Security in Quantum Cryptography vs. Nonlocal Hidden Variables [1]

Diederik Aerts*, Marek Czachor†,* and Marcin Pawłowski†

*Centrum Leo Apostel (CLEA) and Foundations of the Exact Sciences (FUND)
Vrije Universiteit Brussel, 1050 Brussels, Belgium
†Katedra Fizyki Teoretycznej i Informatyki Kwantowej, Politechnika Gdańska, 80-952 Gdańsk, Poland

Abstract. In order to prove equivalence of quantum mechanics with nonlocal hidden-variable theories of a Bohm type one *assumes* that all the possible measurements belong to a restricted class: (a) we measure only positions of particles and (b) have no access to exact values of initial conditions for Bohm's trajectories. However, in any computer simulation based on Bohm's equations one relaxes the assumption (b) and yet obtains agreement with quantum predictions concerning the results of positional measurements. Therefore a theory where (b) is relaxed, although in principle allowing for measurements of a more general type, cannot be experimentally falsified within the current experimental paradigm. Such generalized measurements have not been invented, or have been invented but the information is qualified, but we cannot exclude their possibility on the basis of known experimental data. Since the measurements would simultaneously allow for eavesdropping in standard quantum cryptosystems, the arguments for security of quantum cryptography become logically circular: Bohm-type theories do not allow for eavesdropping because they are fully equivalent to quantum mechanics, but the equivalence follows from the assumption that we cannot measure hidden variables, which would be equivalent to the possibility of eavesdropping... Here we break the vicious circle by a simple modification of entangled-state protocols that makes them secure even if our enemies have more imagination and know how to measure hidden-variable initial conditions with arbitrary precision.

Keywords: quantum cryptography, security, hidden variables, Bohmian mechanics
PACS: 03.67.Dd, 03.65.Ud, 03.65.Ta

THE FUNDAMENTAL PROBLEM OF QUANTUM CRYPTOGRAPHY?

There is a general agreement that quantum mechanics can be replaced by a nonlocal hidden-variable theory [1]. Such a theory involves additional degrees of freedom that we assume to be beyond our reach. However, statistics of the standard measurements would not be changed even if we could access the hidden variables. The proof is trivial: In any computer simulation based on Bohm trajectories we know the initial conditions in question, and yet obtain the correct quantum probabilities [2] satisfying no-eavesdropping criteria. Paradoxically, the criteria are fulfilled even though the eavesdropping is possible [3–7]. There is no contradiction with Bell's theorem because Bohm's hidden variables are nonlocal. This nonlocality has to be taken into account in the computer simulation

[1] An extended version of D. Aerts, M. Czachor, and M. Pawłowski, Phys. Rev. A **73**, 034303 (2006); Erratum — Phys. Rev. A **73**, 059901(E) (2006)

CP889, *Foundations of Probability and Physics - 4,*
edited by G. Adenier, C. A. Fuchs, and A. Yu. Khrennikov

but this is not a problem (for examples of such simulations cf. [4]). Hence the question: Do we base the analysis of security on a *belief* that nonlocal hidden variables do not exist, even though one cannot prove it?

A possible alternative answer comes from those schools of quantum mechanics that develop modern Bohm-type theories [8–13]. Basically all of them argue that the exact knowledge of Bohm trajectories should not be possible. Still, it is easy to see that

(a) there is no general agreement as to the conceptual structure of the 'final' theory since different schools develop different Bohm-type theories;

(b) it is difficult to find an independent-expert opinion on several aspects of Bohm theories, because different schools often do not quote one another;

(c) no-go theorems are in general based on assumptions about possible future theories, but formulated within a paradigm of an old theory (think of the Bohm theory itself as a counterexample to the famous no-go theorem of von Neumann on hidden variables).

So even a superficial analysis shows that doubts as to the ultimate character of some statements are not completely unjustified. Of particular interest is the result from [8] that links limitations on measurements of initial conditions with the form of probability density in position space: Exact knowledge of Bohm trajectories is possible only if $\rho(x) \neq |\psi(x)|^2$. Since such distributions would lead to observable differences from quantum mechanics, one concludes that the eavesdropping is detectable and we are back to the claim that quantum cryptography is absolutely secure. Simultaneously, the authors seem to agree that one of the consequences of their reasoning is the necessity of a faster-than-light communication if $\rho(x) \neq |\psi(x)|^2$. It is not accidental that the argument is very similar to the one for faster-than-light effects in nonlinear quantum mechanics [14–23]. As shown by Mielnik [24] the densities $\rho(x) = |\psi(x)|^\alpha$, $\alpha \neq 2$, are characteristic of a class of nonlinear Schrödinger equations. Mielnik's equations are 'nonlocal-looking but physically local' in the sense of [25], i.e. allow for Polchinski-type miltiparticle extensions of the form introduced in [26]. In this formalism the nonlinear theory is not more nonlocal than the linear one, and $\alpha = 2$ does not play a privileged role. But in Bohm-theories $\alpha = 2$ is important for locality. A natural guess is that the analysis of correlation experiments in Bohm theories does not take into account all the possible subtleties. And measurements of position are correlational.

If there are any doubts or conflicting opinions of experts, a code-maker has the duty to assume the worst possible scenario. In our case it is simpler to modify quantum cryptosystems in a way that maintains their security even if nonlocal hidden variables exist and can be known to our enemies, than to make sure that no subtlety is overlooked in the proof that the assumption is wrong. Paradoxically, the fact that the hidden variables are nonlocal can be used as a protection against eavesdropping. This is the main message of this paper. The modification is cosmetic and can be easily implemented experimentally. Still, it does not work for single-particle cryptosystems, such as BB84.

In order to understand the modification one first has to develop some intuitions concerning nonlocal hidden variable models. All the ideas can be illustarted by means of the toy model introduced in [27, 28] and further elaborated in [29].

WAY OUT OF THE PROBLEM: TOY-MODEL ILLUSTRATION

Take a mass m located on a unit circle. Its position is described by an angle $0 \le \theta < 2\pi$. We now take two additional masses: $0 \le m_1 \le 1$ located at angle α, and $m_2 = 1 - m_1$ located at $\alpha + \pi$. The experiment looks as follows: If the gravitational force between m_1 and m is greater from this between m_2 and m, then the mass m moves from its initial position θ to the new position α; otherwise the mass m moves to the position $\alpha + \pi$. We say the result is $+1$ if m arrives at α, and -1 if it arrives at $\alpha + \pi$, and denote the random variable so constructed A_α. After the measurement is completed we remove masses m_1 and m_2, but m remains in its new location. We can now repeat the experiment with new pair of masses m'_1 and $m'_2 = 1 - m'_1$, located at β and $\beta + \pi$, respectively. The appropriate random variable is denoted by A_β

We are interested in finding probabilities in a series of measurements performed on mass m under the assumption that (i) before the first measurement θ is distributed uniformly, and (ii) in each measurement we randomly select (with uniform distribution) m_1, m'_1, and so on.

In the first measurement we know neither θ nor m_1. Since both θ and m_1 are distributed uniformly the results ± 1 are equally probable. In the second mesurement the position of the mass m is known from the first measurement ($\theta = \alpha$ if the result is $+1$ and $\theta = \alpha + \pi$ in the oposite case) but we do not know m'_1 in the measurement of A_β. The squared distances r_1^2 (or r_2^2) between m and m'_1 (or m and m'_2), read

$$r_1^2 = 4\sin^2\big((\alpha - \beta)/2\big), \quad r_2^2 = 4\cos^2\big((\alpha - \beta)/2\big).$$

The gravitational forces are therefore

$$\begin{aligned} |F_1| &= Gmm'_1/r_1^2 = (Gmm'_1/4)\sin^{-2}\big((\alpha - \beta)/2\big), \\ |F_2| &= Gmm'_2/r_1^2 = (Gmm'_2/4)\cos^{-2}\big((\alpha - \beta)/2\big). \end{aligned}$$

Now $|F_1| > |F_2|$ if $\sin^2\big((\alpha - \beta)/2\big) < m'_1$. The probability that randomly chosen $m'_1 \in [0,1]$ is greater than $\sin^2\frac{\alpha-\beta}{2}$ is $1 - \sin^2\frac{\alpha-\beta}{2} = \cos^2\frac{\alpha-\beta}{2}$. Therefore the probabilities are $p(A_\alpha = \pm 1) = 1/2$,

$$\begin{aligned} p(A_\beta = \pm 1 | A_\alpha = \pm 1) &= \cos^2\big((\alpha - \beta)/2\big), \\ p(A_\beta = \mp 1 | A_\alpha = \pm 1) &= \sin^2\big((\alpha - \beta)/2\big). \end{aligned}$$

The latter two conditional probabilities correspond to first measuring A_α and then A_β. Let us note that the probabilities make sense only for measurements performed one after another, since the mass m must reach α or $\alpha + \pi$ in the first measurement, and β or $\beta + \pi$ in the second one. But it makes no sense to consider m reaching simultaneously α and $\beta \neq \alpha$.

The hidden variables can be split into two groups. The angle θ describing the position of m after or before a measurement is a property of the "system" (plays a role of polarization). Measurements change θ. This parameter is unknown only before the first measurement. After the measurement of A_α the motion of m fixes the value of θ to either

$\theta = \alpha$ or $\theta = \alpha + \pi$. The conditional probabilities follow from our lack of knowledge about m_1', m_1'', and so on, in subsequent measurements. These masses may be regarded as properties of the polarizers. The result of experiment is determined by the polarization θ and the state of the polarizer.

There is only one situation where we know with probability 1 the result of a next measurement: This is when the two polarizers are parallel. Let us note that in the second measurement there exists a possibility that the result will be opposite to what was found in the first measurement, but the probability of this event is zero (it happens only if $m_1' = 0$).

In the BB84 protocol [32] Alice will send to Bob a "polarized particle" with polarization α (i.e. the mass m is located at $\theta = \alpha$). An eavesdropper Eve can look at the position of m and has as much information as Alice. Eve does not know the state of the device of Bob but it is irrelevant: She will read the key with zero probability of error.

Now consider two copies of the system described in the previous sections. Instead of a single m we now have m_A and m_B located on two different circles with positions θ_A and θ_B, respectively. We assume that m_A and m_B are connected by a rigid rod that imposes the constraint $\theta_A = \theta_B + \pi$. The measurement that changes the state of one of the masses respects this constraint, that is, the two masses move simultaneously due to their rigid connection. One has to exclude the experiments when Alice and Bob make the measurements simultaneously, but the probability of such events is zero if the detection times are chosen randomly. We shall see later that the rod is here analogous to Bohm's quantum potential for entangled states: Both particles react to a measurement performed on a single particle.

Let us note that the source produces pairs of particles with randomly chosen θ_A and $\theta_B = \theta_A + \pi$. If Bob, say, makes the first measurement and Eve knows both θ_A and θ_B, she nevertheless cannot predict the result: She does not know the state m_1^B of Bob's polarizer. After Bob's measurement the massess m_A and m_B on the two circles move in a way dictated by the single-spin model. The key is created at this very last moment and Eve cannot infer the values found by Alice and Bob since the states of their devices are beyond her reach.

Obviously, in such a toy model one cannot seriously discuss the security issues. Eve can see the rod and on this basis read the key. This is why the Bohm model is more interesting. Not only can it describe full quantum mechanics, but it simultaneously does include a "rod" (the quantum potential) that is invisible to Eve if she is not entangled with the two particles. The common element of the two nonlocal hidden-variable models is the fact that Eve does not have the full information obout variables that imply the values of the key.

BOHM-MODEL ILLUSTRATION

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

$$\partial S/\partial t + \sum_{j=1}^{n} m_j \vec{v}_j^2/2 + Q + V = 0, \quad (1)$$

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

$\rho = R^2$ is the density of particles, $\vec{v}_j = \vec{\nabla}_j S/m_j$ the velocity if a j-th particle, $V = V(\vec{x}_1,\dots,\vec{x}_n,t)$ the usual potential, and $Q = -\hbar^2\sum_{j=1}^{n}\vec{\nabla}_j^2 R/(2m_j R)$ is the so-called quantum potential. The hidden trajectories are found by integrating $d\vec{q}_j/dt = \vec{v}_j$. If the particles are not entangled (and thus not interacting via V), that is the wave fuction takes the product form $\psi(\vec{x}_1,\dots,\vec{x}_n,t) = \psi_1(\vec{x}_1,t)\dots\psi_n(\vec{x}_n,t)$, then $Q = \sum_{j=1}^{n} Q_j$ where $Q_j = -\hbar^2\vec{\nabla}_j^2 R_j/(2m_j R_j)$. 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 a k-th particle depends on what happens to the remaining $n-1$ particles. What is important, *the influences remain within the entangled system*.

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 [30, 31]. If the eavesdropper does not get entangled, the quantum potential will not carry the information she needs. So this is yet a good news.

Let us now assume that Eve can know the hidden trajectory $\vec{q}(t)$ of the particle carrying the key between the two communicating parties. A Bohmian analysis of spin-1/2 measurements performed via Stern-Gerlach devices [3, 4] shows that the knowledge of $\vec{q}(t_0)$ at some initial time t_0 *uniquely* determines the results of future measurements of spin in any direction ([4], pp. 412-415). The single-particle schemes of the BB84 variety [32] 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 Chapter 11 of [4]. 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 $\vec{v}_1 = (0,-|\vec{v}_1|,0)$ and $\vec{v}_2 = (0,|\vec{v}_2|,0)$, 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 $\vec{q}_1(t) = (0,y_1(t),z_1(t))$ and $\vec{q}_2(t) = (0,y_2(t),z_2(t))$ (cf. the discussion on p. 470 in [4]). The result agrees with the analysis of [5].

Still, if one looks more closely at the derivation given in [4] one notices that the two particles interact with *identical* magnetic fields. We can weaken this assumption. Following [4] we assume that the time of interaction with the Stern-Gerlach magnets is T, the particles are identical, their magnetic moments and masses equal μ and m, and the initial wave functions are Gaussians of half-width σ_0 in the z directions. We also assume that Alice's Stern-Gerlach produces the field $\vec{B}_1(\vec{q}_1) = (0,0,B_0 + Bz_1)$ but, contrary to [4], the Bob field is taken as $\vec{B}_2(\vec{q}_2) = \kappa(0,0,B_0 + Bz_2)$, where κ is a real number (in [4] $\kappa = 1$). Then the velocities in the z direction $(0,0,1)$ read [6]

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

$$\frac{dz_2(t)}{dt} = \frac{\hbar^2 t z_2(t)}{4m^2\sigma_0^4\varepsilon(t)} - \frac{1}{m\varepsilon(t)}B\mu T \tanh\left(\frac{z_1(t)-\kappa z_2(t)}{m\sigma_0^2\varepsilon(t)}B\mu T t\right), \tag{4}$$

where $\varepsilon(t) = 1 + \frac{\hbar^2 t^2}{4\sigma_0^4 m^2}$. The above formulas differ from Eqs. (11.12.15), (11.12.16) found in [4] only by the presence of κ. 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 labs 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 κ which is known only to Bob. If $|\kappa| \gg 1$ then the sign of this term is practically controlled by the sign of κ (recall that the range of z_1 is limited by the size of the Gaussian). Choosing the sign of κ randomly, Bob can flip the spin of the particle which is already in the lab 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 $\text{sign}(\kappa) = +1$, and that if $\text{sign}(\kappa) = -1$ the result will be 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 EPR correlations. If he keeps $\kappa > 0$ then Alice got the result opposite to what he found in his lab because $\vec{B}_1$ and $\vec{B}_2$ are parallel; if he takes $\kappa < 0$ then both Alice and Bob find the same number because $\vec{B}_1$ and $\vec{B}_2$ are anti-parallel. And this is sufficient for producing the key.

FINAL COMMENTS

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 a 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.

We do not know how to perform a hidden-variable attack in practice, but we do not have a convincing proof that the attack is impossible. We cannot even distinguish between true quantum data, where we do not know how to eavesdrop, and those produced by a computer simulation based on Bohm theory, where it is obvious what to do.

One of the fundamental rules of cryptography states that in such a situation one shoud modify a cryptosystem in a way that makes it secure independently of the validity of the basic assumption. (RSA was regarded fundamentally insecure even before the advent of quantum algorithms not because we knew a fast factoring algorithm, but because we could not prove its nonexistence.) The modification we propose is easy to implement in entangled-state protocols, although it will not work in single-particle cryptosystems.

By the way, it would be interesting to see if the leading quantum cryptography groups would pass a test for distinguishing between data taken from and actual experiment and those produced by a computer simulation based on Bohm theory. Would any of the groups accept the challenge?

ACKNOWLEDGMENTS

The work of MC and MP is a part of the Polish Ministry of Scientific Research and Information Technology (solicited) project PZB-MIN-008/P03/2003. We acknowledge the support of the Flemish Fund for Scientific Research (FWO Project No. G.0452.04). 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.

REFERENCES

1. D. Bohm, *Phys. Rev.* **8**5, 166 (1952).
2. D. Bohm, *Phys. Rev.* **8**9, 458 (1953).
3. C. Dewdney, P. R. Holland, A. Kyprianidis, and J.-P. Vigier, *Nature* **3**36, 536-44 (1988).
4. P. R. Holland, *The Quantum Theory of Motion*, Cambridge, Cambridge University Press, 1993.
5. A. Valentini, *Pramana - J. Phys.* **5**9, 269 (2002).
6. M. Pawłowski and M. Czachor, quant-ph/0412058.
7. D. Aerts and M. Czachor, quant-ph/0501003v1.
8. D. Dürr, S. Goldstein, and N. Zanghi, *J. Stat. Phys.* **6**7, 843 (1992); *J. Stat. Phys.* **6**8, 259 (1993)
9. D. Dürr, S. Goldstein, R. Tumulka, and N. Zanghi, *Phys. Rev. Lett.* **9**3, 090402 (2004).
10. G. Horton and C. Dewdney, *J. Phys. A: Math. Gen.* **3**7, 11935 (2004).
11. P. Holland and C. Philippidis, *Phys. Rev. A* **6**7, 062105 (2003).
12. G. D. Barbosa and N. Pinto-Neto, *Phys. Rev. D* **6**9, 065014 (2004).
13. P. Holland, *Ann. Phys. (NY)* **3**15, 503 (2005).
14. R. Haag and U. Bannier, *Comm. Math. Phys.* **6**0, 1 (1978).
15. N. Gisin, *Helv. Phys. Acta* **6**2, 363 (1989); Phys. Lett. A **1**43, 1 (1990).
16. J. Polchinski, *Phys. Rev. Lett.* **6**6, 397 (1991).
17. M. Czachor, *Found. Phys. Lett.* **4**, 351 (1991).
18. G. Svetlichny, *Found. Phys.* **2**8, 131 (1998); preprint appeared in 1990.
19. T. F. Jordan, *Ann. Phys.* **2**25, 83 (1993).
20. W. Lücke, in *Nonlinear, Deformed, and Irreversible Quantum Systems*, edited by H.-D. Doebner, V. K. Dobrev, and P. Nattermann, World Scientific, Singapore, 1995.
21. G. A. Goldin and G. Svetlichny, *J. Math. Phys.* **3**5, 3322 (1994).
22. B. Mielnik, *Phys. Lett. A* **2**89, 1 (2001).
23. C. Simon, V. Buzek and N. Gisin, *Phys. Rev. Lett.* **8**7, 170405 (2001); P. Bona, *Phys. Rev. Lett.* **9**0, 208901 (2003).
24. B. Mielnik, *Comm. Math. Phys.* **3**1, 221 (1974); *Comm. Math. Phys.* **1**01, 123 (1983).
25. M. Czachor, *Phys. Rev. A* **5**7 4122 (1998).
26. M. Czachor and H.-D. Doebner, *Phys. Lett. A* **3**01, 139 (2002).
27. D. Aerts, *J. Math. Phys.* **2**7, 202 (1986)
28. D. Aerts, *Helv. Phys. Acta* **6**4, 1 (1991).
29. M. Czachor, *Found. Phys. Lett.* **5**, 249 (1992)

30. A. K. Ekert, *Phys. Rev. Lett.* **6**7, 661 (1991).
31. C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett.* **6**8, 557 (1992).
32. C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing — Bangalore, New York, IEEE, 1984.