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

Xiangfu Zou[1,2*] and Daowen Qiu[1†]
[1] *Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China*
[2] *School of Mathematics and Computational Science, Wuyi University, Jiangmen 529020, China*

(Dated: October 21, 2010)

Recently Boyer and Mor [arXiv:1010.2221 (2010)] pointed out the first conclusion of Lemma 1 in our original paper [Phys. Rev. A **79**, 052312 (2009)] is not correct, and therefore, the proof of Theorem 5 based on Lemma 1 is wrong. Furthermore, they gave a direct proof for Theorem 5 and affirmed the conclusions in our original paper. In this reply, we admit the first conclusion of Lemma 1 is not correct, but we need to point out the second conclusion of Lemma 1 is correct. Accordingly, all the proofs for Lemma 2, Lemma 3, and Theorems 3–6 are only based on the the second conclusion of Lemma 1 and therefore are correct.

PACS numbers: 03.67.Dd, 03.67.Hk

The idea of semiquantum key distribution (SQKD) in which one of the parties (Bob) uses only classical operations was recently introduced [1]. Also, an SQKD protocol (BKM2007) using all four BB84 [2] states was suggested [1]. Based on this, we presented some SQKD protocols which Alice sends less than four quantum states and proves them all being completely robust [3]. In particular, we proposed two SQKD protocols in which Alice sends only one quantum state $|+\rangle$. Very recently, Boyer and Mor [4] pointed out the first conclusion of Lemma 1 in our original paper [3] is not correct, and therefore, the proof of Theorem 5 based on Lemma 1 is wrong. Furthermore, they gave a direct proof for Theorem 5 and affirmed the conclusions in Ref. [3].

In this reply, we first thank professors Boyer and Mor [4] for their attention to our work and admit the first conclusion of Lemma 1 in Ref. [3] is not correct. Particularly, we want to thank them for they not only pointed out the error in our paper but also gave a proof for Theorem 5 and confirmed the result of Theorem 5 in our original paper.

In this reply, we would also like to point out the second conclusion of Lemma 1 is correct. Accordingly, all the proofs for Lemma 2, Lemma 3, and Theorems 3–6 are only based on the the second conclusion of Lemma 1 and therefore are correct. To delete the first conclusion of Lemma 1 in Ref. [3], we only need to define the final combining state $\rho_i'^{AB}$ of Alice's ith particle and Bob's ith particle and modify Lemma 1 as follows.

Lemma 1. Let ρ'^{AB} denote Alice and Bob's final combining state and let $\rho_i'^{AB}$ be the final combining state of Alice's ith particle and Bob's ith particle. If the attack (U_E, U_F) induces no error on CTRL and TEST bits, then ρ'^{AB} satisfies the following conditions:

(1) If $b_i = 0$, then $\rho_i'^{AB} = (|\phi_i\rangle\langle\phi_i|)_A \otimes (|0\rangle\langle 0|)_B$, i.e., Alice's ith final state is the sent state $|\phi_i\rangle$;

(2) If $b_i = 1$, then $\rho_i'^{AB} = (x|00\rangle + y|11\rangle)(\overline{x}\langle 00| + \overline{y}\langle 11|)$ when the sent state $|\phi_i\rangle = x|0\rangle + y|1\rangle$, i.e., the final combining state of Alice's ith particle and Bob's ith particle is the pure state $x|00\rangle + y|11\rangle$.

Proof. (1) The case of $b_i = 0$.

The ith bit is a CTRL bit. Alice's final quantum state $\rho_i'^{A} \neq |\phi_i\rangle\langle\phi_i|$ can be detected by Alice as an error with some non-zero probability. Also, Bob's ith final state is $|0\rangle$ since it is not acted any operation. Thereby $\rho_i'^{AB} = (|\phi_i\rangle\langle\phi_i|)_A \otimes (|0\rangle\langle 0|)_B$.

(2) The case of $b_i = 1$.

The probability of the ith bit being a TEST bit is about $\frac{1}{2}$. Also, if $|\phi_i\rangle = x|0\rangle + y|1\rangle$, $\rho_i'^{AB} \neq (x|00\rangle + y|11\rangle)(\overline{x}\langle 00| + \overline{y}\langle 11|)$ can be detected by Alice and Bob as an error with some non-zero probability when the ith bit is a TEST bit. Therefore $\rho_i'^{AB} = (x|00\rangle + y|11\rangle)(\overline{x}\langle 00| + \overline{y}\langle 11|)$. ■

The proof of Lemma 2 in Ref. [3] is only based on the second conclusion of Lemma 1 in Ref. [3]. That is, Lemma 2 in Ref. [3] also holds when Lemma 1 is reformed as the above form. Because the proofs of Lemma 3 and Theorems 3–6 are only based on Lemma 2 in Ref. [3], these results still hold.

*Electronic address: xf.zou@hotmail.com (Xiangfu Zou);
†Electronic address: issqdw@mail.sysu.edu.cn (Daowen Qiu).

[1] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).
[2] C. H. Bennett and G. Brassard, In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984), pp. 175-179.
[3] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, Phys. Rev. A **79**, 052312 (2009).
[4] M. Boyer and T. Mor, arXiv:1010.2221.