Physics Letters A ••• (••••) •••–•••

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Robustness of reference-frame-independent quantum key distribution against the relative motion of the reference frames

Tanumoy Pramanik [a], Byung Kwon Park [a,b], Young-Wook Cho [a], Sang-Wook Han [a], Yong-Su Kim [a,b], Sung Moon [a]

[a] Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea
[b] Department of Nano-Materials Science and Engineering, Korea University of Science and Technology, Daejeon, 34113, Republic of Korea

A R T I C L E I N F O

Article history:
Received 20 May 2017
Received in revised form 1 June 2017
Accepted 1 June 2017
Available online xxxx
Communicated by A. Eisfeld

Keywords:
Quantum key distribution
Reference frame fluctuation
Decay state

A B S T R A C T

Reference-Frame-Independent quantum key distribution (RFI-QKD) is known to be robust against slowly varying reference frames. However, other QKD protocols such as BB84 can also provide secrete keys if the speed of the relative motion of the reference frames is slow enough. While there has been a few studies to quantify the speed of the relative motion of the reference frames in RFI-QKD, it is not yet clear if RFI-QKD provides better performance than other QKD protocols under this condition. Here, we analyze and compare the security of RFI-QKD and BB84 protocol in the presence of the relative motion of the reference frames. In order to compare their security in real world implementation, we also consider the QKD protocols with decoy state method. Our analysis shows that RFI-QKD provides more robustness than BB84 protocol against the relative motion of the reference frames.

1. Introduction

Quantum key distribution (QKD) promises enhanced communication security based on the laws of quantum physics [1,2]. Since the first QKD protocol has been introduced in 1984, there has been a lot of theoretical and experimental effort to improve the security and the practicality of QKD [3,4]. These days, QKD research is not only limited in laboratories [5–9] but also in industries.[1]

In general, QKD requires a shared common reference frame between two communicating parties, Alice and Bob. For example, the interferometric stability or the alignment of the polarization axes are required for fiber based QKD using phase encoding and polarization encoding free-space QKD, respectively. However, it can be difficult and costly to maintain the shared reference frame in real world implementation. For instance, it is highly impractical to establish a common polarization axes in earth-to-satellite QKD due to the revolution and rotation of the satellite with respect to the ground station [10–16].

A recently proposed reference-frame-independent QKD (RFI-QKD) provides an efficient way to bypass this shared reference frame problem [17]. In RFI-QKD, Alice and Bob share the secrete keys via a decoherence-free basis while check the communication security with other bases. Both free-space [18] and telecom fiber [19,20] based RFI-QKD have been successfully implemented. It is remarkable that the concept of the reference frame independent can be applied to measurement-device-independent QKD [21,22].

Unlike to its name, however, the security of the original theory of RFI-QKD is guaranteed when the relative motion of the reference frames is slow comparing to the system repetition rate [17]. It is because the eavesdropper information is bounded by the entanglement left in the bipartite state shared between Alice and Bob which is independent of the relative motion of the reference frames. [23]. If the reference frames of Alice and Bob are deviated with a fixed angle, however, one can easily compensate the deviation and implement an ordinary QKD protocol. Therefore, the effectiveness of RFI-QKD over other QKD protocols becomes clear when there is rapid relative motion of the reference frames during the QKD communication. There has been few studies to quantify the speed of the relative motion of the reference frames in RFI-QKD [24,25]. Without the performance comparison with other QKD protocols, however, these studies do not show the effectiveness of RFI-QKD over other QKD protocols.

In this paper, we report the security of RFI-QKD and BB84 protocol in the presence of the relative motion of the reference frames of Alice and Bob. In order to compare the performances in real world implementation, we also consider the decoy state method. By comparing the security analyses, we found that RFI-QKD is

E-mail addresses: tanu.pra99@gmail.com (T. Pramanik), yong-su.kim@kist.re.kr (Y.-S. Kim).

[1] For example, ID Quantique, MagiQ Technologies, QuintessenceLabs, and SeQureNet.

http://dx.doi.org/10.1016/j.physleta.2017.06.002

Please cite this article in press as: T. Pramanik et al., Robustness of reference-frame-independent quantum key distribution against the relative motion of the reference frames, Phys. Lett. A (2017), http://dx.doi.org/10.1016/j.physleta.2017.06.002

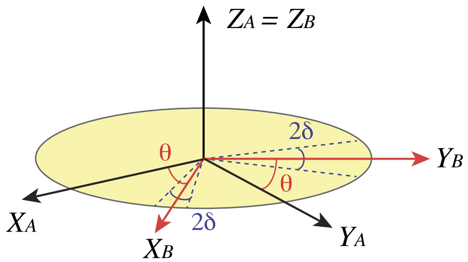

Fig. 1. The polarization axes of Alice and Bob. θ and 2δ denote the fixed angle deviation, and the range of the relative motion of the polarizations axes, respectively.

more robust than BB84 protocol against the relative motion of the reference frames.

2. QKD with a fixed reference frame deviation

In this section, we review the security proof of RFI-QKD and BB84 protocol with a fixed reference frame deviation. A shared reference frame is required for both fiber based QKD with phase and free-space QKD with polarization encoding. It corresponds to the interferometric stability and the polarization axes for fiber based QKD and free-space QKD, respectively. In the following, we will consider free-space QKD with polarization encoding for simplicity. However, we note that our analysis is also applicable for fiber based QKD with phase encoding.

2.1. RFI-QKD protocol

Fig. 1 shows the polarization axes of Alice and Bob with a deviation angle θ. Since Alice and Bob should face each other in order to transmit the optical pulses, their Z-axes, which corresponds to left- and right-circular polarization states, are always well aligned. On the other hand, the relation of their X and Y-axes, which correspond to linear polarization states such as horizontal, vertical, $+45°$, and $-45°$ polarization states, depend on θ. The relations of the polarization axes are

$$X_B = X_A\cos\theta + Y_A\sin\theta,$$
$$Y_B = Y_A\cos\theta - X_A\sin\theta,$$
$$Z_B = Z_A, \tag{1}$$

where the subscripts A and B denote Alice and Bob, respectively.

In RFI-QKD, Alice and Bob share the secrete keys via Z-axis, as it is unaffected by the polarization axes deviation. In this basis, the quantum bit error rate (QBER) becomes

$$Q_{ZZ} = \frac{1-\langle Z_A Z_B\rangle}{2}. \tag{2}$$

Here, the subscripts ij where $i, j \in \{X, Y, Z\}$ denote that Alice sends a state in i basis while Bob measures it in j basis. The probability distributions of the measurement outcomes in X and Y-axes are used to estimate the knowledge of an eavesdropper, Eve. Her knowledge can be estimated by a quantity C which is defined as

$$C = \langle X_A X_B\rangle^2 + \langle X_A Y_B\rangle^2 + \langle Y_A X_B\rangle^2 + \langle Y_A Y_B\rangle^2. \tag{3}$$

Note that the quantity C is independent of the deviation angle θ. The knowledge of Eve is bounded by

$$I_E[Q_{ZZ}, C] = (1-Q_{ZZ})H\left[\frac{1+u}{2}\right] + Q_{ZZ}H\left[\frac{1+v}{2}\right], \tag{4}$$

where

$$u = \min\left[\frac{1}{1-Q_{ZZ}}\sqrt{\frac{C}{2}}, 1\right],$$
$$v = \frac{1}{Q_{ZZ}}\sqrt{\frac{C}{2} - (1-Q_{ZZ})^2u^2}, \tag{5}$$

and $H[x] = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy of x.

The secret key rate in the RFI-QKD protocol is given by [17]

$$r_{RFI} = 1 - H[Q_{ZZ}] - I_E[Q_{ZZ}, C]. \tag{6}$$

It is notable that Eq. (6) is independent of a fixed deviation rotation θ [17]. The security proof shows that $r_{RFI} \geq 0$ for $Q_{ZZ} \lesssim 15.9\%$.

In practice, the effective quantum state that Bob receives from Alice can have errors due to the transmission noise and experimental imperfection. Assuming the noise and the imperfection are polarization independent, we can model the Bob's receiving quantum state ρ_B as

$$\rho_B = p\rho_A + \frac{1-p}{2}I, \tag{7}$$

where ρ_A, $1-p$ and I are the state prepared by Alice, the strength of noise, and a two dimensional identity matrix, respectively. Supposing Alice and Bob choose $\mathcal{F}$ and $\mathcal{G}$ for their bases, respectively, $\langle\mathcal{F}_A\mathcal{G}_B\rangle$ can be written as a state dependent form of $\langle\mathcal{F}_A\mathcal{G}_B\rangle = \mathrm{Tr}[(\mathcal{F}_A\otimes\mathcal{G}_B)\cdot\rho_{AB}]$ where $\mathcal{F}, \mathcal{G} \in \{X, Y, Z\}$, and $\rho_{AB} = \rho_A\otimes\rho_B$. Therefore, the QBER Q_{ZZ} and the quantity C become

$$Q_{ZZ} = \frac{1-p}{2}, \tag{8}$$
$$C = 2p^2 = 2(1-2Q_{ZZ})^2. \tag{9}$$

In this case, $r_{RFI} \geq 0$ for $Q_{ZZ} \lesssim 12.6\%$.

2.2. BB84 protocol

In this section, we consider the secrete key rate of BB84 with a fixed reference frame deviation. Due to the symmetry, the QBER of X, and Y-axes are the same, and they are given as

$$Q_{XX} = \frac{1-\langle X_A X_B\rangle}{2}$$
$$= \frac{1-p\cos\theta}{2} = Q_{YY}. \tag{10}$$

If Alice and Bob utilize X and Y axes, the overall QBER $Q_{\overline{XY}}$ is

$$Q_{\overline{XY}} = \frac{1}{2}(Q_{XX} + Q_{YY})$$
$$= \frac{1}{2}(1-p\cos\theta). \tag{11}$$

Since we know that Z-axis is rotation invariant, one can get lower QBER by using Z-axis instead of Y-axis. In this case, the overall QBER $Q_{\overline{XZ}}$ is given by

$$Q_{\overline{XZ}} = \frac{1}{2}(Q_{XX} + Q_{ZZ})$$
$$= \frac{1}{2}\left(1 - p\cos^2\frac{\theta}{2}\right). \tag{12}$$

The secrete key rate of BB84 with $\{X, Y\}(\{X, Z\})$ bases is given by [3,4]

$$r_{BB84}^{XZ\,(XY)} = 1 - 2H\left[Q_{\overline{XZ}\,(\overline{XY})}\right]. \tag{13}$$

Apparently, Eq. (13) is dependent on the reference frame deviation θ. However, one can easily compensate the deviation if θ is invariant during the QKD communication. For BB84 protocol, $r_{BB84}^{XZ\,(XY)} \geq 0$ for $Q_{ZZ} \lesssim 11\%$ when $\theta = 0$.