Quantum Cryptography Without Bell's Theorem and Without EPR

Charles H. Bennett

IBM Research Division, T. J. Watson Research Center
Yorktown Heights, NY 10598, USA.

Gilles Brassard

Département IRO, Université de Montréal, C.P. 6128, succursale "A"
Montréal (Québec), Canada H3C 3J7

N. David Mermin

Laboratory of Atomic and Solid State Physics, Cornell University
Ithaca, NY 14853 – 2501, USA

March 6, 1995

Ekert has described how Einstein–Podolsky–Rosen (EPR) pairs can generate identical random numbers in remote places, with the violation of Bell's inequality certifying the absence of eavesdropping. We show that Bell inequalities are not needed for such an EPR procedure, point out that the non–locality of an EPR scheme that suggests its security is also a potential source of insecurity, and prove a general security theorem that closes this and other loopholes. We note that the EPR scheme is, in fact, equivalent to the single particle key distribution scheme of Bennett and Brassard.

In a striking "practical application" of Einstein–Podolsky–Rosen [1] (EPR) correlations and Bell's theorem [2], Ekert [3], elaborating a suggestion of Deutsch [4], has described a quantum key distribution scheme in which two separated observers perform measurements on a sequence of EPR–correlated pairs of particles in order to generate identical random numbers. By a statistical test that confirms the expected violation of Bell's inequality, they are able to verify that the EPR pairs were not subjected to eavesdropping by a third party.

We show here, however, that neither Bell's inequality nor EPR–correlated states are an essential part of the generation and certification of such a shared random secret. We first demonstrate the security against eavesdropping of a simpler but conceptually equivalent version of Ekert's procedure, which uses only the perfect EPR correlations both to construct the shared random number and to test for listening in.

Ekert conjectured, but did not prove, that his scheme was also secure against a more sophisticated attack—replacement of the true EPR source by a fake source designed to imitate correct EPR statistics while leaking information to an adversary. We prove that such a source cannot exist for our scheme, and generalize this proof to cover all known attacks allowed by the laws of quantum mechanics. Finally, we show that our simpler realization of Ekert's EPR scheme is equivalent to the original key distribution scheme of Bennett and Brassard [5] (BB84), which uses ordinary single particle states instead of EPR pairs, and we prove an analogous security theorem for the BB84 procedure.

Because they rely on a Bell inequality to certify the absence of eavesdropping, each of Ekert's two observers must choose randomly among three coplanar axes for their random spin measurements on the separated particles (0°, 45°, and 90° for one of them and 45°, 90°, and 135° for the other). In our simplified EPR scheme, the observers, whom we call Albert and Boris, each choose randomly between 0° and 90°, which we take to define the x–axis ($\rightarrow$) and z–axis ($\uparrow$). After a series of EPR pairs have been prepared and measured, Albert and Boris announce to each other (and to any adversary, Nathan, who may be listening) which axes they used, but not the results of the measurements. They then agree to discard all instances in which they happened to measure along different axes, as well as instances in which measurements failed because of imperfect quantum efficiency of the detectors. The remaining instances, in which both observers successfully measured the same spin component, ought to be perfectly correlated, if the measurements indeed have been performed on singlet states. To verify that this is so, Albert and Boris publicly compare their measurement results on a sufficiently large random subset (more than half) of the undiscarded instances. If Albert and Boris find that this tested subset is indeed perfectly correlated, they can infer that the remaining untested subset is probably also perfectly correlated, and therefore a suitable source of the shared random number they require.

Ekert shows that if an adversary attempted to eavesdrop by performing arbitrary Stern–Gerlach measurements on one or both of the particles on their way from the EPR source to the legitimate observers, then the linear combination of correlation coefficients appearing in the Clauser–Horne–Shimony–Holt [6] version of Bell's inequality could have no more than half the value it has in the undisturbed singlet state. The analogous bound for our scheme, corresponding to Ekert's Eqs. (5) and (7), is

$$-1 \leq S = \int \rho(n^a, n^b) dn^a dn^b ((n^a \cdot x)(n^b \cdot x) + (n^a \cdot z)(n^b \cdot z)) \leq 1, \qquad (1)$$

as opposed to the value $(-1)+(-1) = -2$ that S has in the undisturbed singlet state.

It might appear that the ultimate security of these procedures lies in the fact that the EPR effect permits two unimpeachably random numbers each to make Heisenberg's "transition from the possible to the actual" in two far-apart places and yet be born as identical twins. Since prior to their miraculous twin birth the numbers do not exist at all, Nathan is in the hopeless position of trying to intercept non-existent information. This, however, is too superficial a view. The real worry for Albert and Boris is that the very magic of the mechanism that suggests they are secure might form the basis for a more sophisticated attack. For if the numbers can miraculously appear to each of them in their remote stations, how can they be sure that Nathan has not substituted for the EPR source a device that produces three particles, cunningly correlated so as to allow information to be brought into existence in *three* remote places, thereby depositing with Nathan some or all of the information Albert and Boris acquire? We shall now prove that such espionage is impossible.

Suppose Nathan deceptively sends Albert and Boris pairs he has prepared himself, entangled with systems available to him for subsequent measurements of his own. [1] The most general entangled state Nathan can prepare is of the form

$$|\Phi\rangle = |\uparrow\uparrow\rangle|A\rangle + |\downarrow\downarrow\rangle|B\rangle + |\uparrow\downarrow\rangle|C\rangle + |\downarrow\uparrow\rangle|D\rangle. \tag{2}$$

where $|\uparrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$, $|\uparrow\downarrow\rangle$, and $|\downarrow\uparrow\rangle$ are a complete orthonormal set of spin states for the pairs being sent to Albert and Boris, and $|A\rangle$, $|B\rangle$, $|C\rangle$, and $|D\rangle$ are Nathan's choices for states of his system, which he does not even have to decide how to measure until after Albert and Boris have gone public.

Even the complete freedom to design an arbitrary entangled state does Nathan no good. If his tampering is to escape detection, the state $|\Phi\rangle$ must be an eigenstate of $\sigma_z^a\sigma_z^b$ with eigenvalue -1, because any pair has a chance of both members being measured along the z–axis, and then being included in the test set. To escape detection with the z test data, Nathan's source is therefore restricted to states of the form

$$|\Phi\rangle = |\uparrow\downarrow\rangle|C\rangle + |\downarrow\uparrow\rangle|D\rangle.$$

But by the same token any pair might instead be measured along the x–axis by both observers, so $|\Phi\rangle$ must also be an eigenstate of $\sigma_x^a\sigma_x^b$ with eigenvalue -1. This further restricts $|\Phi\rangle$ to be of the form

$$|\Phi\rangle = (|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)|C\rangle.$$

Thus the only faked source sure of passing Albert's and Boris' tests is one in which Nathan's system is entirely uncorrelated with the EPR particles, so that a subsequent measurement on it tells him nothing.

So although the EPR effect does not in itself guarantee the security of the scheme, EPR magic cannot be refined to the point where it undermines that security. Indeed, the EPR effect is not needed at all for key distribution, for the simplified EPR scheme is equivalent to the original scheme of Bennett and Brassard[5], which employs only one–particle states.

In the BB84 scheme, a user Alice prepares particles in a random sequence of the four states $|\uparrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$, and $|\rightarrow\rangle$, and sends them to another user Bob, who, like

[1] Such source substitution includes as a special cases the direct Stern–Gerlach measurements on the particles after their emission from an EPR source already discussed, as well as indirect measurements [7][8] in which Nathan causes one or both of the EPR particles to interact coherently with an auxiliary quantum system, to be measured afterward.

Boris, subjects them randomly to measurements of σ_z or σ_x. Alice and Bob proceed just as Albert and Boris did, publicly announcing in each instance whether Alice sent $z-$ or $x-$ eigenstates (but not which variety) and whether Bob measured $z-$ or $x-$ spin components (but not the results of his measurements). They discard instances in which Bob measured σ_x when Alice sent him $|\uparrow\rangle$ or $|\downarrow\rangle$, or measured σ_z in instances when Alice sent $|\leftarrow\rangle$ or $|\rightarrow\rangle$, and they test a random subset of the remaining data, on which they ought to agree if there were no eavesdropping. The only difference between the two schemes is that Alice's random data is chosen by her, while Albert's originates in the random behavior of an EPR particle when he measures it. If Alice wished, however, she could make her four–way random choice by producing an EPR pair herself and measuring one particle along a random axis ($x-$ or $z-$), letting the other particle, now in a known random one of the four states, pass to Bob. The resulting modified BB84 scheme is exactly as strong as the original, since there is no way to tell outside Alice's laboratory which scheme she actually uses.

The security of the BB84 scheme can also be demonstrated directly. The public test in BB84 certifies that the any interaction of an eavesdropper with the particle in transit to Bob has left undisturbed any of the four states that Alice might have sent: $|\uparrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$, and $|\rightarrow\rangle$. But any measurement which fails to disturb non–orthogonal states also yields no information about them. For let the eavesdropper's interaction with the quantum transmission be described by a unitary operator U in the product space of the quantum transmission and the eavesdropper's measuring apparatus. Let $|u\rangle$ and $|v\rangle$ be two non–orthogonal quantum transmissions, such as $|\uparrow\rangle$, $|\rightarrow\rangle$, and let $|a\rangle$ be the eavesdropper's initial quantum state. To evade detection of eavesdropping by Bob, U must leave both $|u\rangle$ and $|v\rangle$ undisturbed so that

$$U(|u\rangle|a\rangle) = |u\rangle|a'\rangle \text{ and } U(|v\rangle|a\rangle) = |v\rangle|a''\rangle, \tag{3}$$

where $|a'\rangle$ and $|a''\rangle$ are two other normalized quantum states of the eavesdropper. But since U is unitary,

$$\langle u|v\rangle = \langle a|\langle u|v\rangle|a\rangle = \langle a'|\langle u|v\rangle|a''\rangle = \langle u|v\rangle\langle a'|a''\rangle. \tag{4}$$

Since $\langle u|v\rangle \neq 0$, it follows that $\langle a'|a''\rangle = 1$, which for normalized states requires that $|a'\rangle = |a''\rangle$. So the eavesdropper is left in the same state $|a'\rangle$ after having interacted with $|u\rangle$ or $|v\rangle$ or indeed any linear combination, such as the other two standard transmissions $|\downarrow\rangle$ and $|\leftarrow\rangle$. Just as in the EPR security theorem, the only attack that can avoid detection is the one that yields no information.

Thus the apparent differences between the EPR and BB84 schemes are superficial. We have disposed of an apparent weakness of the EPR scheme not shared by BB84 — its susceptibility to source substitution. An apparent weakness of the BB84 scheme not shared by EPR is the fact that the information sought by the eavesdropper exists at the time of eavesdropping, whereas in the EPR scheme it is only created later. But the existence or non–existence of the information at the moment of espionage is irrelevant. In neither EPR nor BB84 can the adversary attempt merely to *read* the information. In the EPR case, the adversary's only hope is to create information that Albert and Boris will read and accept as legitimate without realizing that it is now possessed by the adversary as well. We have shown this to be impossible, because anything but a true singlet, uncorrelated with the adversary, will reveal the tampering through deviations from the expected EPR statistics. In the BB84 case, the information does exist, and an adversary can even learn part of it, but, because it is encoded in nonorthogonal states, the adversary can only extract it at the cost of once again disturbing the expected correlations, tipping off Alice and Bob to the presence of an eavesdropper.

So far we have treated the individual quantum transmissions (ie launching and measuring a single particle or EPR pair) as independent events whose results are combined classically by the legitimate participants for purposes of testing and key generation, and can also only be combined classically by an adversary for purposes of eavesdropping. But Wiesner, in the seminal paper [9] that originated the use of non-orthogonal states such as $|\uparrow\rangle$ and $|\rightarrow\rangle$ for cryptographic purposes, raised the possibility of a very powerful adversary whose apparatus interacts coherently with the entire sequence of transmissions, treating them all as a single quantum state in the product space of all the individual experiments and performing an arbitrary indirect measurement on the entire sequence. Our proofs of security of the EPR and BB84 schemes are easily generalized to cover even such an attack. In the EPR case, the only state of N pairs of particles that gives correct EPR statistics for each pair is one whose projection into the 4^N–dimensional Hilbert space of all pairs is a product of singlets, so any substitute source except an uninformative product of singlets risks detection. In the single–particle scheme, the existence of a set of 2^N non–orthogonal states (*e.g.* states with some $|\uparrow\rangle$ particles and some $|\rightarrow\rangle$ particles), none of which is supposed to be disturbed by the eavesdropper, and which together span the entire 2^N dimensional Hilbert space of N particles, guarantees that the eavesdropper also fails to learn anything about any N–particle state.

Turning to more practical matters of cryptography, in any of these schemes, the eavesdropper has a significant chance of learning a small amount of the key without detection, *e.g.* by eavesdropping on just a few particles, none of which might happen to fall into the tested subset. A more useful version of the BB84 scheme which has recently been implemented experimentally [10] replaces the simple subset test by more sophisticated error–correction and hashing techniques. This allows Alice and Bob to arrive at a highly secret key even when their raw data has been compromised by eavesdropping at the statistical margin of detectability or by other sources of leakage (*e.g.* the use instead of single–photon states of low–intensity coherent or incoherent light pulses, which can sometimes be split by an adversary), and even when the data has been significantly corrupted by eavesdropping and noisy detectors.

Gilles Brassard is supported in part by the Natural Sciences and Engineering Research Council of Canada. David Mermin is supported by the National Science Foundation, Grant No. PHY 9022796, and has benefited from many conversations with Oreste Piccioni about EPR roulette and the relevance or irrelevance of Bell's theorem.

References

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

[2] J. S. Bell, Physics **1**, 195 (1965).

[3] A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

[4] D. Deutsch, Proc. Roy. Soc. **A 400**, 97 (1985).

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

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[7] E. B. Davies and J. T. Lewis, *J. Math. Phys.* **17**, 239 (1970).

[8] P. A. Benioff, *J. Math. Phys.* **13**, 231, 908, 1347 (1972).

[9] S. Wiesner, "Conjugate Coding" manuscript ca 1970 unpublished until it appeared in *Sigact News* **15**(1), 78 (1983).

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, **5**, to appear (1992).