Pis'ma v ZhETF, vol.62, iss.12, pp.940 - 945 © 1995 December 25

ON THE KEY GENERATION FOR N USERS IN QUANTUM CRYPTOGRAPHY

S.N.Molotkov, S.S.Nazin

Institute of Solid State Physics of RAS

142432 Chernogolovka, Moscow distr., Russia

Submitted 9 November 1995

The problem of key generation for N equivalent users in quantum cryptography is considered. An N-particle wave function allowing simultaneous distribution of the key among N users is put forward. We also propose a scheme for generation and distribution of a key table for N users based on two non-orthogonal states which does not involve any entangled states which seems to be very promising for practical realizations.

Cryptography has a long history and exists for at least two and a half thousand years. One of the main goals of cryptography is generation and distribution of the key available to two or more legitimate users who can use this key to exchange secret information through a public communication channel. In the conventional (classical) cryptography the key (e.g. a random sequence of units and zeros which can be employed to encode an alphabet or any other set of symbols) should be delivered to each legitimate user through a secret communication channel. In the classical cryptography, there is no fundamental protection from eavesdropping during the process of key distribution leaving the legitimate users unaware of the spying act (here "fundamental" means guaranteed by the laws of nature rather than complexity of adopted procedure).

There is a problem of whether it is possible to design a key distribution technique which is fundamentally protected from eavesdropping. A positive solution to this problem (at least in the case of two users) is given by quantum cryptography [1].

The research in this field were initiated by the papers of Ekert [1] and Bennet and Brassard [2]. Several later studies were devoted to development of various key generation schemes for the case of two users [3–5] and their experimental realization [6,7].

Key security in quantum cryptography actually originates in the subtle way in which quantum mechanics combines chance and certainty. Wave function provides the maximum possible information about the system offered by Nature (and there are no additional hidden variables) [8]. The wave function describes a set of potential possibilities contained in the system which are randomly realized during the measurement (interaction of the system with a classical device). The wave function prepared in a special way can guarantee identity of keys constructed by two legitimate users on the basis of simultaneous measurements of two commuting observable. Although each of these observables taken separately can randomly take one of the two values, the measurement of any one of them allows to predict with absolute certainty which value will be obtained in the measurement of the other observable. The key table (outcomes of measurements) is not known in advance to anybody and is not stored anywhere; instead, it comes into being in the course of measurements.

In this report we wish to find out whether it is possible to generate and distribute the key in a system of N ($N > 2$) equivalent users. The problem is that in the known key distribution schemes for two users the key arises only during a long series of quantum mechanical measurements whose results are of fundamentally stochastic nature. Therefore, these schemes cannot be used to transmit any specific key from one user to the other, so that is not clear how to establish a common key shared by all users.

When analyzing various key generation procedures, it is convenient to deal with the spin 1/2 particles. Although these schemes can hardly be implemented in practice (unlike the photon-based techniques already realized experimentally [6,7]), they are very suitable for examination of arising fundamental issues.

Similar to a number of other schemes, our approach is based on the Einstein–Podolsky–Rosen (EPR) effect (for historical reasons usually referred to as the EPR paradox although it is a direct consequence of conventional interpretation of quantum mechanics) [9]. It is known that the spin measurements performed by two distant observers on a system consisting of two particles emitted by a source in the singlet state

$$|\Psi> = \frac{1}{\sqrt{2}}(|\uparrow>|\downarrow> - |\downarrow>|\uparrow>), \tag{1}$$

give rise to non-local correlations. If the axes (polarization analyzers) used by the two observers (hereafter referred to as users A and B) have the same orientation, each of them obtains for the spin component along the specified axis (s_A and s_B) in a random way either $\uparrow$ or $\downarrow$ with equal probabilities. Hence, we have two random variables s_A and s_B. However, quantum mechanics states that these two random variables related to spatially separated events are perfectly correlated: if one of the users detects spin $\uparrow$, he knows for certain that the measurement performed by the other user yielded $\downarrow$, and vice versa. If we assume that the spin up projection corresponds to 1 and spin down to 0, the users A and B will have after a series of measurements two perfectly correlated random sequences of units and zeros which can be used to encode any symbol set. It is important that these random sequences are not stored anywhere and are not transmitted through any channels (public or secret) but arise only during the measurements.

Ekert [1] showed that additional measurements of the spin component along different axes allow to detect eavesdropping at the stage of key distribution if after the measurements are completed, A and B exchange certain information through a public channel.

Consider now the possibility of key generation for the system of N ($N > 2$) *equivalent* users. Similar to the case of two users, we shall search for an N-particle wave function satisfying the following requirements:

1) each user considered separately can obtain in his measurements various values of the measured physical quantity in a random way;

2) all the random variables constructed in this way by all N users are perfectly correlated, i.e. each user can determine the measurement results obtained by *all the rest* users from his own result;

3) a part of the measurement series can be used to detect eavesdropping during the key distribution.

We wish to demonstrate that all the above requirements can be met if one uses the N-particle wave function

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow,\uparrow,\ldots,\uparrow\rangle - |\downarrow,\downarrow,\ldots,\downarrow\rangle), \tag{2}$$

which in fact is a slightly modified Mermin function [10] (here $\uparrow$ and $\downarrow$ correspond to spin-up and spin-down states, respectively, along the z-axis common for all users). It is obvious that in any separate spin component measurement (along the z-axis) each user will obtain either $+1/2$, or $-1/2$ with equal probabilities; however, the results obtained by all users are perfectly correlated since they all simultaneously obtain the same spin component. In addition, it is easily checked that if the measurements are performed along the x-axis, only the outcomes with odd number of users measuring negative spin projections occur. Indeed, taking advantage of known formulas (with obvious notation)

$$|\uparrow\rangle_z = \frac{|\uparrow\rangle_x + |\downarrow\rangle_x}{\sqrt{2}}, \qquad |\downarrow\rangle_z = \frac{|\uparrow\rangle_x - |\downarrow\rangle_x}{\sqrt{2}},$$

relating the states with definite spin component along x- and z-axes, one can see that in the linear combination (2) all the terms containing even number of $\downarrow$ states are cancelled; in other words, the wave function given by Eq.(2) belongs to the subspace of the operator $\sigma_{x1}\cdot\sigma_{x2}\ldots\sigma_{xn}$ with the eigenvalue equal to -1.

Thus, the wave function (2) can be used for a simultaneous key distribution among N users in just the same way as the singlet state (1) for two users. After a long series of measurements the public channel is used to find out in which measurements all users had the same orientation of their analyzers (i.e. they were all along x- or z-axis; in each separate measurement each user randomly chose his analyzer orientation). If all the measurements along the x-axis gave $\sigma_{x1}\cdot\sigma_{x2}\ldots\sigma_{xn} = -1$, the remaining series of measurements along the z-axis can be used to construct a code shared by all N users.

Because of the random analyzer orientation in each measurement, there exists no "eavesdropping strategy" (e.g., substitution of the original source by sending N particles in appropriate pure spin-up and spin-down states along the z-axis) which could not be detected by legitimate users.

It is useful to analyze the key generation process [1] from the viewpoint of information theory [11]. It is known that the knowledge about the system is measured by the information entropy

$$H = -\sum_i P_i \lg_2 P_i, \tag{3}$$

where subscript i labels possible outcomes in the system, and P_i is the probability of the i-th event. In the EPR-type scheme we have two outcomes with equal probabilities $P_1 = P_2 = 1/2$:

	A	B
P_1	$\uparrow$ (1)	$\downarrow$ (0)
P_2	$\downarrow$ (0)	$\uparrow$ (1)

Complete information about each measurement contains

$$H = -2\frac{1}{2}\lg_2(\frac{1}{2}) = 1 \text{ bit}, \tag{4}$$

which is shared by the two users who actually do not exchange any information (identity of their measurement results is guaranteed by quantum mechanics). This single bit represents information contained in the system as a whole.

Suppose that we have a source generating three spin 1/2 particles in the following two states with equal probabilities:

$$|\Psi>_{\frac{1}{2}}=\frac{1}{\sqrt{2}}|\uparrow>(|\uparrow>|\downarrow>-|\downarrow>|\uparrow>), \tag{5}$$

and

$$|\Psi>_{-\frac{1}{2}}=\frac{1}{\sqrt{2}}|\downarrow>(|\downarrow>|\uparrow>-|\uparrow>|\downarrow>),$$

In each measurement act, user A performs two measurements on particles 1 and 2, and user B measures the spin component of particle 3 along the z-axis. Possible outcomes are listed in the following table:

	1	2	3	4
A	↑ (1)	↑ (1)	↓ (0)	↓ (0)
	↑ (1)	↓ (0)	↓ (0)	↑ (1)
B	↓ (0)	↑ (1)	↑ (1)	↑ (1)

It is easily seen that all four outcomes occur with equal probabilities $P_1 = P_2 = P_3 = P_4 = 1/4$. Total information about the system in each measurement contains

$$H_{1234}=-4\frac{1}{4}\lg_2(\frac{1}{4})=2 \text{ bits.} \tag{6}$$

This information is actually redundant, since the key identity requires only one bit of information. Therefore, the available information amounting to 1 bit should be announced through a public channel. After a series of measurements is completed, user A (who possesses more information) announces the measurements which yielded ↑ (1), ↓ (0) and ↑ (1), ↓ (0) (outcomes 2 and 4 in the table). The second user B compares announced measurements with his own results. In the absence of eavesdropping, he would find a perfect correlation in agreement with the table, or otherwise the entire measurement series is discarded. If no eavesdropping is detected, users A and B are left with identical keys defined by the outcomes 1 and 3. The information announced through a public channel contains

$$H_{24}=-2\frac{1}{4}\lg_2(\frac{1}{4})=1 \text{ bit.} \tag{7}$$

Remaining secret information shared by the users (the key) contains

$$H_{1234}-H_{24}=1 \text{ bit.} \tag{8}$$

The fact that the proposed key distribution procedure invoves entangled states can be considered as a serious disadvantage from the point of view of its practical implementation since only the photon-based entangled states seem to allow experimental realization. Two-photon entangled states have already been realized [6] on the basis of second non-linear susceptibility $\chi^{(2)}$. Therefore, a similar approach to the generation of N-photon states would require the N-th order susceptibility which seems unrealistic for $N \geq 4$. Therefore, it would be

interesting to find out whether there exists a scheme for N users which does not involve N-photon entangled states and hence is not based on high-order susceptibilities. We argue that the answer to this question is positive and such a scheme can be realized on any two non-orthogonal states.

The possibility of using any two non-orthogonal states in quantum cryptosystems with two users was first mentioned by Bennet [2]. In the present work we extend his argument to the case of N users.

The scheme is formally rather simple. Suppose that the key table should be delivered to N legitimate users (A, B, C, etc.). We assume that each user has a source of two non-orthogonal states $|u_0\rangle$ and $|u_1\rangle$ ($\langle u_0|u_1\rangle \neq 0$) and an analyzer corresponding to the measurement of two projection operators, $\hat{P}_0 = 1 - |u_0\rangle\langle u_0|$, and $\hat{P}_1 = 1 - |u_1\rangle\langle u_1|$, so that $\langle u_0|P_0|u_0\rangle = 0$ and $\langle u_1|P_1|u_1\rangle = 0$. The method consists in consecutive "propagation" of the key table from one user to the other. Suppose that user A sends a random sequence of states $|u_0\rangle$ and $|u_1\rangle$ to user B who measures either P_0 or P_1 also in random way. A long series of such measurements yields the following results. In the events when user A sent the state $|u_0\rangle$ ($|u_1\rangle$) and user B measured $\hat{P}_0$ ($\hat{P}_1$), the measurement gave zero. Otherwise, when user A sent $|u_0\rangle$ ($|u_1\rangle$) and user B measured $\hat{P}_1$ ($\hat{P}_0$), the measurement gave a positive number. Then user B announces through a public channel which measurements gave non-zero results. These measurements are discarded from the series. In this way users A and B obtain two identical random sequences (when user A sends $|u_0\rangle$ and user B measures $\hat{P}_0$ we have logical zero, while when user A sends $|u_1\rangle$ and user B measures $\hat{P}_1$ we have logical unit). At the next stage user B generates with his source the states $|u_0\rangle$ and $|u_1\rangle$ corresponding to the obtained random sequence and sends them to user C who again performs random measurements of $\hat{P}_0$ and $\hat{P}_1$. After that user C employs the public channel to announce to all users in which measurements a positive result was obtained and users C, B, and A discard these events. Now three users have identical random sequences of units and zeros (although shorter than the initial sequence). The procedure is repeated in a similar way by all the rest users. To enhance the scheme reliability, the end N-th user can close the loop by sending his final random sequence of states $|u_0\rangle$ and $|u_1\rangle$ to the first user A.

When the process is completed all N users have the identical random sequence which can be used as a key table. Security of the scheme as a whole follows from security at each stage [12].

Thus, the proposed scheme does not require N-photon entangled states and allows using any two non-orthogonal states (e.g. single-photon states with clockwise and counterclockwise helicity).

The fundamental difference between the EPR-like schemes and the scheme based on non-orthogonal states is that in the EPR approach employing an entangled state, the measurement (interaction with a classical device) amounts to the realization of one of the possibilities contained in the wavefunction. The outcome of each particular measurement cannot be predicted and cannot be controlled. The specially chosen state only guarantees a complete correlation among the results obtained by all users. As to the scheme based on non-orthogonal states, the user itself chooses which of the two already realized possibilities he wishes to measure.

It is important to note that detection of eavesdropping is of fundamentally statistical nature and requires a long measurement series whose results are partially announced through a public channel. However, a fundamental limitation stems from

the fact that there is no way to make sure that a particular measurement whose result was not announced through a public channel did not suffer from invasion by an adversary or from the channel malfunctions. Which strategy should be followed by legitimate users to counteract possible invasion by an adversary or the technical channel malfunctions is still an open problem and requires a special analysis.

This work was supported by the Russian Foundation for Fundamental Research.

---

1. A.Ekert, Phys. Rev. Lett. **67**, 661 (1991).
2. C.H.Bennet, Phys. Rev. Lett. **68**, 3121 (1992).
3. C.H.Bennet and S.J.Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
4. C.H.Bennet, G.Brassard C.Crépeau et al., Phys. Rev. Lett. **70**, 1895 (1993).
5. L.Goldenberg and L.Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
6. A.K.Ekert, J.G.Rarity, P.R.Tapser, and G.M.Palma, Phys. Rev. Lett. **69**, 1293 (1992).
7. J.G.Rarity and P.R.Tapser, Phys. Rev. **A45**, 2052 (1992).
8. D.Bohm, *Quantum Theory*, Prentice Hall, Engelwood Cliffs, NJ, 1951.
9. A.Einstein, B.Podolsky, and N.Rosen, Phys. Rev. **47**, 777 (1935).
10. N.D.Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
11. C.Shannon, Bell Syst. Techn. J. **27**, 379, 263 (1948).
12. C.H.Bennet, G.Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).