Security evaluation of quantum key distribution with weak basis-choice flaws

Shi-Hai Sun,[1,*] Zhi-Yu Tian,[1] Mei-Sheng Zhao,[2] and Yan Ma[2]

[1] *School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai, Guangdong 519082, China*
[2] *QuantumCTek Co. Ltd., Hefei, Anhui 230000, China*

Introduction- Based on the principle of quantum mechanics, "*quantum cryptography*" is a possible means of implementing unconditional secure communication. One famous quantum cryptography approach is quantum key distribution (QKD) combined with One-Time pad. Since the proposal of the first QKD protocol BB84, QKD has attracted much interest. The unconditional security of QKD had been proven in both perfect and imperfect devices. QKD has also been experimentally demonstrated in fibers, free space, and satellites. However, because practical devices are imperfect, some assumptions of the theoretical analysis may be violated in practical situations. If the gap between theory and practice is exploited by an eavesdropper (Eve), the security of the final key may be broken.

In the BB84 protocol, both Alice and Bob must determine how to prepare and measure the quantum states. For this purpose, they require random bits. In practical situations, the random bits may be weakly known or controlled by Eve, and the security of the generated key is compromised. A typical attack that exploits the weak randomness of QKD is wavelength attack. To mitigate this problem, we develop an analytical formula that estimates the key rate for both the single photon source (SPS) and the weak coherent source (WPS). In numerical simulations, our method significantly increased the key rate over the original method of Li et al. [1].

Main Results- For BB84 protocol, the key rate can be written as

$$\begin{aligned} r_{sps} &\geq 1 - H(e_b) - H(e_p), \\ r_{wps} &\geq -Q_\mu f_{EC} H(E_\mu) + Q_1[1 - H(e_p^1)]. \end{aligned} \tag{1}$$

Here the subscript "sps" and "wps" represent the key rate is estimated for SPS and WPS, respectively. e_b is the bit error, e_p is the phase error for single photon pulse. Q_μ (E_μ) is the gain (error rate) of signal state, Q_1 is the gain of single photon pulse. $H(\cdot)$ is the Shannon function.

Due to the imperfection of random bit, the phase error e_p and e_p^1 do not equal with the bit error in X-basis (e_b^x), thus a new method is required to bound the phase error with given flaws of random bit and the bit error (e_b^x). In this paper, we proved that the upper bound of phase error rate can be written as (see full text for details)

$$e_p \leq \frac{1+2\varepsilon_1}{1-2\varepsilon_1} e_b^X + \frac{1}{2} - \sqrt{\frac{1}{4} - \varepsilon_0^2}. \tag{2}$$

Here ε_0 and ε_1 are the flaws of random bit used by Alice and Bob, which is defined as

$$\begin{aligned} \left| p\left(x_0 = k | \lambda_0 = i\right) - \frac{1}{2} \right| &\leq \varepsilon_0, \\ \left| p\left(x_1 = k' | \lambda_1 = j\right) - \frac{1}{2} \right| &\leq \varepsilon_1, \end{aligned} \tag{3}$$

in which x_0 (x_1) is the random bit for bit (basis), λ_0 and λ_1 are the hidden variable controlled by Eve.

With the analysis given above, we can estimate the key rate under imperfect random bit, which is shown in Fig.1, which clearly show that our method can improve the performance of QKD system even if the random bits used by Alice and Bob are weakly controlled by Ev.

Conclusions- We evaluated the security of QKD with weak basis-choice flaws. The previous analysis of Li *et al.* [1] was extended by applying a tight analytical bound for estimating the phase error. The final key rate was significantly improved by the proposed approach. For example, when $\varepsilon_0 = \varepsilon_1 = 0.1$ and the bit error rate exceeded 3.4%, no final key was generated by the previous method, but a final key rate of 0.45 was achieved by our method. Applying our analysis, we evaluated the security of a practical QKD system in which Bob passively chooses his basis with a BS. In experiments using a practical BS with typical parameters, the key rate was reduced by less than 6%. Thus, the proposed method improves the QKD performance even in weak randomness scenarios.

Acknowledgment- The authors thank H.W. Li for helpful discussions on the simulation. This work was supported by the National Natural Science Foundation of China (NSFC) (11674397).

[1] H. W. Li, Z. Q. Yin, S. Wang, Y. J. Qian, W. Chen, G. C. Guo, and Z. F. Han, Sci. Rep. **5**, 16200 (2015).
[2] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

* sunshh8@mail.sysu.edu.cn

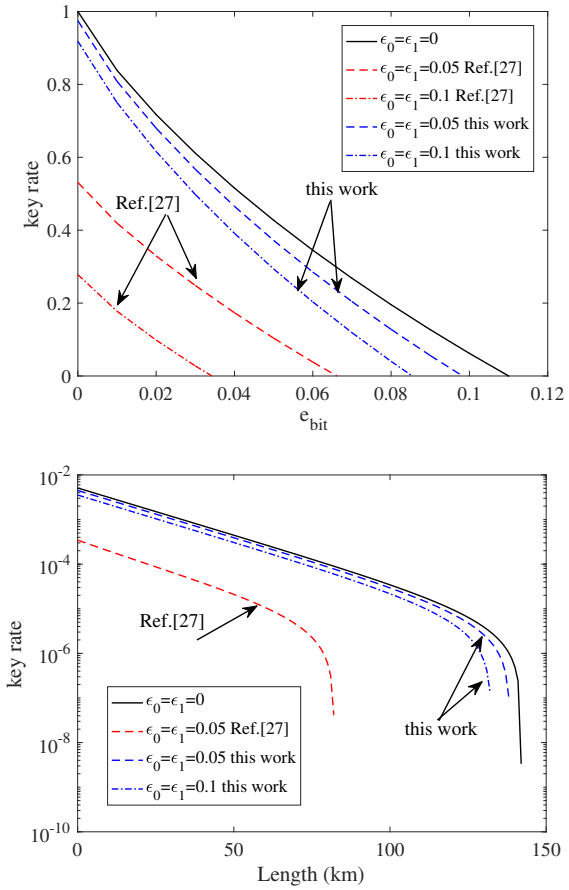

FIG. 1. Key rates in the original analysis [1] (red lines) and the method proposed in this paper (blue lines). Results are plotted for SPS (left) and WPS (right). The black solid line is the result of the ideal case without basis-choice flaws. To simplify the simulation, we assume $\varepsilon_0 = \varepsilon_1$ and infinite decoy states. The WPS case employs the experimental results of GYS [2]; thus, the signal state intensity is $s = 0.48$ and the other parameters are set as follows: dark count rate $Y_0 = 1.7 \times 10^{-6}$, background error rate $e_0 = 0.5$, fiber loss 0.21 dB/km, Bob's transmittance $\eta_{Bob} = 0.045$, and error rate of optical devices $e_{det} = 3.3\%$. The method of Ref. [1] generates no key in the case of WPS with $\varepsilon_0 = \varepsilon_1 = 0.1$.