Research Article | Vol. 29, No. 12 / 7 June 2021 / Optics Express 18966

Optics EXPRESS

Countermeasure for security loophole caused by asymmetric correlations of reference frame independent quantum key distribution with fewer quantum states

KYONGCHUN LIM,[1,2] BYUNG-SEOK CHOI,[1] JU HEE BAEK,[1] MINCHUL KIM,[1] JOONG-SEON CHOE,[1] KAP-JOONG KIM,[1] YOUNG-HO KO,[1] AND CHUN JU YOUN[1,3]

[1] *Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea*
[2] *lim.kc@etri.re.kr*
[3] *cjyoun@etri.re.kr*

Abstract: One of the challenging issues in free-space quantum key distribution (QKD) is the requirement of active compensation of the reference frame between the transmitter and receiver. Reference frame independent (RFI) QKD removes active compensation, but it requires more quantum states. A recent proposal can effectively reduce the required quantum states, but this can be achieved assuming the correlations defined in RFI QKD are symmetric. In a real QKD system, such symmetric correlations cannot always be satisfied owing to the device imperfections and optical misalignment. We theoretically analyze the effect of asymmetric correlations. Consequently, we report that the asymmetry causes security loopholes and provide a countermeasure to prevent them. Furthermore, we provide the experimental results of a free-space RFI QKD system to verify the countermeasure for the aforementioned problem. In conclusion, our work provides feasibility of the practical RFI QKD system with fewer quantum states by effectively preventing the security loophole.

1. Introduction

Quantum key distribution (QKD) is a promising solution for secure communication based on quantum physics. It does not depend on computational complexity, which is inevitable in conventional non-quantum cryptography. With the significant increase in the exchange of private information in communication networks, the importance of QKD has increased, which has led to many advances in the QKD field. With the rapid progress of fiber-based QKD [1–4], research on free-space QKD has been extended to various applications, such as in vehicles [5], aircrafts [6,7], and drones [8,9]. Furthermore, QKD has been employed in a satellite, suggesting that free-space QKD can overcome the distance limitations of fiber-based QKD [10].

In free-space QKD, the transmitter and receiver are not fixed because typically their installation location vibrates or they are installed in a moving object. However, since the conventional BB84 protocol requires a shared reference frame of polarization or phase between the two remote parties, they should be accompanied by active reference frame compensation in such situations [11]. The use of active compensation, however, makes a QKD system complex, thus, a reference frame independent (RFI) QKD was proposed [12]. RFI QKD uses two more quantum states having reference frame independent properties such as right and left circular polarization in a polarization encoding scheme. The two more quantum states require more state preparation and detection than that for the BB84 protocol.

The requirement of preparation and detection of more number of states in RFI QKD can be a burden in free-space QKD owing to limited load capacity and space. There has been a proposal

#427055 https://doi.org/10.1364/OE.427055
Journal © 2021 Received 8 Apr 2021; revised 21 May 2021; accepted 25 May 2021; published 2 Jun 2021

Optics EXPRESS

to reduce the required states by channel estimation from the reduced states [13]. This technique is also applied to RFI QKD, where it decreases two states out of six states [14]. Another proposal achieves a reduction of required states in an easier way based on the symmetry of the correlations defined in RFI QKD [15]. However, usually, symmetry does not hold in a practical QKD system owing to imperfections of optical components and optical misalignments.

Practical QKD systems with the newly proposed protocol can have security loopholes owing to their imperfection. Such security loopholes and the corresponding countermeasures have been proposed [16–20] to ensure the security of practical QKD systems. Since RFI QKD with fewer quantum states has been proposed recently, it is important to consider its possible security loopholes. Specifically, we find that the security loophole comes from unavoidable asymmetric implementation of RFI QKD due to device imperfections.

In this study, we theoretically analyze cases with asymmetric correlations and how the asymmetry affects the security of RFI QKD with fewer quantum states. We also provide a simple countermeasure to prevent security loopholes caused by the asymmetry. To verify the theoretical results, we demonstrate a free-space RFI QKD system with fewer quantum states without the security loophole and measure its performance.

2. Reference frame independent quantum key distribution

RFI QKD is fundamentally based on the QKD protocol called the six-state protocol [21]. Unlike the six-state protocol, RFI QKD estimates eavesdropping and generates secret keys from independent properties to the rotation of the reference frame. Here, the reference frame corresponds to a polarization axis in the QKD using polarization encoding. To specify this, we introduce an entanglement-based RFI QKD protocol that can be identically transformed to RFI QKD with prepare and measure scheme [12].

In conventional RFI QKD using polarization encoding, a transmitter, Alice, prepares a Bell state $|\phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and shares it with a receiver, Bob. Alice and Bob measure the part of $|\phi\rangle$ with one of the measurement bases $\{Z_A, X_A, Y_A\}$ and $\{Z_B(\zeta), X_B(\zeta), Y_B(\zeta)\}$, respectively. Choice of measurement basis can be based on random number generator [22–24]. Here, ζ represents the relative angle of the polarization axes between Alice and Bob. In conventional RFI QKD, the measurement bases are assumed to be ideal, thus they can be expressed as the following relationships based on Pauli matrices $\{\sigma_Z, \sigma_X, \sigma_Y\}$.

$$\begin{aligned} Z_A &= \sigma_Z, \\ X_A &= \sigma_X, \\ Y_A &= \sigma_Y, \\ Z_B(\zeta) &= \sigma_Z \cos(2\zeta) - \sigma_X \sin(2\zeta), \\ X_B(\zeta) &= \sigma_Z \sin(2\zeta) + \sigma_X \cos(2\zeta), \\ Y_B(\zeta) &= \sigma_Y. \end{aligned} \tag{1}$$

Here, 2ζ comes from the fact that the relative rotation angle ζ of the polarization axes doubles in the Bloch sphere. Note that only the Y basis corresponding to the circular polarization basis is not altered by the relative angle ζ because the direction of the circular polarization is not affected by it, whereas the other two bases corresponding to the linear polarization bases are altered. Hereafter, we express $Y_B(\zeta) = Y_B$ to simplify notation.

After sharing the Bell state, Alice and Bob measure them with the aforementioned bases. After measuring the shared Bell state, Alice and Bob calculate correlations and quantum bit error rates (QBERs) based on the measurement results. For $i \in \{Z_A, X_A, Y_A\}, j \in \{Z_B(\zeta), X_B(\zeta), Y_B\}$, the correlations, $C_{ij} = \langle ij \rangle$, indicate the similarity of the measurement results, as in [12]. Because

Optics EXPRESS

QBER also has a similar meaning to C_{ij}, QBER Q_{ij} can be expressed with C_{ij} as follows:

$$Q_{ij} = \frac{1 - C_{ij}}{2}. \tag{2}$$

The sifted keys can be obtained only when Alice and Bob measure the Bell state with Y_A and Y_B bases, respectively, because $Q_{Y_AY_B}$ is independent of ζ. Based on $Q_{Y_AY_B}$, Alice and Bob perform error correction on the sifted keys.

To estimate information leakage to an eavesdropper, Eve, RFI QKD utilizes the security parameter C_{conv}.

$$C_{\text{conv}} = C^2_{Z_AZ_B(\zeta)} + C^2_{Z_AX_B(\zeta)} + C^2_{X_AZ_B(\zeta)} + C^2_{X_AX_B(\zeta)}. \tag{3}$$

From Eqs. (1) and (3), one can find that C_{conv} is independent of ζ, although each C_{ij} is dependent on ζ. Based on C_{conv}, Alice and Bob perform privacy amplification on the error-corrected sifted keys to obtain the final secret keys. Under ideal error correction and privacy amplification, the corresponding secret key rate R can be calculated as follows:

$$R = 1 - H(Q_{Y_AY_B}) - I_E(C_{\text{conv}}, Q_{Y_AY_B}), \tag{4}$$

where $H(\cdot)$ represents the binary entropy. I_E is the information leakage due to eavesdropping and is expressed as follows:

$$I_E(C_{\text{conv}}, Q_{Y_AY_B}) = (1 - Q_{Y_AY_B})H\left(\frac{1+u}{2}\right) + Q_{Y_AY_B}H\left(\frac{1+v}{2}\right), \tag{5}$$

where

$$u = \min\left[\frac{1}{1 - Q_{Y_AY_B}}\sqrt{\frac{C_{\text{conv}}}{2}}, 1\right], \tag{6}$$

$$v = \frac{1}{Q_{Y_AY_B}}\sqrt{\frac{C_{\text{conv}}}{2} - (1 - Q_{Y_AY_B})^2u^2}. \tag{7}$$

3. Fewer quantum state technique and effect of channel asymmetry

As a cost-effective solution of an RFI QKD system, several studies have considered fewer quantum state preparations [14,15,25–27]. In this section, we first discuss one of the studies that exploit the symmetry of the correlations C_{ij} in a practical situation, and then, we point out security loopholes caused by the asymmetry. Here, symmetry implies that knowing one correlation directly indicates knowing another correlation. For an ideal RFI QKD, as in [15], each term in C_{conv} has relationships such that

$$\begin{aligned} C_{Z_AZ_B(\zeta)} &= C_{X_AX_B(\zeta)}, \\ C_{Z_AX_B(\zeta)} &= -C_{X_AZ_B(\zeta)}. \end{aligned} \tag{8}$$

This implies that one of the measurement bases is not required to estimate C_{conv}, which reduces state preparation or state detection. In other words, RFI QKD can be implemented with a 4-state preparation in a transmitter or 4-state detection in a receiver, whereas the original RFI QKD requires 6-state preparation and detection. Equation (3) can be equivalently transformed to

$$C_{\text{conv}} = 2\left(C^2_{Z_AZ_B(\zeta)} + C^2_{Z_AX_B(\zeta)}\right) := C'_{\text{conv}}. \tag{9}$$

In [15], it is provided that RFI QKD can also be implemented with 3-state. However, in this paper, we focus on 4-state case only because 3-state case can be easily obtained based on the analysis of 4-state case.

Optics EXPRESS

In a practical situation, it is impossible to satisfy the symmetry in Eq. (8) owing to the limitations of a practical system where quantum states in a transmitter and receiver are not perfectly prepared and measured. Optical misalignment also breaks the symmetry. Therefore, we propose that the measurement bases of Alice and Bob should be generalized to reflect such practical issues. The generalization is based on the expression of an arbitrary axis with two angles on the Bloch sphere because each basis can be expressed as axis in the Bloch sphere, which changes Eq. (1) as follows:

$$\begin{aligned}
Z'_A &= [\sigma_Z \cos(2\theta_1) - \sigma_X \sin(2\theta_1)] \cos 2\phi_1 + \sigma_Y \sin(2\phi_1),\\
X'_A &= [\sigma_Z \sin(2\theta_2) + \sigma_X \cos(2\theta_2)] \cos 2\phi_2 + \sigma_Y \sin(2\phi_2),\\
Y'_A &= \sigma_Y,\\
Z'_B(\zeta) &= \{\sigma_Z \cos[2(\theta_3+\zeta)] - \sigma_X \sin[2(\theta_3+\zeta)]\} \cos 2\phi_3 + \sigma_Y \sin(2\phi_3),\\
X'_B(\zeta) &= \{\sigma_Z \sin[2(\theta_4+\zeta)] + \sigma_X \cos[2(\theta_4+\zeta)]\} \cos 2\phi_4 + \sigma_Y \sin(2\phi_4),\\
Y'_B(\zeta) &= \sigma_Y,
\end{aligned} \tag{10}$$

where θ_k and ϕ_k for $k = 1, 2, 3, 4$ represent degree of linear and circular polarizations, respectively, to express an arbitrary measurement basis deviating from the ideal measurement basis. Here, we assume that Y'_A and $Y'_B(\zeta)$ are still ideal for focusing on the effect of the asymmetry on the security parameter because they are not used to estimate it. Based on Eq. (10), C_{ij} is expressed as follows:

$$\begin{aligned}
C_{Z'_A Z'_B(\zeta)} &= \cos[2(\theta_1 - \theta_3 - \zeta)] \cos(2\phi_1) \cos(2\phi_3) + \sin(2\phi_1) \sin(2\phi_3),\\
C_{Z'_A X'_B(\zeta)} &= -\sin[2(\theta_1 - \theta_4 - \zeta)] \cos(2\phi_1) \cos(2\phi_4) + \sin(2\phi_1) \sin(2\phi_4),\\
C_{X'_A Z'_B(\zeta)} &= \sin[2(\theta_2 - \theta_3 - \zeta)] \cos(2\phi_2) \cos(2\phi_3) + \sin(2\phi_2) \sin(2\phi_3),\\
C_{X'_A X'_B(\zeta)} &= \cos[2(\theta_2 - \theta_4 - \zeta)] \cos(2\phi_2) \cos(2\phi_4) + \sin(2\phi_2) \sin(2\phi_4).
\end{aligned} \tag{11}$$

Then, the correlation relationships in Eq. (8) can be expressed as follows:

$$\begin{aligned}
C_{Z'_A Z'_B(\zeta)} &= C_{X'_A X'_B(\zeta)} + \epsilon_1(\zeta),\\
C_{Z'_A X'_B(\zeta)} &= -C_{X'_A Z'_B(\zeta)} + \epsilon_2(\zeta),
\end{aligned} \tag{12}$$

where $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$ indicate asymmetry of the correlations. They are defined as $C_{Z'_A Z'_B(\zeta)} - C_{X'_A X'_B(\zeta)}$ and $C_{Z'_A X'_B(\zeta)} + C_{X'_A Z'_B(\zeta)}$, respectively, and can be easily calculated from Eq. (11). Due to the asymmetry, knowing one correlation does not provide any information about another correlation. For example, knowing $C_{Z'_A Z'_B(\zeta)}$ does not imply knowing $C_{X'_A X'_B(\zeta)}$ owing to $\epsilon_1(\zeta)$. Equation (12) directly affects the security parameter, hence, C'_{conv} is transformed as follows:

$$\begin{aligned}
C'_{\text{prop}} &= 2\left(C^2_{Z'_A Z'_B(\zeta)} + C^2_{Z'_A X'_B(\zeta)}\right),\\
&= C^2_{Z'_A Z'_B(\zeta)} + C^2_{Z'_A X'_B(\zeta)} + \left[C_{X'_A X'_B(\zeta)} + \epsilon_1(\zeta)\right]^2 + \left[-C_{X'_A Z'_B(\zeta)} + \epsilon_2(\zeta)\right]^2,\\
&= C_{\text{prop}} + f[\epsilon_1(\zeta), \epsilon_2(\zeta)],
\end{aligned} \tag{13}$$

where $C_{\text{prop}} = C^2_{Z'_A Z'_B(\zeta)} + C^2_{Z'_A X'_B(\zeta)} + C^2_{X'_A Z'_B(\zeta)} + C^2_{X'_A X'_B(\zeta)}$, which indicates that the security parameter in RFI QKD without fewer quantum states becomes dependent on ζ in a practical scenario. Note that this has no impact on the security loophole. The security parameter without fewer quantum states does not demonstrate the security loophole because it considers all of the correlations in Eq. (11). On the other hand, the security loophole can happen in case of the security parameter with fewer quantum states because it does not consider all of the correlations in Eq. (11), so that there are cases where it can overestimate other correlations that are not

Optics EXPRESS

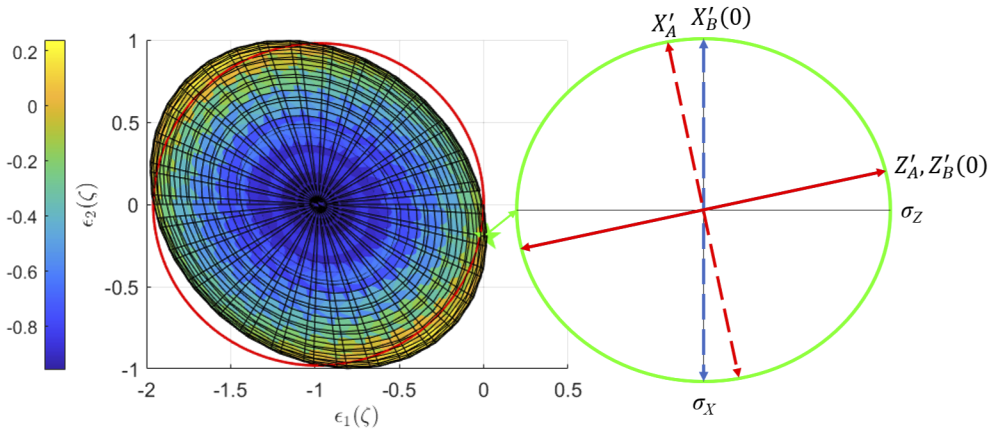


Fig. 1. Security parameter difference, $C'_{\text{prop}} - C_{\text{prop}}$, in terms of asymmetry of the correlations $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$. The right figure represents the bases of Alice and Bob on the Bloch sphere when $\epsilon_1(\zeta) = 0.02$ and $\epsilon_2(\zeta) = -0.1987$.

measured. Here, we can identify that C'_{prop} deviates from C_{prop} as $f[\epsilon_1(\zeta), \epsilon_2(\zeta)]$. Owing to the term $f[\epsilon_1(\zeta), \epsilon_2(\zeta)]$, the security parameter with fewer quantum states can cause a critical loophole in the security. For some ζ, where $C'_{\text{prop}} > C_{\text{prop}}$, the information leakage to Eve is underestimated. Extremely speaking, the estimation of information leakage with fewer quantum states can judge no eavesdropping in a quantum channel, although it actually takes place.

In order to analyze the effect of the difference in the security parameter owing to asymmetry with respect to $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$, we reconstruct $C'_{\text{prop}} - C_{\text{prop}}$.

$$C'_{\text{prop}} - C_{\text{prop}} = \left[\epsilon_1(\zeta) + C_{X'_A X'_B}(\zeta)\right]^2 + \left[\epsilon_2(\zeta) - C_{X'_A Z'_B}(\zeta)\right]^2 - C^2_{X'_A X'_B}(\zeta) - C^2_{X'_A Z'_B}(\zeta). \tag{14}$$

Considering that the security loophole from the underestimation of eavesdropping happens when $C'_{\text{prop}} > C_{\text{prop}}$,

$$\left[\epsilon_1(\zeta) + C_{X'_A X'_B}(\zeta)\right]^2 + \left[\epsilon_2(\zeta) - C_{X'_A Z'_B}(\zeta)\right]^2 > C^2_{X'_A X'_B}(\zeta) + C^2_{X'_A Z'_B}(\zeta). \tag{15}$$

This provides that the security loophole happens when $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$ are located outside of the circle centered at $(-C_{X'_A X'_B}(\zeta), C_{X'_A Z'_B}(\zeta))$ with radius $\sqrt{C^2_{X'_A X'_B}(\zeta) + C^2_{X'_A Z'_B}(\zeta)}$. Figure 1 shows the effect based on Eq. (15). Here, Fig. 1 can be obtained as follows. For each θ_k, ϕ_k, and ζ, we find $C_{X'_A X'_B}(\zeta)$, $C_{X'_A Z'_B}(\zeta)$, $\epsilon_1(\zeta)$, $\epsilon_2(\zeta)$, and $C'_{\text{prop}} - C_{\text{prop}}$ from Eqs. (11)–(13). Only for θ_k, ϕ_k, and ζ satisfying $C_{X'_A X'_B}(\zeta) = 0.98$ and $C_{X'_A Z'_B}(\zeta) = 0$, we collect the corresponding $\epsilon_1(\zeta)$, $\epsilon_2(\zeta)$, and $C'_{\text{prop}} - C_{\text{prop}}$, which are then reorganized to show the values of $C'_{\text{prop}} - C_{\text{prop}}$ with respect to $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$ as shown in Fig. 1. The axes of $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$ are carefully chosen such that $-1 \le C_{ij} \le 1$. One can find that there is physically feasible range of $\epsilon_1(\zeta)$ and $\epsilon_2(\zeta)$ from Fig. 1. The red circle in Fig. 1 indicates that $C'_{\text{prop}} = C_{\text{prop}}$. Therefore, outside of the red circle corresponds to security loophole. For example, the security loophole happens at $\epsilon_1(\zeta) = 0.02$ and $\epsilon_2(\zeta) = -0.1987$ expressed as the green star in Fig. 1, which corresponds to the case where $(\theta_1, \theta_2, \theta_3, \theta_4, \phi_1, \phi_2, \phi_3, \phi_4, \zeta) = (0.1, 0.1002, 0.1002, 0, 0, 0, 0, 0, 0)$. In this case, Z'_A, X'_A, Z'_B, and X'_B are deviated from ideal bases 5.7295°, 5.741°, 5.741°, and 0°, respectively, in terms of polarization angle. Note that, in such practical case, the security loophole can happen by a little deviation from the ideal case where $\epsilon_1(\zeta) = 0$ and $\epsilon_2(\zeta) = 0$. This infers that practical RFI QKD can be easily vulnerable to the security loophole, except for the ideal RFI QKD.

Optics EXPRESS

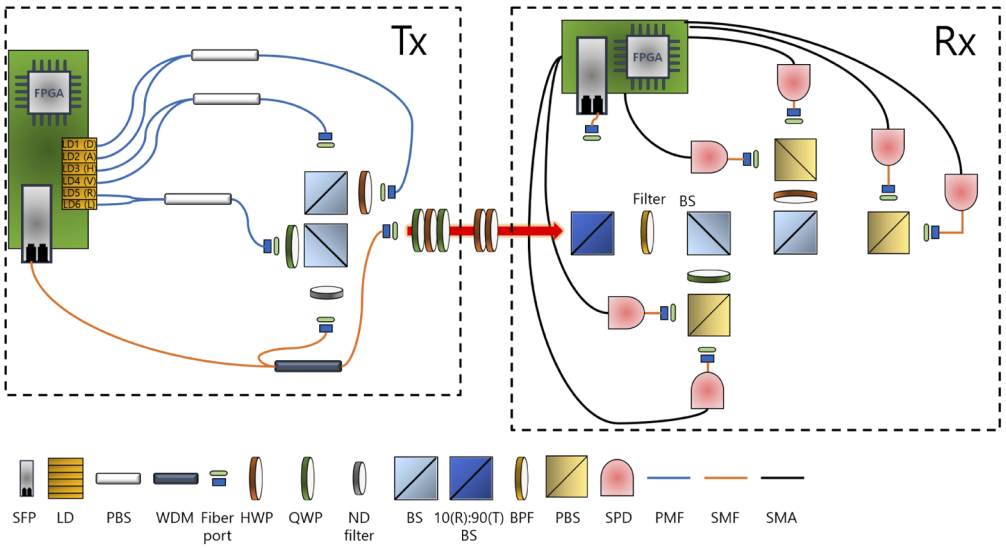


Fig. 2. Experimental setup of RFI QKD at 1550 nm. The transmitter has a 6-channel 1550 nm laser diode (LD) array chip. Both the transmitter and receiver are fully controlled by a field-programmable gate array (FPGA) board. SFP: Small form-factor pluggable transceiver, PBS: Polarization beamsplitter, WDM: Wavelength division multiplexer, HWP: Half-wave plate, QWP: Quarter-wave plate, ND filter: Neutral density filter, BS: Beamsplitter, BPF: Bandpass filter, SPD: Single-photon detector, PMF: Polarization maintaining fiber, SMF: Single-mode fiber, SMA: SubMiniature version A.

To solve the security loophole caused by the asymmetric correlations, we propose a conservative estimation method as a countermeasure by using the lower bound of C_{prop}, $\underline{C}'_{\text{prop}}$, based on Eq. (13).

$$\begin{aligned} C_{\text{prop}} &\geq C'_{\text{prop}} - f[\epsilon_1(\zeta^*), \epsilon_2(\zeta^*)], \\ &:= \underline{C}'_{\text{prop}}, \end{aligned} \tag{16}$$

where

$$\zeta^* = \underset{\zeta}{\text{argmax}} f\,[\epsilon_1(\zeta), \epsilon_2(\zeta)]. \tag{17}$$

To calculate Eq. (16), parameters representing the practical system in Eq. (11) are required, and they can be obtained from an experiment. For each correlation, we utilized the experimental results for $\zeta = 0$, $\pi/4$, and $\pi/2$. This process is required only once when a free-space RFI QKD system is initially implemented. Once the initial information is obtained, we can calculate Eq. (16). Because the security parameter with fewer quantum states based on Eq. (16) is always lower than or equal to the security parameter in the original RFI QKD, the aforementioned security loophole can be prevented. In other words, Eq. (16) provides a safe estimation of the security parameter even if we exploit fewer quantum states.

4. Experimental setup

In this section, we explain our experimental setup for free-space RFI QKD to identify the aforementioned security loophole caused by the asymmetric correlations and verify our proposed countermeasure.

We implemented a free-space RFI QKD system for the preparation and measurement scheme shown in Fig. 2. The transmitter consists of a 6-channel array laser diode (LD) chip, whose

Optics EXPRESS

center wavelength and full width half maximum (FWHM) are approximately 1550.4 and 0.4 nm, respectively. To generate a pulsed coherent state as a quantum signal from the LD chip, we exploit the gain switching method [28]. The field-programmable gate array (FPGA) board randomly injects an electrical pulse with 250 ps FWHM into each LD at a clock rate of 100 MHz. The quantum signal of each LD in the 6-channel array LD chip is encoded as horizontal (H), vertical (V), diagonal (D), anti-diagonal (A), right circular (R), and left circular (L) polarizations through the polarization encoding part consisting of the beamsplitter (BS), polarization beamsplitter (PBS), and wave plates. The encoded quantum signal is attenuated to a mean photon number per pulse of 0.1 and combined with a 1560 nm wavelength synchronization signal using the wavelength division multiplexer (WDM). Before leaving the transmitter, the combined signal passes through a polarization controller consisting of wave plates to compensate for the polarization rotation by the single-mode fiber (SMF). The output signal of the transmitter passes the free-space quantum channel. The quantum channel has two half-wave plates to implement reference frame rotation. A single half-wave plate can represent the reference frame rotation but causes a $\pi/2$ phase shift. Thus, one additional half-wave plate is used to compensate for the phase shift. This can be easily verified using the Jones matrices.

The signal received by the receiver first passes 10:90 BS to be divided into the quantum and synchronization signals. The reflected signal is used to synchronize the clock signal between the transmitter and receiver, while the transmitted signal passes the optical bandpass filter with an FWHM of 2 nm to remove the synchronization signal from the quantum signal. The filtered quantum signals are decoded by the decoding part consisting of BS, PBS, and wave plates. The decoded signal is injected into an InGaAs avalanche photodiode (APD)-based single-photon detectors (SPDs) through the SMF. Each SPD has a detection efficiency, dark count rate, and gate-width of approximately 10%, 110 counts per second, and 1 ns, respectively. The FPGA board injects a trigger signal generated using the received synchronization signal into each SPD to detect a quantum signal. Detection signals of SPDs are collected by the FPGA board to measure QBERs and key rates in real time.

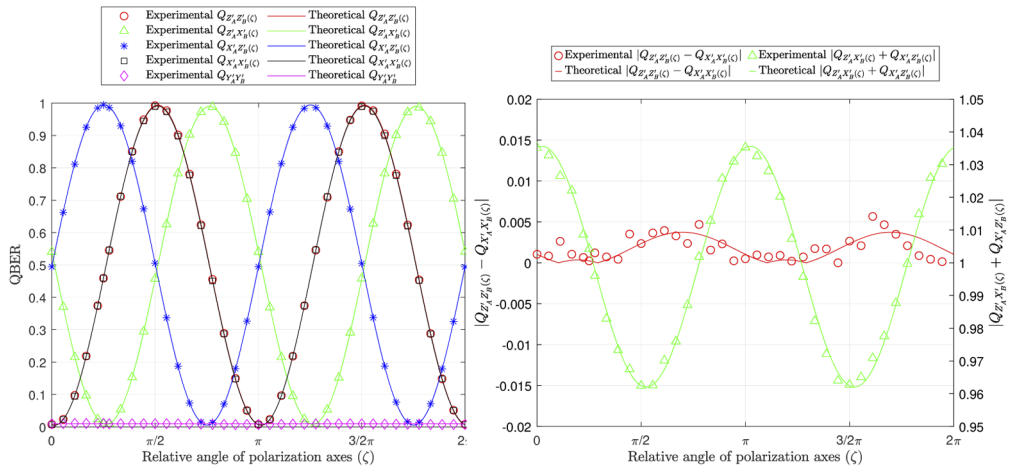
5. Results and discussion

In this section, we show the aforementioned effect of asymmetric correlations and the validity of our proposed method through experimental results.

First, we verified our experimental setup for free-space RFI QKD. Compared to previous studies on RFI QKD, our free-space RFI QKD system shows a similar aspect in terms of the QBER, as shown in Fig. 3(a). Here, $Q_{Y_AY_B}$ is approximately 0.87% and almost independent of the relative angle of the polarization axes ζ, while the QBERs of the other bases oscillate with respect to ζ. Here, in order to find the angles of our system, we utilize curve fitting method constructing a curve based on Eq. (11) that has the best fit to a series of our experimental data of the correlations, which estimates (θ_1, θ_2, θ_3, θ_4, ϕ_1, ϕ_2, ϕ_3, ϕ_4,) as (0.05, 0.04, 0.04, 1.57, 1.47, 1.47, 1.56, 0.027). Unlike previous results [15], we find that the relationships $C_{Z'_AZ'_B}(\zeta) = C_{X'_AX'_B}(\zeta)$ and $C_{X'_AZ'_B}(\zeta) = -C_{Z'_AX'_B}(\zeta)$, which correspond $Q_{Z'_AZ'_B}(\zeta) - Q_{X'_AX'_B}(\zeta) = 0$ and $Q_{X'_AZ'_B}(\zeta) + Q_{Z'_AX'_B}(\zeta) = 1$, do not hold at all, which is well shown in Fig. 3(b). This is unavoidable because implementing a real system is always accompanied by non-ideal components and misalignment of the optical path. Considering that $\zeta = 0$, the QBER differences $|Q_{Z'_AZ'_B}(0) - Q_{X'_AX'_B}(0)|$ and $|Q_{Z'_AX'_B}(0) - Q_{X'_AZ'_B}(0)|$ are 0.1% and 4.63%, respectively.

One can find that the differences can severely affect the security of a free-space RFI QKD system. Figure 4 shows the security parameters depending on the estimation method and shows how the differences can cause the security loophole. First, it is pointed out that the security parameter C_{prop} without fewer quantum states oscillates with respect to ζ owing to the asymmetric correlations. We also find a security loophole where $C'_{\text{prop}} > C_{\text{prop}}$. On the other hand, it is theoretically as well as experimentally proved that the proposed estimation method $\underline{C}'_{\text{prop}}$ never

Optics EXPRESS



(a) (b)

Fig. 3. (a) Experimental QBER performances of the free-space RFI QKD system with respect to the relative angle of polarization axes. Solid lines and symbols represent theoretical and experimental QBERs, depending on the bases of Alice and Bob. (b) The differences between QBERs.

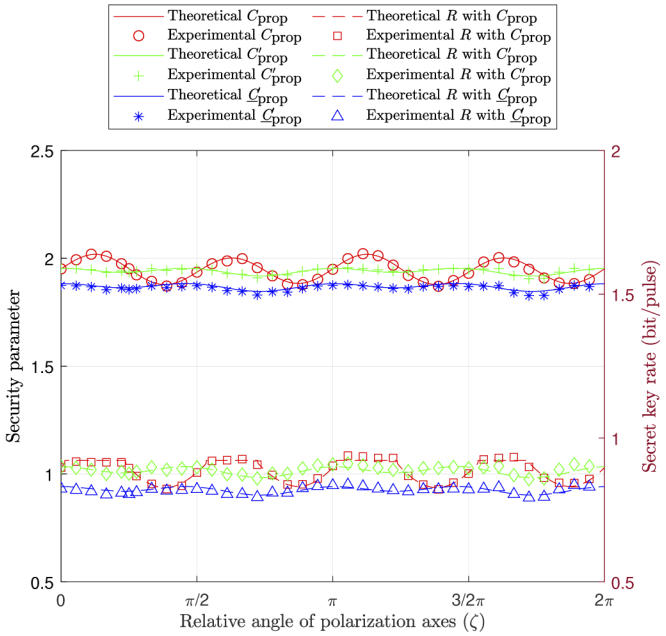


Fig. 4. Experimental security parameters and the corresponding secret key rates of the free-space RFI QKD system with respect to the relative angle of polarization axes. The left and right vertical axes indicate the security parameter and the corresponding secret key rate, respectively. Solid lines and circle, plus sign, asterisk represent theoretical and experimental security parameters, while dotted lines and square, diamond, triangle represent theoretical and experimental secret key rates, respectively.

underestimates information leakage because it conservatively estimates the information leakage,

Optics EXPRESS

i.e., $C_{\text{prop}} \geq \underline{C}'_{\text{prop}}$. In our experiment, the proportion of overestimation, i.e., $(C_{\text{prop}} - \underline{C}'_{\text{prop}})/C_{\text{prop}}$, is measured to be lower than 7.71%.

Since the security parameter is directly related to the secret key rate according to Eq. (4), the corresponding secret key rate also oscillates and decreases in the proposed method, as shown in Fig. 4. Note that the flatness with respect to some ζ in Fig. 4 is due to the limiting u in Eq. (6). Because C'_{prop} underestimates information leakage, its use can mislead to a higher secret key rate. On the other hand, our proposed countermeasure based on $\underline{C}'_{\text{prop}}$ prohibits such misunderstanding and guarantees the security of RFI QKD even if it decreases the secret key rate to at most 13% compared to the RFI QKD using six quantum states. We emphasize that, for some ζ, the proposed countermeasure can prevent the security loophole without a loss of the secret key rate and achieve more than 90% of the secret key rate of the original RFI QKD protocol for over half of entire range of the relative angle from 0 to 2π.

6. Conclusion

Reducing the required quantum states in a free-space RFI QKD system significantly simplifies the implementation of the system. To achieve this, exploiting the symmetry of the correlations was proposed. However, it is difficult to satisfy the symmetric correlations in practical RFI QKD systems because of non-ideal components and optical misalignment. We found that such asymmetry of the correlations causes security loopholes because it overestimates the security parameter for some relative angles of the reference frame. To prevent the security loopholes, we proposed a countermeasure for estimating the lower bound of the security parameter obtainable with RFI QKD with full states. The accompanied experimental results validate our proposed countermeasure under a free-space RFI QKD with fewer quantum states. Under long transmission distance and finite-key analysis, there is a result that secret key rate of RFI QKD can be compromised by the change of reference frame as in [26]. We expect that the proposed countermeasure is expected that it is more robust to the aspect because the proposed countermeasure is based on the worst-case in terms of reference frame. Therefore, we believe that this work provides feasibility of RFI QKD with fewer quantum states in a practical situation.

Funding. Institute for Information and Communications Technology Promotion (1711126425).

Acknowledgement. The authors would like to thank Dr. Haeyoung Rha for helping with real-time data processing with the FPGA system.

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-distance quantum key distribution secure against coherent attacks," Optica **4**(1), 163–167 (2017).
2. J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution over multicore fiber," Opt. Express **24**(8), 8081–8087 (2016).
3. Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," Opt. Express **26**(5), 6010–6020 (2018).
4. X.-B. An, H. Zhang, C.-M. Zhang, W. Chen, S. Wang, Z.-Q. Yin, Q. Wang, D.-Y. He, P.-L. Hao, S.-F. Liu, X.-Y. Zhou, G.-C. Guo, and Z.-F. Han, "Practical quantum digital signature with a gigahertz BB84 quantum key distribution system," Opt. Lett. **44**(1), 139–142 (2019).
5. J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver," Opt. Express **23**(26), 33437–33447 (2015).
6. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," Nat. Photonics **7**(5), 382–386 (2013).
7. C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, "Airborne demonstration of a quantum key distribution receiver payload," Quantum Sci. Technol. **2**(2), 024009 (2017).

Optics EXPRESS

8. A. D. Hill, J. Chapman, K. Herndon, C. Chopp, D. J. Gauthier, and P. Kwiat, "Drone-based quantum key distribution," in *7th International Conference on Quantum Cryptography (QCrypt)*, (2017).
9. H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Drone-based entanglement distribution towards mobile quantum networks," Natl. Sci. Rev. **7**(5), 921–928 (2020).
10. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**(7670), 43–47 (2017).
11. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the International Conference on Computers, Systems & Signal Processing*, (1984), pp. 175–179.
12. A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," Phys. Rev. A **82**(1), 012304 (2010).
13. K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," Phys. Rev. A **90**(5), 052314 (2014).
14. C. Wang, S.-H. Sun, X.-C. Ma, G.-Z. Tang, and L.-M. Liang, "Reference-frame-independent quantum key distribution with source flaws," Phys. Rev. A **92**(4), 042319 (2015).
15. D. Lee, S. Hong, Y.-W. Cho, H.-T. Lim, S.-W. Han, H. Jung, S. Moon, K. J. Lee, and Y.-S. Kim, "Reference-frame-independent, measurement-device-independent quantum key distribution using fewer quantum states," Opt. Lett. **45**(9), 2624–2627 (2020).
16. S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," Phys. Rev. A **91**(6), 062301 (2015).
17. H. Ko, B.-S. Choi, J.-S. Choe, K.-J. Kim, J.-H. Kim, and C. J. Youn, "Critical side channel effects in random bit generation with multiple semiconductor lasers in a polarization-based quantum key distribution system," Opt. Express **25**(17), 20045–20055 (2017).
18. H. Ko, B.-S. Choi, J.-S. Choe, K.-J. Kim, J.-H. Kim, and C. J. Youn, "High-speed and high-performance polarization-based quantum key distribution system without side channel effects caused by multiple lasers," Photonics Res. **6**(3), 214–219 (2018).
19. P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Eavesdropping and countermeasures for backflash side channel in quantum cryptography," Opt. Express **26**(16), 21020–21032 (2018).
20. Z. Wu, A. Huang, X. Qiang, J. Ding, P. Xu, X. Fu, and J. Wu, "Robust countermeasure against detector control attack in a practical quantum key distribution system: comment," Optica **7**(10), 1391–1393 (2020).
21. D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett. **81**(14), 3018–3021 (1998).
22. K. Park, S. Park, B. G. Choi, T. Kang, J. Kim, Y.-H. Kim, and H.-Z. Jin, "A lightweight true random number generator using beta radiation for IoT applications," ETRI J. **42**(6), 951–964 (2020).
23. Z. Zheng, Y. Zhang, M. Huang, Z. Chen, S. Yu, and H. Guo, "Bias-free source-independent quantum random number generator," Opt. Express **28**(15), 22388–22398 (2020).
24. Q. Luo, Z. Cheng, J. Fan, L. Tan, H. Song, G. Deng, Y. Wang, and Q. Zhou, "Quantum random number generator based on single-photon emitter in gallium nitride," Opt. Lett. **45**(15), 4224–4227 (2020).
25. J. Wang, H. Liu, H. Ma, and S. Sun, "Experimental study of four-state reference-frame-independent quantum key distribution with source flaws," Phys. Rev. A **99**(3), 032309 (2019).
26. H. Liu, J. Wang, H. Ma, and S. Sun, "Reference-frame-independent quantum key distribution using fewer states," Phys. Rev. Appl. **12**(3), 034039 (2019).
27. R. Tannous, Z. Ye, J. Jin, K. B. Kuntz, N. Lütkenhaus, and T. Jennewein, "Demonstration of a 6 state-4 state reference frame independent channel for quantum key distribution," Appl. Phys. Lett. **115**(21), 211103 (2019).
28. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104**(26), 261112 (2014).