Comment on "Semiquantum-key distribution using less than four quantum states"

Michel Boyer[1] and Tal Mor[2]

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

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

(Received 10 October 2010; published 11 April 2011)

For several decades it was believed that information-secure key distribution requires both the sender and receiver to have the ability to generate and/or manipulate quantum states. Earlier, we showed that quantum key distribution in which one party is classical is possible [Boyer, Kenigsberg, and Mor, Phys. Rev. Lett. **99**, 140501 (2007)]. A surprising and very nice extension of that result was suggested by Zou, Qiu, Li, Wu, and Li [Phys. Rev. A **79**, 052312 (2009)]. Their paper suggests that it is sufficient for the originator of the states (the person holding the quantum technology) to generate just one state. The resulting semiquantum key distribution, which we call here "quantum key distribution with classical Alice" is indeed completely robust against eavesdropping. However, their proof (that no eavesdropper can get information without being possibly detected) is faulty. We provide here a fully detailed and direct proof of their very important result.

DOI: 10.1103/PhysRevA.83.046301 PACS number(s): 03.67.Dd, 03.67.Hk

A two-way quantum key distribution (QKD) protocol in which one of the parties (Bob) uses only classical operations was recently introduced [1]. A very interesting extension in which the originator always sends the same state $|+\rangle$ (while in [1] all four BB84 states are sent) was suggested by Zou *et al.* [2]. In both those semiquantum-KD (SQKD) protocols, the qubits go from the originator Alice to (classical) Bob and back to Alice. Bob either reflects a received qubit without touching its state (CTRL), or measures it in the standard (classical) basis and sends back his result as $|0\rangle$ or $|1\rangle$ (SIFT).

We prefer to call the originator in [2] Bob (and not Alice), and to call the classical party Alice: usually in quantum cryptography, Alice is the sender of some nontrivial data, e.g., she is the one choosing the quantum states. The originator in [2] does not have that special role, as the state $|+\rangle$ is always sent (and we could even ask Eve to generate it). The classical person is then the one actually choosing a basis and knowing which of the three states ($|0\rangle$, $|1\rangle$, or $|+\rangle$) is sent back to the originator, thus it is natural to name that classical person Alice. We call the originator Bob, and we call the SQKD protocol of Zou *et al.* "QKD with classical Alice."

QKD with classical Alice [2] is indeed completely robust against eavesdropping. However, their proof (that no eavesdropper can get information without being possibly detected), is faulty. Their result is stated in Theorem 5 which relies, after many steps, on their Lemma 1. Since the Lemmas are correct and only parts of the proofs are wrong, it is not at all easy to pinpoint errors. We explicitly single out two interwoven problems in Lemma 1: (a) They state (Lemma 1, first lines) that "Alice's final state ρ'^A is a product state" (in SQKD Protocol 2), prior to saying "If the attack (U_E, U_F) induces no error on CTRL...". Using our terminology, this means that *The originator's final state ρ'^B is a product state (in the classical Alice protocol)*, however, this statement is inaccurate; in order to prove that Bob's final state is a product state one must make use of the fact that the attack induces no errors on CTRL bits. (b) They state (Proof of Lemma 1, first lines): "Because Alice sends a qubit only after receiving the previous one, the qubits she received are in a tensor product form, i.e. $\rho'^A = {\rho_1'}^A \otimes \cdots \otimes {\rho_N'}^A$". Using our terminology, this means that *Because the originator (Bob) sends a qubit only after receiving the previous one, the qubits he received are in a tensor product form, i.e. $\rho'^B = {\rho_1'}^B \otimes \cdots \otimes {\rho_N'}^B$*. That is not true in general. Consider, for instance, an attack on two consecutive qubits: if Eve has a one-qubit probe initialized as $|0\rangle$ and uses each of the two incoming qubits from Bob as a control bit to apply a controlled-NOT gate (such that the NOT is applied onto her probe), then her probe keeps the parity of the two qubits sent by Bob; if the classical party (Alice) reflects both qubits (CTRL), the final global state is $\frac{1}{2}[[|00\rangle_B + |11\rangle_B]|0\rangle_E + [|01\rangle_B + |10\rangle_B]|1\rangle_E]$ and, once Eve's state is traced out, the resulting state in Bob's hands is not a product state.

We now prove that the final result is indeed correct: robustness can be proven, directly, as follows. The originator Bob keeps in a quantum memory all qubits he received from Alice. When N qubits have been sent and received, classical Alice announces publicly the qubits she reflected; the originator Bob then checks that he received $|+\rangle$ on those positions (CTRL). For the qubits measured by Alice, a sample is chosen to be checked for errors (TEST).

Without loss of generality, we assume Eve uses a unique probe space for the attacks on all qubits and that her initial state $|E_0\rangle$ is pure. The analysis is now done bitwise, by induction. It is assumed that the Bob + Alice + Eve global state prior to Eve attacking qubit number i is a tensor product state $|\psi_{i-1}^{BA}\rangle \otimes |E_{i-1}\rangle$, where $|\psi_{i-1}^{BA}\rangle$ is in Bob + Alice's hands and Eve's current state $|E_{i-1}\rangle$ is independent of all bits measured by Alice (SIFT). That induction hypothesis obviously holds for $i = 1$, before the first qubit is sent [3]. Eve knows that Bob only sends $|+\rangle$ and she is free to send whatever state she wants to Alice. Without loss of generality (WLG) (although she is assumed classical) Alice may delay measuring by using a one-qubit probe and an XOR gate to SIFT [1]. The global state before she decides whether she sifts or reflects can now be written

$$|\psi_{i-1}^{BA}\rangle \otimes [|00\rangle_{BA}|E_0'\rangle + |10\rangle_{BA}|E_1'\rangle],$$

where $|E_b'\rangle$ are two unnormalized states of Eve's probe. In particular, if Eve "does nothing" ($|E_0'\rangle = |E_1'\rangle$), Bob +

Alices's state for the ith qubit is $|+0\rangle$. On the qubit coming back, Eve applies the unitary V_i; if Alice sifted, the global state before Eve applies V_i is $|\psi_{i-1}^{BA}\rangle \otimes [|00\rangle_{BA}|E_0'\rangle + |11\rangle_{BA}|E_1'\rangle]$. Once Eve has applied V_i, it must be such that $V_i|0\rangle_B|E_0'\rangle = |0\rangle_B|F_0'\rangle$ else the TEST (in the classical basis) can detect an error, and similarly $V_i|1\rangle_B|E_1'\rangle = |1\rangle_B|F_1'\rangle$. Due to the linearity of quantum mechanics, if classical Alice reflects (CTRL), the resulting final state must be

$$\left|\psi_{i-1}^{BA}\right\rangle \otimes [|00\rangle_{BA}|F_0'\rangle + |10\rangle_{BA}|F_1'\rangle].$$

Replacing now $|0\rangle_B$ by $[|+\rangle_B + |-\rangle_B]/\sqrt{2}$ and $|1\rangle_B$ by $[|+\rangle_B - |-\rangle_B]/\sqrt{2}$ gives

$$\left|\psi_{i-1}^{BA}\right\rangle \otimes \left[|+0\rangle_{BA}\frac{|F_0'\rangle + |F_1'\rangle}{\sqrt{2}} + |-0\rangle_{BA}\frac{|F_0'\rangle - |F_1'\rangle}{\sqrt{2}}\right];$$

for $|-\rangle_B$ to have probability 0 of being measured by Bob, $|F_0'\rangle = |F_1'\rangle$ must hold; letting $|E_i\rangle = \sqrt{2}|F_0'\rangle = \sqrt{2}|F_1'\rangle$, the final global state is $|\psi_i^{BA}\rangle \otimes |E_i\rangle$ with $|\psi_i^{BA}\rangle = |\psi_{i-1}^{BA}\rangle \otimes |\psi_i'^{BA}\rangle$, where $|\psi_i'^{BA}\rangle = (1/\sqrt{2})[|00\rangle_{BA} + |11\rangle_{BA}]$ if Alice shifts, and $|\psi_i'^{BA}\rangle = |+0\rangle_{BA}$ if she reflects.

This completes the induction proof and we deduce that after all N qubits have been processed, the final global state is $|\psi_N^{BA}\rangle \otimes |E_N\rangle$ and Eve's state $|E_N\rangle$ is independent of all Alice's choices, and thus of her information bits. That proves the robustness of the protocol.

We proved here that the very nice protocol suggested by Zou *et al.* (which we call here "QKD with classical Alice") is completely robust. We would like to emphasize that the results in [2] hold. As for Lemma 1, its statement can be slightly improved by moving the sentence "Alice's final state... is a product state... in SQKD Protocol 2." to right after "... the following conditions:". Proving Lemma 1, however, is another matter, and it is unclear to us how the original proof can be adjusted. Interestingly, it follows directly from our proof above that the final Bob + Alice state $|\psi_N^{BA}\rangle$ is $|\psi_0^{BA}\rangle \otimes \bigotimes_{i=1}^{N} |\psi_i'^{BA}\rangle$, where $|\psi_0^{BA}\rangle$ is the Bob + Alice state before the protocol, and the $|\psi_i'^{BA}\rangle$ are exactly those states announced by [2] in their Lemma 1, which thus proves it for the "one-state" protocol.

The work of M.B. was supported in part by FQRNT through INTRIQ. The work of T.M. was supported in part by FQRNT through INTRIQ, by NSERC, and by the Israeli MOD Research and Technology Unit.

[1] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).

[2] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, Phys. Rev. A **79**, 052312 (2009).

[3] For simplicity, we formally assume an initial state $|\psi_0^{BA}\rangle$ for the Bob + Alice system, to avoid a void state.