Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch

Kejin Wei,[1,2,3] Weijun Zhang,[4] Yan-Lin Tang,[5] Lixing You,[4] and Feihu Xu[1,2,*]

[1]*Shanghai Branch, Hefei National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Shanghai 201315, China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Guangxi Key Laboratory for Relativistic Astrophysics, School of Physics Science and Technology, Guangxi University, Nanning 530004, China*

[4]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

[5]*QuantumCTek Corporation Limited, Hefei, Anhui 230088, China*

(Received 20 December 2018; published 20 August 2019)

Superconducting nanowire single-photon detector (SNSPD) is a promising candidate for achieving high-rate quantum key distribution (QKD) over long distances, and it has been widely employed in recent QKD experiments. However, SNSPD is naturally polarization sensitive, which, if unchecked, could leave a back door for an eavesdropper to perform quantum hacking. Here, we experimentally study the polarization dependency on the detection efficiency of SNSPD and propose a quantum hacking attack to exploit this vulnerability. We experimentally characterize the polarization-dependent efficiencies of different SNSPDs and perform risk analysis on the security of a standard phase-encoding QKD implementation. Our experimental data and security analysis show that, if the effect of polarization-dependent efficiency is unnoticed, an eavesdropper can successfully hack the QKD implementation using the polarization-rotation attack. Countermeasures are also discussed. The result is important for the future design of secure implementations of QKD.

DOI: 10.1103/PhysRevA.100.022325

I. INTRODUCTION

Quantum key distribution (QKD) allows two separated parties (normally called Alice and Bob) to share a string of secure key bits in the presence of an eavesdropper [1,2]. Over the past two decades, much effort has been put toward building a high-performance and long-distance QKD system [3,4]. The security of QKD is guaranteed by the laws of quantum mechanics, provided that the properties and behaviors of the actual components conform to the device models in the security proof [5,6]. Unfortunately, practical implementations may have device imperfections, which leave exploitable security loopholes to eavesdropping Eve. Indeed, Eve has exploited such loopholes to perform several so-called quantum hacking attacks [7–16]. See Ref. [3] for a review on this topic.

In fiber-based QKD implementations, superconducting nanowire single-photon detector (SNSPD) has been widely adopted [17–24] because of its remarkable features of high detection efficiency and low dark count rate [25]. Recently, record-breaking distances of QKD experiments over 404 [22] and 421 km [24] have been reported. As a result, SNSPD is believed to be the key component for the widespread applications of QKD. It is thus highly important to investigate the implementation security of SNSPD in a practical QKD system. The blinding attacks against SNSPDs have been studied in Refs. [26,27].

Here, we consider the security aspects of practical QKD due to the polarization-dependent mismatch (PDM) of the detection efficiency of SNSPDs. Originating from the meander-type geometry in an SNSPD, its detection efficiency is naturally polarization sensitive; i.e., the detection efficiency varies with change of the polarization of the incident light. In practice, most QKD systems use two separate SNSPDs for the detection of different quantum states. The PDM of the detection efficiency of the two SNSPDs, arising from imperfections in fabrication or different optical structures of the design of SNSPDs, can introduce a security loophole [7]. We experimentally characterize the polarization-dependent efficiencies of different SNSPDs and confirm that the PDM indeed exists even for two SNSPDs which have the same design, including the width of nanowires, the thickness of the film, and so on. Exploiting such a loophole, we propose a simple attack for a standard phase-encoding QKD implementation [28] which adopts two separate SNSPDs for the detection, and we perform a security analysis about the amount of information that Eve can acquire. If Eve performs an intercept-resend operation [7], the PDM-dependent attack is also applicable to other time-bin phase-encoding systems [24,29].

We remark that high-quality SNSPDs are critical to achieving high-performance and long-distance QKD. Unfortunately, few previous demonstrations utilizing SNSPDs have focused

[*] feihuxu@ustc.edu.cn

on the effects of the PDM for the implementation security of QKD. In our work, we prove that the PDM indeed exists in a practical QKD system which consists of two SNSPDs. Hence, there is a need to show the QKD community that the PDM in SNSPDs should be taken care of. With our work, we wish to highlight this unnoticed imperfection and to guide future QKD implementations, using SNSPDs for detection, for a proper system design so as to avoid this security issue.

The organization of this paper is as follows. In Sec. II, we first explain the origin of polarization-dependent efficiency mismatch of SNSPDs in detail and then experimentally characterize the polarization-dependent efficiency of different types of SNSPDs. In Sec. III, we present an attack which allows Eve to acquire the secret key without introducing any quantum bit error rate. Finally, in Sec. IV, we discuss the countermeasures and providing some concluding remarks.

II. POLARIZATION-DEPENDENT EFFICIENCY MISMATCH OF SNSPDS

To achieve high-rate and long-distance performances, several existing QKD systems use SNSPDs to detect photons. Unlike traditional InGaAs avalanche photo diodes [30], the operating principle of SNSPDs is the creation and disappearance of a photon-induced resistive hotshot over the nanowire [25]. To enhance the coupling efficiency and absorption efficiency, the nanowire is arranged in a meander-type geometry (see Fig. 1) across the active area of the SNSPD. This geometry leads to a much higher absorbance of photons with parallel polarization to the nanowire ($A_{\parallel}$) than that of photons with perpendicular polarization to the nanowire ($A_{\perp}$). The values $A_{\parallel}$ and $A_{\perp}$ mainly depend on optical properties of fabricated structures of the SNSPD, such as the width of nanowires, the thickness of the film, and so forth [31,32]. Consequently, detection efficiency η of an SNSPD is naturally polarization dependent, and it can be described by $\eta = |A_{\parallel}E_{\parallel}|^2 + |A_{\perp}E_{\perp}|^2$, where $E_{\parallel}$ and $E_{\perp}$ denote the electric field component of input photon parallel and perpendicular to the nanowires, respectively.

In practical implementation of QKD, Bob usually uses two separate SNSPDs for the detection of random bit "0" and bit "1." In the calibration, Bob can use a polarization controller, placed before each of SNSPDs, to maximize and unify the detection efficiency of two SNSPDs. However, due to fabrication imperfections or different optical structures in the design of SNSPDs, the polarization-dependent efficiencies of the two SNSPDs are inevitably different. This effect is illustrated in Fig. 2. We show a standard time-bin phase-encoding BB84 QKD system [28], which is similar to the recent experiments in Refs. [18,24]. Alice encodes the secret bit by using an asymmetric Mach-Zehnder interferometer. In Bob's station, the secret bit information is decoded by an asymmetric Faraday-Michelson interferometer followed by two SNSPDs (labeled as D_0 for bit "0" and D_1 for bit "1"). The Farady-Michelson interferometer provides a polarization-insensitivity phase modulation [33]. As shown clearly in the right side of Fig. 2, at polarization angle p_0, the efficiency of SNSPD_0 $[\eta_0(p_0)]$ is much higher than that of SNSPD_1 $[\eta_1(p_0)]$, i.e., $\eta_0(p_0) > \eta_1(p_0)$; at polarization angle p_1 the situation is opposite, i.e., $\eta_0(p_1) < \eta_1(p_1)$.

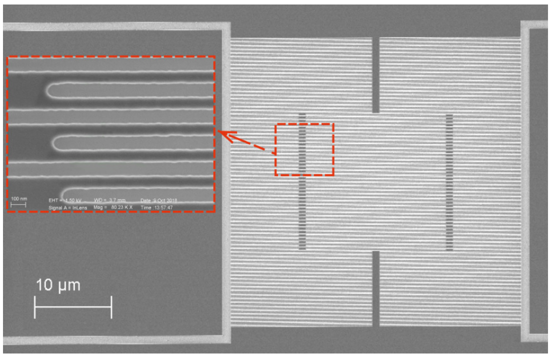


FIG. 1. Scanning electron micrograph of a meander-type SNSPD. A long narrow wire is arranged in a meander-type geometry across the active area of a detector. The red dashed inset shows a high-magnification image of the nanowires.

We experimentally characterize the polarization dependency curves of different SNSPDs. The detectors are measured at a 1550-nm wavelength. The light emits from a continuous-wave tunable laser source (Keysight, 81940A, polarization extinction ratio ≈16 dB) is attenuated to the single-photon level by serial tunable attenuators (Keysight, 81570A). The polarization of the light is controlled by a two-port polarization controller (Keysight N7786B) and is placed between the light source and the attenuators. The detectors used in the experiment are fabricated from NbN thin films. A distributed Bragg reflector (DBR) cavity structure is adopted to enhance the optical absorption of the nanowires. The detectors are front-side fiber coupling and the incident light transmitted from the fiber is vertically illuminated the nanowire via air. The detailed parameters of all measured detectors are listed in Table I.

Here, we consider two cases. In the first case, we choose two SNSPDs which have the same design and fabrication process, including the width of nanowires, the thickness of the film, etc. In theory, the shapes of polarization sensitivity curve should be highly identical. However, manufacturing a SNSPD requires many steps of complex processes involving several elaborate nanofabrications and optical alignment techniques [34], which inevitably introduce device imperfections. That is, it is rather challenging to fabricate two detectors which have identical polarization sensitivities. Hence, polarization-dependent efficiency mismatch unavoidably exists in two SNSPDs. In Fig. 3(a), we show the experimental results for two such SNSPDs. Similar to the calibration process in QKD, by setting the bias voltage and adjusting the polarization controller, we get an uniform efficiency $\eta = 75\%$ at the starting polarization angle $\theta = 0$. With varying θ, the curves show noticeable mismatch. In particular, the maximum mismatch occurs at $p_0 = 1.3$, where $\frac{\eta_0}{\eta_1} = 0.895$. At $\theta = 2.9$, the value $\frac{\eta_1}{\eta_0}$ reaches 0.982, which implies the maximum mismatch under the condition $\eta_1 > \eta_0$.

In the second case, we consider that two SNSPDs reach the same peak efficiency but have different optical designs, such as different geometry type or geometric dimensions of nanowires. Recently, SNSPD is experiencing a stage of rapid evolution. Several research groups around the world have improved the efficiency of SNSPD with a wide

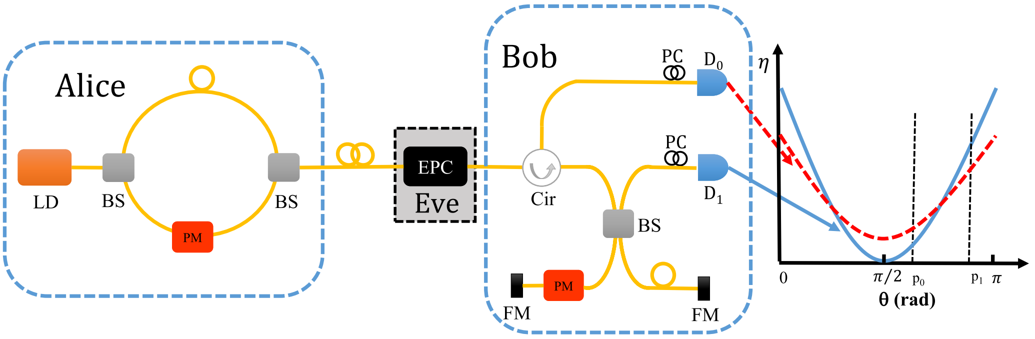


FIG. 2. The schematic of time-bin phase-encoding QKD implementation [28] and conceptually polarization-dependent efficiency mismatch of two SNSPDs. Alice encodes the secret bit by using an asymmetric Mach-Zehnder interferometer. Bob uses an Farady-Michelson interferometer to decode information. The basis is chosen by a phase modulator (PM), and detections are recorded by two SNSPDs. Before each detector, a polarization controller (PC) is used to maximize and unify the efficiency. The red (blue) curve corresponds to the efficiency of SNSPD. At polarization angle p_0, $\eta_0(p_0) \gg \eta_1(p_0)$, while at polarization angle p_1, $\eta_0(p_1) \ll \eta_1(p_1)$. To perform our attack, Eve employs an electrical polarization control (EPC) to randomly shift the polarization of each signal to either p_0 or p_1. Abbreviations of other components: LD, laser diode; BS, beam splitter; Cir, cirulator; FM, Faraday mirror; D$_0$ (D$_1$), SNSPD; η, detection efficiency; θ, polarization angle.

variety of strategies [35]. For example, by using different materials and optical structures, the reported efficiencies in both Refs. [36,37] are greater than 90%. It is likely that two SNSPDs with different geometric parameters of nanowires may be adopted in a QKD system. We perform a test of two such detectors. For the first detector, the width and thickness of nanowires are 50 and 6 nm respectively. For the second one, the width is 80 nm and the thickness is 7 nm. After careful adjustments, they have almost the same peak efficiency (≈29%) at the starting polarization angle [see Fig. 3(b)]. The polarization-dependent efficiency curves are significantly different and the maximum mismatch is up to 0.330 at $\theta = 1.7$.

III. EAVESDROPPING STRATEGIES EXPLOITING POLARIZATION-DEPENDENT EFFICIENCY MISMATCH

A. Attack

We propose a polarization-rotation attack exploiting PMD of SNSPDs. The hacking strategy is similar to the time-shift attack [8,9], which is the faked state attack [7]. Here, we focus on the efficiency mismatch in the polarization domain. In this attack, Eve could find two critical polarization angles fulfilling conditions that, at polarization angle p_0, the efficiency of D$_0$, $\eta_0(p_0)$, is much higher than that of D$_1$, $\eta_1(p_0)$, while at polarization angle p_1 the situation is opposite, where $\eta_0(p_1) \ll \eta_1(p_1)$. Here, we neglect the effect of polarization rotation by a Faraday mirror. Before our security analysis, to show the scale of efficiency mismatch between two SNSPDs, we define a mismatch ratio $\gamma = \max\{\frac{\eta_1(p_0)}{\eta_0(p_0)}, \frac{\eta_0(p_1)}{\eta_1(p_1)}\}$, $\gamma \in [0, 1]$. Here, to minimize Eve's knowledge about the final key, γ is defined as the maximum efficiency difference of the two polarization angles. As shown in Fig. 2, in our attack, Eve artfully inserts an electrical polarization control (EPC) in the quantum channel and randomly shifts the polarization of each signal to either p_0 or p_1. If Eve chooses polarization p_0 (p_1), whenever Bob broadcasts a successful detection event in the postprocessing process, with the probability of $1/(\gamma + 1)$, the bit value will be "0" ("1"). At last, Eve has a probability of $1/(\gamma + 1)$ to steal the sifted key, which is higher than randomly guessing. In the extreme case where $\gamma = 0$, the probability is equal to 1, so Eve can acquire full information on the sifted key. Note that our attack does not tamper the degrees of encoded freedom; therefore, Eve never introduces any additional errors.

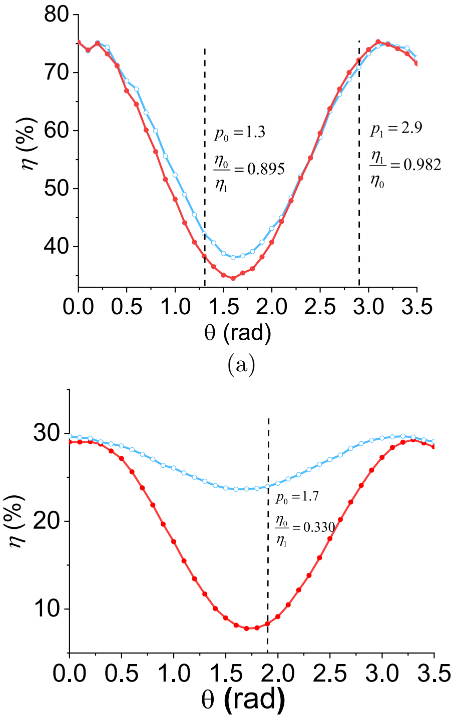
The above attack is difficult for the case of Fig. 3(b), due to lack of cross section between two efficiency curves. If Eve performs the attack, unbalanced clicks between two detectors are introduced, which is easily detected by Bob. Nonetheless, the shared key bits are frail. That is, Eve can shift each signal to p_0 and the bit value will be "0" with the probability of $1/(\gamma + 1)$. To reduce the unbalanced clicks, Eve mixes shifting and not shifting the polarization with a certain probability.

B. Security analysis

We will show that if Alice and Bob are not aware of the existence of the above polarization-rotation attack, the final shared key bits are overestimated and are not guaranteed to provide information-theoretic security. The following analysis

TABLE I. Comparisons of physical parameter of SNSPDs.

Detectors		Design width/pitch (nm)	Thickness (nm)	Cavity structures	Polarization extinction ratio
Case one	1st	80/160	7	Air/NbN/DBR	2.0
	2nd	80/160	7	Air/NbN/DBR	2.2
Case two	1st	50/100	6	Air/NbN/DBR	1.3
	2nd	80/160	7	Air/SiO/NbN/DBR	3.8



(a)

(b)

FIG. 3. Efficiencies of two detectors versus polarization angle. The red (blue) curve represents the measured efficiency of D_0 (D_1). (a) The first case: Both detectors have the same parameters (width: 80 nm, thickness: 7 nm). (b) The second case: Two detectors have different parameters (width: 50 nm vs 80 nm, thickness: 6 nm vs 7 nm).

is based on the security proofs by Maurer and Wolf [38], where the upper bound of the secret key between Alice and Bob in the presence of Eve, denoted by R, is given by

$$R \leqslant \min\{I(A;B), I(A;B|E)\}. \tag{1}$$

Here, A, B, and E denote the final key bits obtained by Alice, Bob, and Eve, respectively. $I(A;B)$ is mutual information between Alice's and Bob's key bits. $I(A;B|E)$ is the intrinsic conditional mutual information between A and B when given E, which is can be written as

$$I(A;B|E) = H(A|E) - H(A|BE), \tag{2}$$

where $H(A|E)$ and $H(A|BE)$ denote the Shannon entropy of A when given E and A when given B and E, respectively. In our work, since Alice and Bob have the same key bits, Eq. (2) can be expressed as

$$I(A;B|E) = 1 - I(B;E). \tag{3}$$

Here we assume equal probability for the final bit"0" and "1" obtained by Alice, and $I(B;E)$ denotes the mutual information between B and E. In principle, if Eve cannot steal any information about the key bits of Alice and Bob, after the postprocessing, the key rate is equal to 1. Whenever $I(B;E) > 0$, the final key between Alice and Bob is compromised if they are unaware of the presence of Eve.

Now, consider the case in our work, where the probability that Eve has a correct guess of Bob's bit is $1/(\gamma + 1)$, so Eve's knowledge about the final key is given by

$$I(B;E) = 1 - h[1/(\gamma + 1)], \tag{4}$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is binary Shannon entropy function. Combining Eqs. (4), (3), and (1), we have the upper bound of the secure key rate

$$R \leqslant h[1/(\gamma + 1)]. \tag{5}$$

Note that $h[1/(\gamma + 1)] < 1$ since γ ranges from 0 to 1 except for $\gamma = 1$. It means that Alice and Bob overestimate a key rate which is insecure. To quantify this upper bound, Fig. 4 shows a plot of the security key rate R as a function of the mismatch ratio γ. We also substitute in the experimental values $\gamma = 0.982$, 0.895, obtained from the first case. To quantify the leaked information in the second case, we assume that Bob is negligent to check the unbalance clicks. We get the upper bound of the second case by substituting the observed experimental value $\gamma = 0.330$, which is plotted as black dot in Fig. 4. Figure 4 illustrates that our attack indeed causes a moderate decrease in the secure key rate. For the worst case, Eve's information about the final key reaches 0.192.

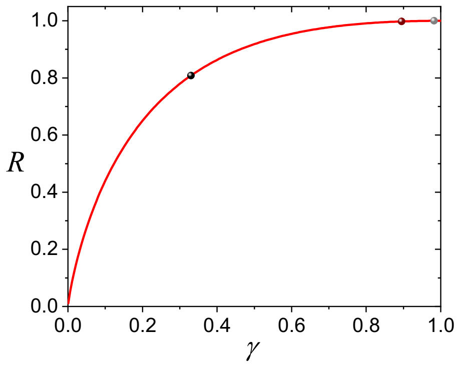


FIG. 4. Security rate as a function of the mismatch ratio γ. The black, wine, and gray dots denote the upper bounds calculated from the experimental data $\gamma = 0.330$, 0.895, 0.982.

IV. DISCUSSION

There are various countermeasures against our attack. First, Bob can utilize an additional device, such as a polarizer, in front of each SNSPD to filter out the unwanted polarization components or place an electrical polarization control, before each SNSPD, to randomly control the polarization of input light. We also note that a few reported phase-encoding systems have contained a linear polarizer [18], but most of systems did not contain it and hence are vulnerable to our attack [33,39]. Second, one can develop polarization-insensitive SNSPDs to avoid the polarization-dependent efficiency mismatch. Important progress has been made in this direction [40,41]. Third, we may develop refined security proofs by taking the effects of PDM into the security proofs [42,43]. Fourth, since Eve employs polarization as a control parameter to shift detector efficiencies, the proposed attack is not valid for polarization-encoding QKD systems [44]. Finally, the advanced QKD protocols, such as measurement-device-independent QKD [45] or twin-field QKD [46], are immune to our attack and all detector attacks.

Here, we have three additional remarks. First, some previous works [31,32] have shown that SNSPDs are naturally polarization sensitive. However, the PDM between two SNSPDs were not mentioned or characterized. In particular, it is unknown whether the PDM exists for two SNSPDs, even when they have the same design. In this work, we perform a careful characterization for different types of SNSPDs and conclude that the PDM indeed exists for SNSPDs in the two cases of both different designs and the same designs.

Second, it is known that the security of QKD is compromised with the existence of efficiency mismatch (EM) in the QKD community. Previous quantum hacking strategies, using different freedoms of pulses to make the EM, such as time freedom [7,8] and spatial freedom [47], have been reported. However, to our knowledge, none of previous quantum hacking strategies have used the polarization freedom to alter the detection efficiencies and then cause the PDM. More importantly, none of previous work reported the EM problem for SNSPDs. In our work, we prove that a practical QKD system utilizing SNSPDs exists PDM, which will introduce a security loophole.

Third, in our work, to simplify the analysis, we assume the phase modulator has a symmetric modulation ratio between TE mode and TM mode. This polarization-insensitive phase-modulation schemes is realized in many reported phase-encoding systems [28,48–50], and the polarization-insensitive phase modulator was well studied, which had many applications in the optoelectronics community [51]. We expect that polarization-insensitive phase modulators will be used in the future design of QKD implementations. Furthermore, the main conclusion of our work that the PDM would harm the security of a QKD system would not change in a QKD system with an standard phase modulator which has an asymmetric modulation ratio (about 1:3) [52]. Although the polarization of the output state is influenced by a standard polarization-sensitive phase modulator, the detection efficiency of each detector is still varying with polarization of input state. Hence, the PDM still exists between the two detectors.

In summary, we have shown that two practical SNSPDs indeed have an effect of polarization-dependent efficiency mismatch. Such an effect was ignored in previous QKD implementations. Eve can comprise the security of practical QKD systems by exploiting the polarization-dependent efficiency mismatch, by using, e.g., the polarization-rotation attack. If unnoticed, Alice and Bob generate an overestimated secure key rate, which compromises the information-theoretic security. Our work highlights the importance of good characterization of components in the QKD implementation. Recently, by using new technologies and devices, several advances have been achieved in the field of QKD, such as increasing the maximum distance [24] and silicon photonic chip-based QKD [53,54]. However, new components might impose new imperfections. It is very important to check whether these imperfections are harmless or dangerous.

ACKNOWLEDGMENTS

This work was supported by National Key R&D Program of China (Grant No. SQ2018YFB050101), the National Natural Science Foundation of China (Grants No. 61771443 and No. 61705048), Fundamental Research Funds for the Central Universities (Grant No. WK2340000083), the Guangxi Science Foundation (Grant No. 2017GXNSFBA198231), and the Thousand Young Talent Program of China, Shanghai Science and Technology Development Funds (Grant No. 18JC1414700).

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (IEEE, New York, 1984).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[4] F. Xu, X. M. Q. Zhang, H.-K. Lo, and J.-W. Pan, arXiv:1903.09051 (2019).

[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[7] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[8] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Info. Comput. **7**, 73 (2007).

[9] Y. Zhao, C.-H. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[10] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[12] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commnun. **2**, 349 (2011).

[13] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[14] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[15] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Phys. Rev. Lett. **112**, 070503 (2014).

[16] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Phys. Rev. A **92**, 022304 (2015).

[17] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photon. **1**, 343 (2007).

[18] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, New J. Phys. **11**, 045009 (2009).

[19] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[20] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).

[21] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).

[22] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).

[23] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li *et al.*, Phys. Rev. Lett. **122**, 160501 (2019).

[24] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussiéres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018).

[25] M. N. Chandra, G. T. Michael, and H. H. Robert, Supercond. Sci. Tech. **25**, 063001 (2012).

[26] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New. J. Phys. **13**, 113042 (2011).

[27] M. G. Tanner, V. Makarov, and R. H. Hadfield, Opt. Express **22**, 6734 (2014).

[28] R. H. Hadfield, J. L. Habif, J. Schlafer, R. E. Schwall, and S. W. Nam, Appl. Phys. Lett. **89**, 241129 (2006).

[29] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Appl. Phys. Lett. **112**, 171108 (2018).

[30] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, Light Sci. Appl. **4**, e286 (2015).

[31] V. Anant, A. J. Kerman, E. A. Dauler, J. K. W. Yang, K. M. Rosfjord, and K. K. Berggren, Opt. Express **16**, 10750 (2008).

[32] Q. Guo, H. Li, L. You, W. Zhang, L. Zhang, Z. Wang, X. Xie, and M. Qi, Sci. Rep. **5**, 9616 (2015).

[33] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Gun, Opt. Lett. **30**, 2632 (2005).

[34] E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita, Opt. Eng. **53**, 53 (2014).

[35] T. Yamashita, S. Miki, H. Terai, and Z. Wang, Opt. Express **21**, 27177 (2013).

[36] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photon. **7**, 210 (2013).

[37] W. Zhang, L. You, H. Li, J. Huang, C. Lv, L. Zhang, X. Liu, J. Wu, Z. Wang, and X. Xie, Sci. China-Phys. Mech. Astron. **60**, 120314 (2017).

[38] U. M. Maurer and S. Wolf, IEEE. T. Inform. Theory **45**, 499 (1999).

[39] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Optic. **47**, 533 (2000).

[40] V. B. Verma, F. Marsili, S. Harrington, A. E. Lita, R. P. Mirin, and S. W. Nam, Appl. Phys. Lett. **101**, 251114 (2012).

[41] L. Redaelli, V. Zwiller, E. Monroy, and J. M. Gérard, Supercond. Sci. Tech. **30**, 035005 (2017).

[42] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Info. Comput. **9**, 0131 (2009).

[43] O. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[44] 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 *et al.*, Nature (London) **549**, 43 (2017).

[45] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[46] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).

[47] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).

[48] B. Qi, L.-L. Huang, H.-K. Lo, and L. Qian, Opt. Express **14**, 4264 (2006).

[49] B. Qi, L. Huang, H. Lo, and L. Qian, *2006 IEEE International Symposium on Information Theory* (IEEE, New York, 2006), pp. 2090–2093.

[50] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang *et al.*, Opt. Express **22**, 21739 (2014).

[51] P. Tang, D. J. Towner, A. L. Meier, and B. W. Wessels, Appl. Phys. Lett. **85**, 4615 (2004).

[52] A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications* (Oxford University Press, Oxford, UK, 2007).

[53] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, Optica **3**, 1274 (2016).

[54] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, Optica **4**, 172 (2017).