PHYSICAL REVIEW
LETTERS

VOLUME 67 5 AUGUST 1991 NUMBER 6

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert
Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom
(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

PACS numbers: 03.65.Bz, 42.80.Sa, 89.70.+c

Cryptography, despite a colorful history that goes back to 400 B.C., only became part of mathematics and information theory this century, in the late 1940s, mainly due to the seminal papers of Shannon [1]. Today, one can briefly define cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it. However, as the computational process associated with transforming the information is always performed by physical means, one cannot separate the mathematical structure from the underlying laws of physics that govern the process of computation [2]. Deutsch has shown that quantum physics enriches our computational possibilities far beyond classical Turing machines [2], and current work in quantum cryptography originated by Bennett and Brassard provides a good example of this fact [3].

In this paper I will present a method in which the security of the so-called key distribution process in cryptography depends on the completeness of quantum mechanics. Here completeness means that quantum description provides maximum possible information about any system under consideration. The proposed scheme is based on the Bohm's well-known version of the Einstein-Podolsky-Rosen *gedanken experiment* [4]; the generalized Bell's theorem (Clauser-Horne-Shimony-Holt inequalities) [5] is used to test for eavesdropping. From a theoretical point of view the scheme provides an interesting and new extension of Bennett and Brassard's original idea, and from an experimental perspective offers a practical realization by a small modification of experiments that were set up to test Bell's theorem. Before I proceed any further let me first introduce some basic notions of cryptography.

Originally the security of a cryptotext depended on the secrecy of the entire encrypting and decrypting procedures; however, today we use ciphers for which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers a set of specific parameters, called a *key*, is supplied together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key, and this key, which is very important, may consist of any *randomly chosen,* sufficiently long string of bits. Once the key is established, subsequent communication involves sending cryptograms over a public channel which is vulnerable to total passive interception (e.g., public announcement in mass media). However, in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and a very secure channel. Since the interception is a set of measurements performed by the eavesdropper on this channel, however difficult this might be from a technological point of view, *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 [3]. In the following I describe a quantum channel which distributes the key

without any "element of reality" associated with the key and which is protected by the completeness of quantum mechanics.

The channel consists of a source that emits pairs of spin-$\frac{1}{2}$ particles, in a singlet state. The particles fly apart along the z axis, towards the two legitimate users of the channel, say, Alice and Bob, who, after the particles have separated, perform measurements on spin components along one of three directions given by unit vectors $\mathbf{a}_i$ and $\mathbf{b}_j$ $(i,j=1,2,3)$, respectively, for Alice and Bob. For simplicity, both $\mathbf{a}_i$ and $\mathbf{b}_j$ vectors lie in the x-y plane, perpendicular to the trajectory of the particles, and are characterized by azimuthal angles: $\phi_1^a=0$, $\phi_2^a=\frac{1}{4}\pi$, $\phi_3^a=\frac{1}{2}\pi$ and $\phi_1^b=\frac{1}{4}\pi$, $\phi_2^b=\frac{1}{2}\pi$, $\phi_3^b=\frac{3}{4}\pi$. Superscripts "a" and "b" refer to Alice and Bob's analyzers, respectively, and the angle is measured from the vertical x axis. The users choose the orientation of the analyzers randomly and independently for each pair of incoming particles. Each measurement, in $\frac{1}{2}\hbar$ units, can yield two results, $+1$ (spin up) and -1 (spin down), and can potentially reveal one bit of information.

The quantity

$$E(\mathbf{a}_i,\mathbf{b}_j)=P_{++}(\mathbf{a}_i,\mathbf{b}_j)+P_{--}(\mathbf{a}_i,\mathbf{b}_j) - P_{+-}(\mathbf{a}_i,\mathbf{b}_j)-P_{-+}(\mathbf{a}_i,\mathbf{b}_j) \quad (1)$$

is the correlation coefficient of the measurements performed by Alice along $\mathbf{a}_i$ and by Bob along $\mathbf{b}_j$. Here $P_{\pm\pm}(\mathbf{a}_i,\mathbf{b}_j)$ denotes the probability that result ± 1 has been obtained along $\mathbf{a}_i$ and ± 1 along $\mathbf{b}_j$. According to the quantum rules

$$E(\mathbf{a}_i,\mathbf{b}_j)=-\mathbf{a}_i\cdot\mathbf{b}_j\,. \quad (2)$$

For the two pairs of analyzers of the same orientation ($\mathbf{a}_2,\mathbf{b}_1$ and $\mathbf{a}_3,\mathbf{b}_2$) quantum mechanics predicts total anticorrelation of the results obtained by Alice and Bob: $E(\mathbf{a}_2,\mathbf{b}_1)=E(\mathbf{a}_3,\mathbf{b}_2)=-1$.

Let us also, following Clauser, Horne, Shimony, and Holt [5], define a quantity composed of the correlation coefficients for which Alice and Bob used analyzers of different orientation,

$$S=E(\mathbf{a}_1,\mathbf{b}_1)-E(\mathbf{a}_1,\mathbf{b}_3)+E(\mathbf{a}_3,\mathbf{b}_1)+E(\mathbf{a}_3,\mathbf{b}_3)\,. \quad (3)$$

Again, quantum mechanics requires

$$S=-2\sqrt{2}\,. \quad (4)$$

After the transmission has taken place, Alice and Bob can announce in public the orientations of the analyzers they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they used different orientation of analyzers, and a second group for which they used the same orientation of their analyzers. They discard all measurements in which either or both of them failed to register a particle at all. Subsequently, Alice and Bob can reveal publicly the results they obtained but within the first group of measurements only. This allows them to establish the value of S, which, if the particles were not directly or indirectly "disturbed," should reproduce the result of Eq. (4). This assures the legitimate users that the results they obtained within the second group of measurements are anticorrelated and can be converted into a secret string of bits—the key. This secret key may be then used in a conventional cryptographic communication between Alice and Bob.

The eavesdropper cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. The eavesdropper may try to substitute his own prepared data for Alice and Bob to misguide them, but as he does not know which orientation of the analyzers will be chosen for a given pair of particles, there is no good strategy to escape from being detected. In this case his intervention will be equivalent to introducing elements of *physical reality* to the measurements of the spin components. This can be easily seen if we put appropriately modified (by the eavesdropper perfect measurement) correlation coefficients into Eq. (3). We obtain

$$S=\int \rho(\mathbf{n}_a,\mathbf{n}_b)\,d\mathbf{n}_a\,d\mathbf{n}_b[(\mathbf{a}_1\cdot\mathbf{n}_a)(\mathbf{b}_1\cdot\mathbf{n}_b)-(\mathbf{a}_1\cdot\mathbf{n}_a)(\mathbf{b}_3\cdot\mathbf{n}_b)+(\mathbf{a}_3\cdot\mathbf{n}_a)(\mathbf{b}_1\cdot\mathbf{n}_b)+(\mathbf{a}_3\cdot\mathbf{n}_a)(\mathbf{b}_3\cdot\mathbf{n}_b)]\,, \quad (5)$$

where $\mathbf{n}_a$ and $\mathbf{n}_b$ are two unit vectors (for particles a and b, respectively), oriented along the directions of the quantization axes for which the eavesdropper acquired information about the spin component of a given particle. This information could be acquired either through a direct, "brute" measurement of the spin components or through a more subtle attack on the source, e.g., substituting a source that produces a state of two spin-$\frac{1}{2}$ particles correlated with another quantum system on which the actual measurement will be performed by the eavesdropper. The normalized probability measure $\rho(\mathbf{n}_a,\mathbf{n}_b)$ describes the eavesdropper strategy (probability of intercepting a spin component along a given direction for a particular measurement). If only one particle (say, a) is exposed to the measurement performed by the eavesdropper along the direction $\mathbf{n}_a$, one may put $\mathbf{n}_b=-\mathbf{n}_a$ as a particular case in Eq. (5).

Simple calculation for a given orientation of $\mathbf{a}_1,\mathbf{a}_3$ or $\mathbf{b}_1,\mathbf{b}_3$ gives

$$S=\int \rho(\mathbf{n}_a,\mathbf{n}_b)\,d\mathbf{n}_a\,d\mathbf{n}_b[\sqrt{2}\mathbf{n}_a\cdot\mathbf{n}_b]\,, \quad (6)$$

which implies

$$-\sqrt{2}\le S\le\sqrt{2}\,, \quad (7)$$

and contradicts Eq. (4) for any strategy described by the measure $\rho(\mathbf{n}_a,\mathbf{n}_b)$. This way it has been shown that the generalized Bell's theorem can have a practical application in cryptography, namely, it can test the safety of the key distribution. It is not a mathematical difficulty of a particular computation, but a fundamental physical law that protects the system, and as long as quantum theory is not refuted as a complete theory the system is secure.

Regarding more refined attacks associated with the faked source of three (or more) correlated particles, one may think, for example, about delayed measurement on the third particle which is correlated with the two spin-$\frac{1}{2}$ particles. By "delayed" I mean "after the orientation of the analyzers has been publicly revealed by Alice and Bob." However, as we want the two particles to be in pure, singlet state, and Alice and Bob test for it through Bell's theorem, then we cannot correlate the third particle with the other two without disturbing the purity of the singlet state. Therefore I conjecture that there is no universal (good for all orientations $\mathbf{a}_i,\mathbf{b}_j$) state of the faked source which will pass the statistical test of the legitimate users on the subsystem of the two correlated particles a and b. As Alice and Bob can also delay their public communication, the eavesdropper faces the problem of storing the third particle undisturbed for an appropriately long period of time.

I have already mentioned that the proposed channel can be realized as a modification of experiments that tested Bell's theorem. In particular, the celebrated experiment of Aspect and co-workers [6], in which polarized photons were used instead of spin-$\frac{1}{2}$ particles, would be the most obvious choice. In the experiment, every 10 ns pairs of photons were emitted in a radiative atomic cascade of calcium. Acousto-optical switches were used to change the orientation of the analyzers in a time short compared with the photon transit time, and the detection efficiency was over 95%. Apart from changing the main objective of the experiment, and some details in the setup, one will also need software to simulate Alice, Bob, and optionally the eavesdropper. The modifications are minor, so it raises hopes for experimental realization in the nearest future.

The authors thanks D. Deutsch, P. L. Knight, K. Burnett, S. M. Barnett, C. H. Bennett, A. Zeilinger, P. Grangier, G.M. Palma, and P. G. H. Sandars for interesting comments and discussion. This work was supported by Pirie-Reid Fund at Oxford University.

[1] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[2] D. Deutsch, Proc. Roy. Soc. London A **400**, 97 (1985); **425**, 73 (1989).

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology (to be published); C.H. Bennett and G. Brassard, SIGACT News **20**, 78 (1989); see also S. Wiesner, SIGACT News **15**, 78 (1983).

[4] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935); D. Bohm, *Quantum Theory* (Prentice Hall, Englewood Cliffs, NJ, 1951).

[5] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1965); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[6] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).