Protecting Fiber-Optic Quantum Key Distribution Sources against Light-Injection Attacks

Anastasiya Ponosova,[1,2,*] Daria Ruzhitskaya,[1,2] Poompong Chaiwongkhot,[3,4,5,6]
Vladimir Egorov,[7,8] Vadim Makarov,[1,2,9] and Anqi Huang[10,†]

[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[3] *Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[4] *Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[5] *Department of Physics, Faculty of Science, Mahidol University, Bangkok 10400, Thailand*
[6] *Quantum technology foundation (Thailand), Bangkok 10110, Thailand*
[7] *Leading research center for Quantum internet, ITMO University, Birzhevaya line 14, St. Petersburg 199034, Russia*
[8] *SMARTS-Quanttelecom LLC, 6 liniya V.O. 59, St. Petersburg 199178, Russia*
[9] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China*
[10] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China*

(Received 3 February 2022; revised 9 July 2022; accepted 29 August 2022; published 14 October 2022)

A well-protected and characterized source in a quantum key distribution system is needed for its security. Unfortunately, the source is vulnerable to light-injection attacks, such as Trojan-horse, laser-seeding, and laser-damage attacks, in which an eavesdropper actively injects bright light to hack the source unit. The hacking laser could be a high-power one that can modify properties of components via the laser-damage attack and also further help the Trojan-horse and other light-injection attacks. Here we propose a countermeasure against the light-injection attacks, consisting of an additional sacrificial component placed at the exit of the source. This component should either withstand high-power incoming light while attenuating it to a safe level that cannot modify the rest of the source, or get destroyed into a permanent high-attenuation state that breaks up the line. We demonstrate experimentally that off-the-shelf fiber-optic isolators and circulators have these desired properties, at least under attack by a continuous-wave high-power laser.

DOI: 10.1103/PRXQuantum.3.040307

I. INTRODUCTION

Quantum key distribution (QKD) allows one to securely establish a secret key between two remote parties, usually called Alice and Bob [1,2]. Its informational-theoretical security is based on quantum physics, instead of any computational complexity [3–6]. This makes QKD, in principle, unhackable even by a superpowerful quantum computer. Thus, QKD is a promising candidate for quantum-safe cryptography in the era of quantum computing that is approaching with currently feasible quantum supremacy [7]. However, in practice, it is a long journey to achieve an unhackable QKD system due to imperfect devices in real life [8–32]. The imperfections in realistic QKD systems can be exploited by an adversary equipped with current technology to learn the secret information [11,18].

The quantum hacking discloses the practical security performance of QKD systems, which then stimulates the community to enhance the security hardness of QKD implementation. For example, a decade ago, various loopholes were discovered at the receiver side that works on

[*] nastya-aleksi@mail.ru
[†] angelhuang.hn@gmail.com

detecting quantum states received from a quantum channel [8,11,12,15,16]. To defeat the attacks on the quantum-state detection, measurement-device-independent QKD (MDI QKD) [33] and twin-field QKD (TF QKD) [34,35] were proposed, in which there were no security assumptions about the quantum-state measurement. Therefore, these protocols can defeat all attacks on a measurement unit. In addition, MDI-QKD and TF-QKD schemes with well-protected senders that prepare characterized quantum states are believed to be practically secure, eliminating the threat of quantum hacking [36]. Unfortunately, quantum hackers are ingenious—it has been shown that they can learn or even manipulate the characteristics of components in the source unit by light-injection attacks, like the Trojan-horse attack [37,38], laser-seeding attack [27,39,40], laser-damage attack [24,28], and power-meter attack [41]. Since the modified characteristics are often unpredictable, it is difficult to build a security model that counters these active attacks. Consequently, these attacks may be the effective tools in Eve's suitcase to crack the security of MDI-QKD and TF-QKD systems.

A fiber-optic isolator or circulator, which is often placed as the last component in the source unit [42–48], is believed to protect a fiber-based QKD system from the adversary's injecting light through a quantum channel. For example, Lucamarini *et al.* [49] thoroughly analysed the necessary amount of isolation as countermeasure against the Trojan-horse attack and upper bounded the remaining information leakage. Then the security can be restored by a privacy amplification. This countermeasure is also being standardized by the European Telecommunications Standards Institute (ETSI) [50]. From this point of view, protecting the source unit by isolation components seems to be a promising solution, achieving a practically secure source, especially for MDI QKD and TF QKD. Nevertheless, the actual amount of isolation may be affected by unknown attacks on the isolating component [28]. Guaranteeing the practical security of the QKD system under such a realistic situation is still challenging.

Here we show that an additional sacrificial isolation component placed at the exit of the source that is not accounted for in the security model can be an effective countermeasure against light-injection attacks. We experimentally demonstrate that, when the adversary illuminates isolators and circulators with a high-power continuous-wave (cw) laser, 6.4–42.4 dB residual isolation remains, although the high-power laser temporarily or permanently decreases their isolation values by 15.2–34.5 dB. Since the isolation components under the high-power attack are still able to provide a significant amount of isolation, they protect other optical components behind them in the QKD source unit from modification by the laser-damage attack. However, since this additional isolation component, the last in the QKD source, might be affected by the eavesdropper, it should not be counted in the effective isolation needed to prevent light-injection attacks. That is, the required isolation as countermeasure against light-injection attacks should be calculated starting from the component after our sacrificial isolation component.

The article is structured as follows. In Sec. II we describe the experimental setup and methodology to test the fiber-optic isolators and circulators. Measurement results are presented in Sec. III. We discuss the effects of this attack and application of this countermeasure in Sec. IV and conclude in Sec. V.

II. EXPERIMENTAL METHODOLOGY

A. Experimental setup for testing isolators

Our experimental setup simulates a hacking scenario in which Eve hacks the system from the quantum channel to the source unit. Figure 1 illustrates the measurement configuration used for testing fiber-optic isolators. The samples under test are illuminated by a high-power laser (HPL), consisting of a cw 1550 nm seed laser diode (QPhotonics QFBGLD-1550-100) followed by an erbium-ytterbium-doped fiber amplifier (QGLex custom-made unit) [28]. The laser is transmitted through a single-mode fiber to mimic the attack via the quantum channel. As we focus on the effect of optical power on the tested sample, the polarization of the laser is not characterized. Laser output power can be varied from 0.16 to 6.7 W at the isolator under test. During the experiment, the illumination power is set by the interface of a control software according to a calibration curve made before the experiment. Optical power meter 1 (OPM1; Grandway FHP2B04), connected through the 1% arm of a beam splitter (BS), monitors the power emitted by the high-power laser in real time. The laser light transmitted through the samples in the backward direction is continuously monitored by OPM2 (Thorlabs PM200 with S154C sensor). The isolation is determined by comparing the power measured by OPM2

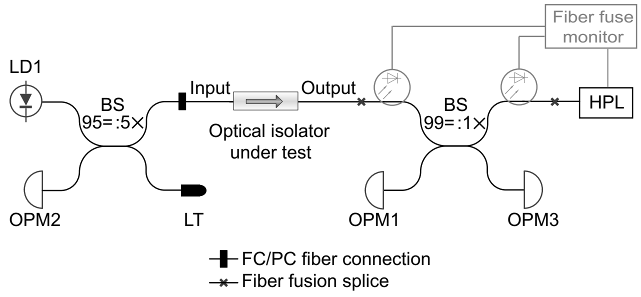

FIG. 1. Experimental setup for testing isolators. LD, laser diode; OPM, optical power meter; LT, light trap; HPL, high-power laser. The coupling ratio of the beam splitter (BS) denoted 95 =: 5× means that 95% of light passes to the port horizontally opposite in the graphical symbol of the BS, while 5% of light is coupled across to the other port.

with the laser power launched into the sample, taking into account the 95:5 coupling ratio of the BS.

A fiber-pigtailed 1550-nm laser diode (LD1, Gooch and Housego AA1406) with 10.5-mW optical power is used to measure the insertion loss of the isolator under test. The transmitted power is measured after 99:1 BS using OPM3 (Thorlabs PM200 with S155C sensor). The insertion loss is then determined by comparing the power measured by OPM3 with the input one, taking into account the additional 20-dB attenuation from the 99:1 BS. Our setup is equipped with a fiber fuse monitor, which shutdowns the high-power laser automatically in case the fiber fuse is detected, preventing any extensive damage to the equipment [28]. Fortunately, the fiber fuse has not occurred during the tests reported in this article. Moreover, a temperature map of the samples is measured by a thermal imaging camera (Fluke TiS45), which is placed over the samples and saves thermal images every 3 s during each experiment. It is notable that during the testing on ISO PM1 as an initial trial, there is no thermal images recording yet.

B. Experimental setup for testing circulators

To determine the testing setup for fiber-optic circulators, we first discuss two configurations that a three-port circulator can have in the QKD system. In the first scenario, the circulator is employed to direct Alice's optical pulses [44,46,48,51,52]. That is, the optical pulses first pass from port 1 to port 2. Then the pluses are reflected back to port 2 and transmitted to port 3 as the output of the QKD sender. Thus, the isolation values between each port pair matter to the security of the QKD system. In the second scenario, the circulator is used to monitor the injected light [42,53]. If the injected light is detected by a monitor connected at port 3, Alice and Bob may interrupt their QKD session without secret key leakage. However, it has been shown that the laser-damage attack might decrease the sensitivity of the monitor [24] and the high-speed optical pulses might bypass the alarming mechanism of the monitor [41]. In this case, the success of the light-injection attack will highly rely on the monitor's properties and signal processing, instead of the isolation provided by the circulator, which is out of the scope of the present study.

As discussed above, in this study we focus on testing the isolation characterization of a circulator configured in the first scenario, while testing the whole configuration in this scenario will be future work. The experimental setup of testing the circulator is shown in Fig. 2. The measurement settings at ports 1 and 3 are the same as described hereinabove for isolator testing in Sec. II A. In addition to that, a laser diode (LD2, Gooch and Housego AA1406) and an optical power meter (OPM4, Thorlabs PM200 with S154C sensor) are placed at port 2 via a 50:50 BS. LD1, LD2, and the HPL are used one at a time to prevent measurement errors caused by reflected light. Isolation and insertion loss are estimated for each pair of circulator's ports via a procedure similar to that described in Sec. II A.

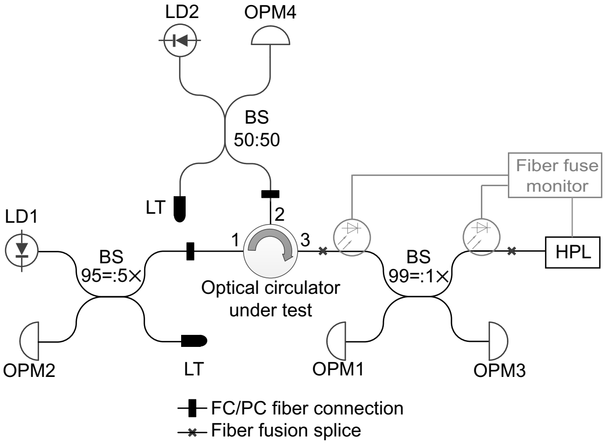

FIG. 2. Experimental setup for testing circulators.

C. Test procedure

Before starting the test on the optical isolators and circulators, we experimentally verify that up to 6.7 W none of the components in the setup, excluding the optical isolators and circulators, change their characteristics during the test. In particular, the splitting ratios of the BS are not seen to notably change. Thus, the only changes observed in the following test are in the isolators and circulators under test.

We define a successfully "hacked" isolation component as one having a temporal or permanent isolation decrease without losing light transmission capability in the forward direction, within our measurement accuracy of about 1 dB. We also note when the insertion loss increases permanently. Such an increase would lead (with a threshold that depends on the particular QKD system) to the secret key failing to be generated. This means that the eavesdropper would not be able to learn any secret information.

The test procedure is the following for each component under test. Firstly, the initial isolation and insertion loss are measured in the experimental setup before illumination by the HPL. Then each sample is exposed to a constant power level starting from 0.16 W for at least 60 s (except for the sample ISO PM 1, which is exposed for at least 10 s as the initial test). The exposure period may be increased up to 900 s during the testing if necessary. During the illumination, the isolation of the isolator under test is monitored. For circulators, the isolation values from port 3 to port 1 and from port 3 to port 2 are measured during the illumination. If isolation reduction is detected, the laser power is kept constant until the isolation value becomes stable. After each round of illumination, the HPL is turned off, and we measure the insertion loss of the sample under test again. For isolators, LD1 is turned on, and the insertion loss is measured by OPM3. For circulators, LD1 and LD2 are turned on alternately, and insertion losses from port 1 to port 2 and from port 2 to port 3 are measured by OPM4 and OPM3. In addition, LD2 is also used to measure the isolation from port 2 to port 1 with the assistance of OPM2. The temporary changes in isolation and insertion loss are recorded during the measurement.

We repeat the testing procedure above with the laser power of the HPL incremented by 100–500 mW. The testing stops if irreversible damage to the sample is incurred. For some samples, the testing stops before the sample is fully damaged. This is because we would like to measure the permanent decrease in isolation, while the sample is still operational.

III. RESULTS

A. Test results for fiber-optic isolators

We test four models of fiber-optic isolators used in real QKD systems: one sample of models 1, 2, and 4 (ISO PM 1, ISO PM 2, and ISO 4) and two samples of isolator model 3 (ISO 3-1 and ISO 3-2). All the isolators have a similar design and operation principle except that ISO PM 1 and ISO PM 2 are polarization dependent, while the other two models are polarization insensitive. According to their specifications, all the tested isolators should operate correctly at a maximum cw power of 500 mW, except for ISO PM 2, whose maximum operating power is 300 mW. The operating temperature range of all the samples is −5 °C to +70 °C. Owing to our confidentiality agreements with the QKD system manufacturers, we cannot publicly disclose the part numbers of the components tested in this study. They are ordinary commercial off-the-shelf products.

A summary of the laser-damage results is presented in Table I. The tested samples are vulnerable to the high-power injection laser, exhibiting the temporary reduction of isolation by 15.2–34.5 dB at a certain illumination power (see the "Maximum decrease of isolation" column in Table I). As a result, 17.2–42.4 dB isolation remains before samples become inoperable (see the "Minimum isolation" column), which is less than every sample's specified minimum isolation value. In addition, ISO PM 1 and ISO 3-2 are destroyed at 6.7 and 3.8 W injected laser power applied for 900 and 90 s, respectively. Detailed results of the testing are given in Fig. 3.

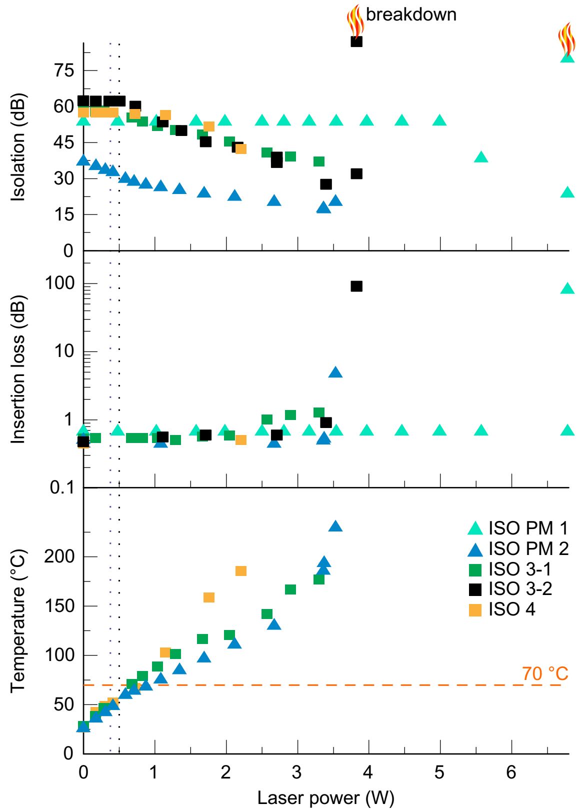

FIG. 3. Isolators' parameters under testing. The points represent the minimum isolation value, maximum insertion loss value, and highest surface temperature achieved at each applied power of the HPL. The temperature is only measured for three samples. The leftmost vertical dotted line is the maximum specified operating power of 300 mW for ISO PM 2. The rightmost vertical dotted line is the maximum specified operating power of 500 mW for the other samples.

The characteristics of ISO PM 1 differ significantly from the other samples because of the shorter laser exposure time at the beginning of its test, which is not enough to observe significant changes in isolation. However, when the exposure period is lasting longer with optical power higher than 5 W, the decrease in isolation is illustrated.

As can be seen from the topmost plot in Fig. 3, the isolation reduction under the high-power laser is observed for all samples. It does not happen until the applied laser

TABLE I. Testing results of isolators. All measurements are at 1550 nm.

	Specified	Initial			Maximum	
Sample	minimum isolation (dB)	Insertion loss (dB)	Isolation (dB)	Minimum isolation (dB)	decrease of isolation (dB)	Irreversible damage at
ISO PM 1	46	0.66	53.7	21.8 @ 6.7 W, 360 s	31.9	6.7 W, 900 s
ISO PM 2	28	0.50	37.0	17.2 @ 3.37 W, 820 s	19.8	Was not tested
ISO 3-1	46	0.45	58.1	37.1 @ 3.3 W, 260 s	21.0	Was not tested
ISO 3-2	46	0.55	62.1	27.6 @ 3.4 W, 800 s	34.5	3.8 W, 90 s
ISO 4	55	0.52	57.6	42.4 @ 2.2 W, 200 s	15.2	Was not tested

power exceeds the maximum operating power specified by the manufacturer, except for ISO PM 2, for which isolation reduction from its maximum value by 3.4 dB is observed in the operating power range. However, even for this sample, the measured isolation conforms to the specification when the illumination laser power is in the operating range (specified minimum isolation of ISO PM 2 is 28 dB; see Table I). The "breakdown" points in Fig. 3 indicate that ISO PM 1 and ISO 3-2 are fully damaged at laser powers of 6.7 and 3.8 W—they exhibit extremely large insertion loss and isolation. For the other samples, we stopped the laser exposure before completely destroying them, observing a permanent decrease in isolation by 3.9 dB for ISO PM 2 and a temporary decrease in isolation for ISO 3-1 and ISO 4.

Interestingly, before being destroyed, the isolators keep operating in the forward direction (see their insertion loss values in the middle plot in Fig. 3), while their isolation values are reduced. The insertion loss varies slightly by 0.5–1.1 dB, which leads to the loss of only 22% forward transmitted power at most. Once the irreversible damage happens for ISO PM 1 and ISO 3-2, their insertion loss is larger than 80 dB.

The sample's surface temperature (see the bottommost plot in Fig. 3) rises with the illumination power. It seems to be related to the isolation value. The isolation of polarization-insensitive samples ISO 3-1 and ISO 4 begins dropping when their measured temperature exceeds the maximum specified operating temperature of +70 °C.

In order to understand the mechanism of isolation decrease and isolators' damage, we analyze the thermal images and disassemble the tested samples as shown in Fig. 4. Figure 4(a) illustrates the surface temperature maps, the temperature curve, and the isolation curve of ISO PM 2 in one experiment. The thermal profile of the isolator under a high-power laser shows that the sample is heated inhomogeneously across its surface. Specifically, the tested sample is heated at the side opposite to the input port where the high-power laser is applied, which is also observed in all the other tested samples. This is because the injected high-power laser emission is rejected to be coupled from the isolator to the optical fiber [54], and next, the rejected light is absorbed inside the package to cause this local heating.

Moreover, after applying laser power higher than the sample's specified maximum operating value (300 mW), the amount of isolation drops rapidly with the power. After cooling, the isolation reverts close to the initial value. Figure 4(b) shows the external and internal designs of tested samples ISO 3-1 and ISO 3-2. After the disassembly of the sample, we found a destroyed blackened side of the optical assembly, which matches the point of the highest surface temperature marked in the thermal images. Thus, we infer that high temperature causes this destruction.

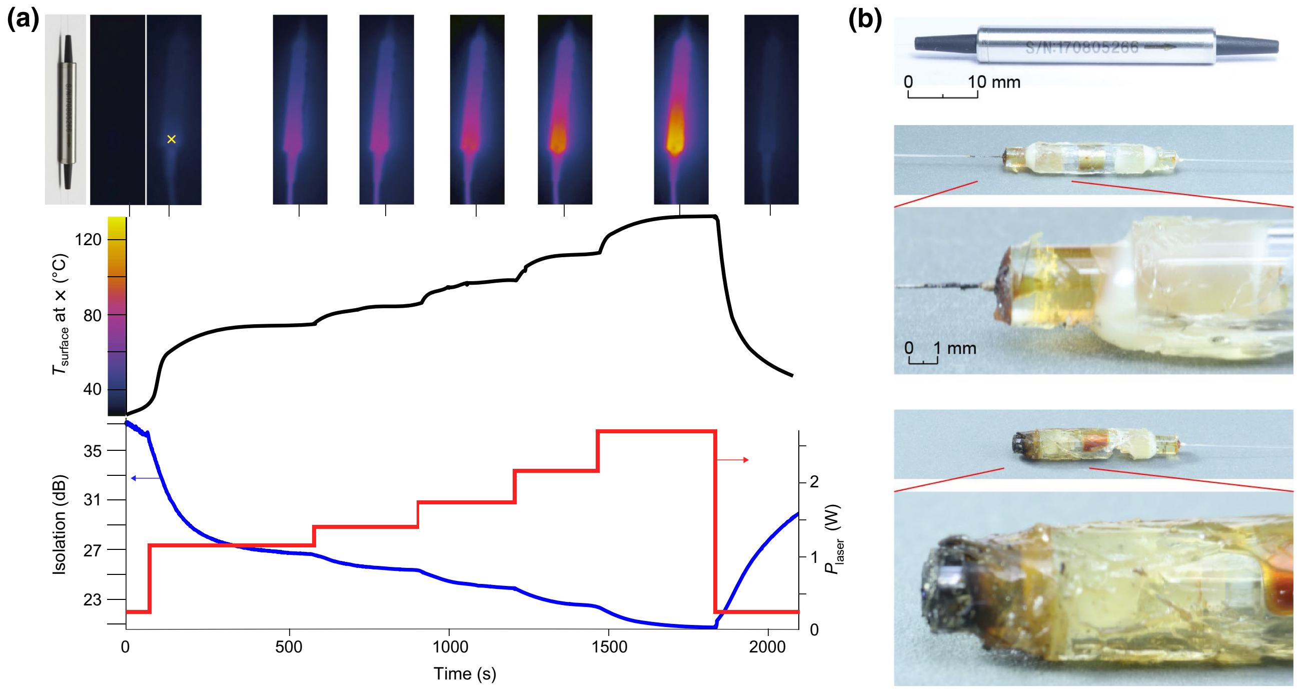

FIG. 4. Analysis of the isolator response to high-power laser exposure. (a) Isolation and temperature profile of ISO PM 2 under stepwise-increasing laser power. The temperature is measured at the hottest surface point, marked with a cross on the thermal camera images. (b) Photographs of (top to bottom) ISO 3-1 before testing, decapsulated ISO 3-1 showing its internal design (partial damage after illumination by 3.3 W is visible), and decapsulated ISO 3-2 showing damage after illumination by 3.8 W laser power.

To further verify the cause of isolation change, we theoretically simulate the working model of an isolator, with the details given in the Appendix. There, we calculate the temperature dependence of the Verdet constant and isolation changes for a single-stage polarization-dependent isolator. The analysis shows that the polarization rotation angle depends on temperature. As a result, when the temperature becomes high, the light injected in the backward direction is not fully reflected by the isolator's polarizer but is partially transmitted. Thus, the amount of isolation is reduced under high temperature. These modeling results correlate well with the experimental data of ISO PM 2, which may provide a reasonable explanation of the decrease in isolation observed in our experiment.

B. Test results for fiber-optic circulators

We test three fiber-optic circulators. Samples of CIR 1 and CIR 2 are polarization insensitive, while CIR PM 3 is polarization dependent. Similar to the isolators, the specified operating power is 500 mW for CIR 1 and CIR 2 (300 mW for CIR PM 3), and the operating temperature range is from 0 °C to +70 °C.

A summary of our testing results is given in Table II. The isolation is temporarily reduced not only between the ports illuminated by the laser (from port 3 to port 2) but also between the unilluminated ports (from port 2 to port 1). Specifically, the isolation from port 3 to port 2 (port 2 to port 1) decreases by 20.6–33.4 dB (26.7–28.7 dB) at maximum. The residual isolation is 6.4–32.3 dB from port 3 to port 2 and 34.7–38.3 dB from port 2 to port 1, which is lower than the minimum isolation specified by the component manufacturer for all the samples. Thus, the transmission paths from port 1 to port 2 and from port 2 to port 3 are vulnerable to Eve's high-power injection attack.

The detailed measurement data are presented in Fig. 5, showing isolation from port 3 to port 2, from port 3 to port 1, and from port 2 to port 1, as well as the maximum surface temperature under different illumination powers. The values of isolation from port 3 to port 2 and port 2 to port 1 are obviously decreased with increasing laser power, as the coupling ratio mainly depends on the polarization rotation provided by a Faraday mirror inside the circulator. However, the isolation from port 3 to port 1 remains essentially unchanged under all experimental conditions for all the tested samples, which is due to no coupling between these two ports according to the internal scheme. Similar to the isolators under test, the temperature of the sample's surface also rises with the laser power.

For both polarization-insensitive samples, the minimum remaining isolations from port 3 to port 2 are 32.2 dB (CIR 1) and 32.3 dB (CIR 2) at laser powers of 3.6 and 4.6 W, respectively. After that, the isolation value rises for CIR 1, and we thus stop our testing of it at a laser power of 4.8 W without observing any irreversible damage. Meanwhile,

TABLE II. Testing results of circulators. All measurements are at 1550 nm.

Sample	Specified minimum isolation for all ports (dB)	Initial				Minimum isolation (dB)		Maximum decrease of isolation (dB)		Irreversible damage at
		Insertion loss (dB)		Isolation (dB)						
		1 to 2	2 to 3	2 to 1	3 to 2	2 to 1	3 to 2	2 to 1	3 to 2	
CIR 1	45	1.03	1.07	61.4	60.6	34.7 @ 3.6 W	32.2 @ 3.6 W	26.7	28.4	Was not tested
CIR 2	40	0.72	0.83	67.0	65.7	38.3 @ 4.6 W	32.3 @ 4.6 W	28.7	33.4	4.6 W, 910 s
CIR PM 3	25	1.00	0.80	37.0	27.0	Was not tested	6.4 @ 0.7 W	Was not tested	20.6	0.9 W, 90 s

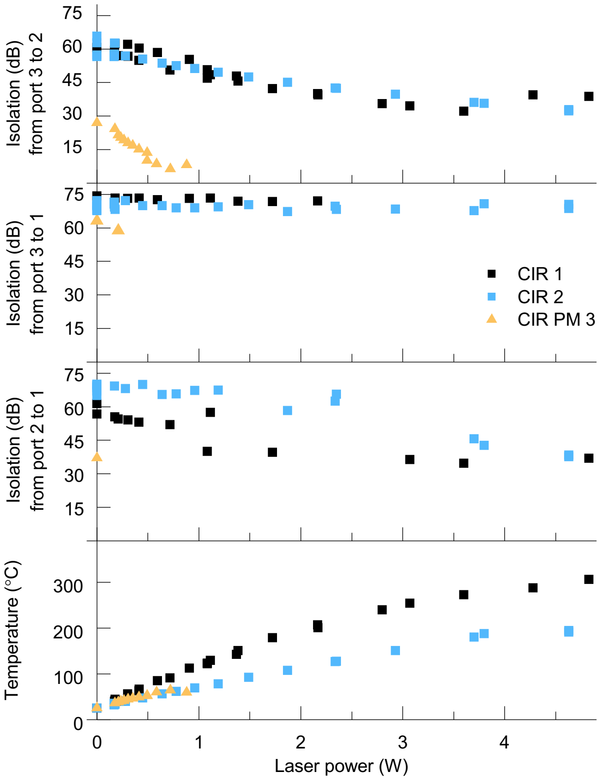

FIG. 5. Circulators' values of isolation and the maximum surface temperature under testing. Each point represents the minimum isolation achieved under each applied power.

irreversible damage happens for CIR 2 when its insertion loss increases to 2.5 dB from port 2 to port 3 at 4.6 W.

Moreover, for each of these two samples, we measure the isolation from port 2 to port 1 immediately after the laser exposure and find that the sample's heating also temporarily reduces it. Take CIR 1 as an example. Figure 6 illustrates its recovery after the laser exposure, in which the value of isolation reduces to about 35 dB once after being illuminated by the HPL. After the HPL is switched off, the isolation then recovers to 55 dB in 400 s, during which the sample's surface temperature decreases from 272 °C to 44 °C.

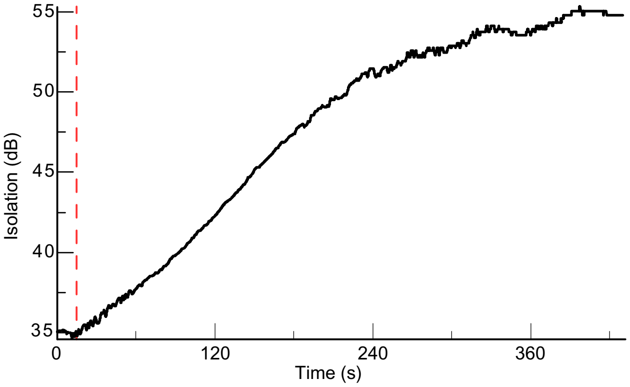

FIG. 6. Isolation of CIR 1 from port 2 to port 1 recovers gradually after illumination by 3.6 W laser power. The vertical dashed line is the HPL's switch-off time.

Surprisingly, for the polarization-sensitive sample, CIR PM 3, the isolation from port 3 to port 2 falls rapidly with increasing laser power, dropping to only 6.4 dB at the input laser power of 700 mW. At 900 mW, the insertion loss from port 2 to port 3 increases irreversibly to 15.5 dB. Since port 2 and port 3 of this sample are supposed to be used in the QKD system purely as an isolator, we do not measure the change in insertion loss from port 1 to port 2, isolation from port 2 to port 1, and isolation from port 3 to port 1.

IV. DISCUSSION AND COUNTERMEASURES

The experimental results shown above provide two opposite insights into the security of a QKD system. We first discuss the hacking aspect of the vulnerabilities in a QKD system caused by the isolation reduction of the tested isolators and circulators. Then, from the defence point of view, we propose a possible countermeasure to protect the QKD source from these vulnerabilities.

The isolation reduction introduced by high-power laser opens loopholes for at least two possible attacks on QKD, the Trojan-horse attack [37,38] and the laser-seeding attack [27,39,40]. Regarding the Trojan-horse attack, the isolation of the source strongly impacts the secure key rate and transmission distance. The reduced isolation of the source allows Eve to inject more Trojan-horse light into Alice, which is assumed to linearly increases the reflection light. Given a 15.2–34.5 dB decrease in isolation obtained from our testing results, the photon number of the reflection pulse increases by about 2–3 orders from the safe value. These amounts of increase in leaked photon number result in the maximum transmission distance shortening by 20–100 km according to the various theoretical security analyses [49,55–57].

Regarding the laser-seeding attack, an injection power of the order of 100 nW after passing the built-in isolator of Alice's laser to reach the laser cavity is sufficient for achieving a successful attack [27]. According to our experimental result, the maximum power transmitted through the isolation component is 190 mW, assuming that the injected power is 10 W [28] and the isolation is reduced to 17.2 dB as in ISO PM 2. (Although the minimum value of isolation obtained in our experiment is 6.4 dB for CIR PM 2, we exclude this type of circulator from the analysis owing to its poor performance and we do not recommend it for use in QKD systems.) To prevent the laser-seeding attack, other components in the QKD source should provide about 62.7 dB of isolation. Assuming that the built-in isolation of the laser is typically 30 dB, the success of the laser-seeding attack relies on the attenuation value of an optical attenuator on Alice's side. If the attenuation value is less than 32.7 dB, the security of the QKD system might be compromised under a laser-seeding attack. It is notable that in the above analysis, we assume that an attenuator on Alice's side works as designed, which does not affect the effectiveness of abovementioned attacks. Regarding the possible vulnerabilities of attenuators, the decreased attenuation under a laser-damage attack has been investigated in Ref. [28].

Most importantly, our study also provides a possible countermeasure against the light-injection attacks—adding an extra isolation component to the source unit to be the first one illuminated by the injected light. Its minimum residual isolation upper bounds the maximum power that can transmit through to reach other optical components. Specifically, the minimum observed isolations are 6.4 and 17.2 dB for polarization-dependent circulator CIR PM 3 and isolator ISO PM 2, respectively. Typical minimum residual isolation is more than 20 dB for all the polarization-insensitive components. Therefore, the injected power is limited to less than 190 mW, which cannot successfully conduct the laser-damage attack on any optical components according to the previous testing [21,24,28]. If the attacker attempts to further increase the illumination power, the first component fails permanently with a very high insertion loss, which results in a denial of service and thus protects the QKD system from leakage of secret information [24]. Moreover, the isolation required for protection against the Trojan-horse attack and the laser-seeding attack should be calculated starting from the component behind this sacrificial isolator or circulator. Therefore, the extra isolator or circulator placed at Alice's output would protect the rest of the QKD source against light-injection attacks.

V. CONCLUSION

In this paper, we study the effect of a high-power laser on fiber-optic isolators and circulators and propose an effective countermeasure against light-injection attacks on a QKD system. This study first raises awareness of insecure isolation components—isolators and circulators—in QKD systems. Specifically, the testing shows that the values of isolation provided by the optical isolators and circulators under test are reduced to 17.2 and 6.4 dB at minimum when high-power laser light is injected into them in the reverse direction. This decrease in isolation opens loopholes, which may allow Eve to conduct the Trojan-horse attack, the laser-seeding attack, and possibly other attacks that inject light into the source. The testing methodology proposed in this study is general and applicable to other commercial fiber-optic isolators and circulators. To enhance the protection of the QKD source unit, an extra isolation component, an optical isolator or circulator, is needed to defeat the light-injection attacks. The residual isolation of this extra component is sufficient to protect the other components behind it. Any isolation calculated for countermeasure against the Trojan-horse attack and the laser-seeding attack shall be started from the components behind this sacrificial isolation component. Our study shows that the source unit in the QKD system needs this additional layer of protection to be secure.

ACKNOWLEDGMENTS

We thank K. Wei, F. Xu, and our industry partners for providing us with device samples. This work is funded by the Ministry of Science and Education of Russia (programs 5-in-100, NTI center for quantum communications, and Grant No. 075-11-2021-078), the Russian Science Foundation (Grant No. 21-42-00040), the Canada Foundation for Innovation, MRIS of Ontario, the National Natural Science Foundation of China (Grants No. 61901483 and No. 62061136011), the National Key Research and Development Program of China (Grant No. 2019QY0702), and the Research Fund Program of State Key Laboratory of High Performance Computing (Grant No. 202001-02). P.C. acknowledges support from a DPST scholarship and the NSRF via the Program Management Unit for Human Resources & Institutional Development, Research and Innovation (Grant No. B05F640051).

A.P., D.R., V.E., A.H., and P.C. conducted the experiment. A.P., D.R., V.E., A.H., and V.M. analyzed the data. A.P., D.R., and A.H. wrote the article with help from all authors. A.H. and V.M. supervised the project.

APPENDIX: THEORETICAL TEMPERATURE DEPENDENCE OF THE VERDET CONSTANT AND ISOLATION IN FIBER-OPTIC ISOLATORS

1. Faraday effect in a polarization-dependent isolator

An optical isolator is a component that only allows unidirectional transmission of the optical signal. The principal scheme of a polarization-dependent isolator is shown in Fig. 7. It consists of an input polarizer, a Faraday rotator, and an output polarizer called an analyzer. The optical axis of the second polarizer is oriented at an angle $\beta = 45^\circ$ with respect to the first polarizer. In this configuration, the optical signal coming from the left-hand side passes through the first polarizer whose optical axis is in the vertical direction, which matches the polarization of the input optical signal. Then a Faraday rotator rotates the polarization of the optical signal by 45° in a clockwise direction. If there is an introduced laser beam from the optical circuit on the right-hand side, this optical signal has to pass through the Faraday rotator from right to left. Since the Faraday rotator is a nonreciprocal device, the polarization state of the reflected optical signal will rotate for an additional 45° in the same direction as the input signal, thus becoming perpendicular to the optical axis of the first polarizer.

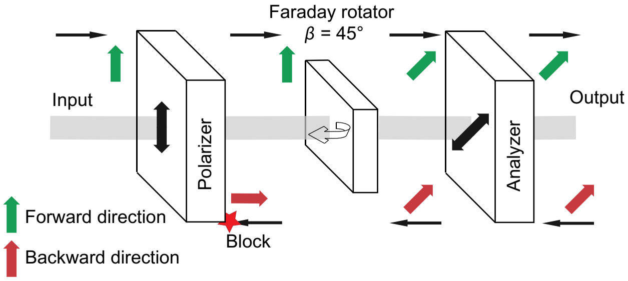

FIG. 7. Optical configuration of a polarization-sensitive optical isolator.

As shown above, an optical isolator is based on the Faraday effect [58]. The polarization plane of a linearly polarized light beam during propagation in a magneto-optical crystal is rotated by an angle θ. The direction of rotation is dependent on the direction of the magnetic field and not on the direction of light propagation. The relation between the angle of polarization rotation and the magnetic field in a crystal is

$$\theta = V(\lambda, T)BL, \tag{A1}$$

where B is the longitudinal magnetic field component in T, L is the length of the path where the light and magnetic field interact in m, and $V(\lambda, T)$ is the Verdet constant depending on the wavelength of the propagating light λ and temperature of the magneto-optic crystal T in rad/(T m). Here we consider only the temperature dependence.

The temperature dependence of the Verdet constant and hence the angle of Faraday rotation leads to variation in the isolation coefficient with temperature. Modern single-mode isolators have a high stability of isolation in the temperature range 5–70 °C. Thermal effects can be neglected for typical optical circuits, such as QKD systems, with laser power less than 300–500 mW. However, when the high-power laser is applied in the reverse direction, its emission is partially absorbed inside the isolator and induces heating of the magneto-optic crystal [59]. The temperature dependence of the Verdet constant causes changes in the angle of polarization plane rotation [see Eq. (A1)] [60,61]. For optical isolators, this means reducing the isolation coefficient in the reverse direction and losing power and degraded beam quality in the forward direction. Thermal effects can be mitigated by a careful choice of the magneto-optical material in the component [60]. The most widespread materials for a single-stage fiber isolator in the near infrared band are rare-earth garnets [61–63]. Here we consider the following types of garnets: yttrium iron garnet (YIG), terbium gallium garnet (TGG), and bismuth-substituted yttrium iron garnet (Bi:YIG).

2. Verdet constant model

In a general case, the Verdet constant of rare-earth garnet is impacted by several different contributions [64–66]. In our case, only temperature-dependent contributions are considered: the paramagnetic contribution V_{pm} (for more detail, see Ref. [67]) and frequency-independent gyromagnetic term V_{gm} (detail in Ref. [58]). The Verdet constant as a function of temperature has the appearance

$$V(T) = V_{\mathrm{pm}} + V_{\mathrm{gm}} = -\frac{A\lambda_0^2}{T - T_w} + \frac{B}{T - T_w} + C, \tag{A2}$$

where λ_0 is the wavelength of the dominant electronic transition, T_w is the Curie temperature, and A, B, C are constants depending on the properties of the chosen material.

Using data from Refs. [67–75], the dependence of the Verdet constant is obtained within a temperature range −20 °C–175 °C, as presented in Fig. 8. These dependencies have been calculated with fixed operating wavelength $\lambda = 1550$ nm. As reflected in Fig. 8, the crystal TGG exhibits the least stability with temperature. This means that isolators based on TGG are most susceptible to thermal effects at $\lambda = 1550$ nm. Isolators based on YIG or Bi:YIG should be more temperature stable.

3. Isolation model

Next, we analyze the change in isolation with varying crystal temperature in the proposed model with the ideal polarizer and analyzer. The polarization planes of the polarizer and the analyzer are oriented relative to each other at the angle β, and the Faraday rotator provides the 45° rotation of the polarization plane of the propagating light with a central wavelength of 1550 nm. In our model, the magnetic field is constant and independent of temperature (but in real systems the magnetic field might introduce changes in isolation). According to

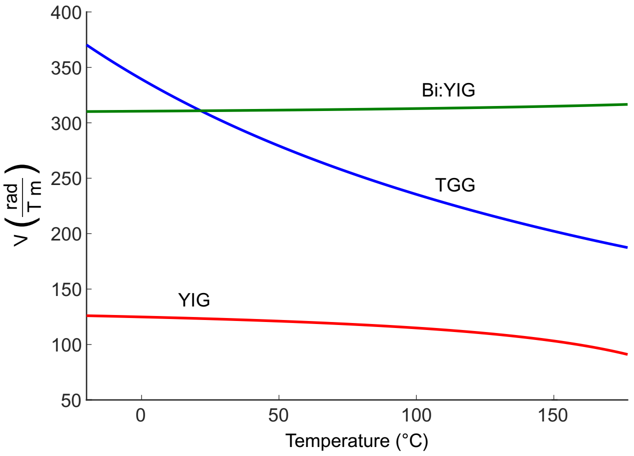

FIG. 8. The temperature dependence of the Verdet constant for TGG, YIG, and Bi:YIG at 1550 nm wavelength.

Malus's law, after passing through the Faraday rotator and the polarizer, the intensity of a beam of plane-polarized light varies as $I = I_0 \cos^2(\theta + \beta)$, where I_0 is the initial intensity [62,67]. The isolation coefficient is then defined as $\alpha = -10 \log \cos^2(\beta + \theta)$. [The insertion loss may be found from a similar formula using rotation angles equal to $(\beta - \theta)$.] After substituting the value of θ from Eq. (A1), the temperature dependence of the isolation coefficient takes the form

$$\alpha(T) = -10 \log \left[\beta + \frac{V(T)}{V(25\,^\circ\mathrm{C})} k \right], \tag{A3}$$

where k is the coefficient depending on the initial isolation value at a temperature of 25 °C [76]. Let us use the initial isolation value of 40 dB, because it is within a typical specification range of 32–40 dB for single-stage isolators at room temperature [76]. The isolation of 40 dB corresponds to a rotation angle for polarization plane in the Faraday rotator of either $\theta = 44.43^\circ$ or $\theta = 45.57^\circ$, depending on the direction of rotation. The calculation results for isolation and insertion loss are presented in Fig. 9.

The model predicts sharp peaks in the isolation value. It should be noted that generally there are no pronounced peaks in our experimental results of the isolation coefficient when the components are heated by the laser. This may be explained by the internal scattering in the crystal, which leads to a partial change in the plane of polarization. However, this factor is not considered in this model.

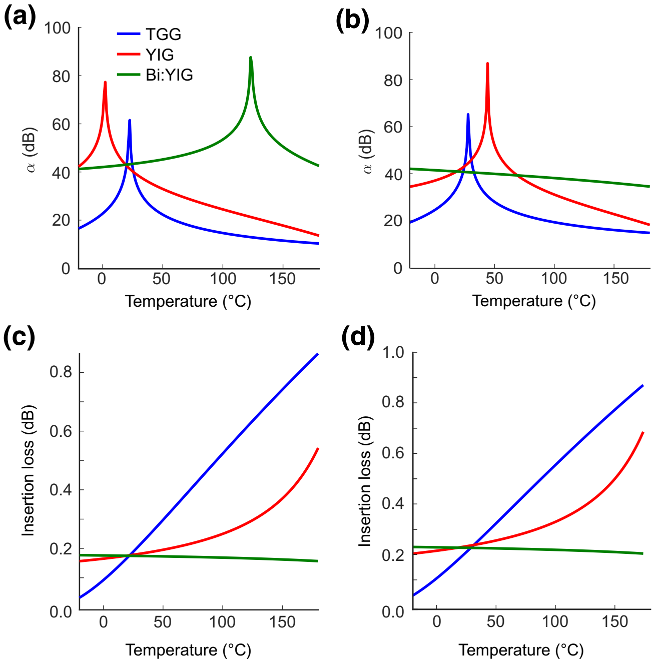

FIG. 9. Dependence of the isolation coefficient (a),(b) and insertion loss (c),(d) on temperature for TGG, YIG, and Bi:YIG. Panels (a) and (c) correspond to $\theta = 44.43^\circ$; panels (b) and (d) correspond to $\theta = 45.57^\circ$.

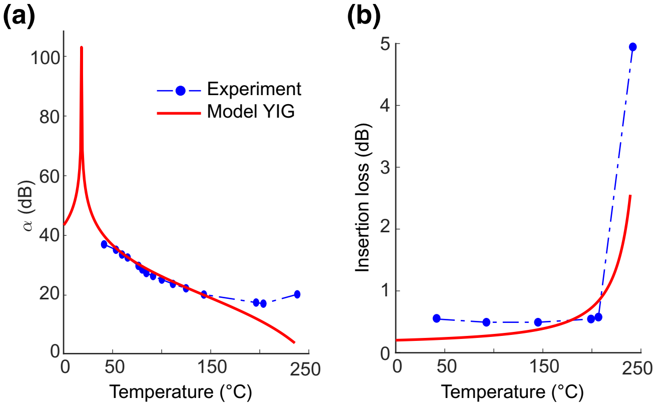

FIG. 10. Comparison of experimental results for ISO PM 2 and the model for YIG with $\theta = 44.43^\circ$ for (a) the isolation coefficient and (b) insertion loss.

4. Outcome

Our model shows that the change in the isolation coefficient with temperature depends heavily on the material of the magneto-optical crystal, even though each garnet may provide the same isolation value at room temperature. The crystal TGG has demonstrated the sharpest decrease in the isolation coefficient in the operating temperature range of isolators. This is because the operating wavelength range for this garnet is from 700 to 1100 nm [67]. The Bi:YIG crystal is specially designed for applications demanding high values of the isolation coefficient over a wide temperature range [59,74]. According to the calculation, the isolation coefficient is more than 40 dB in the temperature range −20 °C–180 °C. Such a high isolator stability is achieved due to the optimal crystal composition [68]. Additional doping provides several sublattices in the crystal structure, which compensate the temperature dependence of the Verdet constant of each other (and thus stabilise the isolation). In YIG, our model predicts that the isolation decreases by about 10 dB at 70 °C. When temperature increases significantly (up to 175 °C), isolation drops to about 15 dB. The obtained result fits well with the experimental data for ISO PM 2. The comparison between the experiment and model is shown in Fig. 10.

In summary, our model shows that Bi:YIG has the weakest dependence of the isolation coefficient on temperature and therefore it is the most advanced garnet for the isolators resilient to the laser-damage attack. In addition, we may assume that the magneto-optic crystal in isolator ISO PM 2 is YIG.

[1] C. H. Bennett and G. Brassard, in *Proc. International Conference on Computers, Systems, and Signal Processing (Bangalore, India)* (IEEE Press, New York, 1984), p. 175.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[5] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[6] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[7] F. Arute, *et al.*, Quantum supremacy using a programmable superconducting processor, Nature **574**, 505 (2019).

[8] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A **74**, 022313 (2006). erratum ibid. **78**, 019905 (2008)

[9] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).

[10] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, Opt. Express **15**, 9388 (2007).

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Thermal blinding of gated detectors in quantum cryptography, Opt. Express **18**, 27938 (2010).

[13] F. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12**, 113026 (2010).

[14] Hong-Wei Li, Shuang Wang, Jing-Zheng Huang, Wei Chen, Zhen-Qiang Yin, Fang-Yi Li, Zheng Zhou, Dong Liu, Yang Zhang, Guang-Can Guo, Wan-Su Bao, and Zheng-Fu Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, Phys. Rev. A **84**, 062308 (2011).

[15] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, After-gate attack on a quantum cryptosystem, New J. Phys. **13**, 013043 (2011).

[16] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, Controlling a superconducting nanowire single-photon detector using tailored bright illumination, New J. Phys. **13**, 113042 (2011).

[17] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Superlinear threshold detectors in quantum cryptography, Phys. Rev. A **84**, 032320 (2011).

[18] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[19] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system, Phys. Rev. A **83**, 062331 (2011).

[20] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device Calibration Impacts Security of Quantum Key Distribution, Phys. Rev. Lett. **107**, 110501 (2011).

[21] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser Damage Helps the Eavesdropper in Quantum Cryptography, Phys. Rev. Lett. **112**, 070503 (2014).

[22] 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**, 062301 (2015).

[23] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, IEEE J. Quantum Electron. **52**, 8000211 (2016).

[24] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, and C. M. S. Sajeed, Creation of backdoors in quantum communications via laser damage, Phys. Rev. A **94**, 030302 (2016).

[25] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, Quantum key distribution with distinguishable decoy states, Phys. Rev. A **98**, 012330 (2018).

[26] Yong-Jun Qian, De-Yong He, Shuang Wang, Wei Chen, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han, Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors, Phys. Rev. Appl. **10**, 064062 (2018).

[27] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-Seeding Attack in Quantum Key Distribution, Phys. Rev. Appl. **12**, 064043 (2019).

[28] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Laser Damage Attack Against Optical Attenuators in Quantum Key Distribution, Phys. Rev. Appl. **13**, 034017 (2020).

[29] Shihai Sun and Anqi Huang, A review of security evaluation of practical quantum key distribution system, Entropy **24**, 260 (2022).

[30] Poompong Chaiwongkhot, Jiaqiang Zhong, Anqi Huang, Hao Qin, Sheng-cai Shi, and Vadim Makarov, Faking photon number on a transition-edge sensor, EPJ Quantum Technol. **9**, 23 (2022).

[31] Anqi Huang, Akihiro Mizutani, Hoi-Kwong Lo, Vadim Makarov, and Kiyoshi Tamaki, Characterisation of state preparation uncertainty in quantum key distribution, ArXiv:2205.11870.

[32] Binwu Gao, Zhihai Wu, Weixu Shi, Yingwen Liu, Dongyang Wang, Chunlin Yu, Anqi Huang, and Junjie Wu, Ability of strong-pulse illumination to hack self-differencing avalanche photodiode detectors in a high-speed quantum-key-distribution system, Phys. Rev. A **106**, 033713 (2022).

[33] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[34] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[35] Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Wei Chen, Yong-Gang Zhu, Pavel V.

Morozov, Alexander V. Divochiy, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[36] C. Bennett, The slippery slope between quantum information and public information, and why cheap DIY randomness is better than expensive DI randomness, (2017) QCrypt 2017 rump session, http://2017.qcrypt.net/events-in-qcrypt-2017/rump-session/.

[37] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[38] N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New J. Phys. **16**, 123030 (2014).

[39] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Effect of source tampering in the security of quantum cryptography, Phys. Rev. A **92**, 022304 (2015).

[40] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, Hacking Quantum Key Distribution via Injection Locking, Phys. Rev. Appl. **13**, 034008 (2020).

[41] Shihan Sajeed, Igor Radchenko, Sarah Kaiser, Jean-Philippe Bourgoin, Anna Pappa, Laurent Monat, Matthieu Legré, and Vadim Makarov, Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing, Phys. Rev. A **91**, 032326 (2015).

[42] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, Faraday-Michelson system for quantum cryptography, Opt. Lett. **30**, 2632 (2005).

[43] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[44] J. Wang, X. Qin, Y. Jiang, X. Wang, L. Chen, F. Zhao, Z. Wei, and Z. Zhang, Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units, Opt. Express **24**, 8302 (2016).

[45] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z.-L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, Quantum key distribution with hacking countermeasures and long term field trial, Sci. Rep. **7**, 1978 (2017).

[46] X.-X. Xia, Z. Zhang, H.-B. Xie, X. Yuan, J. Lin, S.-K. Liao, Y. Liu, C.-Z. Peng, and Q. Z. Pan, LED-based fiber quantum key distribution: Toward low-cost applications, Photonics Res. **7**, 1169 (2019).

[47] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics, Phys. Rev. X **10**, 031030 (2020).

[48] H. Liu, Z.-W. Yu, M. Zou, Y.-L. Tang, Y. Zhao, J. Zhang, X.-B. Wang, T.-Y. Chen, and J.-W. Pan, Experimental 4-intensity decoy-state quantum key distribution with asymmetric basis-detector efficiency, Phys. Rev. A **100**, 042313 (2019).

[49] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

[50] Work Programme of GS QKD 010 Quantum Key Distribution (QKD), Implementation security protection against Trojan horse attacks in one-way QKD systems, https://portal.etsi.org/webapp/workProgram/Report˙Schedule.asp?WKI˙ID=43375, visited 5 May 2014.

[51] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, Proof-of-concept of real-world quantum key distribution with quantum frames, New J. Phys. **11**, 095001 (2009).

[52] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **112**, 190503 (2014).

[53] Shuang Wang, *et al.*, Field and long-term demonstration of a wide area quantum key distribution network, Opt. Express **18**, 21739 (2014).

[54] Micha Berent, Andon A. Rangelov, and Nikolay V. Vitanov, Broadband Faraday isolator, J. Opt. Soc. Am. A **30**, 149 (2013).

[55] Kiyoshi Tamaki, Marcos Curty, and Marco Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

[56] Weilong Wang, Kiyoshi Tamaki, and Marcos Curty, Finite-key security analysis for quantum key distribution with leaky sources, New J. Phys. **20**, 083027 (2018).

[57] lvaro Navarrete and Marcos Curty, Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks, ArXiv:2202.06630v1.

[58] A. K. Zvezdin and V. A. Kotov, *Modern Magnetooptics and Magnetooptical Materials*, Condensed Matter Physics (CRC Press, 1997).

[59] H. Kiriyama, *et al.*, High-contrast, high-intensity petawatt-class laser and applications, IEEE J. Sel. Top. Quantum Electron. **21**, 232 (2015).

[60] I. L. Snetkov, A. V. Voitovich, O. V. Palashov, and E. A. Khazanov, Review of Faraday isolators for kilowatt average power lasers, IEEE J. Quantum. Electron. **50**, 434 (2014).

[61] E. A. Khazanov, Thermooptics of magnetoactive media: Faraday isolators for high average power lasers, Phys. Usp. **59**, 886 (2016).

[62] R. C. Booth and E. A. D. White, Magneto-optic properties of rare earth iron garnet crystals in the wavelength range 1.1–1.7 μm and their use in device fabrication, J. Phys. D: Appl. Phys. **17**, 579 (1984).

[63] K. M. Mukimov, B. Yu. Sokolov, and U. V. Valiev, The Faraday effect of rare-earth ions in garnets, Phys. Status Solidi A **119**, 307 (1990).

[64] O. Slezák, R. Yasuhara, A. Lucianetti, and T. Mocek, Temperature-wavelength dependence of terbium gallium garnet ceramics Verdet constant, Opt. Mater. Express **6**, 3683 (2016).

[65] R. Serber, The theory of the Faraday effect in molecules, Phys. Rev. **41**, 489 (1932).

[66] A. D. Buckingham and P. J Stephens, Magnetic optical activity, Annu. Rev. Phys. Chem. **17**, 399 (1966).

[67] David Vojna, Ryo Yasuhara, Hiroaki Furuse, Ondrej Slezak, Simon Hutchinson, Antonio Lucianetti, Tomas Mocek, and Miroslav Cech, Faraday effect measurements of holmium oxide (Ho_2O_3) ceramics-based magneto-optical materials, High Power Laser Sci. Eng. **6**, e2 (2018).

[68] Weizhong Zhao, Magneto-optic properties and sensing performance of garnet YbBi:YIG, Sens. Actuator A Phys. **89**, 250 (2019).

[69] R. W. Cooper, W. A. Crossley, J. L. Page, and R. F. Pearson, Faraday rotation in YIG and TbIG, J. Appl. Phys. **39**, 565 (1968).

[70] W. A. Crossley, R. W. Cooper, J. L. Page, and R. P. van Stapele, Faraday rotation in rare-earth iron garnets, Phys. Rev. **181**, 896 (1969).

[71] G. Stevens, T. Legg, and P. Shardlow, in *Components and Packaging for Laser Systems II*, Vol. 9730, edited by Alexei L. Glebov and Paul O. Leisher, International Society for Optics and Photonics (SPIE, 2016), p. 1.

[72] S. Matsumoto and S. Suzuki, Temperature-stable Faraday rotator material and its use in high-performance optical isolators, Appl. Opt. **25**, 1940 (1986).

[73] B. Vertruyen, R. Cloots, J. S. Abell, T. J. Jackson, R. C. da Silva, E. Popova, and N. Keller, Curie temperature, exchange integrals, and magneto-optical properties in off-stoichiometric bismuth iron garnet epitaxial films, Phys. Rev. B **78**, 094429 (2008).

[74] D. Vojna, O. Slezák, A. Lucianetti, and T. Mocek, Verdet constant of magneto-active materials developed for high-power Faraday devices, Appl. Sci. **9**, 3160 (2019).

[75] S. Kumari and S. Chakraborty, Study of different magneto-optic materials for current sensing applications, J. Sens. Sens. Syst. **7**, 421 (2018).

[76] Y. Konno and H. Kume, Optical isolator and method for assembling same, US patent US5204868A, granted 1993-04-20.