No Signaling and Quantum Key Distribution

Jonathan Barrett,[1,2,*] Lucien Hardy,[3,†] and Adrian Kent[4,‡]

[1]*Physique Théorique, Université Libre de Bruxelles, CP 225, Boulevard du Triomphe, 1050 Bruxelles, Belgium*
[2]*Centre for Quantum Information and Communication, CP 165/59, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium*
[3]*Perimeter Institute, 35 King Street North, Waterloo, Ontario N2J 2W9, Canada*
[4]*Centre for Quantum Computation, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, United Kingdom*

(Received 19 May 2004; published 27 June 2005)

Standard quantum key distribution protocols are provably secure against eavesdropping attacks, if quantum theory is correct. It is theoretically interesting to know if we need to assume the validity of quantum theory to prove the security of quantum key distribution, or whether its security can be based on other physical principles. The question would also be of practical interest if quantum mechanics were ever to fail in some regime, because a scientifically and technologically advanced eavesdropper could perhaps use postquantum physics to extract information from quantum communications without necessarily causing the quantum state disturbances on which existing security proofs rely. Here we describe a key distribution scheme provably secure against general attacks by a postquantum eavesdropper limited only by the impossibility of superluminal signaling. Its security stems from violation of a Bell inequality.

DOI: 10.1103/PhysRevLett.95.010503 PACS numbers: 03.67.Hk, 03.65.Ta, 03.65.Ud, 03.67.Dd

With the discoveries of quantum cryptography [1] and quantum key distribution [2,3], it is now well understood that cryptographic tasks can be guaranteed secure by physical principles. For example, we now have protocols for various important tasks, including key distribution, that are provably secure provided quantum theory is correct [4]. Protocols for bit commitment have been developed with security based only on the impossibility of superluminal signaling [5,6]. The possibility of basing cryptographic security on known superselection rules has also recently been discussed [7,8].

In this Letter we investigate whether it is possible to devise a quantum key distribution scheme that is provably secure if superluminal signaling is impossible. We allow for eavesdroppers who can break the laws of quantum mechanics, as long as nothing they can do implies the possibility of superluminal signaling. In general, this will mean that the security proofs of existing quantum key distribution protocols are no longer valid, as we can no longer assume that quantum theory correctly predicts the trade-off between the information that Eve can extract and the disturbance she must necessarily cause.

As we show below, there is an intimate connection between the possibility of such a protocol and the violation of a Bell inequality [9,10]. Nonlocal (in the sense of Bell inequality violating) correlations constitute an exploitable resource for this task, just as entanglement is a resource for conventional quantum key distribution. We present a quantum scheme, involving Bell violation, that is secure against general attacks by a nonsignaling Eve.

One motivation for this work is practical: existing security proofs assume the validity of quantum theory, and while quantum theory has been confirmed in an impressive range of experiments, it remains plausible that some future experiment will demonstrate a limit to its domain of validity. Admittedly, it is also conceivable that some future experiment could demonstrate the possibility of superluminal signaling. But the possibilities are logically independent: quantum theory could fail without violating standard relativistic causality, and vice versa. A cryptographic scheme that can be guaranteed secure by either of two physical principles is more trustworthy than one whose security relies entirely on one.

There are also compelling theoretical motivations. Understanding which cryptographic tasks can be guaranteed secure by which physical principles improves our understanding of the relationship between information theory and physical theory. Our work also demonstrates a new way of proving security for quantum protocols, which may be useful in other contexts, and sheds new light on nonlocality and its relation to secrecy.

A quantum protocol for secret bit distribution.—We assume that Alice and Bob have a noise-free quantum channel and an authenticated classical channel. Consider the following protocol, which we show below generates a single shared secret bit, guaranteed secure against general attacks by postquantum eavesdroppers. Define the bases $X_r = \{\cos\frac{r\pi}{2N}|0\rangle + \sin\frac{r\pi}{2N}|1\rangle, -\sin\frac{r\pi}{2N}|0\rangle + \cos\frac{r\pi}{2N}|1\rangle\}$ for integer r. For each basis, we define outcomes 0 and 1 to correspond, respectively, to the projections onto the first and second basis elements. Thus X_{r+N} contains the same basis states as X_r with the outcome conventions reversed; i.e., we interpret the bases X_{-1} and X_N below to be X_{N-1} and X_0 with outcomes reversed. We take the security parameters N and M (defined below) to be large positive integers. To simplify the analysis, we will take $M \ll N$.

1. Alice and Bob share $n = MN^2$ pairs of systems, each in the maximally entangled state $|\psi_-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$.

2. Alice and Bob choose independent random elements r_A^i and r_B^i of the set $\{0, 1, \ldots, N-1\}$ for each i from 1 to MN^2, and measure their ith particle in the bases $A_i \equiv X_{r_A^i}$ and $B_i \equiv X_{r_B^i}$.

3. When all their measurements are complete, Alice and Bob announce their bases over a public, authenticated, classical channel.

4. Alice and Bob abort the protocol and restart unless

$$2MN \leq \sum_i \sum_{c=-1,0,1} |\{j:A_j = X_i, B_j = X_{i+c}\}|.$$

(The expected size of the sum is $3MN$. The probability of the condition failing is of order $e^{-MN/6}$.)

5. The outcomes are kept secret for one randomly chosen pair for which the bases chosen were X_i and X_{i+c} for some i and $c = -1$, 0, or 1. We call bases of this form *neighboring or identical*. The outcomes are announced for all the remaining pairs (for all basis choices).

6. Alice and Bob abort the protocol if their outcomes a and b are not anticorrelated (i.e., $a \neq b$) in all the cases where they chose neighboring or identical bases.

7. If the protocol is not aborted, their unannounced outcomes define the secret bit, which is taken by Alice to be equal to her outcome and by Bob to be opposite to his.

Eavesdropping attacks.—To analyze the security of this protocol, we must describe formally the actions available to postquantum eavesdroppers. To give Eve maximum power, we assume that each pair of systems is produced by a source under her control. In a general, or collective, attack, Eve prepares $2n + 1$ systems in a postquantum state λ, sending n systems to Alice, n to Bob, and keeping 1. The state λ defines measurement probabilities

$$\mathrm{P}_\lambda(abe|ABE),$$

where $A = \{A_1, \ldots, A_n\}$, $B = \{B_1, \ldots, B_n\}$ are sets of Alice's and Bob's possible measurement choices and $E = \{E_1\}$ is a set containing a possible measurement choice of Eve, with corresponding outcomes a, b, e. This state may be nonquantum and nonlocal, but must not allow signaling even if the parties cooperate. Thus, for any partitionings $A = A^1 \cup A^2$, $B = B^1 \cup B^2$, and $E = E^1 \cup E^2$ (possibly including empty subsets), and any alternative choices $\bar{A}^2, \bar{B}^2, \bar{E}^2$, we require that

$$\sum_{a^2 b^2 e^2} P_\lambda(a^1 a^2 b^1 b^2 e^1 e^2 | A^1 A^2 B^1 B^2 E^1 E^2) = \sum_{\bar{a}^2 \bar{b}^2 \bar{e}^2} P_\lambda(a^1 \bar{a}^2 b^1 \bar{b}^2 e^1 \bar{e}^2 | A^1 \bar{A}^2 B^1 \bar{B}^2 E^1 \bar{E}^2). \quad (1)$$

Eve may wait until all Alice's and Bob's communications are finished before performing her measurement.

We need a further technical assumption. It seems natural to postulate that, once Eve has prepared a postquantum state λ, the range of measurements available to her and their outcome probabilities are (up to relabelings) *time independent*. In fact, a slightly weaker assumption suffices: we assume that in postquantum theory, as in quantum theory, measurements on a shared state cannot be used to send signals between the parties in any configuration (even if not spacelike separated). If this assumption were dropped, one could allow a theory in which information about the bases and outcomes of any measurements carried out by Alice and Bob propagates to Eve at light speed, so she can obtain these data by a later measurement timelike separated from Alice's and Bob's. While theories of this type may seem implausible, or even pathological, they can be made internally consistent without allowing superluminal communication [11]. Clearly, secure key distribution would be impossible if Eve could exploit a theory of this type.

One can justify excluding this possibility by extending a standard cryptographic assumption to postquantum cryptology. Conventional security analyses of quantum key distribution require that Alice's and Bob's laboratories are completely secure against Eve's scrutiny—a necessary cryptographic assumption, which does not follow from the laws of quantum theory. Similarly, in the postquantum context, we assume that *no* information about events in Alice's and Bob's laboratories—in particular, their measurements or outcomes—subsequently propagates to Eve. Put another way, Alice and Bob have to assume they can establish secure laboratories, else cryptography is pointless. The aim is to guarantee secure key distribution modulo this assumption. We shall prove that the protocol above is indeed secure against general attacks.

Proof of security.—We define A_j, B_j to be Alice's and Bob's basis choices for the jth pair; these are random variables, each measurement occurring with probability $1/N$. We also define a_j, b_j to be their measurement outcomes and write

$$t_j = \frac{1}{3N} \sum_{c=-1,0,1} \sum_{i=0}^{N-1} \mathrm{P}_\lambda(a_j \neq b_j | A_j = X_i, B_j = X_{i+c}).$$

(Recall that X_{-1} and X_N are X_{N-1} and X_0 with outcomes reversed.) Note that if λ is local we have $t_j \leq 1 - \frac{2}{3N}$. Thus this is a generalized Bell inequality (it is in fact similar to the chained Bell inequality of Braunstein and Caves [12]). If there is no eavesdropping, so that genuine singlet states are shared, then quantum mechanics gives $t_j = 1 - O(1/(N^2))$, for all j, thus violating the inequality for large enough N. This is crucial for the security of the protocol; it is violation of this inequality that allows Eve's knowledge to be bounded. Below, we shall derive a lower bound on the value of t_s for the secret pair s, given that Alice's and Bob's tests are passed, and given that Eve is not using a strategy that almost always fails the tests. Then we show that the lower bound on t_s implies an upper bound on Eve's information, which can be made arbitrarily small as M, N become large.

From now on, we assume that there is at least one pair for which Alice's and Bob's measurements were neighboring or identical (otherwise they will abort). Let s, a random variable, be the index of the pair chosen to define the secret bit. A postquantum state λ determines the probability $P_\lambda(\text{pass})$ that Alice's and Bob's tests are passed, so that they do not abort the protocol.

Lemma.—For any λ such that $P_\lambda(\text{pass}) > \epsilon$, we have that

$$P_\lambda(a_s \neq b_s|\text{pass}) > 1 - 1/(2MN\epsilon).$$

Proof.—Let m, a random variable, be the number of pairs for which the measurements were neighboring or identical. For a given pair, let C be the condition that the measurements were neighboring or identical and the outcomes anticorrelated. If the secret pair satisfies C, then Alice and Bob will agree on the value of the secret bit. We denote by $\#(C)$ the number of pairs for which C holds. Define the following four mutually exclusive and collectively exhaustive events:

$$\begin{aligned} E_0&: \quad m < 2MN, \\ E_1&: \quad m \geq 2MN \quad \text{and} \quad \#(C) < m - 1, \\ E_2&: \quad m \geq 2MN \quad \text{and} \quad \#(C) = m - 1, \\ E_3&: \quad m \geq 2MN \quad \text{and} \quad \#(C) = m. \end{aligned}$$

Note that if E_0 or E_1 occurs, then Alice and Bob will definitely abort. If E_3 occurs, then Alice and Bob will definitely not abort. A given postquantum state λ defines a probability for each of these four events, which we write as $P_\lambda(E_i) \equiv q_i$.

Now we have $P_\lambda(\text{pass}) = q_3 + q_2 P_\lambda(\text{pass}|E_2)$. If E_2 occurs, then the test will only be passed if the secret pair do not satisfy C. This means that we have

$$P_\lambda(\text{pass}|E_2) = \sum_{i=2MN}^{MN^2} P(m = i|E_2)/i \leq 1/(2MN). \quad (2)$$

But $P_\lambda(\text{pass}) > \epsilon$, so we can write $q_3 > \epsilon - q_2/(2MN)$. Therefore,

$$\begin{aligned} &P_\lambda(a_s \neq b_s|\text{pass}) \\ &\quad = \frac{q_3}{q_3 + q_2 P_\lambda(\text{pass}|E_2)} > 1 - 1/(2MN\epsilon), \quad (3) \end{aligned}$$

where the inequality follows from the fact that the right hand side of the first line either equals 1 or is monotonically increasing with q_3. QED.

It follows from the lemma above, the no signaling condition (1) and the chain rule for conditional probabilities that, conditioned on passing the test,

$$t_s > 1 - 1/(2MN\epsilon). \quad (4)$$

From now on, we assume that the test is passed, and we can consider that Alice, Bob, and Eve share three systems, such that Eq. (4) is satisfied. We now show that the knowledge that Eve can get by performing a measurement on her system is small.

We do this by contradiction. Thus suppose that with probability $\delta > 0$, Eve gets an outcome e_0 such that

$$P_\lambda(a_s = b, b_s = \bar{b}|A_s = X_k, B_s = X_{k+d}, e_0) > (1/2)(1 + \delta'),$$

for some k and $d = -1$, 0, or 1, where $\delta' > 0$ and $b \in \{0, 1\}$. Define

$$\begin{aligned} p_i^A &\equiv P_\lambda(a_s = b|A_s = X_i, e_0) \\ p_i^B &\equiv P_\lambda(b_s = \bar{b}|B_s = X_i, e_0), \end{aligned}$$

The no signaling condition (1) ensures that p_i^A is independent of which measurement Bob performs, and similarly that p_i^B is independent of which measurement Alice performs. This enables us to write $p_k^A, p_{k+d}^B > (1/2)(1 + \delta')$. Now

$$\begin{aligned} &P_\lambda(a_s \neq b_s|A_s = X_i, B_s = X_{i+c}, e_0) \\ &\quad = P_\lambda(a_s = b, b_s = \bar{b}|A_s = X_i, B_s = X_{i+c}, e_0) \\ &\qquad + P_\lambda(a_s = \bar{b}, b_s = b|A_s = X_i, B_s = X_{i+c}, e_0) \\ &\quad \leq \min(p_i^A, p_{i+c}^B) + \min(1 - p_i^A, 1 - p_{i+c}^B) \\ &\quad = 1 - |p_i^A - p_{i+c}^B|. \end{aligned}$$

Now, using (1) again and the triangle inequality, we have

$$\begin{aligned} &\sum_{c=-1,0,1} \sum_{i=0}^{N-1} P_\lambda(a_s \neq b_s|A_s = X_i, B_s = X_{i+c}, e_0) \\ &\quad \leq 3N - \sum_{c=-1,0,1} \sum_{i=0}^{N-1} |p_i^A - p_{i+c}^B| \\ &\quad \leq 3N - \sum_{i=0}^{N-1} |p_i^A - p_{i+1}^A| \\ &\quad \leq 3N - |2p_k^A - 1| \leq 3N - \delta'. \end{aligned}$$

This implies that, conditioned only on passing the test,

$$t_s \leq 1 - (\delta\delta')/(3N). \quad (5)$$

For any fixed $\delta, \delta' > 0$, we can choose M, N, ϵ such that this is inconsistent with Eq. (4). M must also be chosen so that quantum correlations are unlikely to fail the test. For example, taking $M = N^{3/4}, \epsilon = N^{-1/4}$ achieves this for sufficiently large N. [Note that if Alice's and Bob's outcomes are classically correlated via a local hidden variable theory, the chances of passing the test are very small, and there exists no choice of parameters for which Eqs. (4) and (5) are inconsistent.]

Although we restricted the security parameter $M \ll N$ to simplify the discussion, the protocol can be generalized to allow M arbitrarily large. In this case, Alice's and Bob's security test is that the number of pairs for which the outcomes are not anticorrelated should be statistically consistent with quantum predictions; the method of our security proof generalizes to cover this case.

Discussion.—The above security proof shows that our protocol allows Alice and Bob to generate a single shared bit and guarantee its security even against collective attacks by a postquantum Eve. The protocol can be generalized to generate an arbitrary shared secret bit string, with the same security guarantee.

Nonlocality is crucial to the success of the protocol. It is easy to see that if Alice and Bob were violating no Bell inequality, then Eve could eavesdrop perfectly by preparing each pair of systems in a postquantum state that is deterministic (where deterministic means that all probabilities defined by the state are 0 or 1) and local. This would give Eve perfect information about Alice's and Bob's measurement outcomes. On the other hand, if Alice and Bob are violating a Bell inequality, then at least some of the postquantum states prepared by Eve must be nonlocal. But any state that is deterministic and nonlocal allows signaling [13]. So this trivial eavesdropping strategy is not available to Eve.

More generally, we can say that the protocol works because, once the no signaling condition is assumed, nonlocal correlations satisfy a monogamy condition analogous to that of entanglement in quantum theory. The monogamy of nonlocality was first noted in Ref. [14], where it was shown that no signaling implies that there exist certain sets of nonquantum correlations such that Alice's and Bob's outcomes cannot be correlated with a third party. Here we have shown that there are quantum correlations with the same property, and used these to construct a key distribution protocol.

It is interesting to contrast the Ekert quantum key distribution protocol [3], in which a test of the Clauser-Horne-Shimony-Holt (CHSH) inequality [10] is performed. It may appear as if nonlocality is playing a crucial rôle here, too. In this case, however, the purpose of the CHSH inequality test is to verify that the shared states are close to singlets—and this is a task that other measurements, not involving nonlocality, can perform equally well [15].

We thank Daniel Gottesman for stressing the power of collective attacks by a postquantum Eve and spurring our interest in producing a general security proof. J. B. thanks Nicolas Cerf, Nicolas Gisin, Serge Massar, and Stefano Pironio for helpful discussions and acknowledges financial support from the Communauté Française de Belgique Grant No. ARC 00/05-251, the IUAP programme of the Belgian government Grant No. V-18, and the EU Project RESQ (IST-2001-37559). J. B. and L. H. acknowledge HP Bursaries. A. K. acknowledges financial support from the EU project PROSECCO (IST-2001-39227) and the Cambridge-MIT Institute.

*Electronic address: jbarrett@perimeterinstitute.ca
†Electronic address: lhardy@perimeterinstitute.ca
‡Electronic address: A.P.A.Kent@damtp.cam.ac.uk

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] For example: M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999); R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999); H. Barnum *et al.*, *Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02)* (IEEE, New York, 2002), p. 449; C. Crépeau, D. Gottesman, and A. Smith, *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2002), p. 643; A. Kent in *Quantum Communication, Measurement and Computing (QCMC'02)*, edited by J. Shapiro and O. Hirota, (Rinton Press, New Jersey, USA, 2003); A. Kent, Phys. Rev. Lett. **90**, 237901 (2003); L. Hardy and A. Kent, Phys. Rev. Lett. **92**, 157901 (2004).
[5] A. Kent, Phys. Rev. Lett. **83**, 1447 (1999).
[6] A. Kent, quant-ph/9906103 [J. Cryptology (to be published)].
[7] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A **69**, 052326 (2004).
[8] F. Verstraete and J. I. Cirac, Phys. Rev. Lett. **91**, 010404 (2003).
[9] J S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964), Reprinted in J S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, England, 1987).
[10] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[11] A. Kent, quant-ph/0204106 [Phys. Rev. A (to be published)].
[12] S. Braunstein and C. Caves, Ann. Phys. (Berlin) **202**, 22 (1990).
[13] A. Valentini, Phys. Lett. A **297**, 273 (2002).
[14] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[15] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).