# Entangled-state cryptographic protocol that remains secure even if nonlocal hidden variables exist and can be measured with arbitrary precision

Diederik Aerts,[1] Marek Czachor,[1,2] and Marcin Pawłowski[2]
[1]*Centrum Leo Apostel (CLEA) and Foundations of the Exact Sciences (FUND), Vrije Universiteit Brussel, 1050 Brussels, Belgium*
[2]*Katedra Fizyki Teoretycznej i Metod Matematycznych, Politechnika Gdańska, 80-952 Gdańsk, Poland*
(Received 5 March 2005; revised manuscript received 3 February 2006; published 14 March 2006)

Standard quantum cryptographic protocols are not secure if one assumes that nonlocal hidden variables exist and can be measured with arbitrary precision. The security can be restored if one of the communicating parties randomly switches between two standard protocols.

DOI: 10.1103/PhysRevA.73.034303 PACS number(s): 03.67.Dd, 03.65.Ta, 03.65.Ud

It is known that quantum mechanics can be replaced without difficulty by a nonlocal-hidden-variable theory [1–13]. Simultaneously, it is a rather popular belief that an exact knowledge of nonlocal hidden variables would destroy the security of quantum cryptography. In this Brief Report we do not want to get into the crossfire of the discussion if such exact knowledge is possible or not in a hidden-variable theory that is exactly equivalent to standard quantum mechanics. Perhaps, the problem we discuss is present only in theories that are "infinitesimally close" to quantum mechanics. We are not experts in nonlocal hidden variables and, keeping in mind that impossibility proofs may only prove our lack of imagination, prefer to assume the worst possible scenario: Nonlocal hidden variables exist and can be exactly known to our enemies. We harness the nonlocality as a means of protection by a simple modification of a quantum protocol. The idea is illustrated on nonrelativistic Bohm theory, but one can argue that the effect is typical of all nonlocal-hidden-variable theories.

Bohm's theory in its simplest nonrelativistic version [1] involves nonlocal hidden variables $\boldsymbol{q}_j(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n,t)$ that have a meaning of trajectories. The Schrödinger equation for an $n$-particle wave function $\psi(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n,t)$ is related by the rule $\psi=R\exp(iS/\hbar)$ to the system of partial differential equations involving the Hamilton-Jacobi and continuity equations

$$\partial S/\partial t+\sum_{j=1}^{n} m_j\boldsymbol{v}_j^2/2+Q+V=0, \tag{1}$$

$$\partial\rho/\partial t+\sum_{j=1}^{n}\boldsymbol{\nabla}_j(\rho\boldsymbol{v}_j)=0. \tag{2}$$

$\rho=R^2$ is the density of particles, $\boldsymbol{v}_j=\boldsymbol{\nabla}_j S/m_j$ the velocity of the $j$th particle, $V=V(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n,t)$ the usual potential, and $Q=-\hbar^2\Sigma_{j=1}^{n}\boldsymbol{\nabla}_j^2 R/(2m_jR)$ the so-called quantum potential. The hidden trajectories are found by integrating the "guidance equation" $d\boldsymbol{q}_j/dt=\boldsymbol{v}_j$. If the particles are not entangled (and thus not interacting via $V$), that is, the wave fuction takes the product form $\psi(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n,t)=\psi_1(\boldsymbol{x}_1,t)\cdots\psi_n(\boldsymbol{x}_n,t)$, then $Q=\Sigma_{j=1}^{n}Q_j$ where $Q_j=-\hbar^2\boldsymbol{\nabla}_j^2R_j/(2m_jR_j)$. Such particles cannot communicate via the quantum potential. However, for entangled states the particles do interact via $Q$ even if in the sense of $V$ they are uninteracting. Systems described by entangled states are thus nonlocal: The dynamics of the $k$th particle depends on what happens to the remaining $n-1$ particles. What is important, the influences remain within the entangled system. The quantum potential is a useful conceptual tool in this context, but the Bohm theory needs only the Schrödinger and guidance equations.

An eavesdropper (Eve) attempting to read the secret code via the quantum potential, would have to get entangled (in the quantum sense) with the information channel and would be detected by the usual means, say, an Ekert-type procedure [14,15]. If the eavesdropper does not get entangled, the quantum potential will not carry the information she needs.

Let us now assume that Eve can know the hidden trajectory $\boldsymbol{q}(t)$ of the particle carrying the key between the two communicating parties. A Bohmian analysis of spin-1/2 measurements performed via Stern-Gerlach devices [4,5] shows that the knowledge of $\boldsymbol{q}(t_0)$ at some initial time $t_0$ *uniquely* determines the results of future measurements of spin in any direction ([5], pp. 412–415). Single-particle schemes of the variety of the Bennet-Brassard 1984 protocol [16] are thus clearly insecure from this perspective. To make matters worse, a similar statement can be deduced from the analysis of two-electron singlet states described in detail in Chap. 11 of [5]. If two Stern-Gerlach devices are aligned along the same direction (0, 0, 1) and the particles propagate toward the Stern-Gerlach devices of Alice and Bob with velocities $\boldsymbol{v}_1=(0,-|\boldsymbol{v}_1|,0)$ and $\boldsymbol{v}_2=(0,|\boldsymbol{v}_2|,0)$, respectively, then the results of spin measurements are always opposite (that is why we use them for generating the key) but are uniquely determined by the sign of $z_1(t_0)-z_2(t_0)$, where the respective trajectories are $\boldsymbol{q}_1(t)=(0,y_1(t),z_1(t))$ and $\boldsymbol{q}_2(t)=(0,y_2(t),z_2(t))$ (cf. the discussion on p. 470 in [5]). The result agrees with the analysis of [6].

Still, if one looks more closely at the derivation given in [5] one notices that the two particles interact with *identical* magnetic fields. We can weaken this assumption. Following [5] we assume that the time of interaction with the Stern-Gerlach magnets is $T$, the particles are identical, their magnetic moments and masses equal $\mu$ and $m$, and the initial wave functions are Gaussians of half-width $\sigma_0$ in the $z$ direction. We also assume that Alice's Stern-Gerlach magnet produces the field $\boldsymbol{B}_1(\boldsymbol{q}_1)=(0,0,B_0+Bz_1)$ but, contrary to [5], the Bob field is taken as $\boldsymbol{B}_2(\boldsymbol{q}_2)=\kappa(0,0,B_0+Bz_2)$, where $\kappa$ is a real number (in [5] $\kappa=1$). Then the velocities in the $z$ direction (0, 0, 1) read

 

$$dz_1(t)/dt = \hbar^2 t z_1(t)/[4m^2\sigma_0^4\varepsilon(t)] + [m\varepsilon(t)]^{-1}B\mu T \tanh\{[m\sigma_0^2\varepsilon(t)]^{-1} \times [z_1(t) - \kappa z_2(t)]B\mu T t\}, \quad (3)$$

$$dz_2(t)/dt = \hbar^2 t z_2(t)/[4m^2\sigma_0^4\varepsilon(t)] - [m\varepsilon(t)]^{-1}\kappa B\mu T \tanh\{[m\sigma_0^2\varepsilon(t)]^{-1} \times [z_1(t) - \kappa z_2(t)]B\mu T t\}, \quad (4)$$

where $\varepsilon(t)=1+\frac{\hbar^2 t^2}{4\sigma_0^4 m^2}$. The above formulas differ from Eqs. (11.12.15) and (11.12.16) found in [5] only by the presence of $\kappa$. This apparently innocent generalization has a fundamental meaning for the quantum protocol. For reasons that are identical to those discussed by Holland in his book the signs of spin found in the laboratories of Alice and Bob depend on the sign of the term under tanh. However, as opposed to the case of identical magnetic fields this sign is controlled not only by the initial values of $z_1(t_0)$ and $z_2(t_0)$, in principle known to Eve, but also by the parameter $\kappa$ which is known only to Bob. If $|\kappa| \gg 1$ then the sign of this term is practically controlled by the sign of $\kappa$ (recall that the range of $z_1$ is limited by the size of the Gaussian). Choosing the sign of $\kappa$ randomly, Bob can flip the spin of the particle which is already in the laboratory of Alice and is beyond the control of Eve. Eve knows, by looking at $z_1(t_0)$ and $z_2(t_0)$, what will be the result of Alice's measurement if $\mathrm{sgn}(\kappa) = +1$, and that if $\mathrm{sgn}(\kappa)=-1$ the result will be the opposite. But she does not know this sign if Bob keeps it secret. It follows that she gains nothing by watching the trajectory. But Bob always knows the result of Alice's measurement due to the Einstein-Podolsky-Rosen correlations. If he keeps $\kappa>0$ then Alice got the result opposite to what he found in his laboratory because $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ are parallel; if he takes $\kappa<0$ then both Alice and Bob find the same number because $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ are antiparallel. And this is sufficient for producing the key.

Let us finally clarify here one point that can be easily misunderstood at a first reading of our protocol. In the Ekert protocol we have four settings of experimental devices that are used for testing the Bell inequality: $(A,B)$, $(A,B')$, $(A',B)$, $(A',B')$. This part of the data cannot be used for producing the key. We need one more setting, say $(C,C)$, that will be used for the key. In our protocol we have in addition the setting $(C,-C)$. One can even think of our protocol as a version of the Ekert one but with two alternative measurements corresponding to the same observable.

What is important, from the hidden-variable point of view we *can* predict what will be the results (for each pair of particles) of $(C,C)$ and $(C,-C)$ measurements. If the initial hidden variables are such that the results of the measurement of $(C,C)$ would yield, say, $(C,C)=(+,-)$ then the result of $(C,-C)$ is not $(C,-C)=(+,+)$, as one might naively expect, but $(C,-C)=(-,-)$. It is the bit of Bob that does not change even though it is Bob who flips his device. This is how the nonlocality works and why Eve does not know the key.

The work of M.C. and M.P. is a part of the Polish Ministry of Scientific Research and Information Technology (solicited) Project No. PZB-MIN-008/P03/2003. We acknowledge the support of the Flemish Fund for Scientific Research (FWO Project No. G.0335.02). We are indebted to S. Goldstein, P. R. Holland, R. Tumulka, P. Horodecki, and D. Mayers for their comments on preliminary versions of this work.

[1] D. Bohm, Phys. Rev. **85**, 166 (1952).
[2] D. Bohm and B. J. Hiley, *The Undivided Universe* (Routledge, London, 1993).
[3] D. Bohm, Phys. Rev. **89**, 458 (1953).
[4] C. Dewdney, P. R. Holland, A. Kyprianidis, and J.-P. Vigier, Nature (London) **336**, 536 (1988).
[5] P. R. Holland, *The Quantum Theory of Motion* (Cambridge University Press, Cambridge, U.K., 1993).
[6] A. Valentini, Pramana, J. Phys. **59**, 269 (2002).
[7] T. Durt and Y. Pierseaux, Phys. Rev. A **66**, 052109 (2002).
[8] D. Dürr, S. Goldstein, and N. Zanghi, J. Stat. Phys. **67**, 843 (1992); **68**, 259 (1993).
[9] D. Dürr, S. Goldstein, R. Tumulka, and N. Zanghi, Phys. Rev. Lett. **93**, 090402 (2004).
[10] G. Horton and C. Dewdney, J. Phys. A **37**, 11935 (2004).
[11] P. Holland and C. Philippidis, Phys. Rev. A **67**, 062105 (2003).
[12] G. D. Barbosa and N. Pinto-Neto, Phys. Rev. D **69**, 065014 (2004).
[13] P. Holland, Ann. Phys. (N.Y.) **315**, 503 (2005).
[14] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[15] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[16] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984).