Passive round-robin differential-quadrature-phase-shift quantum key distribution with untrusted detectors

Hongwei Liu, Haiqiang Ma†, Wenxiu Qu, Tianqi Dou, Yitian Chen, Jipeng Wang and Yuemei Li
School of Science, State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications, Beijing 100876, China
†*Corresponding author*
Email: hqma@bupt.edu.cn

Quantum key distribution (QKD) allows two legitimate parties (commonly named Alice and Bob) to share their secure keys with an information-theoretic secure way. Since the first protocol, so called BB84 algorithm, was proposed, QKD has attracted public attention and many similar protocols are presented. However, these protocols inherently rely on the original version of Hersenberg's uncertainty principle, which dictates that the more information Eve has obtained, the more disturbance she should have caused on the signal. Recently, a new approach named round-robin differential-phase-shift (RRDPS) QKD [1] and its alternative scheme [2], [3] was proposed, the costs of privacy amplification of this protocol is estimated without any monitoring, but depends only on the state prepared by Alice. This distinctive property causes the protocol to have a better tolerance of bit errors and finite-length effects. However, realistic experimental apparatus, which is never ideal, post a serious and non-trivial threat to the security of these protocols as eavesdropper (called Eve) may exploit loopholes due to apparatus imperfections. There are some related work being published recently [4], [5], which are targeted to the detectors, the most complex implements in the system. In this poster, we present a new passive round-robin differential-quadrature-phase-shift (RRDQPS) QKD scheme, in which Alice and Bob prepare their own state by using X or Y basis independently, then Bob uses Hong-Ou-Mandel (HOM) type interference to get the detected events with time slots and broadcasts this information to Alice. Finally, they can calculate a secure key by using this detected information. Since the clicks of detectors are publicly announced, our scheme can immune to all attacks against the detectors.

We describe a setup of our scheme as fig.1. Alice and Bob prepares an block-wise phase random optical pulse train consisting of L pulses independently. These pulses pass through an asymmetric Mach-Zehnder interferometer (AMZI) successively, whose function is encoding time-bin of X or Y basis on these pulses. Let us consider a simple case when both Alice and Bob each has exactly one photon in their L-pulse block. The states of Alice and Bob can be represented by

$$\begin{aligned} |\psi\rangle_p &= \frac{e^{i\delta_p}}{\sqrt{2L}} \sum_{K=1}^{L} \left(p_{i,r}^\dagger + e^{i\phi_{pi}} p_{i,s}^\dagger\right)|0\rangle \\ &= \frac{e^{i\delta_p}}{\sqrt{2L}} \sum_{K=1}^{L} \left(p_{i,r}^\dagger + i^{a_{pi}}(-1)^{s_{pi}} p_{i,s}^\dagger\right)|0\rangle \end{aligned} \tag{1}$$

where δ_p is a common random phase shift of all pulses in the block. p represents legitimate party, Alice or Bob. $\phi_{pi} = \frac{\pi}{2}a_{pi} + \pi s_{pi}$ is the relative phase between signal state $|s\rangle$ and reference state $|r\rangle$ of ith pulse. $p_{i,r}^\dagger$ and $p_{i,s}^\dagger$ are the creation operators of reference's and signal's ith position respectively. $a_{pi} \in \{0,1\}$ designates the choice of X or Y basis for ith pulse and $b_{pi} \in \{0,1\}$ denotes the random bit value of ith pulse. That is, the relative phase on X basis is $\phi_{piX} \in \{0,\pi\}$ and on Y basis is $\phi_{piY} \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$. Since there are two photon in a block, one from Alice and one from Bob, Bob would obtain at most two detection clicks. He postselects to choose the block where there are exactly two detections and announces his basis choice, detection results and positions i , j with time-bin r , s (if i=j or basis choice mismatched with Alice's, the results is discard).

After the interference and Bob's postselection. the

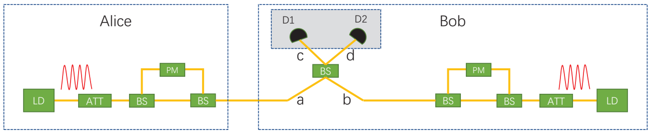

Figure 1. Passive RRDQPS-QKD scheme. Alice and Bob use a local laser to generate an L-pulse reference independently, which are then encoded to time-bin of X or Y basis by AMZI. Bob records the coincidence clicks. LD: laser diode; ATT: variable attenuator; BS: a 50/50 beam splitter (fiber); PM: phase modulator; D1 & D2 in gray box means these two detector are untrusted.

TABLE 1. Detector clicks corresponding to Alice's and Bob's raw key

ith Time-bin	jth Time-bin	Alice's key	Bob's key
$c(d)_i$ & $c(d)_j$ clicks:			
r	s	s_{aj}	s_{bj}
s	r	s_{ai}	s_{bi}
s	s	$s_{ai} \oplus s_{aj}$	$s_{bi} \oplus s_{bj}$
$c(d)_i$ & $d(c)_j$ clicks:			
r	s	s_{aj}	$1 \oplus s_{bj}$
s	r	s_{ai}	$1 \oplus s_{bi}$
s	s	$s_{ai} \oplus s_{aj}$	$1 \oplus s_{bi} \oplus s_{bj}$

quantum state at the two detectors becomes one of

$$\begin{aligned}
&\left[1+(-1)^{s_{aj}+s_{bj}}\right] c_{i,r}^{\dagger} c_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1+(-1)^{s_{aj}+s_{bj}}\right] d_{i,r}^{\dagger} d_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1+(-1)^{s_{ai}+s_{bi}}\right] c_{i,s}^{\dagger} c_{j,r}^{\dagger}\left|0\right\rangle , \\
&\left[1+(-1)^{s_{ai}+s_{bi}}\right] d_{i,s}^{\dagger} d_{j,r}^{\dagger}\left|0\right\rangle , \\
&\left[1+(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right] c_{i,s}^{\dagger} c_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1+(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right] d_{i,s}^{\dagger} d_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1-(-1)^{s_{aj}+s_{bj}}\right] c_{i,r}^{\dagger} d_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1-(-1)^{s_{aj}+s_{bj}}\right] d_{i,r}^{\dagger} c_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1-(-1)^{s_{ai}+s_{bi}}\right] c_{j,r}^{\dagger} d_{i,s}^{\dagger}\left|0\right\rangle , \\
&\left[1-(-1)^{s_{ai}+s_{bi}}\right] d_{j,r}^{\dagger} c_{i,s}^{\dagger}\left|0\right\rangle , \\
&\left[1-(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right] c_{i,s}^{\dagger} d_{j,s}^{\dagger}\left|0\right\rangle , \\
&\left[1-(-1)^{(s_{ai}+s_{aj})+(s_{bi}+s_{bi})}\right] d_{i,s}^{\dagger} c_{j,s}^{\dagger}\left|0\right\rangle
\end{aligned} \tag{2}$$

where $c_{i,r(s)}^{\dagger}$ and $d_{i,r(s)}^{\dagger}$ are the creation operators at the two detectors, respectively. This means Alice and Bob can calculate their raw key by following Table.1.

For intuitive security analysis, we consider another measurement procedure by Bob shown in Fig.2. For a general single photon input for Alice and Bob (Possibly corrupted by Eve),

$$\sum_{i=1}^{L} \gamma_{ai} a_i^{\dagger}\left|0\right\rangle \oplus \sum_{i=1}^{L} \gamma_{bi} b_i^{\dagger}\left|0\right\rangle \tag{3}$$

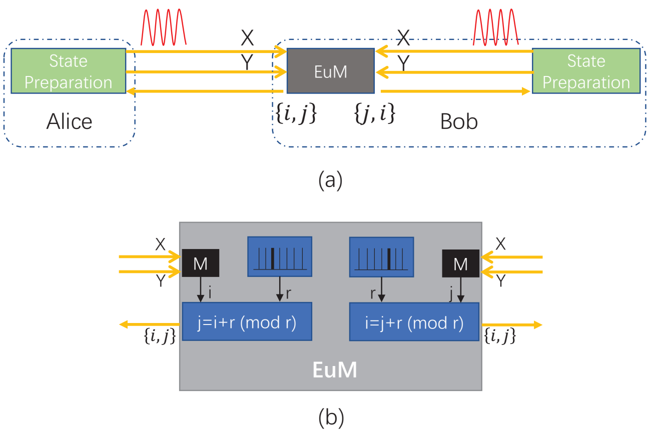

Figure 2. (a).Equivalent measurement model; (b).Detail of EuM unit in (a). Bob obtains a click at position i or j, generates two random numbers $r \in \{1, \ldots, L-1\}$ and $b \in \{0, 1\}$ to obtain $j = i + (-1)^b r$ or $i = j + (-1)^b r$, and publicly announces i and j to Alice.

It is easy to calculate the probability of outputting the pair (i,j) in Fig.1 and Fig.2 is identical as

$$2\left|\gamma_{ai}\gamma_{bj}\right|^2 + 2\left|\gamma_{aj}\gamma_{bi}\right|^2 \tag{4}$$

Thus, the equivalence of two measurement procedure is proved. In practice, a single photon state source is often replaced by a weak laser pulse, which can be described by a coherent state. In this scenario, one can make our scheme secure again by using decoy-state technical. Furthermore, due to the detection results are announced publicly, the attacks for detector executed by Eve cannot weaken our scheme, especially for the attack method proposed in [4], [5]. Two bases are used for state preparation, so the encoded states are non-orthogonal and Eve cannot fully identify the transmitted signal, this characteristic will further enhance the security of our scheme. It is noted that the security of original RRDPS-QKD protocol is ensured by the information causality and complementarity, which means Bob are required to switch measurement procedure between Fig.1 and Fig.2 arbitrary, thus, the measurement unit in our scheme may cannot place at untrusted third party. However, our scheme will contribute to the formulation of measurement device independent (MDI) version of RRDPS-QKD and its practical.

Acknowledgment

This work was supported by the National Natural Science Foundation of China Grant No. 61178010 and No. 11374042; the Fund of Open question of State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) No.IPOC2016ZT09.

References

[1] Sasaki T, Yamamoto Y and Koashi M 2014 Practical quantum key distribution protocol without monitoring signal disturbance Nature 509 475C8

[2] Guan J-Y, Cao Z, Liu Y, Shen-Tu G-L, Pelc J S, Fejer M M, Peng C-Z, Ma X, Zhang Q and Pan J-W 2015 Experimental passive round-robin differential phase-shift quantum key distribution Phys. Rev. Lett. 114 180502

[3] Zhou C, Zhang Y-Y, Bao W-S, Li H-W, Wang Y and Jiang M-S 2017 Round-robin differential quadrature phase-shift quantum key distribution Chinese Phys. B 26 20303

[4] Cao Z, Yin Z-Q and Han Z-F 2016 Trustworthiness of measurement devices in round-robin differential-phase-shift quantum key distribution Phys. Rev. A 93 22310

[5] Iwakoshi T 2015 Faked state attack on realistic round robin DPS quantum key distribution systems and countermeasure SPIE Optics+ Optoelectronics (International Society for Optics and Photonics) p 950504