acta physica slovaca vol. 46 No. 3, 439 - 444 June 1996

AN UNCONDITIONALLY SECURE PROTOCOL FOR QUANTUM CRYPTOGRAPHY[1]

Chiara Macchiavello[2], Anna Sanpera[3]
Department of Physics, Oxford University, Parks Road, OX1 3PU Oxford, UK

Received 31 May 1996, accepted 7 June 1996

We provide a brief review of unconditionally secure communications between two parties who have access to a noisy quantum channel and a classical broadcasting channel. The protocol, originally proposed by Deutsch et al. [1], is based on an efficient "quantum privacy amplification" method and allows any eavesdropper's information on the key to be reduced to any prescribed arbitrarily small value.

1. Introduction

Quantum phenomena have provided a way to transmit messages in perfect secrecy, a goal that is not achievable in the realm of classical physics. The basic idea in quantum cryptography [2-4] is to exploit quantum effects, such as the Heisenberg uncertainty relations or the quantum correlations between two separate systems, to establish a common secret key between two parties (Alice and Bob). In existing protocols Alice and Bob detect the presence of an eavesdropper (Eve) by performing quantum measurements on subensembles of the set of transmitted particles and using the results to determine, with any desired degree of confidence, that the transmitted particles are not entangled with any third system such as an eavesdropper. If some entanglement with an external system is detected, Alice and Bob can decide either to restart the transmission of the key from the beginning or, if the degree of eavesdropping is not too high, to apply "privacy amplification" techniques [5]. Such techniques are applied on the "corrupted" sequence of classical bits that Alice and Bob share and allow to distill from this a shorter but safer sequence of random bits that can then be used as the key to transmit the secret message. However, the security of quantum cryptography has so far been proved only for the idealised case where the quantum channel, in the absence of eavesdropping, is noiseless.

In the present paper we describe a quantum protocol [1] that allows to solve the problem of security over noisy channels. In contrast to all previous methods, where

[1]Presented at the 4th central-european workshop on quantum optics, Budmerice, Slovakia, May 31 - June 3, 1996

[2]E-mail address: c.macchiavello1@physics.oxford.ac.uk
[3]E-mail address: a.sanpera1@physics.oxford.ac.uk

0323-0465/96

quantum mechanical effects were used only to detect eavesdropping and privacy amplification was performed in a classical way, our method exploits quantum phenomena both for detecting eavesdropping and for privacy amplification. In the following we shall refer to this new concept of privacy amplification as "quantum privacy amplification" (QPA). A more exhaustive description of the protocol can be found in the original reference [1].

2. Description of the protocol

The protocol starts with the distribution of an ensemble of pairs of two-level particles (also called "qubits") in the state $|\phi^+\rangle$ between Alice and Bob, as first proposed in [3], where

$$|\phi^\pm\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$
$$|\psi^\pm\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \qquad (1)$$

is the so-called "Bell basis". The states $|0\rangle$ and $|1\rangle$ of each particle in (1) denote respectively spin up and spin down states along the z axis (or any two basis states of a two level system). Alice and Bob receive each one particle from each pair.

The original entanglement–based protocol [3] is secure in the ideal case of a perfect source, with a noiseless transmission channel and absence of eavesdropping. In such case Alice and Bob share an ensemble of pairs in the state $|\phi^+\rangle$ and they can establish a secure key by measuring the spin of the particles that they receive along parallel directions (say, along the z axis). In general, however, this will not be the case since each pair would have become entangled with the environment.

The protocol that we propose is based on the transmission of entangled particles, as in the original entanglement–based scheme, but the particles are not immediately measured to establish the key: the measurements are performed as the last step of the protocol and the particles that Alice and Bob receive are first stored and exposed to a QPA procedure. The aim of such procedure is to disentangle the distributed pairs from any external system (including an eavesdropper). In this way the external system will have no information at all about the outcomes of the measurements that Alice and Bob will later perform in order to establish the key. The QPA step is therefore the quantum analogue of classical privacy amplification procedures in the sense that it allows to distill a smaller fraction of "safer" pairs from an ensemble of corrupted pairs, but the ultimate security it provides comes from the fact that it is performed in a quantum mechanical fashion.

Our protocol is composed of four basic steps:

(i) distribution of entangled pairs (analogous to the original scheme [3]);

(ii) evaluation of the maximum information that an eavesdropper could obtain on the state of the distributed pairs;

(iii) quantum privacy amplification;

(iv) measurements to establish the secret key.

We shall mainly describe the second and third steps, which contain the new ingredients needed to guarantee a perfect security of the shared key. To allow for complete generality we analyse the scenario which is the most favorable for an eavesdropper, *i.e.* where the eavesdropper herself is allowed to prepare all the qubit pairs that Alice and Bob will receive and they will subsequently use for cryptography. Any realistic situation involves environmental noise that is not under Eve's control, but this may be treated as a special case in which Eve is not using the full information available to her. The most general state resulting from Eve's preparation can be written as

$$|\Psi\rangle = c_0\,|00\rangle\,|R_0\rangle + c_1\,|01\rangle\,|R_1\rangle + c_2\,|10\rangle\,|R_2\rangle + c_3\,|11\rangle\,|R_3\rangle\,, \qquad (2)$$

where the four states of Eve's system $|R_i\rangle$ are normalised but, in general, not orthogonal to each other. By preparing the state $|\Psi\rangle$, Eve predetermines the joint probability distribution of the four possible outcomes of the spin measurements along the z-axis and therefore she will have some a priori information about the actual bit values registered by Alice and Bob. For example, she knows that Alice will register bit value "0" with probability $|c_0|^2 + |c_1|^2$ and bit value "1" with probability $|c_2|^2 + |c_3|^2$ which gives her $1 - H(|c_0|^2 + |c_1|^2)$ bits of a priori information about Alice's result ($H(p) = -p\log p - (1-p)\log(1-p)$). Similarly she has $1 - H(|c_0|^2 + |c_2|^2)$ bits of a priori information about Bob's result. Eve can also measure her ancilla after Alice's and Bob's measurements and try to determine its relative state $|R_i\rangle$. In general Eve cannot reliably distinguish between those states because they are not orthogonal to each other and an upper bound on the amount of information she can acquire is given by Holevo's theorem [6]:

$$I_{\rm acq} = S(\varrho_R) = -{\rm Tr}\varrho_R \log \varrho_R \qquad (3)$$

where

$$\varrho_R = \sum_{i=0}^{3} |c_i|^2\,|R_i\rangle\langle R_i|\,. \qquad (4)$$

Since the global state (2) is pure, for any set of relative states $\{|R_i\rangle\}$ the von Neumann entropy $S(\varrho_R)$ is equal to the von Neumann entropy $S(\rho)$ where ρ is the reduced density operator describing the state of the two particles $\rho = {\rm Tr}_{\rm ancilla}\,|\Psi\rangle\langle\Psi|$. Thus Eve's acquired information about the outcomes registered by Alice and Bob is bounded by

$$I_{\rm acq} = S(\rho). \qquad (5)$$

The total information available to Eve is then bounded by the sum of the a priori and the acquired information. Alice and Bob can evaluate such bound by choosing at random a subensemble of their pairs and estimating ρ by evaluating spin correlations on this subensemble. If the resulting value of the total information exceeds a prefixed threshold and the resulting key cannot be considered secure, the QPA step is then applied. The way to estimate the maximum amount of information available to Eve that we have just described may not be the only or the most general one, but as we will

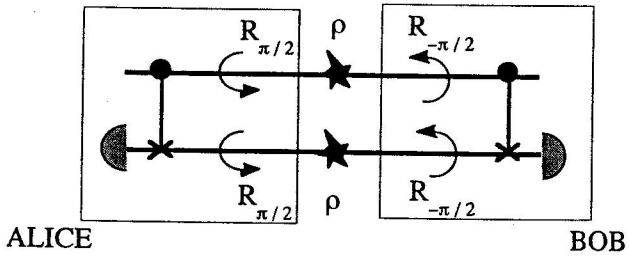

Fig. 1. Schematic representation of the QPA procedure. Alice performs a $\pi/2$ rotation on her particles and a CNOT. Bob performs a $-\pi/2$ rotation and a CNOT. Alice and Bob then measure the target pair and keep the control pair for the following iteration if the results coincide.

now show the QPA procedure that Alice and Bob perform allows to reduce any bound to any arbitrarily small value. Therefore, the security of the protocol is completely indepentent of the criterion adopted to evaluate the degree of eavesdropping at step ii).

For the sake of simplicity, let us now see how the QPA works in the case of an ensemble of pairs of spin 1/2 particles all described by the following density matrix

$$\rho = a\,|\phi^+\rangle\langle\phi^+| + b\,|\psi^-\rangle\langle\psi^-| + c\,|\psi^+\rangle\langle\psi^+| + d\,|\phi^-\rangle\langle\phi^-|, \tag{6}$$

namely a diagonal matrix in the Bell basis representation. Alice and Bob have first to divide the set of particles they receive into groups of two particles each and perform the following simple local operations that represent the basic step of our QPA algorithm, shown in Fig. 1. Alice performs a rotation by $\pi/2$ along the x axis on both her particles and Bob performs a rotation in the opposite direction $R_{-\pi/2}$ along the x-axis on his two particles. Then both Alice and Bob perform a quantum Controlled-NOT operation [7] where one of the pairs gives the two control qubits and the other one the two target qubits. Such operation acts on two qubits and gives

$$|x\rangle\ |y\rangle \longrightarrow |x\rangle|x \oplus y\rangle \qquad (x,y) \in \{0,1\}, \tag{7}$$

where the first qubit is the control and the second the target and $\oplus$ is addition modulo 2. Subsequently Alice and Bob measure the spin z-component of the target qubits and publicly exchange the results they have obtained. If the outcomes coincide they regard the operation as successful and keep the control pair for the second round. If the outcomes do not coincide they agree to discard the two pairs.

We have now described a single step of the QPA procedure. If it is successful the remaining pairs will still be described by a density matrix of the form (6), still diagonal in the Bell basis representation, with diagonal elements $\{a', b', c', d'\}$ given by

$$a' = (a^2 + d^2)/p \tag{8}$$
$$b' = 2bc/p \tag{9}$$

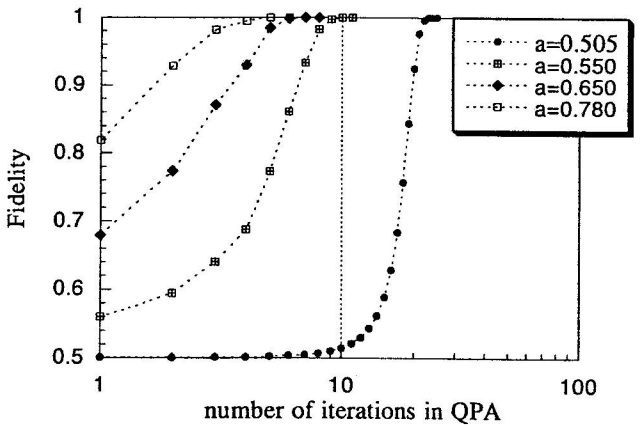

Fig. 2. Average fidelity as a function of the number of iterations for four different values of the initial fidelity a_0.

$$c' = (c^2 + b^2)/p \tag{10}$$
$$d' = 2ad/p \tag{11}$$

Here $p = (a+d)^2 + (b+c)^2$ is the probability of success i.e. that Alice and Bob obtain coinciding outcomes in the measurement on the target pair. If Alice and Bob have sufficiently many pairs at their disposal the procedure just described can be repeated with those pairs which survived the first filtering. The aim of the procedure is to drive the surviving pairs as close as possible to the original uncorrupted state $|\phi^+\rangle$, at the cost of sacrificing some of the distributed pairs (the target pairs and the control pairs that are discarded after the measurements). We take the fidelity

$$F = \langle\phi^+|\,\rho\,|\phi^+\rangle \tag{12}$$

as a measurement of the closeness of the state ρ to the uncorrupted state $|\phi^+\rangle\langle\phi^+|$ [8]. Such quantity is given by the first diagonal element a (or a') of the density matrix in the Bell basis representation. If the initial fidelity a_0 is greater than 0.5 then the average fidelity increases in the process and asymptotically goes to one [1].

In order to check that such condition is fulfilled before starting the QPA procedure Alice and Bob can estimate the initial average fidelity a_0 by measuring spin correlations on a randomly selected set of distributed pairs. The fidelity is given by

$$a = \frac{1}{4}(1 + \langle\sigma_x\sigma_x\rangle - \langle\sigma_y\sigma_y\rangle + \langle\sigma_z\sigma_z\rangle). \tag{13}$$

In Fig. 2 we plot the fidelity as a function of the number of iterations for four different initial states of the form (2) with $b = c = d$. As we can see, the convergence to the unit value is very fast and few iterations of the procedure are needed in practice.

When the fidelity approaches 1 the average density operator of the remaining pairs necessarily approaches the pure state $|\phi^+\rangle\langle\phi^+|$ and the joint state of Eve's ancilla and the particles necessarily approaches a product state of the form

$$\left|\tilde{\Psi}\right\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)\,|R\rangle\,, \tag{14}$$

because a pure state cannot be entangled with another system. The QPA procedure disentangles the particles from the eavesdropper's ancilla and clearly reduces to zero Eve's total information about the outcomes of Alice's and Bob's measurements of the spin components. Alice and Bob can now establish the key without further processing.

5. Conclusions

We have presented a quantum cryptographic protocol that allows for the secure transmission of a secret key through a noisy channel. We have first discussed a way to evaluate the upper bound on the amount of information that an eavesdropper could obtain about the distributed signals between the two legitimate users. We have then presented a "quantum privacy amplification" procedure to be applied on the distributed pairs before the key is established. Although the procedure has been explicitly discussed in the simplest case of an ensemble of distributed pairs all described by the same density matrix (diagonal in the Bell basis), the procedure can be straighforwardly generalized for more complex initial preparations [1]. The method guarantees a complete secrecy of the key that is subsequently established.

Acknowledgements We would like to thank David Deutsch, Artur Ekert, Richard Jozsa and Sandu Popescu for a joint work on quantum privacy amplification, which we reviewed here. C.M. is sponsored by the European Union HCM Programme. A.S. is financially supported by the U.K. Engineering and Physical Science Research Council.

References

[1] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera: *lanl e-print quant-ph/9604039*, submitted to *Phys. Rev. Lett.*;

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

[3] A.K. Ekert: *Phys. Rev. Lett.* **68** (1991) 661;

[4] C.H. Bennett: *Phys. Rev. Lett.* **68** (1992) 3121;

[5] C.H. Bennett, G. Brassard, J.-M. Robert: *SIAM J. Comp.* **17** (1988) 210;

[6] A.S. Holevo: in *Problems of Information Transmission* **9** (1973) 177;

[7] A. Barenco, D. Deutsch, A. Ekert, R. Jozsa: *Phys. Rev. Lett.* **74** (1995) 4083;

[8] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W.K. Wootters: *Phys. Rev. Lett.* **76** (1996) 722;