Pis'ma v ZhETF, vol.63, iss.8, pp.646 - 651 © 1996 April 25

QUANTUM CRYPTOGRAPHY BASED ON QUANTUM DOTS

S.N.Molotkov, S.S.Nazin

Institute of Solid State Physics of RAS

142432 Chernogolovka, Moscow District, Russia

Submitted 21 March 1996

Network protocols are formulated for the phase coding and correlated photon pairs quantum cryptosystems. These protocols allow to lift the restriction on the distance between the two legitimate users imposed by the transmission loss in optical fiber. A single photon source and a source of correlated photon pairs based on quantum dots are proposed.

PACS: 03.65.Bz, 89.70.+c, 42.50.Wm

The basic element in the exchange of information between two legitimate users is the key. Formally, the key is a random sequence of units and zeros shared by legitimate users and unavailable for the eavesdropper. After the key table is mapped on the alphabet (the algorithm of this mapping can be publicly known), the secret information can be transmitted through a public channel. It is proved that if the key length is equal to the length of the message and the key is used only once, a perfect secrecy is achieved [1]. Thus, it is possible to have a perfectly secret cryptosystem if the key secrecy is ensured. The classical cryptography always involves some sort of a "courier" for the key distribution. At this stage, it is impossible to guarantee that any attempt of eavesdropping is detected by the legitimate users.

On the other hand, quantum mechanics opens the way for achieving perfect secrecy of the key distribution which is guaranteed by the laws of Nature rather than the refinement of the adopted procedure. Any attempt of eavesdropping can be detected with the probability which can be made arbitrarily close to unity.

The methods for key distribution used in quantum cryptography can be divided into two groups. The first one unites the schemes based on single quantum states [2–7]. All realistic schemes employ the single-photon states. The key point is that a photon cannot be split in two, which ensures the detection of any eavesdropping attempt (provided that the appropriate information exchange protocol between the legitimate users is adopted). The second group contains the schemes based on EPR-effect [8–10][1)].

Recently, a 30 km long optical fiber cryptosystem has been realized [11–13] which uses a highly attenuated laser radiation as a source of single photons (on the average, each pulse contains 0.1 photon). Generally, a pulse can contain more than one photon (although the probability of such an event is rather low). In that case the excess photons can be used for eavesdropping. Therefore, it is highly desirable to have a source of truly single photons.

In the present paper we wish to propose a number of cryptosystems with the light sources based on quantum dots and free from the above drawback.

[1)]Note that there is an error in Ref.[10] in the description of a network protocol for a cryptosystem based on two non-orthogonal states $|u_0>$ and $|u_1>$: in the series of measurements with project operators $P_0 = 1 - |u_0><u_0|$ and $P_1 = 1 - |u_1><u_1|$ all zero (rater than nonzero) results should be discarded. All the rest measurements yield a perfectly correlated random sequence shared by two users: when user A sends $|u_0\rangle$ ($|u_1\rangle$) and user B has a positive result measuring P_1 (P_0) they have logical zero (unit).

Phase coding with the quantum-dot-based light source

The proposed cryptosystem is a Mach-Zender interferometer [13] exploiting a single-photon source. We propose to use a quantum dot to produce single photons. These quantum dots can be fabricated with the MBE technique applied to the A^3B^5 compounds. Suppose that there is a single size-quantized level doubly degenerate in spin (Fig.1*a*).

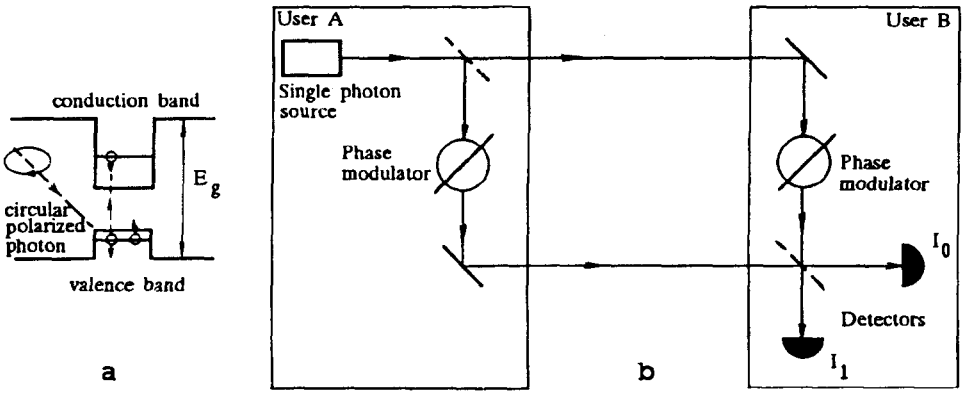

Fig.1. Single photon generation with a quantum dot (a) and the cryptosystem for two users employing the phase-coding protocol (b)

A single electron is excited to the conduction band by the resonant illumination with a circularly polarized light with frequency $\omega \approx \omega_1$. Then the selection rules guarantee that precisely one electron (with appropriate spin) is excited to the doubly degenerate (in spin) level. This consideration is actually extensively used to produce spin-polarized carriers in A^3B^5 semiconductors [14,15]. The reason is that the angular parts of the wavefunctions in the $|j,m>$ basis (for simplicity we assume that the dot possesses the spherical or axial symmetry) in the conduction and valence band can be written as $|\frac{1}{2},\pm\frac{1}{2}>$ and $|\frac{3}{2},\pm\frac{1}{2}>$, respectively [15]. Of course, the light polarization is never perfectly circular and the dot is never a perfect sphere; however, the situation can be improved by placing the system in a uniform magnetic field lifting the spin degeneracy and thus ensuring the excitement of exactly one electron by the resonant radiation.

In the rest of the crystal no carriers are generated since $\hbar\omega_1 < \varepsilon_{gbulk}$. Recombination of the excited electron with a hole in the valence band results in the emission of a single photon. Although the radiative recombination is not the dominant mechanism, the proposed procedure guarantees emission of exactly one photon (note that when a highly attenuated laser radiation is used, a photon is only obtained in each tenth pulse [11]).

It should be noted that during the exciting pulse a stimulated emission of a photon from the quantum dot can occur. To avoid uncontrollable emission of several photon into the optical fiber, one should wait some time after the exciting pulse was cut off, so that only a spontaneous emission of a single photon can take place. Typical radiative recombination times are $\sim 10^{-9}$ s (electron lifetime in the conduction band). The exciting pulse duration should be substantially shorter if one wishes to separate the stimulated (induced by the pulse photons) and spontaneous radiation processes. However, the pulse cannot be too short, since otherwise the inevitable frequency uncertainty would result in the electron excitation not only to the size-quantized level, but also to the bulk crystal conduction band.

The maximum gap between the level and the band edges is determined by the band offsets which for GaAs/AlGaAs compounds are typically several tenths of eV. Therefore, the pulse duration $\sim 10^{-12}$ s allows reliable separation of the spontaneous radiation of single photons.

Network protocol for the phase coding cryptosystem

Actually, the scheme employs interference of a single photon with itself for the key distribution [11]. The scheme allows extension to the key distribution in a network of users. The idea is to gradually transfer the key through a chain of users. Unlike the hierarchy protocol [13], the proposed protocol allows the exchange of information between equivalent users, and, what is more important, allows to distribute a key over the arbitrarily long distances not limited by the transmission loss in the optical fiber employing the users as "relay stations".

Depending on the choice of phases in the arms adopted by the two users A and B (φ_A, φ_B), either one (I_0) or other (I_1) photodetector fires (Fig.1*b*) [11,13]. Intensities at the two detectors are $I_0 \propto \cos^2(\varphi_A - \varphi_B)/2$ and $I_1 \propto$ $\propto 1 - \cos^2(\varphi_A - \varphi_B)/2$ (for semitransparent beam splitters, Fig.1*b*).

The network protocol (which is an extension of the corresponding protocol for two users) is formulated in the following way:

a) User A chooses randomly and independently of user B the phase shift in his arm φ_A from the following four values: 0°, 180°; 90°, 270°. Logical zero corresponds to 0°, 90°, and logical unit is represented by 180°, 270°.

b) User B chooses randomly and independently of user A one of the two values $\varphi_B = 0°$ and $\varphi_B = 90°$. When the photodetector I_0 (I_1) fires, the logical zero (unit) is read off.

c) After a series of measurements is completed, user B employs a public channel to announce which angle ($\varphi_B = 0°$ or $\varphi_B = 90°$) he used in each measurement, but not which photodetector fired.

d) All the measurements when no photodetector fired are discarded. All the measurements where the two users adopted different bases (i.e., B chose $\varphi_B = 0°$ and A used $\varphi_A = 90°$ or 270°, or, vice versa, B chose $\varphi_B = 90°$ and A used $\varphi_A = 0°$ or 180°) are discarded.

e) The rest measurements yield a perfect correlation: if A chose $\varphi_A = 0°$, he knows that B had the detector I_0 firing (since $\varphi_B = 0°$); if A chose $\varphi_A = 180°$, he knows that B had the detector I_1 firing (since $\varphi_B = 0°$); if A chose $\varphi_A = 90°$, he knows that B had the detector I_0 firing (since $\varphi_B = 90°$); if A chose $\varphi_A = 270°$, he knows that B had the detector I_1 firing (since $\varphi_B = 90°$). Similarly, user B can infer which angle was chosen by user A from its own angle φ_B and the knowledge of which the detector fired. Thus the two users share the identical random sequence of units and zeros.

f) To check the absence of eavesdropping during the key generation, results of some measurements are announced through a public channel. These measurements should demonstrate a perfect correlation. Because of the random choice of phases, any eavesdropping destroys the perfect correlation and is inevitably detected; any eavesdropping strategy at least doubles the error rate [13].

g) If no eavesdropping is detected, user B sends to user C the single photons employing successively the left measurements. Since he knows for each

measurement the phase shift chosen by user A, he reproduces in each event this angle $\varphi_B = \varphi_A$ when sending a photon to user C who randomly chooses the phase shift in his arm, just as B did at the preceding stage.

h) When the entire series is exhausted, user C announces through a public channel which base ($\varphi_C = 0°$ or $\varphi_C = 90°$) he used in each measurement. Then user B announces through a public channel (also available for A) which measurements should be discarded because different bases were chosen. The rest measurements should exhibit a perfect correlation. Knowing his own bases and which of the two photodetector fired, user C can determine which angle was employed by user B. At the same time, user B used the same angle as user A at the preceding stage. Since a random subsequence of a random sequence is a random sequence itself, the three users A, B, and C share the same random sequence of units and zeros.

i) After that users B and C disclose the results of some measurements to detect possible eavesdropping (these measurements are discarded by all users). If no eavesdropping is detected, the procedure is repeated by user C with the next user (note that this can be done by any of the users A, B, and C). Security of the system as a whole follows from the security at each stage. As a results, a network of equivalent users is created.

Note that in the proposed scheme the key can be transmitted over the distances exceeding the photon decay length in the optical fiber if the intermediate users are simply used as a sort of "relay stations" (of course, no standard relay device can be used with single photons). Therefore, the proposed protocol lifts the restriction on the key distribution line length in optical fiber quantum cryptosystems.

EPR-cryptosystem with a photon source based on two quantum dots

EPR-based schemes for the key generation involve simultaneous measurements of the photon field at two distant points [9,16] (Fig.2*a*; we shall use the term "EPR-scheme" for the cryptosystem based on a source of correlated photon pairs). Depending on the phase shifts (φ_A and φ_B) in the arms controlled by the two users, their measurements prove to be perfectly correlated. The algorithm for choosing the phase shifts is rather similar to the previous case; the appropriate choice of phase shifts results in simultaneous firing of I_0 and I_0', or I_1' and I_1'. Usually the correlated photon pairs are produced with a laser-illuminated non-linear crystal. In our case an incident photon with frequency ω_0 undergoes a cascade decay into a pair of photons with energies $\omega_1 + \omega_2 = \omega_0$. When using the laser radiation, it is impossible to ensure that exactly one pair of photons is sent into the line. We propose to employ a pair of tunnel-coupled quantum dots to produce a correlated photon pair. Each dot is assumed to have a single size-quantized energy level, one of the dots being smaller than the other, so that its energy level is higher than that in the second dot (Fig.2*a*). The levels are slightly shifted (dashed lines in Fig.2*a*) by the tunnel coupling which should be sufficiently weak. As already discussed, excitation of a single electron to the level 1 is achieved by circularly polarized light. A correlated photon pair is produced in the following way. First the electron undergoes the transition $1 \rightarrow 2$ in the conduction band emitting exactly one photon with frequency $\approx \omega_{12}$, and then it goes from the metastable level 2 to level 3 in the valence band emitting exactly one photon with energy $\approx \omega_{23}$. The distance between the quantum dots is chosen to make the tunnel coupling between them sufficiently weak. This coupling determines the electron lifetime for the transition $1 \rightarrow 2$ (τ_{12}). The interband

radiative recombination times τ_{23} is actually the parameter of the material, and for the A^3B^5 compounds is $10^{-8} \div 10^{-9}$ s. The barrier between the dots can always be made wide enough to ensure the inequalities $\tau_{12} \gg \tau_{23}$. In that case the second photon is emitted immediately after the first one. If the delay time in the interferometer arm ΔT is chosen so that $\tau_{23} \ll \Delta T \ll \tau_{12}$ (Fig.2*b*), the photons can be considered as emitted simultaneously. These inequalities are sufficient for a perfect correlation in the photocounts of two distant observers [16]. In fact, this scheme is close to the generation of correlated photon pairs through an atomic metastable level [16]. Of course, the efficiency of the cascade processes is of the order $\tau_{23}/\tau_{12} \ll 1$ due to the possibility of a direct recombination $1 \to 3$ with the characteristic time $\tau_{13} \approx \tau_{23}$. In the EPR protocol the events where only one photon was emitted (only one photodetector fired) are discarded and the low probability of the cascade process is the inevitable price for security. Note that the EPR protocol also allows the key distribution over the networks from one user to another, although at first glance there is a fundamental difference between the phase coding and EPR protocols (since in the second case useful information comes into being only in the course of measurements unlike the first case where it is extracted from a series of states prepared in advance).

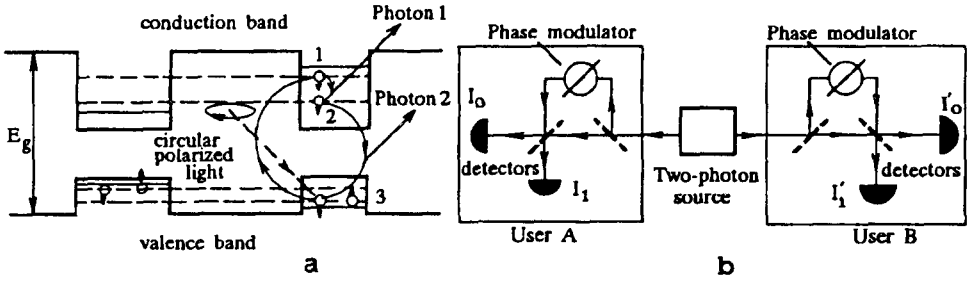

Fig.2. Generation of a pair of correlated photons from two tunnel-coupled quantum dots (a) and the corresponding cryptosystem (b)

The network protocol for an EPR-cryptosystem is a direct extension of the scheme for two users [9] modified for a chain of users.

a) Users A and B randomly and independently of each other choose the phase shifts φ_A and φ_B from the two values $\varphi_A = 0°$, $90°$ and $\varphi_B = 0°$, $-90°$.

b) The probability of simultaneous firing of two detectors I_0, I'_0 or I_1, I'_1 (Fig.2*b*) is $p(I_0, I'_0) = p(I_1, I'_1) \propto 1 - \cos(\varphi_A + \varphi_B)$ (perfect correlation, the photons hit either I_0, I'_0, or I_1, I'_1 if $\varphi_A + \varphi_B = 0^0$). In the case $\varphi_A + \varphi_B = 90^0$ one has a perfect anticorrelation: either one photon hits I_0 and the second one I'_1, or vice versa the first photon hits I_1 and the second one I'_0.

c) After a series of measurements is completed, the measurements where only one detector fired or where $\varphi_A + \varphi_B \neq 0$ are discarded. If the absence of eavesdropping the rest measurements should be perfectly correlated and constitute the key. The check for eavesdropping is again performed by publicly disclosing results of some measurements which should exhibit a perfect correlation (or anticorrelation). If the disclosed results reveal only a partial correlation, the users can conclude that an attempt of eavesdropping took place.

d) Then user B employs his EPR source to carry out a series of measurements with user C who chooses his phase shift φ_C randomly and independently of B. In each particular measurement user B chooses the same phase shift φ_B as he chose in his joint measurements with A (user B knows which angle was chosen by A).

e) The measurements where only one detector fired or where $\varphi_B + \varphi_C \neq 0$ are discarded. In approximately half of the measurements, where $\varphi_B + \varphi_C = 0$ the pairs (I_0, I_0') or (I_1, I_1') can occur. Then user B announces to users A and C through a public channel the measurements where there was no coincidence with the preceding series with user A. As a result, only those measurements are left which yielded identical results for all three users. In this scheme approximately $1/2 \cdot 1/2 \cdot 1/2 = 1/8$ of the measurements performed by users A and B are discarded. The secrecy is again ensured by the secrecy of each stage in the chain.

It should be emphasized that for any adopted protocol the test for eavesdropping in quantum cryptography is of statistical nature (eavesdropping can only be detected in a series of measurements, rather than in a single measurement). Needless to say, any practical scheme should take into account all the imperfections inherent to a particular physical system chosen to implement the adopted protocol (finite spectrum width of a correlated photon pair source, scatter in the optical phase modulator characteristics, etc). All these imperfections will inevitably increase the error rate in the transmission line. Strictly speaking, the eavesdropper can avoid detecting if the additional error rate introduced by his activity does not exceed the "natural" error rate in the line. However, in that case the amount of information about the distributed key obtained by him will be proportionally small (legitimate users should agree on which error rate is considered as allowed).

The authors wish to thank I.I.Tartakovsky, M.V.Lebedev, S.T.Pavlov, and S.V.Iordansky for reading the manuscripit and useful remarks.

This work was supported by the Russian Fund for Fundamental Research grant 96-02-19396.

---

1. C.E.Shannon, Bell Syst. Techn. J. **28**, 657 (1949).
2. C.H.Bennet, G.Brassard, and N.D.Mermin, Phys. Rev. Lett. **68**, 557 (1992).
3. C.Bennet, Phys. Rev. Lett. **68**, 3132 (1992).
4. S.J.D.Phoenix, Phys. Rev. **A48**, 96 (1993).
5. S.M.Barnett and S.J.D.Phoenix, Phys. Rev. **A48**, R5 (1993).
6. A.K.Ekert, B.Huttner, G.M.Palma, and A.Peres, Phys. Rev. **A50**, 1047 (1994).
7. L.Goldenberg and L.Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
8. A.K.Ekert, Phys. Rev. Lett. **67**, 661 (1991).
9. A.K.Ekert, J.G.Rarity, P.R.Tapster, and G.M.Palma, Phys. Rev. Lett. **69**, 1293 (1992).
10. S.N.Molotkov and S.S.Nazin, Pis'ma v ZhETF **62**, 940 (1995).
11. C.Marand and P.D.Townsend, Optics Lett. **20**, 1695 (1995).
12. R.J.Hughes, D.M.Alde, P.Dyer, et al., Contemporary Phys. **36**, 149 (1995).
13. S.J.D.Phoenix and P.D.Townsend, Contemporary Phys. **36**, 165 (1995).
14. A.I.Ekimov and V.I.Safarov, Pis'ma v ZhETF **12**, 193 (1970) [JETP Lett. **12** (1970)].
15. M.I.D'yakonov and V.I.Perel', Zh. Eksp. Teor. Fiz. **60**, 1954 (1971) [Sov. Phys. JETP. **133**, 1053 (1971)].
16. J.D.Franson, Phys. Rev. Lett. **62**, 2205 (1989); Phys. Rev. Lett. **67**, 290 (1991).