Trustworthiness of measurement devices in round-robin differential-phase-shift quantum key distribution

Zhu Cao,[1] Zhen-Qiang Yin,[2,3,*] and Zheng-Fu Han[2,3]

[1]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*

[2]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

[3]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

(Received 1 October 2015; published 8 February 2016)

Round-robin differential-phase-shift quantum key distribution (RRDPS QKD) has been proposed to raise the noise tolerability of the channel. However, in practice, the measurement device in RRDPS QKD may be imperfect. Here, we show that, with these imperfections, the security of RRDPS may be damaged by proposing two attacks for RRDPS systems with uncharacterized measurement devices. One is valid even for a system with unit total efficiency, while the other is valid even when a single-photon state is sent. To prevent these attacks, either security arguments need to be fundamentally revised or further practical assumptions on the measurement device should be put.

DOI: 10.1103/PhysRevA.93.022310

I. INTRODUCTION

Quantum key distribution (QKD) enables an information-theoretic secure way of sharing a key between two distant parties, Alice and Bob [1,2]. In QKD, Alice sends quantum signals to Bob, who measures to obtain raw keys. Due to disturbance in the channel or eavesdropping, the raw keys might not be identical or secure. So Alice and Bob perform error correction and privacy amplification to recover secure identical keys. In traditional QKDs, both error correction and privacy amplification costs are estimated from the error rates in the channel, which leads to an upper bound on the allowable error rate. For example, the error rate threshold for the celebrated Bennett-Brassard 1984 (BB84) QKD protocol is 25% [1].

Recently, a QKD protocol, called round-robin differential-phase-shift (RRDPS) QKD [3], was proposed. This scheme and its passive equivalent scheme [4] were proven to be secure even under highly noisy channels, essentially removing the bound on the error rate. This desired property is achieved as they manage to directly compute the privacy amplification cost characterized by the phase error e_{ph} without estimating the disturbance in the channel.

However, practical implementations of the RRDPS schemes [4–7] may be imperfect. For example, in the security proof of the RRDPS schemes [3,4], Bob's measurement device is assumed to be a well-defined projective measurement acting on incoming single-photon states. However, this assumption may be spoiled in practice because current detectors can malfunction under bright pulse illumination [5]. As another example, the beam splitter in the measurement device is assumed to have a transmission-reflection ratio of one half. However, in practice the transmission-reflection ratio of the beam splitter varies with different wavelengths and can thus be manipulated by adjusting the wavelength [8].

In this work, we show that these imperfections in the measurement device may call the security of RRDPS into question. This is not obvious because the key security argument of RRDPS protocol is that Alice's key is completely determined by the density matrix of her prepared state and Bob's r is chosen by him instead of the measurement device. These are not changed when the measurement device is imperfect. To model the imperfections, we consider the worst-case scenario in which Bob's measurement device is untrusted and then propose two attacks to break the security. One must impose that Bob's untrusted measurement device cannot communicate the measured keys with the adversary Eve outside Bob's environment because otherwise no secure keys can be established. This can be done by, e.g., putting a shield around Bob's workstation.

In the following, we will first describe the untrusted measurement scenario in detail and then describe our two attacks. Finally, we conclude with a few interesting open questions.

II. UNTRUSTED MEASUREMENT RRDPS

In the original RRDPS protocol, as shown in Fig. 1(a), Alice's preparation of random bits sequence $s_1, \ldots, s_L$ and corresponding L-pulse state can be regarded as the following operations equivalently. Alice first prepares the quantum state

$$|\Psi\rangle_1 = \frac{1}{2^{L/2}} \prod_{k=1}^{L} [|0\rangle_k + (-1)^{\hat{n}_k} |1\rangle_k] |\Psi\rangle_B, \tag{1}$$

where $|\cdot\rangle_k$ represents Alice's ancillary qubits, $\hat{n}_k$ is the photon number operator acting on $|\Psi\rangle_B$, and $|\Psi\rangle_B$ is the encoding state which will be sent to Bob via a quantum channel. Alice's bit s_k can be viewed as the output of Z-basis measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ on ancilla $|k\rangle$. Next, Alice sends the quantum state to Bob. Bob splits the input to two paths, applies a random delay r to one of the paths, obtains $i, j = i + r, s_i \oplus s_j$ through the detectors' outcomes, and announces i and j to Alice. On receiving i and j, Alice performs a controlled-NOT gate to her ancilla $|\cdot\rangle_i$ and $|\cdot\rangle_j$, in which $|\cdot\rangle_i$ is the control qubit and $|\cdot\rangle_j$ is the target. Then Alice can measure $|\cdot\rangle_j$ with the Z basis to obtain her sifted key bit $s_i \oplus s_j$.

*yinzq@ustc.edu.cn

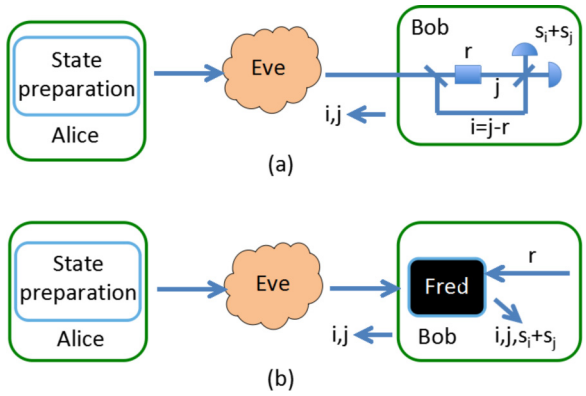

FIG. 1. (a) Original RRDPS [3]. Alice sends a pulse train to Bob, who splits the pulse train into two paths, adds a delay r to one of the paths, measures the interference to obtain $s_i \oplus s_j$, i, j, and publicly announces i, j. (b) Untrusted measurement variant. Instead of performing the operations himself, Bob gives an untrusted measurement device, Fred, the pulse train along with a random r, and Fred outputs $s_i \oplus s_j$, i, $j = i + r$. One possible implementation of Fred could be exactly the same as the corresponding part of the original RRDPS.

When the measurement is untrusted, as shown in Fig. 1(b), Alice prepares the same state and sends it to Bob. After receiving the incoming state, Bob inputs a random delay value r to his untrusted device and obtains i, j $(j - i = r)$ and an estimated value of $s_i \oplus s_j$. The remaining procedures are the same, in which Bob publicly announces i, j and Alice performs the controlled-NOT gate accordingly. Here untrusted means that Bob's device is an unknown quantum measurement device, called Fred, which could be manufactured by the adversary Eve. We assume here that Fred cannot actively disclose any information outside of Bob's environment bypassing Bob (e.g., by sending light signals). This assumption in particular eliminates the possibility of Fred telling Eve, who is outside, the measurement result $s_i \oplus s_j$ because Bob never announces it.

III. PROPOSED ATTACK 1

Before describing the first attack, we set down some useful notations. For a function $f(n)$, $\Theta(f(n))$ stands for a function $g(n)$ which satisfies $c_1 f(n) \leqslant g(n) \leqslant c_2 f(n)$ for some constants c_1, c_2 independent of n, while $\omega(f(n))$ stands for a function $g(n)$ which satisfies $g(n) > cf(n)$ for any constant c.

The key idea of the attack is that Eve and Fred can cooperate to announce the (i, j) pair. This is fundamentally different from the original RRDPS. To see the difference, examine the following example. Suppose the range of i, j is $\{1,2,3,4\}$. In the original RRDPS, Eve chooses i. Then Bob chooses a random $j \neq i$ and thus has three choices of j. However, when Bob's measurement device is held by another adversary Fred who cooperates with Eve, the adversaries could restrict the (i, j) pair output to $(1,2),(1,4),(2,4)$. For any i that can be announced, j has only two choices and thus is not uniformly random any longer.

The setting of the attack is as follows. The pulse train contains n pulses, and Alice sends a pulse train containing $(n-1)/2$ photons. Note that according to the state preparation of RRDPS, each photon is in the state

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{s_i} |i\rangle. \tag{2}$$

Eve first splits these $(n-1)/2$ photons and performs a passive interference with each photon. Then Eve obtains the relative phases of $(n-1)/2$ random pairs of (i, j), with details given in Appendix A.

A critical property of the relative phase is its transitivity. This can be easily shown as follows. If both $s_i \oplus s_j$ and $s_j \oplus s_k$ are known, then

$$s_i \oplus s_k = (s_i \oplus s_j) \oplus (s_j \oplus s_k) \tag{3}$$

is also known. For ease of presentation, we construct a graph with n nodes corresponding to the n pulses in the pulse train. If Eve detects the relative phase of (i, j), we add an edge between nodes i and j. Then by the aforementioned property, if node i and node k can be connected by a path of nodes, their relative phase is known. Furthermore, by a well-known random graph result [9] since each edge appears with probability

$$p = \frac{\frac{n-1}{2}}{\binom{n}{2}} = \frac{1}{n}, \tag{4}$$

there exists a connected component of size $\Theta(n^{2/3})$. Thus the relative phases between the $\Theta(n^{2/3})$ nodes in this connected component are all known by Eve. For a moderate size of $n = 1000$, simulations show that with $p = 1/40$ edge probability, there exists a connected component of size at least 200 at a 99% confidence level.

Eve proceeds to send the corresponding indices of these $m = \Theta(n^{2/3})$ nodes and their phases to Fred. Denote the indices as $a_1, \ldots, a_m$. By calculations of the probability in Appendix B, we show that with probability approaching 1, $\{|a_i - a_j|, 1 \leqslant i, j \leqslant n\}$ will contain almost all numbers in the set $\{1, \cdots, n-1\}$. For a moderate size $m = 200$ and $n = 1000$, simulations show that at a 99% confidence level, at least 95% of elements in $\{1, \cdots, n-1\}$ appear as differences of a_i. Thus when Bob inputs a delay r to Fred, he could announce a corresponding pair a_i, a_j such that

$$|a_i - a_j| = r \tag{5}$$

and also outputs $s_{a_i} \oplus s_{a_j}$ to Bob. However, since a_i, a_j are publicly announced, Eve, who is outside Bob's environment, can also recover $s_{a_i} \oplus s_{a_j}$ perfectly without causing any disturbance.

Finally, we note that, if some delay r is absent, Fred could announce loss when Bob inputs this r. So in the asymptotic limit, the existence of a majority of delays from $\{1, \ldots, n-1\}$ could already guarantee that Fred will output with almost unit probability.

Now we turn to the implications of this attack. Let us examine the phase-error formula for RRDPS protocol. In the original work [3], the phase-error formula is $e_{ph} = n_{ph}/(L-1)$, where L is the number of pulses in the pulse train and n_{ph} is the number of photons that Alice sends. We plug in $n_{ph} = (n-1)/2$ and $L = n$ and get $e_{ph} = 1/2$. This means that there are no secure keys, which does not contradict the fact that Eve has obtained all the information that Alice and Bob share.

However, the phase error in the original paper is not tight. Indeed, the phase error was later improved [4,10] and is given by $e_{ph} = [1-(1-2/L)^{n_{ph}}]/2$. The improvement relies on the fact that when Eve chooses i and Bob chooses a random $j \neq i$ for multiple photons, a phase error happens only with an odd number of photons. By plugging in $n_{ph} = (n-1)/2$ and $L = n$, we have $e_{ph} = (1-1/e)/2$ when n is large. This implies that secure keys can be generated and a contradiction occurs. This shows that in the untrusted measurement setting, with even unit efficiency, careful study of the phase error is needed since the model is no longer equivalent to the original RRDPS protocol. Through the proposed attack, Eve can learn key bits without introducing any additional error rates. In the following, we propose another attack, in which Eve can learn key bits with the help of additional error rates when total loss is larger than 3 dB.

IV. PROPOSED ATTACK 2

In the second attack, Eve and Fred will obtain Alice's key bit with certainty but introduce 50% bit error rate and 50% channel loss between Alice and Bob.

Consider that Alice prepares the following single-photon encoding state:

$$\begin{aligned}|\Psi\rangle_1 = \frac{1}{\sqrt{L}}(&e^{i\alpha_1}|1\rangle_1|0\rangle_2|0\rangle_3\cdots|0\rangle_L \\ &+ e^{i\alpha_2}|0\rangle_1|1\rangle_2|0\rangle_3\cdots|0\rangle_L \\ &+ e^{i\alpha_3}|0\rangle_1|0\rangle_2|1\rangle_3\cdots|0\rangle_L + \cdots \\ &+ e^{i\alpha_L}|0\rangle_1|0\rangle_2|0\rangle_3\cdots|1\rangle_L). \end{aligned} \tag{6}$$

Then Eve launches an attack in the following way:

$$\begin{aligned}|\Psi\rangle_2 = \frac{1}{\sqrt{L}}(&e^{i\alpha_1}|1\rangle_1|0\rangle_2|0\rangle_3\cdots|0\rangle_L|1\rangle_E \\ &+ e^{i\alpha_2}|0\rangle_1|1\rangle_2|0\rangle_3\cdots|0\rangle_L|2\rangle_E \\ &+ e^{i\alpha_3}|0\rangle_1|0\rangle_2|1\rangle_3\cdots|0\rangle_L|3\rangle_E + \cdots \\ &+ e^{i\alpha_L}|0\rangle_1|0\rangle_2|0\rangle_3\cdots|1\rangle_L|L\rangle_E), \end{aligned} \tag{7}$$

where $|n\rangle_E$ is the ancilla of Eve and ${}_E\langle n|m\rangle_E = \delta_{mn}$. Eve sends this ancilla E to Bob's device (Fred) and retains Alice's encoding state $|\rangle_1|\rangle_2\cdots|\rangle_L$ in her quantum memory. Fred simply measures E according to Bob's input r. For example, if $r = 1$, Fred measures E with the basis $(|1\rangle_E \pm |2\rangle_E, |2\rangle_E \pm |3\rangle_E, \cdots)$, which is the same as the r-delay interference and will output a pair of i and j definitely. If Fred obtains $|i\rangle_E + |j\rangle_E$, Fred will inform Bob of i, j, and a random key bit. If Fred obtains $|i\rangle_E - |j\rangle_E$, Fred will inform Bob that there is no click in this run. For instance, if Fred observes $(|1\rangle_E + |2\rangle_E)$ in this run, then Alice's encoding state becomes

$$\begin{aligned}|\Psi\rangle_3 = \frac{1}{\sqrt{2}}(&e^{i\alpha_1}|1\rangle_1|0\rangle_2|0\rangle_3|0\rangle_L \\ &+ e^{i\alpha_2}|0\rangle_1|1\rangle_2|0\rangle_3|0\rangle_L). \end{aligned} \tag{8}$$

Since this state is retained by Eve, she can learn Alice's sifted key bit $\alpha_1 \oplus \alpha_2$ easily. Although this attack introduces a high error rate, it implies that the security of RRDPS in the untrusted measurement scenario will depend on the error rate, which is completely different from the original RRDPS protocol. Hence one may conjecture that Eve's information on key bits depends on the error rate in the untrusted measurement setting, while the original RRDPS protocol states that monitoring signal disturbance is not necessary for placing a bound on Eve's information.

The error rate 50% can be reduced by mixing performing and not performing this attack together with a probability of 1/2 each. Then the error rate drops to 25%, while the same feature, channel-dependent phase error, still holds. Hence when Bob's device is untrusted, the RRDPS protocol is not secure, and monitoring signal disturbance would be necessary. This finding may shed light on the future security proof of RRDPS in the untrusted measurement scenario.

V. DISCUSSION

In summary, we have shown that the security of RRDPS protocol can be damaged when the measurement device is not perfect and consequently does not satisfy the assumptions of the protocol. We prove this by giving two concrete attacks for RRDPS with a completely untrusted measurement device. In addition to showing a warning sign for the trustworthiness of the measurement device, our work raises two interesting questions.

The first question is how to prove the security of RRDPS with untrusted measurement. Our result shows that in the untrusted measurement setting, the security analysis is significantly different from the original RRDPS and thus calls for more scrutiny in the analysis of the untrusted measurement setting. We show in Appendix C that it can be proven to be secure in the perfect case where there is no error and no loss. We therefore conjecture that it could also be made secure under a general lossy and erroneous channel when one correctly characterizes the information leakage. But the security proof may require transforming the experiment setup to a completely different intermediate model.

The second question is motivated by the fact that our untrusted measurement assumption may not be satisfied by a current-technology-hackable measurement device. Hence it would interesting to see how our attacks can be modified and implemented in a current experimental RRDPS setup.

Note added in proof. We notice that another attack to RRDPS has been proposed in Ref. [11].

ACKNOWLEDGMENTS

The authors would like to thank X. Ma for enlightening discussions. This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), the National Natural Science Foundation of China (Grant No. 61475148), and the 1000 Youth Fellowship program in China.

APPENDIX A: PASSIVE INTERFERENCE

In the passive interference, Eve prepares a superposed state with plain phases,

$$|\psi_0\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|i\rangle, \tag{A1}$$

and interferes with Alice's photon with a beam splitter which results in a mixture of the two click events [4],

$$[1+(-1)^{s_i+s_j}]c_i c_j, \quad [1-(-1)^{s_i+s_j}]c_i d_j, \tag{A2}$$

where c_i denotes the first detector clicks at the ith time and d_j denotes the second detector clicks at the jth time. Thus by examining whether the two clicks are from the same detector or from different detectors, Eve can determine the value of $s_i \oplus s_j$ for a random pair (i,j).

APPENDIX B: EQUIDISTRIBUTION OF DIFFERENCES

In this section, we will prove a technical result which is involved in the attack analysis, namely,

$$\lim_{n\to\infty} \mathbb{E}\left[\frac{\#\{|a_i-a_j|, 1\leqslant i,j\leqslant m\}}{n}\right] = 1, \tag{B1}$$

where $m=\Theta(n^{2/3})$ and $a_1,\ldots,a_m$ are chosen at random from $\{1,\ldots,n\}$. Actually, we will prove a stronger result which replaces $m=\Theta(n^{2/3})$ by $m=\omega(\sqrt{n})$. It is stronger because if the conclusion holds for a specific m, it naturally also holds for bigger m. The conclusion is intuitively true because $\omega(\sqrt{n})$ numbers have more than

$$\binom{2\sqrt{n}}{2} > n \tag{B2}$$

differences, and these differences have sufficient randomness in $\{0,\ldots,n-1\}$.

Now let us start the proof. First, fix a constant $\epsilon>0$. Let $A=\{a_i : i<m/2\}\cap\{1,\cdots,\epsilon n\}$. In mathematical expectation, A contains $\epsilon m/2=\omega(n)$ elements. By concentration, we have $|A|\geqslant\sqrt{n}$ with high probability.

Now suppose that $|A|\geqslant\sqrt{n}$ holds, i.e., there are $\sqrt{n}$ distinct values in $\{1,\ldots,\epsilon n\}$ for the first $m/2$ elements. Then for the last $m/2$ elements, they are independent, and each element has probability $\sqrt{n}/n$ to be distance d away from some element in A for any $d\in[1,n-\epsilon n]$. Thus the probability that none of the last $m/2$ elements are distance d from some element in A is $(1-1/\sqrt{n})^{m/2}$, which vanishes as n goes to infinity.

So, using linearity of expectation for all $d\in[1,n-\epsilon n]$, we have

$$\lim_{n\to\infty} \mathbb{E}\left[\frac{\#\{|a_i-a_j|, 1\leqslant i,j\leqslant m\}}{n}\right] \geqslant 1-\epsilon \tag{B3}$$

for any $\epsilon>0$. Since ϵ can be arbitrarily small, our result holds and the proof is complete.

Remark. Note that $m=\omega(\sqrt{n})$ is actually tight. One cannot hope to improve the bound to $m=\Omega(\sqrt{n})$. The reason is as follows. Suppose there is some constant c such that $m=c\sqrt{n}$; then in $[1,n/c^3]$ and $[n-n/c^3,n]$, about $2\sqrt{n}/c^2$ numbers are selected. Then differences in $[n-n/c^3,n]$ will appear for about n/c^4 times. Thus when $n\to\infty$, the upper bound on the expectation value of the number of differences dividing n is $1-1/c^3+1/c^4$, not 1.

APPENDIX C: SECURITY FOR THE PERFECT CASE

For simplicity, we consider the case that $L=3$ in this proof since this proof can cover higher-L cases easily. Only collective attack is considered here. Alice's encoding state can be written as $|\Psi\rangle=(-1)^{k_1}|1\rangle+(-1)^{k_2}|2\rangle+(-1)^{k_3}|3\rangle$. Besides no loss and error, we also assume that for the events for which Fred outputs i, j, Alice finds that $k_l(l\neq i,j)$ have equal zeros and ones conditioned on $(k_i,k_j)=(a,b)$ for all $a,b\in\{0,1\}$.

The general collective attack model is that Eve applies a unitary transformation U_E to the traveling photon and her ancilla $|E\rangle$. Note that after Eve's operation U_E, the incoming photon will be transformed to an unknown and arbitrary information carrier, labeled $|F\rangle$, sent to Fred. Then depending on Bob's input r, Fred uses unitary transformation $U_F^{(r)}$ acting on $|F\rangle$ to generate $|i\rangle+(-1)^{k_i\oplus k_i}|j\rangle$ to Bob. When Fred generates $|1\rangle\pm|2\rangle$, the density matrix of $|E\rangle$ is given by

$$\begin{aligned}\rho_E &= \sum_{k_3}\mathrm{tr}[(|1\rangle\langle 1|+|2\rangle\langle 2|)P\{U_E[(-1)^{k_1}|1\rangle \\ &\quad +(-1)^{k_2}|2\rangle+(-1)^{k_3}|3\rangle]|E\rangle|F\rangle\}] \\ &= \mathrm{tr}[(|1\rangle\langle 1|+|2\rangle\langle 2|)P\{U_E[(-1)^{k_1}|1\rangle \\ &\quad +(-1)^{k_2}|2\rangle]|E\rangle|F\rangle\}+P\{U_E|3\rangle|E\rangle|F\rangle\}],\end{aligned} \tag{C1}$$

where $P\{|x\rangle\}=|x\rangle\langle x|$. From (C1), to analyze Eve's ancilla $|E\rangle$, Alice's encoding state is equivalent to a mixture of components $P\{(-1)^{k_1}|1\rangle+(-1)^{k_2}|2\rangle\}$ and $P\{|3\rangle\}$. Evidently, in the perfect case, the events that Fred outputs 1 and 2 can correspond only to that Alice emits $(-1)^{k_1}|1\rangle+(-1)^{k_2}|2\rangle$. Furthermore, in the perfect case, Fred's operation $U_F^{(1)}$ generates $(-1)^{k_1}|1\rangle+(-1)^{k_2}|2\rangle$ without error, which means

$$\begin{aligned}U_E(|1\rangle+|2\rangle)|E\rangle &= |F_{12+}\rangle|E_{12+}\rangle, \\ U_E(|1\rangle-|2\rangle)|E\rangle &= |F_{12-}\rangle|E_{12-}\rangle,\end{aligned} \tag{C2}$$

and

$$\begin{aligned}U_F^{(1)}|F_{12+}\rangle &= |1\rangle+|2\rangle, \\ U_F^{(1)}|F_{12-}\rangle &= |1\rangle-|2\rangle.\end{aligned} \tag{C3}$$

On the other hand, when $r=2$, and Fred outputs 1 and 3, we have

$$\begin{aligned}U_E(|1\rangle+|3\rangle)|E\rangle &= |F_{13+}\rangle|E_{13+}\rangle, \\ U_E(|1\rangle-|3\rangle)|E\rangle &= |F_{13-}\rangle|E_{13-}\rangle,\end{aligned} \tag{C4}$$

and

$$\begin{aligned}U_F^{(2)}|F_{13+}\rangle &= |1\rangle+|3\rangle, \\ U_F^{(2)}|F_{13-}\rangle &= |1\rangle-|3\rangle.\end{aligned} \tag{C5}$$

Since unitary transformation U_E, $U_F^{(1)}$, and $U_F^{(2)}$ must preserve the inner product, it is easy to see that the module of the product of $|E_{13+}\rangle$ and $|E_{13-}\rangle$ must be 1, which implies that $|E_{13+}\rangle$ and $|E_{13-}\rangle$ can differ only by a phase. Hence Eve cannot obtain any information on $k_1\oplus k_3$ through her ancilla $|E\rangle$. Similarly, we can prove that Eve cannot learn $k_1\oplus k_2$ and $k_2\oplus k_3$.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) **509**, 475 (2014).
[4] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **114**, 180502 (2015).
[5] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photonics **9**, 827 (2015).
[6] S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, Nat. Photonics **9**, 832 (2015).
[7] Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, W. Chen, Y. Xu, J.-Y. Guan, S.-K. Liao, J. Yin, Q. Zhang, X. Ma, C.-Z. Peng, and J.-W. Pan, arXiv:1505.08142.
[8] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Phys. Rev. A **84**, 062308 (2011).
[9] P. Erdős and A. Rényi, Magy. Tud. Akad. Mat. Kut. Int. Kozl. **5**, 17 (1960).
[10] Z. Zhang, X. Yuan, Z. Cao, and X. Ma, arXiv:1505.02481.
[11] T. Iwakoshi, in *Proceedings of SPIE 9505 on Quantum Optics and Quantum Information Transfer and Processing 2015* (Prague, Czech Republic, 2015), p. 950504.