Quantum Key Distribution with Classical Bob

Michel Boyer,[1] Dan Kenigsberg,[2] and Tal Mor[2]

[1]*Département IRO, Université de Montréal, Montréal (Québec) H3C 3J7 Canada*

[2]*Computer Science Department, Technion, Haifa 32000 Israel*

(Received 5 September 2006; published 5 October 2007)

Secure key distribution among two remote parties is impossible when both are classical, unless some unproven computation-complexity assumptions are made, such as the difficulty of factorizing large numbers. On the other hand, a secure key distribution is possible when both parties are quantum. What is possible when only one party (Alice) is quantum, yet the other (Bob) has only classical capabilities? We present a protocol with this constraint and prove its robustness against attacks: we prove that any attempt of an adversary to obtain information necessarily induces some errors that the legitimate users could notice.

DOI: 10.1103/PhysRevLett.99.140501 PACS numbers: 03.67.Dd

Introduction.—Processing information using quantum two-level systems (qubits), instead of classical two-state systems (bits), has lead to many striking results such as the teleportation of unknown quantum states and quantum algorithms that are exponentially faster than their known classical counterpart. Given a quantum computer, Shor's factoring algorithm would render many of the currently used encryption protocols completely insecure, but as a countermeasure, quantum information processing has also begot quantum cryptography. Quantum key distribution was invented by Bennett and Brassard (BB84) to provide a new type of solution to one of the most important cryptographic problems: the transmission of secret messages. A key distributed via quantum cryptography techniques can be secure even against an eavesdropper with unlimited computing power, and the security is guaranteed forever.

The conventional setting is as follows: Alice and Bob have labs that are perfectly secure, they use qubits for their quantum communication, and they have access to an unjammable public classical communication channel.

In the well-known BB84 protocol as well as in all other suggested protocols, both Alice and Bob perform quantum operations on their qubits (or on their quantum systems). Here we present, for the first time, a protocol in which one party (Bob) is classical. For our purposes, any two orthogonal states of the quantum two-level system can be chosen to be the computational basis $|0\rangle$ and $|1\rangle$. For reasons that will soon become clear, we shall now call the computational basis "classical" and we shall use the classical notations $\{0, 1\}$ to describe the two quantum states $\{|0\rangle, |1\rangle\}$ defining this basis. In the protocol we present, a quantum channel leads from Alice's lab to the outside world and back to her lab. Bob can access a segment of the channel, and whenever a qubit passes through that segment Bob can either let it go undisturbed or (1) measure the qubit in the classical $\{0, 1\}$ basis and (2) prepare a (fresh) qubit in the classical basis and send it.

If *all* parties were limited to performing only operations (1) and (2) or doing nothing, they would always be working with qubits in the classical basis, thus "classical bits"; the resulting protocol would then be equivalent to a *fully* classical protocol, and therefore, the operations themselves shall here be considered classical. We thus term this protocol "QKD protocol with classical Bob."

The question of how "quantum" a protocol should be in order to achieve a significant advantage over all classical protocols is of great interest. For example, Refs. [1–4] discuss whether entanglement is necessary for quantum computation, Ref. [5] shows nonlocality without entanglement, and Refs. [6,7] discuss how much of the information carried by various quantum states is actually classical. We extend this discussion into another domain: quantum cryptography. "Semiquantum" protocols of various types might even have advantages over fully quantum protocols, if they are easier to implement in practice. For instance, NMR quantum computing is among the most successful implementations of quantum computing devices while the performed NMR experiments were proven to use no entanglement [1]. The potential practical advantages of semiquantum key distribution are left for future research.

To define our protocol we follow the definition (see, for instance, [8]) of the most standard QKD protocol, BB84. The BB84 protocol consists of two major parts: a first part that is aimed at creating a *sifted key*, and a second (fully classical) part aimed at extracting an error-free, secure, final key from the sifted key. In the first part of BB84, Alice randomly selects a binary value and randomly selects in which basis to send it to Bob, either the computational ("Z") basis $\{|0\rangle, |1\rangle\}$ or the Hadamard ("X") basis $\{|+\rangle, |-\rangle\}$. Bob measures each qubit in either basis at random. An equivalent description is obtained if Alice and Bob use only the classical operations (1) and (2) above and the Hadamard quantum gate H. After all qubits have been sent and measured, Alice and Bob publish which bases they used. For approximately half of the qubits Alice and Bob used mismatching bases and these qubits are discarded. The values of the rest of the bits make the sifted key. The sifted key is identical in Alice's and Bob's hands if the protocol is error free and if there is no eavesdropper (known as Eve) trying to learn the shared bits or some function of them. In the second part, Alice and Bob use some of the bits of the sifted key (the TEST bits) to test the error rate, and if it is below some preagreed threshold, they select an INFO string from the rest of the sifted key. Finally, an error correcting code (ECC) is used to correct the errors on the INFO string (the INFO bits), and privacy amplification (PA) is used to derive a shorter but unconditionally secure final key from these INFO bits. At this point we would like to mention a key feature relevant to our protocol: it is sufficient to use qubits in just one basis, Z, for generating the INFO string, while the other basis is used only for finding the actions of an adversary [9].

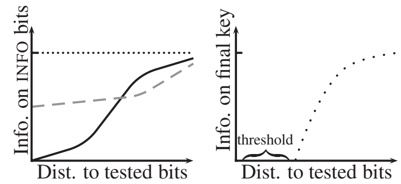
A conventional measure of security is the information Eve can obtain on the final key, and a security proof usually calculates (or puts bounds on) this information. The strongest (most general) attacks allowed by quantum mechanics are called *joint attacks*. These attacks are aimed to learn something about the final (secret) key directly, by using a probe through which all qubits pass, and by measuring the probe after all classical information becomes public. Security against all joint attacks is considered as "unconditional security". The security of BB84 (with perfect qubits sent from Alice to Bob) against all joint attacks was first proven in [8,10,11] via various techniques.

Robustness.—An important step in studying security is a proof of robustness; see, for instance, [12] for robustness proof of their entanglement-based protocol and [13] for suggesting a protocol secure against the photon-number-splitting (PNS) attack and for proving its robustness. Robustness of a protocol means that any adversarial attempt to learn some information on the key necessarily induces some disturbance. It is a special case, in zero noise, of the more general "information versus disturbance" measure which provides explicit bounds on the information available to Eve as a function of the induced error.

Definitions.—A protocol is said to be *completely robust* if nonzero information acquired by Eve on the INFO string (before Alice and Bob perform the ECC step) implies nonzero probability that the legitimate participants find errors on the bits tested by the protocol. A protocol is said to be *completely nonrobust* if Eve can acquire the INFO string without inducing any error on the bits tested by the protocol. A protocol is said to be *partly robust* if Eve can acquire some limited information on the INFO string without inducing any error on the bits tested by the protocol.

Partly robust protocols could still be secure, yet completely nonrobust protocols are automatically proven insecure (cf. Fig. 1). As one example, BB84 is fully robust when qubits are used by Alice and Bob but it is only partly robust if photon pulses are used and sometimes two-photon pulses are sent.

Here we prove that our protocol for "quantum key distribution with classical Bob" is completely robust. Another protocol and a proof of its robustness are omitted for the sake of brevity and will be provided in a future work.



(a) (b)

FIG. 1. (a) Eve's maximum (over all attacks) information on the INFO string vs the allowed disturbance on the bits tested by Alice and Bob, in a completely robust (solid line), partly robust (dashed line), and completely nonrobust (densely dotted line) protocol. (b) Robustness should not be confused with security; Eve's maximum information on the final key vs allowed disturbance in a secure protocol; such a protocol could be completely or partly robust.

A mock protocol and its complete nonrobustness.—Consider the following mock protocol: Alice generates a random qubit in the Z basis. She chooses randomly whether to do nothing or to apply Hadamard gate to transform the qubit to the X basis. Bob flips a coin to decide whether to measure Alice's qubit in the Z basis (to "SIFT" it) or to reflect it back ("CTRL"), without causing any modification to the information carrier. In case Alice chose Z and Bob decided to SIFT, i.e., to measure in the Z basis, they share a random bit that we call SIFT bit (that may or may not be confidential). In case Bob chose CTRL, Alice can check if the qubit returned unchanged by measuring it in the basis she sent it. In case Bob chose to SIFT and Alice chose the X basis, they discard that bit. The above iteration is repeated for a predefined number of times. At the end of the quantum part of the protocol, Alice and Bob share, with high probability, a considerable amount of SIFT bits (also known as the "sifted key"). In order to make sure that Eve cannot gain much information by measuring (and resending) all qubits in the Z basis, Alice can check whether they have a low-enough level of discrepancy on the X basis CTRL bits. In order to make sure that their sifted key is reliable, Alice and Bob must sacrifice a random subset of the SIFT bits, which we denote as TEST bits, and remain with a string of bits which we call INFO bits.

By comparing the value of the TEST bits, Alice and Bob can estimate the error rate on the INFO bits. If the error rate on the INFO bits is sufficiently small, they use an appropriate ECC in order to correct the errors. If the error rate on the X basis CTRL bits is sufficiently small, Alice and Bob can bound Eve's information and use an appropriate privacy amplification (PA) in order to obtain any desired level of privacy.

At first glance, this protocol may look like a nice way to transfer a secret bit from quantum Alice to classical Bob: it is probably resistant to opaque (intercept-resend) attacks and probably also against all collective attacks (where Eve uses a different probe in each access to each qubit).

However, it is completely nonrobust; Eve could learn all bits of the INFO string using a trivial attack that induces no error on the bits tested by Alice and Bob (the TEST and CTRL bits). She would not measure the incoming qubit, but rather perform a CNOT from it into a $|0^E\rangle$ ancilla. If Alice chose Z and Bob decided to SIFT, she measures her ancilla and obtains an exact copy of their common bit, thus inducing no error on TEST bits and learning the INFO string. If, however, Bob decides on CTRL, i.e., reflects the qubit, Eve would perform another CNOT from the returning qubit into her ancilla. This would reset her ancilla, erase the interaction she performed, and induce no error on CTRL bits, thus removing any chance of her being caught.

A semiquantum key distribution protocol.—The following protocol remedies the above weakness by not letting Eve know which is a SIFT qubit (that can be safely measured in the computational basis) and which is a CTRL qubit (that should be returned to Alice unchanged). By always returning all qubits Bob forces Eve to delete any information she gained, or else some error is potentially induced. The protocol is aimed at creating an n-bit INFO string for generating a shorter shared secret key.

Let the integer n be the desired length of the INFO string, and let $\delta > 0$ be some fixed parameter. (1) Alice generates $N = 8n(1 + \delta)$ random qubits in the Z basis. For each of the qubits, she randomly selects whether to apply the Hadamard gate ("X") or do nothing ("Z"). (2) For each qubit arriving, Bob chooses randomly either to reflect it (CTRL) or to measure it in the Z basis and resend it in the same state he found (to SIFT it). Bob sends the first qubit to Alice after receiving the last qubit, in the same order he received them [14]. (3) Alice measures each qubit in the basis she sent it. (4) Alice publishes which were her Z bits and Bob publishes which ones he chose to SIFT.

It is expected that for approximately $N/4$ bits, Alice used the Z basis for transmitting and Bob chose to SIFT; these are the SIFT bits, which form the sifted key. For approximately $N/4$ bits, Alice used the Z basis and Bob chose CTRL; we refer to these bits as Z-CTRL. For approximately $N/4$ bits, Alice used the X basis and Bob chose CTRL; we refer to these bits as X-CTRL. The rest of the bits (those sent in the X basis but chosen as SIFT by Bob) are ignored. (5) Alice checks the error rate on the CTRL bits and if either the X error rate or the Z error rate is higher than some predefined threshold P_{CTRL}, the protocol aborts. (6) Alice chooses at random n SIFT bits to be TEST bits. She publishes which are the chosen bits. Bob publishes the value of these TEST bits. Alice checks the error rate on the TEST bits and if it is higher than some predefined threshold P_{TEST}, the protocol aborts.

The protocol aborts if there are not enough bits to perform step 6 or 7; this happens with exponentially small probability. (7) Alice and Bob select the first n remaining SIFT bits to be used as INFO bits. (8) Alice publishes ECC and PA data; she and Bob use them to extract the m-bit final key from the n-bit INFO string.

A proof of robustness.—We show that Eve cannot obtain information on INFO bits without being detectable.

Modeling the protocol.—Each time the protocol is executed, Alice sends to Bob a state $|\phi\rangle$ which is a product of N qubits, each of which is either $|+\rangle$, $|-\rangle$, $|0\rangle$, or $|1\rangle$; those qubits are indexed from 1 to N. Each of them is either measured by Bob in the Z basis and resent as it was measured, or simply reflected. Let $m = \{m_1, \ldots, m_r\}$ be a set of $r < N$ integers $1 \leq m_1 < \ldots < m_r \leq N$, describing the qubits chosen by Bob as SIFT. For $i \in \{0, 1\}^N$, we denote $i_m = i_{m_1} \ldots i_{m_r}$ the substring of i of length r selected by the positions in m; of course, $|i_m\rangle = |i_{m_1} \ldots i_{m_r}\rangle$.

In the protocol, it is assumed that Bob has no quantum register; he measures the qubits as they come in. The physics would, however, be exactly the same if Bob used a quantum register of r qubits initialized in state $|0^B\rangle$ (r qubits equal to 0), applied the unitary transform defined by $U_m|i\rangle|0^B\rangle = |i\rangle|i_m\rangle$ for $i \in \{0, 1\}^N$, sent back $|i\rangle$ to Alice, and postponed his measurement to be performed on that quantum register $|i_m\rangle$; the qubits indexed by m in $|i\rangle$ are thus automatically both measured and resent, and those not in m simply reflected; the kth qubit sent by Alice is a SIFT bit if $k \in m$ and is either $|0\rangle$ or $|1\rangle$; it is a CTRL bit if $k \notin m$. This physically equivalent modified protocol simplifies the analysis, and we shall thus model Bob's measurement and resending, or reflection, with U_m.

Eve's attack.—Eve's most general attack is comprised of two unitaries: U_E attacking qubits as they go from Alice to Bob and U_F as they go back from Bob to Alice, where U_E and U_F share a common probe space with initial state $|0^E\rangle$. The shared probe allows Eve to make the attack on the returning qubits depend on knowledge acquired by U_E (if Eve does not take advantage of that fact, then the "shared probe" can simply be the composite system comprised of two independent probes). Any attack where Eve would make U_F depend on a measurement made after applying U_E can be implemented by unitaries U_E and U_F with controlled gates.

The final global state.—Delaying all measurements allows considering the final global state of the Eve + Alice + Bob system before all measurements. To a state $|\phi\rangle$ sent by Alice, Eve attaches the probe $|0^E\rangle$, applies U_E to $|0^E\rangle|\phi\rangle$, and sends Bob his part of the system, N qubits. Taking into account Bob's probe $|0^B\rangle$, the global state is now $[U_E \otimes I_M]|0^E\rangle|\phi\rangle|0^B\rangle$, where I_M is the identity on Bob's probe space. Then, Bob applies U_m to his part of the system, which corresponds to applying $I_E \otimes U_m$ to the previous global state where I_E is the identity on Eve's probe space. Eve's attack on the returning qubits corresponds to applying the unitary $U_F \otimes I_M$ and the final global state is

$$[U_F \otimes I_M][I_E \otimes U_m][U_E \otimes I_M]|0^E\rangle|\phi\rangle|0^B\rangle. \qquad (1)$$

Proposition 1.—If U_E induces no error on TEST bits, there are states $|E_i\rangle$ in Eve's probe space s.t. $\forall i \in \{0, 1\}^N$

$$U_E|0^E\rangle|i\rangle = |E_i\rangle|i\rangle. \qquad (2)$$

If, moreover, (U_E, U_F) induces no error on CTRL bits, then there are states $|F_i\rangle$ in Eve's probe space s.t. $\forall i \in \{0, 1\}^N$,

$$U_F|E_i\rangle|i\rangle = |F_i\rangle|i\rangle. \quad (3)$$

Proof.—When U_E is applied onto the computational basis, $U_E|0^E\rangle|i\rangle = \sum_j |E_{i,j}\rangle|j\rangle$. If, for some index k there is some j such that $i_k \neq j_k$ and $|E_{i,j}\rangle \neq 0$, then by choosing m such that $k \in m$, Bob can detect this as an error on bit k. For Eve's attack to be undetectable on TEST bits, U_E must thus be such that $U_E|0^E\rangle|i\rangle = |E_{i,i}\rangle|i\rangle$, namely, $|E_{i,j}\rangle = 0$ for any $j \neq i$, and $|E_i\rangle = |E_{i,i}\rangle$ satisfies Eq. (2). If Alice sent state $|i\rangle$ for $i \in \{0, 1\}^N$, the global state is then $|E_i\rangle|i\rangle|i_m\rangle$ and $U_F|E_i\rangle|i\rangle = \sum_j |F_{i,j}\rangle|j\rangle$. In order for Eve's attack to be undetectable on Z-CTRL bits (whose index is not in m), U_F must be such that $U_F|E_i\rangle|i\rangle = |F_{i,i}\rangle|i\rangle$, namely, $|F_{i,j}\rangle = 0$ for any $j \neq i$ and $|F_i\rangle = |F_{i,i}\rangle$ then satisfies Eq. (3). □

Corollary 1.—If the attack (U_E, U_F) induces no error on TEST and CTRL bits, then (for all $i \in \{0, 1\}^N$ and all m) the final global state (1) if $|\phi\rangle = |i\rangle$ is

$$|F_i\rangle|i\rangle|i_m\rangle. \quad (4)$$

We now show that if Eve's attack is undetectable by Alice and Bob, then Eve's final state $|F_i\rangle$ is independent of the string $i \in \{0, 1\}^N$. More precisely:

Proposition 2.—If (U_E, U_F) is an attack that induces no error on TEST and CTRL bits, and if $|F_i\rangle$ is given by Eq. (4), then for all $i, i' \in \{0, 1\}^N$

$$i, i' \in \{0, 1\}^N \Rightarrow |F_i\rangle = |F_{i'}\rangle. \quad (5)$$

Proof.—Equation (5) means that any of the N bits of $i \in \{0, 1\}^N$ can be flipped at will without affecting Eve's final state $|F_i\rangle$. We thus need only prove that for any two bit strings $i, i' \in \{0, 1\}^N$ that differ only on one bit, say bit k, the equality $|F_i\rangle = |F_{i'}\rangle$ holds. We assume *w.l.g.* that $i_k = 0$ and $i'_k = 1$. If Alice chooses qubit k to be X-CTRL and chooses all the other qubits to be those of i and i', then this means that the state $|\phi\rangle$ she sends is $\frac{1}{\sqrt{2}}[|i\rangle + |i'\rangle]$. Assume now that Bob reflects bit k, i.e., that $k \notin m$. This implies that $i_m = i'_m$. By Eq. (4) and linearity, the final state is $\frac{1}{\sqrt{2}} \times [|F_i\rangle|i\rangle + |F_{i'}\rangle|i'\rangle]|i_m\rangle$. Since we are interested only in Alice's kth qubit, we trace out all the other qubits in Alice and Bob's hands. The resulting state

$$\frac{1}{\sqrt{2}}[|F_i\rangle|0\rangle + |F_{i'}\rangle|1\rangle] \quad (6)$$

must be such that the probability of Alice measuring $|-\rangle$ is 0. Replacing $|0\rangle$ and $|1\rangle$ by their value in terms of $|+\rangle$ and $|-\rangle$, state (6) rewrites as $\frac{1}{2}[|F_i\rangle + |F_{i'}\rangle]|+\rangle + \frac{1}{2}[|F_i\rangle - |F_{i'}\rangle]|-\rangle$ and the probability of measuring $|-\rangle$ is 0 iff $\frac{1}{2} \times [|F_i\rangle - |F_{i'}\rangle] = 0$, i.e., $|F_i\rangle = |F_{i'}\rangle$. □

Theorem 1.—The protocol is completely robust: for any attack (U_E, U_F) inducing no error on TEST and CTRL bits, Eve's final state is independent of m and of the states $|\phi\rangle$ sent by Alice; Eve is thus left with no information on the INFO string.

Proof.—By Proposition 2, there is a state $|F_{\text{final}}\rangle$ in Eve's probe space s.t. for all $i \in \{0, 1\}^N$, Eve's final state $|F_i\rangle = |F_{\text{final}}\rangle$. If Alice sends any superposition $|\phi\rangle = \sum_i c_i|i\rangle$ and Bob chooses any set m of bits to be measured, then Eq. (4), with $|F_i\rangle = |F_{\text{final}}\rangle$ for all i, and linearity gives $|F_{\text{final}}\rangle \sum_i c_i|i\rangle|i_m\rangle$ as the final global state of the system; Eve's probe state $|F_{\text{final}}\rangle$ is independent of $|\phi\rangle$ and m and therefore of the SIFT and INFO bits. □

Conclusion.—We presented a protocol for QKD with one party who performs only classical operations and proved its robustness. We believe that our work sheds light on how much "quantumness" is required in order to perform classically impossible tasks in general and secret key distribution in particular. Notice that Theorem 1 holds for a similar protocol where $N = 1$; Eve is then left with a probe which is independent of Alice's and Bob's choices. By induction, this independence holds for $\tilde{N} \geq 1$ repetitions of the protocol, since Eve's probe is kept independent, round after round. Thus, the following protocol is also completely robust: $\tilde{N} > 1$ qubits are sent one by one, Alice sending a qubit only after receiving the previous one, and Bob resending a qubit immediately after receiving it.

This work was partially supported by the Israeli MOD. We thank Moshe Nazarathy for providing the motivation for this research.

[1] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).

[2] R. Jozsa and N. Linden, R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci. **459**, 2011 (2003).

[3] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor, Theor. Comput. Sci. **320**, 15 (2004).

[4] D. Kenigsberg, T. Mor, and G. Ratsaby, Quantum Inf. Comput. **6**, 606 (2006).

[5] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).

[6] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).

[7] C. A. Fuchs and M. Sasaki, Quantum Inf. Comput. **3**, 377 (2003).

[8] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptology **19**, 381 (2006); *Proceedings of the 32nd ACM Symposium on Theory of Computing* (ACM, New York, 2000), pp. 715–724.

[9] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).

[10] D. Mayers, J. ACM **48**, 351 (2001).

[11] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); proof based on H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[12] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[13] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[14] An alternative requirement is presented in the conclusion.