ARTICLE IN PRESS

[Physics Letters A](http://dx.doi.org/10.1016/j.physleta.2017.06.002) ••• (••••) •••-•••

Contents lists available at [ScienceDirect](http://www.ScienceDirect.com/) 1 67

\mathbb{P}^n and \mathbb{P}^n are \mathbb{P}^n 3 69

www.elsevier.com/locate/pla

11 Dobustness of reference frame independent quantum low distribution 17 $\frac{11}{12}$ Robustness of reference-frame-independent quantum key distribution $\frac{77}{78}$ ¹³ against the relative motion of the reference frames and the setting of the setting of the setting of the set

¹⁵ Tanumoy Pramanik^a, Byung Kwon Park^{a,b}, Young-Wook Cho^a, Sang-Wook Han^a, Tanumoy Pramanik^a, ¹⁶ 82
17 Yong-Su Kim ^{a,b}, Sung Moon ^a 17 83

¹⁸ a Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea

¹⁹ Department of Nano-Materials Science and Engineering, Korea University of Science and Technology, Daejeon, 34113, Republic of Korea

22 ARTICLE INFO ABSTRACT 88

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

24 Article history: **Example 20 State Concept Article Prame-Independent quantum key distribution (RFI-QKD) is known to be robust against slowly 90 action-** $_{25}$ Received 20 May 2017 **Fig. 1.1 Steps 25 Second Protocols** such as BB84 can also provide secrete keys if $_{91}$ exerved in expert on the speed of the relative motion of the reference frames is slow enough. While there has been a few $_{92}$ 27 Available online xxxx
if RFI-QKD provides better performance than other QKD protocols under this condition. Here, we analyze 28 Communicated by A. Eisteld
and compare the security of RFI-QKD and BB84 protocol in the presence of the relative motion of the 29 Treference frames. In order to compare their security in real world implementation, we also consider the ⁹⁶ ^{Countum} key distribution **1966** CIV COND protocols with decoy state method. Our analysis shows that RFI-QKD provides more robustness than 31 Reference frame fluctuation **BB84** protocol against the relative motion of the reference frames. studies to quantify the speed of the relative motion of the reference frames in RFI-QKD, it is not yet clear

32 Decay state **EXECUTE:** The set of the set o

1. Introduction

⁴² a lot of theoretical and experimental effort to improve the security $\frac{22}{1}$ Quantum key distribution (QKD) promises enhanced communiand the practicality of QKD $[3,4]$. These days, QKD research is not only limited in laboratories [\[5–9\]](#page--1-0) but also in industries.¹

In general, QKD requires a shared common reference frame beworld 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 [\[10–16\].](#page--1-0)

A recently proposed reference-frame-independent QKD (RFI-QKD) provides an efficient way to bypass this shared reference frame problem [\[17\].](#page--1-0) In RFI-QKD, Alice and Bob share the secrete

64 130 <http://dx.doi.org/10.1016/j.physleta.2017.06.002>

 65 $0375-9601$ / \odot 2017 Published by Elsevier B.V.

37 **1. Introduction 1. Introduction 103 has a series and the communica- has a series of the communica-** 103 38 104 tion security with other bases. Both free-space [\[18\]](#page--1-0) and telecom 39 Duantum key distribution (OKD) promises enhanced communi- fiber [\[19,20\]](#page--1-0) based RFI-QKD have been successfully implemented. 105 ⁴⁰ cation security based on the laws of quantum physics [\[1,2\].](#page--1-0) Since it is remarkable that the concept of the reference frame indepen-
106 ⁴¹ the first QKD protocol has been introduced in 1984, there has been alleptican be applied to measurement-device-independent QKD [21, $\frac{1}{2}$ 107 It is remarkable that the concept of the reference frame independent can be applied to measurement-device-independent QKD [\[21,](#page--1-0) [22\].](#page--1-0)

⁴³ and the practicality of OKD [3.4] These days, OKD research is not Unlike to its name, however, the security of the original theory 109 44 only limited in laboratories $[5-9]$ but also in industries 1 of RFI-QKD is guaranteed when the relative motion of the refer-⁴⁵ In general OKD requires a shared common reference frame be-
ence frames is slow comparing to the system repetition rate [\[17\].](#page--1-0) ⁴⁶ tween two communicating parties, Alice and Bob. For example, the the Burgary and the eavesdropper information is bounded by the en-⁴⁷ interferometric stability or the alignment of the polarization axes tanglement left in the bipartite state shared between Alice and 113 ⁴⁸ are required for fiber based QKD using phase encoding and polar-
⁴⁸ are required for fiber based QKD using phase encoding and polar-⁴⁹ ization encoding free-space QKD, respectively. However, it can be **trames.** [23]. If the reference frames of Alice and Bob are deviated 115 50 difficult and costly to maintain the shared reference frame in real with a fixed angle, however, one can easily compensate the de-
116 51 world implementation For instance it is bighly impractical to es. Viation and implement an ordinary QKD protocol. Therefore, the 117 52 tablish a common polarization aves in earth-to-satellite OKD due effectiveness of RFI-QKD over other QKD protocols becomes clear 118 53 to the revolution and rotation of the satellite with respect to the when there is rapid relative motion of the reference frames during 119 54 120 the QKD communication. There has been few studies to quantify $\frac{1}{2}$ 121 $\frac{1}{2}$ 121 $\frac{1}{2}$ $\frac{1}{2}$ the speed of the relative motion of the reference frames in RFI-121 $\frac{66}{24,25}$. Without the performance comparison with other QKD $\frac{24,25}{24,25}$. Without the performance comparison with other QKD $\frac{122}{24}$ 57 terms problem in 171 In PEI OKD Alics and Pob charge the escrate protocols, however, these studies do not show the effectiveness of 123 58 124 RFI-QKD over other QKD protocols. 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. [\[23\].](#page--1-0) If the reference frames of Alice and Bob are deviated with a fixed angle, however, one can easily compensate the de-

59 125 In this paper, we report the security of RFI-QKD and BB84 pro-60 126 tocol in the presence of the relative motion of the reference frames 126 61 I WE THE REST RESEALT AND RESEALT A MARKET COMPARE THE PRISON OF ALICE AND **Of Alice and Bob. In order to compare the performances in real** 127 62 $^{-1}$ For example, ID Quantique, MagiQ Technologies, QuintessenceLabs, and Se- WOTId Implementation, we also consider the decoy state method. $\,$ 128 $\,$ 63 129 By comparing the security analyses, we found that RFI-QKD is world implementation, we also consider the decoy state method.

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

66 and the contract of the con

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

QureNet.

11 77 **Fig. 1.** The polarization axes of Alice and Bob. *θ* and 2*δ* denote the fixed angle de-

¹⁴ more robust than BB84 protocol against the relative motion of the $\frac{13.50}{\mu}$ in proctice, the effective quantum state that Bob receives from ⁸⁰ reference frames.

¹⁹ In this section, we review the security proof of RFI-QKD and $\frac{85}{1}$ ²¹ erence frame is required for both fiber based QKD with phase and $\begin{array}{ccc} \sim & \sim & 2 \\ \sim & 2 & 1 \end{array}$ ²⁷ based QKD with phase encoding. ⁹³ and the quantity *C* become based QKD with phase encoding. 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

32 $\frac{118}{118}$, 1 shows the polarization axes of fine this bob with a devi-

In this case, $r_{RFI} \ge 0$ for $Q_{ZZ} \le 12.6$ %. 33 ation angle θ . Since Alice and Bob should face each other in order $\frac{111 \text{ tHIS}}{111 \text{ tHIS}}$ ase, $\frac{1}{R}$ $\frac{1}{R}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{2}$. ₃₄ to transmit the optical pulses, their *Z*-axes, which corresponds to $\frac{1}{2}$ RRRA protocol 35 101 left- and right-circular polarization states, are always well aligned. $\frac{36}{26}$ by the section of the section of the section, we consider the secrete key rate of BB84 with a $\frac{102}{26}$ 37 1.58 in the polarization states such as nonzonial, vertical, fixed reference frame deviation. Due to the symmetry, the QBER of 103 38 104 *X*, and *Y* -axes are the same, and they are given as 39 life polarization axes are 105 Fig. 1 shows the polarization axes of Alice and Bob with a devi-On the other hand, the relation of their *X* and *Y* -axes, which correspond to linear polarization states such as horizontal, vertical, $+45^\circ$, and -45° polarization states, depend on θ . The relations of the polarization axes are

$$
V_B = Y_A \cos \theta + Y_A \sin \theta,
$$

\n
$$
V_B = Y_A \cos \theta - X_A \sin \theta,
$$

\n
$$
V_B = Z_A,
$$
\n(10) $\frac{108}{107}$
\n
$$
V_B = Z_A,
$$
\n(11) If Alice and Bob utilize X and Y axes, the overall QBER Q_{xx} is 110

45 111 where the subscripts *A* and *B* denote Alice and Bob, respectively. $\frac{46}{47}$ In RFI-QKD, Alice and Bob share the secrete keys via *Z*-axis, as $Q_{\overline{XY}} = \frac{1}{2}(Q_{XX} + Q_{YY})$ 112 47 113 m at good, three and bob share the secrete keys via 2 and, as 2 2 and 2 $\frac{48}{10}$ it is unaffected by the polarization axes deviation. In this basis, the $\frac{1}{4}$ $\frac{1}{4$ quantum bit error rate (QBER) becomes

$$
Q_{ZZ} = \frac{1 - \langle Z_A Z_B \rangle}{2}.
$$
 Since we know that Z-axis is rotation invariant, one can get lower
Qzz = $\frac{1 - \langle Z_A Z_B \rangle}{2}$. (2)
QBER by using Z-axis instead of Y-axis. In this case, the overall

53 Here, the subscripts *ij* where *i*, $j \in \{X, Y, Z\}$ denote that Alice $\begin{bmatrix} 1 & 2 & 3 \ 2 & 3 & 6 \end{bmatrix}$ 54 sends a state in *i* basis while Bob measures it in *j* basis. The proba- $\theta = \frac{1}{\theta}(\theta_{yy} + \theta_{zz})$ 55 121 bility distributions of the measurement outcomes in *X* and *Y* -axes 56 are used to estimate the knowledge of an eavesdropper, Eve. Her $1\left(1\right)$ $2\left(1\right)$ 57 knowledge can be estimated by a quantity *C* which is defined as $-\frac{1}{2}$ (1² PCOs $\frac{1}{2}$).

$$
C = (X_A X_B)^2 + (X_A Y_B)^2 + (Y_A X_B)^2 + (Y_A Y_B)^2.
$$
\n(3)

\nThe secret key rate of BB84 with $\{X, Y\}(\{X, Z\})$ bases is given by $\begin{bmatrix} 24 \\ 125 \\ 125 \end{bmatrix}$

⁶⁰ Note that the quantity *C* is independent of the deviation angle *θ* . $\frac{39}{25}$ ($\frac{9}{25}$) $\frac{1}{25}$. $\frac{1}{25}$. T

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

frames, Phys. Lett. A (2017), http://dx.doi.org/10.1016/j.physleta.2017.06.002

where

$$
u = \min\left[\frac{1}{1 - Q_{ZZ}}\sqrt{\frac{C}{2}}, 1\right],
$$

$$
v = \frac{1}{Q_{ZZ}} \sqrt{\frac{C}{2} - (1 - Q_{ZZ})^2 u^2},
$$
\n(5)

 $\frac{1}{7}$

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

 $\frac{X_A}{Y_B}$ $\frac{Z_O}{Z_A}$ $\frac{1}{75}$ The secret key rate in the RFI-QKD protocol is given by [\[17\]](#page--1-0) $\frac{1}{75}$

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

12 viation, and the range of the relative motion of the polarizations axes, respectively. It is included that Eq. (0) is independent of a fixed deviation to- $\frac{12}{13}$ tation θ [\[17\].](#page--1-0) The security proof shows that $r_{RFI} \ge 0$ for $Q_{ZZ} \lesssim \frac{12}{79}$ It is notable that Eq. (6) is independent of a fixed deviation ro-15*.*9%.

 $\frac{15}{15}$ reference frames $\frac{16}{16}$ 16 $\frac{1}{16}$ 82 17 83 **2. QKD with a fixed reference frame deviation** 18 84 polarization independent, we can model the Bob's receiving quanmental imperfection. Assuming the noise and the imperfection are tum state ρ_B as

$$
P_{\text{2D}}
$$
BB84 protocol with a fixed reference frame deviation. A shared ref-
erence frame is required for both fiber based OKD with phase and

²² free-space QKD with polarization encoding. It corresponds to the where $ρ$ _A, 1−p and *I* are the state prepared by Alice, the strength ⁸⁸ ²³ interferometric stability and the polarization axes for fiber based of noise, and a two dimensional identity matrix, respectively. Sup-24 QKD and free-space QKD, respectively. In the following, we will posing Alice and Bob choose $\mathcal F$ and $\mathcal G$ for their bases, respectively, $\frac{90}{91}$ ²⁵ consider free-space QKD with polarization encoding for simplic-
 $\langle \mathcal{F}_A \mathcal{G}_B \rangle$ can be written as a state dependent form of $\langle \mathcal{F}_A \mathcal{G}_B \rangle$ = $\frac{91}{92}$ 26 ity. However, we note that our analysis is also applicable for fiber $Tr[(\mathcal{F}_A \otimes \mathcal{G}_B) \cdot \rho_{AB}]$ where $\mathcal{F}, \mathcal{G} \in \{X, Y, Z\}$, and $\rho_{AB} = \rho_A \otimes \rho_B$.

$$
Q_{ZZ} = \frac{1-p}{2},
$$
 (8)

$$
C = 2p^2 = 2(1 - 2Q_{ZZ})^2.
$$

2.2. BB84 protocol

$$
Q_{XX} = \frac{1 - \langle X_A X_B \rangle}{2}
$$

$$
Q_{XX} = \frac{1 - \langle X_A X_B \rangle}{2}
$$

$$
Q_{XX} = \frac{1 - \langle X_A X_B \rangle}{2}
$$

105
106
108

$$
=\frac{1-p\cos\theta}{2}=Q_{YY}.
$$
 (10)

 $\mathcal{L}_B = \mathcal{L}_A$, $\mathcal{L}_B = \mathcal{L}_B$, $\mathcal{L}_B = \mathcal$

$$
Q_{\overline{XY}} = \frac{1}{2} (Q_{XX} + Q_{YY})
$$

= $\frac{1}{2} (1 - 2\cos{\theta})$ (11)

 $\frac{115}{2}$ $\frac{115}{115}$ $\frac{115}{115}$ $=\frac{1}{2}(1-p\cos\theta).$ (11)

52 **COBER** $Q_{\overline{XZ}}$ **is given by** 118

sends a state in *i* basis while Bob measures it in *j* basis. The proba-
\nibility distributions of the measurement outcomes in *X* and *Y*-axes
\nare used to estimate the knowledge of an eavesdropper, Eve. Her
\nknowledge can be estimated by a quantity *C* which is defined as\n
$$
\frac{1}{2} \left(1 - p \cos^2 \frac{\theta}{2}\right).
$$
\n(12)

by [\[3,4\]](#page--1-0)

Note that the quantity C is independent of the deviation angle
$$
\theta
$$
.
\n
$$
r_{BB84}^{XZ(XY)} = 1 - 2H \left[Q_{\overline{XZ}(\overline{XY})}\right].
$$
\n(13)

 129 Apparently, Eq. (13) is dependent on the reference frame devi- $I_E[Q_{ZZ}, C] = (1 - Q_{ZZ})H$ $\boxed{ }$ $\boxed{ }$ + $Q_{ZZ}H$ $\boxed{ }$ $\boxed{ }$ (4) ation *θ*. However, one can easily compensate the deviation if *θ* 130 131 is invariant during the QKD communication. For BB84 protocol, $r_{BB84}^{XZ\,(XY)} \ge 0$ for $Q_{ZZ} \lesssim 11\%$ when $\theta = 0$. 132

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

Download English Version:

<https://daneshyari.com/en/article/5496202>

Download Persian Version:

<https://daneshyari.com/article/5496202>

[Daneshyari.com](https://daneshyari.com)