F_{11}\rangle = 1 \tag{6}$$

$$\langle F_{00}|F_{10}\rangle + \langle F_{01}|F_{11}\rangle = 0. \tag{7}$$

The resulting global state of the pair and the probe is

$$|\psi'\rangle = \sum_{\alpha,\beta\in\{0,1\}} \frac{|F_{\alpha,\beta}\rangle}{\sqrt{2}}|\alpha\rangle_+|\beta\rangle_+. \tag{8}$$

However, because of the unitarity conditions (equations (5)–(7)), the global state obtained by Eve when she is only accessing one of the photons is not as general as the state she can obtain when she can access both as in equation (1). Therefore this proves that the eavesdropping strategy in which Eve controls the source (i.e. both photons) is potentially stronger than the strategy in which she is allowed to eavesdrop on only one photon.

We now turn our attention to a symmetric subclass of incoherent attacks against BBM92 in which Eve controls the source. We derive the probability that Eve guesses Alice's bit correctly as a function of the error probability that Alice and Bob can estimate from comparing a fraction of the key bits they obtain.

Let $\{|0\rangle_+, |1\rangle_+\}$ be a basis for the polarization state of a single photon. We define its conjugate basis $\{|0\rangle_\times, |1\rangle_\times\}$ by $|0\rangle_\times = (|0\rangle_+ + |1\rangle_+)/\sqrt{2}$ and $|1\rangle_\times = (|0\rangle_+ - |1\rangle_+)/\sqrt{2}$. For any $b \in \{+, \times\}$ we use the shorthand notation $|\alpha\beta\rangle_b$ for the state of a pair of photons in which Alice's photon is in state $|\alpha\rangle_b$ and Bob's photon in the state $|\beta\rangle_b$. We define the Bell basis $\{|\underline{0}\rangle, |\underline{1}\rangle, |\underline{2}\rangle, |\underline{3}\rangle\}$ for the pair of photons Alice and Bob receive by

$$|\underline{0}\rangle = (|00\rangle_+ + |11\rangle_+)/\sqrt{2} \qquad |\underline{1}\rangle = (|00\rangle_+ - |11\rangle_+)/\sqrt{2}$$

$$|\underline{2}\rangle = (|01\rangle_+ + |10\rangle_+)/\sqrt{2} \qquad |\underline{3}\rangle = (|01\rangle_+ - |10\rangle_+)/\sqrt{2}.$$

In the most general incoherent attack, Eve prepares two single photons and a probe in any pure state $|\psi\rangle = \sum_{c=0}^{3} |E_c\rangle|\underline{c}\rangle$, where for simplicity we use the Bell basis. The kets for the probe, $|E_c\rangle$ as previously mentioned are not necessarily normalized or orthogonal, but nevertheless have to obey the overall normalization relation $\sum_{c=0}^{3}\langle E_c|E_c\rangle = 1$. It is straightforward to check that

$$\begin{aligned}|\psi\rangle = {} & \frac{|E_0\rangle + |E_1\rangle}{\sqrt{2}}|00\rangle_+ + \frac{|E_2\rangle + |E_3\rangle}{\sqrt{2}}|01\rangle_+ \\ & + \frac{|E_2\rangle - |E_3\rangle}{\sqrt{2}}|10\rangle_+ + \frac{|E_0\rangle - |E_1\rangle}{\sqrt{2}}|11\rangle_+ \qquad (9)\\ = {} & \frac{|E_0\rangle + |E_2\rangle}{\sqrt{2}}|00\rangle_\times + \frac{|E_1\rangle - |E_3\rangle}{\sqrt{2}}|01\rangle_\times \\ & + \frac{|E_1\rangle + |E_3\rangle}{\sqrt{2}}|10\rangle_\times + \frac{|E_0\rangle - |E_2\rangle}{\sqrt{2}}|11\rangle_\times. \qquad (10)\end{aligned}$$

Eve sends each of the photons to Alice and Bob. After public communication between Alice and Bob, Eve then performs any measurement on her probe. We say that an incoherent attack is furthermore *symmetric* if and only if the kets $|E_c\rangle$ are orthogonal.

The probability that Alice and Bob fail to share the same bit value given that they have chosen the same basis $b \in \{+, \times\}$ reads

$$\epsilon_b = \mathrm{Tr}[\mathbf{1} \otimes (|01\rangle_{bb}\langle 01| + |10\rangle_{bb}\langle 10|)|\psi\rangle\langle\psi|] \tag{11}$$

$$= \begin{cases} z + t & \text{if } b = + \\ y + t & \text{if } b = \times \end{cases} \tag{12}$$

where the identity operator acts on the Hilbert space of the probe and where we have used the shorthand notation $x = \langle E_0|E_0\rangle$, $y = \langle E_1|E_1\rangle$, $z = \langle E_2|E_2\rangle$ and $t = \langle E_3|E_3\rangle$.

We assumed that, after public discussion between Alice and Bob, Eve is aware of their chosen basis, and whether or not their measurements yielded the same bit value. From these data Eve's objective is to guess Alice's bit value α. Assuming that Alice and Bob chose the basis $b = +$ and that their measurement returned the *same* bit value, we see from equation (9) that Eve has to find out whether her probe is in the state $\frac{|E_0\rangle + |E_1\rangle}{\sqrt{x+y}}$, corresponding to $\alpha = 0$ or in the state $\frac{|E_0\rangle - |E_1\rangle}{\sqrt{x+y}}$ corresponding to $\alpha = 1$. Given a quantum system that is equally likely to be in either state $|\eta\rangle$ or $|\chi\rangle$, it is known that the optimal probability of guessing this state correctly is $P_c = \frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\eta|\chi\rangle|^2}$ [9]. In our case, Eve's probability of guessing correctly is

$$P_{c|\text{share},b=+} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \left(\frac{x-y}{x+y}\right)^2}. \tag{13}$$

If Alice and Bob chose the basis $b = +$, but that their measurements returned *different* bit values, Eve has to find out whether her probe is in the state $\frac{|E_2\rangle + |E_3\rangle}{\sqrt{y+z}}$ or $\frac{|E_2\rangle - |E_3\rangle}{\sqrt{y+z}}$. Eve's probability of guessing correctly is now

$$P_{c|\text{not share},b=+} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \left(\frac{z-t}{z+t}\right)^2}. \tag{14}$$

Similar calculations on the conjugate basis give

$$P_{c|\text{share},b=\times} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \left(\frac{x-z}{x+z}\right)^2} \tag{15}$$

and

$$P_{c|\text{not share},b=\times} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \left(\frac{y-t}{y+t}\right)^2}. \tag{16}$$

Given that the choice of the basis b is uniformly distributed, the marginal probability that Eve guesses Alice's bit correctly is

$$P_c = \frac{1-\epsilon_+}{2}P_{c|\text{share},b=+} + \frac{\epsilon_+}{2}P_{c|\text{not share},b=+} + \frac{1-\epsilon_\times}{2}P_{c|\text{share},b=\times} + \frac{\epsilon_\times}{2}P_{c|\text{not share},b=\times} \tag{17}$$

$$= \frac{1}{2} + \frac{1}{2}(\sqrt{xy} + \sqrt{zt} + \sqrt{xz} + \sqrt{yt}) \tag{18}$$

$$= \frac{1}{2} + \frac{1}{2}(\sqrt{1-\epsilon_+ - x} + \sqrt{1-\epsilon_\times - x})(\sqrt{x} + \sqrt{x + \epsilon_+ + \epsilon_\times - 1}) \tag{19}$$

where we have used the normalization condition $x + y + z + t = 1$. Since y, z and t are non-negative numbers, the domain for x is $[1 - \epsilon_+ - \epsilon_\times, 1 - \max(\epsilon_+, \epsilon_\times)]$.

Now given the average error probability $\bar{\epsilon} = \frac{\epsilon_+ + \epsilon_\times}{2}$, the above probability of a correct guess is maximal when $\epsilon_+ = \epsilon_\times = \bar{\epsilon}$. In other words, given the average error probability, the eavesdropping strategy that maximizes the average probability of correct guess is the one for which the error probability is independent of the choice of basis. The resulting probability of correct guess

$$P_c = \tfrac{1}{2} + \sqrt{1 - \bar{\epsilon} - x}(\sqrt{x} + \sqrt{2\bar{\epsilon} + x - 1}) \tag{20}$$

reaches its maximum for $x = 1 - 2\bar{\epsilon} + \bar{\epsilon}^2$ at which point

$$P_c = \tfrac{1}{2} + \sqrt{\epsilon(1 - \epsilon)}. \tag{21}$$

The above formula is identical to the formula obtained by Cirac and Gisin [10] in their study of the security of BB84 against a class of incoherent attacks with similar conditions for symmetry (see figure 1). The fact that our incoherent symmetric eavesdropping strategy has effectively the same power as the BB84 incoherent symmetric eavesdropping strategy is surprising. This is particularly so given that the maximally entangled state $|00\rangle_+ + |11\rangle_+$ has the following interesting property:

$$A \otimes I(|00\rangle_+ + |11\rangle_+) = I \otimes A^T(|00\rangle_+ + |11\rangle_+) \tag{22}$$

where A is any operator. This implies that any operation on one qubit can be executed remotely by performing the transpose of that operation on the other qubit, provided that the state of the two qubits is maximally entangled. In spite of this, there is no operator C such that

$$A \otimes B(|00\rangle_+ + |11\rangle_+) = I \otimes C(|00\rangle_+ + |11\rangle_+) \tag{23}$$

which is why the two-qubit attack is strictly more general than the single-qubit attack. This is, of course, because the operation represented by B will in general result in a non-maximally entangled state which no longer has the property of remote execution of operations.

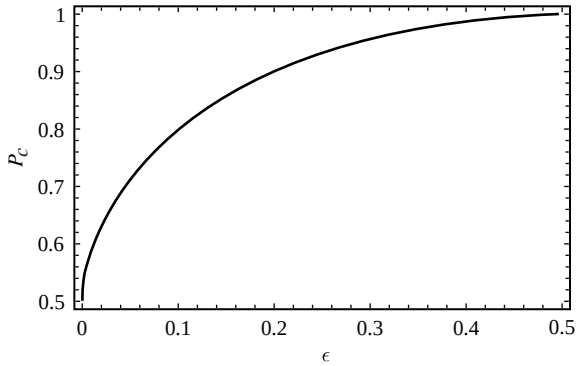

Figure 1. Efficiency of the symmetric two qubit attack. The probability of a correct guess is plotted against the error rate induced by eavesdropping.

Note that the above result can also be expressed as a trade-off between the error rate and the mutual information obtained by Eve about the nature of the state communicated by Alice to Bob. In this case we have a situation equivalent to a binary symmetric channel so that the mutual information is the capacity of that channel and is given by [2]

$$I = 1 + P_c \log P_c + (1 - P_c) \log(1 - P_c). \tag{24}$$

As before, the greater the mutual information gained by Eve the greater the (detectable) error rate induced in the communication.

In this paper we have analysed a symmetric incoherent eavesdropping strategy against the BBM92 quantum key distribution protocol. We have assumed that Eve controls preparation of the entangled photons. In spite of this, we have found that there is no benefit for the purpose of eavesdropping when compared to symmetric incoherent eavesdropping in BB84. We hope that this stimulates further investigation into entanglement-based quantum cryptography.

Acknowledgments

This work was supported in part by the European TMR Research Network ERP-4061PL95-1412, Hewlett Packard and Elsag plc. We gratefully acknowledge interesting discussion with Hans Briegel, Artur Ekert, Norbert Lütkenhaus and Dominic Mayers.

References

[1] Mayers D 2001 *J. ACM* at press
(Mayers D 1998 *Preprint* quant-ph/9802025)
Lo H-K and Chau H F 1999 *Science* **283** 2050–6
Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 1999 *Preprint* quant-ph/9912053
Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[2] Shannon C E and Weaver W 1949 *The Mathematical Theory of Communication* (Urbana, IL: University of Illinois Press)
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (Piscataway, NJ: IEEE) p 175
[4] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[5] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[6] Fuchs C A and Peres A 1996 *Phys. Rev.* A **53** 2038
[7] Brassard G and Salvail L 1994 *Advances in Cryptology, Proc. Eurocrypt'93* (*Lecture Notes in Computer Science* vol 765) (Berlin: Springer) pp 410–23
[8] Uhlmann A 1976 *Rep. Math. Phys.* **9** 273
[9] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)
[10] Cirac J I and Gisin N 1997 *Preprint* quant-ph/9702002