Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution

Anqi Huang,[1,2,3,*] Ruoping Li,[4] Vladimir Egorov,[5] Serguei Tchouragoulov,[6] Krtin Kumar,[2] and Vadim Makarov[7,8,9,4]

[1] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China*
[2] *Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[3] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[4] *Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[5] *Faculty of Photonics and Optical Information, ITMO University, 199034 Kadetskaya line 3b, St. Petersburg, Russia*
[6] *QGLex Incorporated, 105 Schneider Road, Suite 111, Ottawa, Ontario K2K 1Y3, Canada*
[7] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[8] *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*
[9] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*

(Received 11 June 2019; revised manuscript received 10 January 2020; accepted 3 February 2020; published 5 March 2020)

Many quantum key distribution systems employ a laser followed by an optical attenuator to prepare weak coherent states in the source. Their mean photon number must be precalibrated to guarantee the security of key distribution. Here we experimentally show that this calibration can be broken with a high-power laser attack. We test four fiber-optic attenuator types used in quantum key distribution systems, and find that two of them exhibit a permanent decrease in attenuation after laser damage. This results in higher mean photon numbers in the prepared states and may allow an eavesdropper to compromise the key.

DOI: 10.1103/PhysRevApplied.13.034017

I. INTRODUCTION

Ideally, quantum key distribution (QKD) [1,2] promises information-theoretic security owing to the solid foundation of quantum mechanics. However, there are often implementation flaws and equipment imperfections, which can be exploited by an eavesdropper Eve to reduce the security of the secret key. This attempt is referred to as "quantum hacking," drawing the parallel with traditional cybersecurity. The capability of Eve to compromise the security of QKD systems has previously been shown [3–19], especially against single-photon detectors [6,12, 14,17–27], and also was field demonstrated [28] with current technology.

To protect a QKD system from detector-side loopholes, measurement-device-independent QKD (MDI QKD) has been proposed [29] and implemented not only in the laboratory [30,31] but also in the field [32,33]. MDI QKD removes the security assumption about the measurement station, which can even be an untrusted party [29]. However, the sources are still assumed to be in secure laboratories, which might not be true in a practical scenario. Side channels may still exist during quantum-state preparation. Therefore, it is important to further investigate practical vulnerabilities of the source station, to be able to correct and improve its security.

A QKD system often employs a weak coherent laser as a source, with a mean photon number attenuated to single-photon levels using an optical attenuator. Thus, the majority of nonempty pulses contain a single photon, which cannot be split off by Eve and measured separately. There is, however, a small portion of multiphoton pulses from the inherent Poissonian statistics behind the optical attenuation. The side effect of the multiphoton states can be eliminated by applying decoy-state protocol [34–36]. However, if the optical attenuation component itself can be altered and its attenuation decreased, either permanently or temporarily, the assumption about the mean photon number may be broken. Eve can then compromise the security of the QKD system [37–42]. In particular, even a very small increase of the mean photon

*angelhuang.hn@gmail.com

number requires a correction to the secret key rate in decoy-state BB84 and MDI QKD protocols, otherwise the key becomes insecure [40].

In a source's apparatus, an optical attenuator is usually the last component that optical pulses go through before they are sent to a quantum channel [32,43–51] However, for Eve, the attenuator is the first component she sees, looking at the source's apparatus from the network side. High-power laser damage of other components in QKD systems has been demonstrated before [10,13]. We suspect that a high-power laser shining through the output fiber into the source can affect the performance of the attenuator. The changes in its characteristics will then occur before those in other components, because the attenuator dissipates most of the power (assuming a reasonably equal threshold of failure in components). We select four types of optical attenuators from four different QKD systems, in each of which the attenuator is positioned to be the last component in the transmitter and closest to the quantum channel. Here we attempt to alter their performance by laser damage. This has been done in an optical setup similar to a live QKD system.

The paper is structured as follows. We first discuss the power-handling capability of single-mode fiber in Sec. II, which gives us an estimate of the maximum power we can apply in the experiment and also in a live system. Section III introduces the experimental setup and methodology. The testing results are presented in Sec. IV. Briefly, one type of attenuator has survived our testing intact, another exhibited a small temporary attenuation drop, and the remaining two types exhibited a significant and permanent decrease in attenuation. We update the statistical risk prediction for untested QKD systems in Sec. V, discuss ideas for countermeasures in Sec. VI, and conclude in Sec. VII.

II. OPTICAL POWER-HANDLING CAPACITY OF SINGLE-MODE FIBERS

As the first step, we should clarify that how much optical power can be transmitted through a single-mode fiber. Here we set a restriction that Eve can use only the standard single-mode fiber as in a typical QKD system. The amount of optical power that can be sent to the attenuator in the source is limited by the inherent handling capability of the single-mode fiber, as well as the maximum power of the laser used in the attack.

A laser-induced damage threshold (LIDT) of the standard single-mode fiber is theoretically limited by the softening point of silica and its tolerance to thermally induced stress [52]. However, in reality, thermal damage likely happens at the fiber connection points or the interface between the fiber core and the cladding [52,53]. A fiber-fuse phenomenon can be triggered by high temperatures at a fiber-end facet [54,55]. This can be reproduced by contacting the fiber end against an absorptive material, such as metal, or by using a flame (approximately 2700 °C) [56]. It has been experimentally demonstrated that a 2–5-W cw laser can initiate the fiber fuse [54,56]. However, in our testing of a 20-m-long single-mode fiber ending with no termination (a 90° cleave), when no deliberate method is applied attempting to trigger the fiber fuse, it is able to tolerate a 9-W cw laser, the specified maximum power of our laser source.

Power loss in the fiber limits the power that can be delivered to the target. The major threat comes from backward scatterings in the optical fiber, especially the backward stimulated Raman scattering (SRS) and stimulated Brillouin scattering (SBS) [57]. Generally, during light transmission, a fraction of incident light can be transferred from one optical field to another field with frequency shift, due to molecular vibrations of the transmission medium. The frequency-shifted light is called Stokes wave. The intensity of Stokes wave may rapidly increase over distance, which causes further SRS and SBS. This scattered light can travel backward to the laser source and may destroy it. To keep the high-power laser source safe, the SRS and SBS thresholds need to be confirmed. The threshold is defined as the incident pump power P_{th} at which the backward Stokes power P_s becomes equal to the power at the fiber output [57]

$$P_{\text{th}}e^{-\alpha L} = P_s(L), \tag{1}$$

where α is the fiber loss (typically 0.05 km^{-1} at 1550 nm), and L is the transmission distance in km. Equation (1) indicates that the threshold is dependent on the fiber length.

For the backward SRS, its threshold is given by [57]

$$P_{\text{th}}^{\text{SRS}} = \frac{20A_{\text{eff}}}{g_R L_{\text{eff}}}. \tag{2}$$

Here A_{eff} is the effective core area (for the standard single-mode fiber with the core diameter of 8 μm, $A_{\text{eff}} = 50\ \mu\text{m}^2$); g_R is the Raman-gain coefficient, which is 6.67×10^{-14} m/W at 1550 nm [58]; L_{eff} is the effective interaction length defined as [58]

$$L_{\text{eff}} = \frac{1 - e^{-\alpha L}}{\alpha}. \tag{3}$$

Thus, the threshold value is dependent on the transmission distance. The simulation result of $P_{\text{th}}^{\text{SRS}}$ versus transmission distance is given in Fig. 1, which shows that the SRS threshold drops dramatically when the fiber length extends. However, more than 10-W optical power is allowed for transmission distance shorter than 1 km.

On the other hand, the backward SBS plays a key role in limiting the transmission power. SBS can occur at a much

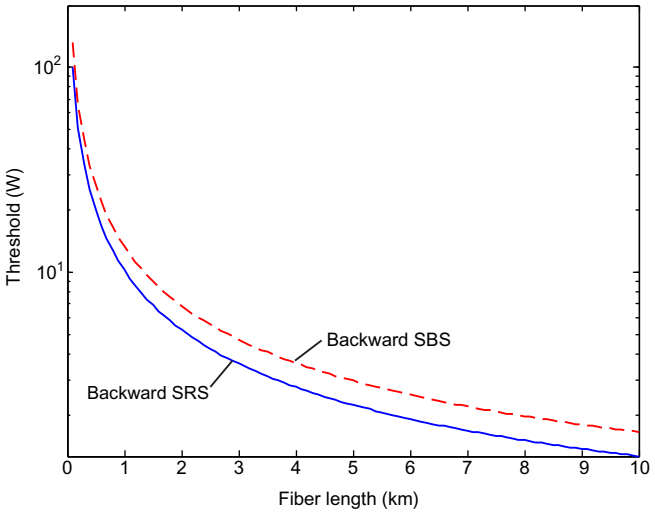

FIG. 1. Simulated backward SRS and SBS thresholds. The latter assumes a wideband source; see text for details.

lower incident power level than that for SRS. The input power threshold is quantified by [57]

$$P_{\text{th}}^{\text{SBS}} = \frac{21A_{\text{eff}}}{g_B L_{\text{eff}}}, \tag{4}$$

where the Brillouin-gain coefficient $g_B = 5 \times 10^{-11}$ m/W [58]. This only allows 2.1 W as maximum input power at $L = 10$ m. Fortunately, the SBS threshold can increase considerably if the spectral width of the pump laser $\Delta\nu_p$ is much larger than the FWHM of the Brillouin-gain spectrum in SBS $\Delta\nu_B$ [58]. Then the SBS threshold in Eq. (4) increases by a factor of $1 + \Delta\nu_p/\Delta\nu_B$. In the experiment, we employ a laser diode with $\Delta\nu_p \approx 10$ GHz; $\Delta\nu_B$ in the single-mode fiber at 1550 nm is 16 MHz. The SBS threshold in this case is also shown in Fig. 1. In this case it is slightly higher that the SRS threshold, i.e., the latter remains the limiting factor.

Overall, at least 10-W cw laser power can safely be transmitted through 1-km single-mode fiber. In most network installations we expect Eve to be able to connect to the quantum channel within this distance of the source. Shorter distance translates to larger fiber-handling capability of cw power, which translates to larger power that Eve can apply to the attenuator in the source. In our experiment, we use an amplified laser source providing up to 9-W cw power and transmit it through a 20-m-long fiber. The feasibility of longer transmission is theoretically verified by the models above.

III. TESTING METHOD

A. Experimental setup

The test of the optical attenuators has been conducted using the setup shown in Fig. 2. The experimental scheme

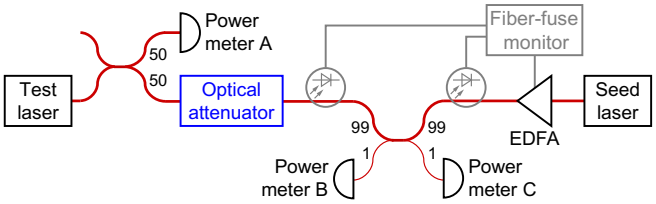

FIG. 2. Simplified diagram of experimental setup, with the optical attenuator as a replaceable device under test. The output of EDFA is fusion spliced to the 99% arm of the fiber beamsplitter. All fibers are standard single mode.

mimics a hacking scenario for a running QKD system. The test laser is a fiber-pigtailed 1550-nm laser diode (Gooch & Housego AA1406), acting as the laser in the source. This laser provides 5-mW cw light to measure the attenuation of the optical attenuator under test. The input of this attenuator is connected to the test laser through a 50:50 fiber beamsplitter (BS). Power meter A (Joinwit JW3208) monitors the power of the test laser, and power meter C (Thorlabs PM200 with S154C sensor) serves to check the attenuation of the optical attenuator before and after optical damage. An erbium-ytterbium-doped fiber amplifier (EDFA) provides up to 9-W cw power, which is applied to the optical attenuator through a 99:1 BS (Thorlabs 10202A-99-FC). A fiber-pigtailed laser diode emitting in a broad 1550.06–1550.14 nm band (QPhotonics QFBGLD-1550-100) set at 20-mW cw power is used as a seed source for the EDFA. Power meter B (Thorlabs PM200 with S146C sensor) measures the optical power at the EDFA's output. This scheme mimics a live scenario in which Eve injects light into QKD source station via the quantum channel.

The attenuation of the optical attenuator is determined by comparing the readings from the power meters A and C, taking into account the additional 20-dB attenuation of the 99:1 BS. This measurement is first performed for each attenuator with the optical amplifier and seed laser turned off, so that the initial attenuation is calibrated before any attempted tampering. The same measurement is repeated again after each laser-damage test. Any attenuation change after activating the EDFA can then be attributed to optical damage within the setup. We verify separately that during and after our testing up to the maximum 9-W power, the beamsplitters do not significantly change their splitting ratio. Thus any measured attenuation change is localized in the optical attenuator. In case bulkhead fiber-optic connectors get burnt (that some of the tested attenuator types use), we treat it as an outcome of Eve's attack that would cause a denial of service in the actual QKD system [13].

Our high-power light source in this experiment is the custom-made 1550-nm erbium-ytterbium-doped fiber amplifier, manufactured by QGLex. It is designed using core pumping at the first stage and double-cladding

pumping at the second stage. This allows for high gain and can accommodate the input seed power as low as 0.4 mW, which is amplified to a maximum of about 9 W (39.5 dBm) through a standard single-mode fiber (SMF-28) with a high slope efficiency of 28%. This amplifier has additional suppression of amplified spontaneous emission (ASE) at 1.0 μm. A significant presence of ASE could lead to spurious lasing at 1.0 μm and limitation of the energy transfer process from the ytterbium ions to the erbium, which would limit the output power level and efficiency. The EDFA exhibits single-mode behavior and a high slope efficiency. Before our experiment, the output power of the EDFA has been calibrated using power meter B (Fig. 2). This calibration provides an accurate relation between the software setpoint for the EDFA and its actual output power.

In case a fiber fuse [54,55] occurs in the device under test while applying high power during the experiment, an automatic monitoring and shutdown system protects the rest of the setup. We implement it with two Si photodiode sensors placed laterally along the fiber jacket. The sensors detect thermal visible light emitted by hot plasma in the fiber fuse as it propagates past them. One sensor is placed at the attenuator output, and another at the output of the EDFA (Fig. 2). If either of them detects light, a monitoring circuit shuts down the pump in the EDFA. This shuts off the emission and stops the fiber fuse at the sensor. This circuit has activated several times during our tests, preventing extensive damage to the equipment.

B. Test procedure

We can define a successfully "hacked" sample as one having a drop in attenuation after optical damage. For variable attenuators, this drop needs to be observed within their range of attenuation setpoints used in a QKD system. To quantify the result, we set a threshold of 1-dB drop in attenuation (which we can reliably measure above experimental errors) after damage, beyond which the attack is deemed to be successful. This drop approximately corresponds to a 26% increase in the mean photon number within the quantum channel. We also arbitrarily define a critical attack failure as the situation when the attenuator exhibits an attenuation increase larger than 3 dB, corresponding to a drop in the mean photon number of about 50%.

For each optical attenuator sample, our testing procedure is the following. The attenuation of the sample under test is set to a value that is typically used in each specific QKD system that employs this type of attenuator. The test laser is always on. The EDFA applies high power starting at 316 mW (25 dBm) for at least 10 s. Afterward, the EDFA is turned off and the attenuation is measured. If no change in the attenuation has occurred, the high power is increased by 0.5–1 dBm and the steps above are repeated. Once a change in attenuation (< -1 dB or >3 dB) is detected, the testing is stopped. If the maximum EDFA power of 9 W is applied with no change in attenuation, the testing is also stopped. We observe that the attenuators heat up during the high-power exposure and take time to cool down, during which temporary changes in attenuation are recorded for some samples. A permanent change in attenuation may then remain after it has fully cooled down to room temperature.

If the decrease of attenuation is observed in one sample, the test is repeated on additional samples of the device to demonstrate the effect more than once.

IV. EXPERIMENTAL RESULTS

A total of four types of optical attenuators are tested. Of these, one type appears to be minimally affected by optical damage up to 9 W (39.5 dBm); another type consistently shows a temporary decrease in attenuation. The two remaining types exhibit permanent changes in attenuation after being subjected to the high-power laser. A summary of the laser-damage results is presented in Table I.

A. Manual variable attenuator

The first attenuator is a manually adjustable type (OZ Optics BB-700-11-1550-8/125-P-60-3A3A-1-1-LL) with a range of 1.5 to 80 dB. It consists of a miniature fiber bench with two collimating lenses, which expand the beam to approximately 1-mm diameter and couple it back into the fiber. The collimated beam is partially obstructed by the opaque tip of a metal screw. Rotating the screw adjusts how much it is inserted into the beam, thus adjusting the amount of attenuation.

We test this attenuator set at 31 dB, corresponding to an almost complete blocking of the beam with the screw. The attenuator's polarization-maintaining fiber pigtail has been spliced to the single-mode fiber at the high-power side, with about 1-dB splice loss, which mimics the way it is connected in the QKD system that employs it. This PM-to-SM connection is not expected to significantly affect the test, because most of the high power is still delivered to the attenuator. The latter is not polarization selective.

We do not observe any change in the attenuation even at the highest available laser power of 9 W (39.5 dBm) applied continuously for 20 min. The attenuator case reached an equilibrium temperature of 234 °C at this power, as measured using a thermal imaging camera. This has led to discoloration of the black anodized coating on the aluminum case, and deformation of plastic strain relief sleeves.

A closer visual inspection of the attenuator is performed to determine the damage mechanism. Upon disassembly, the optical blocking material at the adjustable screw tip reveals a concave dent facing the input fiber where the laser power is delivered. This suggests that the blocking material

TABLE I. Summary of test results for all attenuator samples. For the last attenuator type, the number of samples means the number of individually tested points across the variable-density disk of a single device sample. For variable attenuators, the average change in attenuation after damage Δ is measured at their attenuation setpoint used during the laser damage. "Safe" power does not cause observable changes in attenuation. Attack threshold is the laser power at which the attenuator starts to exhibit more than 1-dB drop in attenuation. Failure threshold denotes the power at which the attenuator begins to fail catastrophically, increasing its attenuation by more than 3 dB.

Type	Manufacturer and part number	Number of samples			Maximum "safe" power (dBm)	Average success Δ (dB)	Average attack threshold (dBm)	Average failure threshold (dBm)
		Total	Success	Failure				
Manual VOA	OZ Optics BB-700-11-1550-8/ 125-P-60-3A3A-1-1-LL	2	0	0	>39.5[a]	...	...	...
Fixed	Unspecified[b]	12	4	6	32.8	−1.37	34.0	37.2
MEMS VOA	Unspecified[b]	13	8	4	34.5	−5.34	36.2	36.6
VDMC VOA	FOD 5418	(25)	(18)	0	32.9	−9.59	34.5	36.5

[a]39.5 dBm is the maximum power tested, limited by our EDFA.
[b]Information withheld at the request of QKD manufacturer.

is being damaged and removed by the laser, likely through vaporization or ablation of the material under high temperature. Consequently, under a higher cw optical power or ablation from a pulsed laser, there might be further damage to the screw with the possibility of a complete perforation. Then a permanent decrease in attenuation might occur. In short, our testing of this attenuator type has been inconclusive, being limited by our experimental capabilities, but a higher power may decrease its attenuation.

B. Fixed attenuator

The second type is a fixed attenuator of nominal attenuation 25 dB. The attenuator is a short cylindrical module having a male ferrule connector with physical contact (FC/PC) connector at one side and female one at another side. Its physical disassembly shows a solid axial cylinder of dark ceramic material roughly 5 mm long placed inline between the input and output fibers, which absorbs incident light. This absorber is placed in a white ceramic ferrule, which is in turn placed in a series of concentric metal sheaths beneath the outer casing.

Illumination power up to 1.91 W (32.8 dBm) does not affect our fixed attenuator samples. However, immediately after the application of approximately 4-W (36-dBm) power, they exhibit a temporary decrease in attenuation. The maximum decrease of approximately 2 dB occurs in one of the two samples at laser shutoff, as shown in Fig. 3. The attenuation then reverts back to the initial state within minutes. It is, however, still possible for Eve to exploit this temporary decrease in attenuation, leaking parts of the secret key [11,37–40]. This vulnerability window then exists only for a limited time after the high-power exposure. At a higher power of approximately 6.3 W (38 dBm), critical damage occurs to the absorptive element of the device, with the attenuation permanently increased by more than 20 dB.

To explain the possible damage mechanisms, we hypothesize that either the absorbing material or the attenuator housing can be made to expand and contract under thermal stress, which would explain the temporary drop in attenuation, as a small amount of optical power can leak to the output between the casing and the absorbing material. For samples suffering from critical damage,

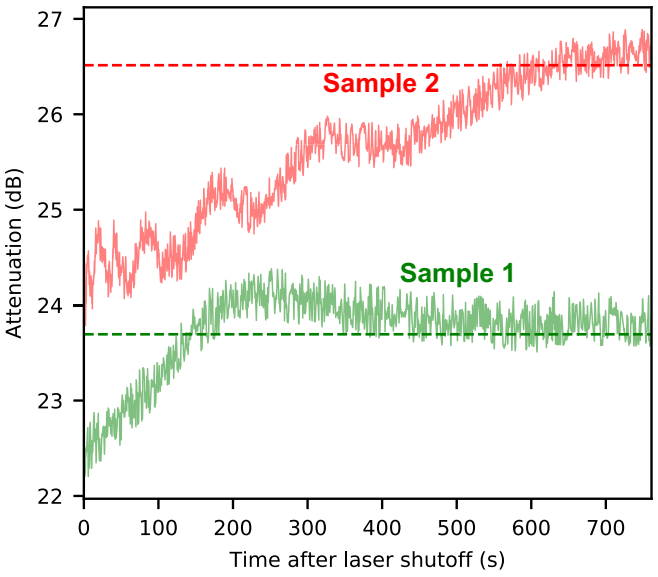

FIG. 3. Behavior of the fixed attenuator immediately after being subjected to a high-power laser at 4 W (36 dBm) for 5 min. A temporary decrease in attenuation is observed until the attenuator cools down in approximately 10 min. The horizontal lines indicate initially measured attenuation before the application of high power.

disassembly shows that the dark ceramic absorbing material has a burned appearance, with irregular dark patches surrounding it. The critical damage that produces a large increase in attenuation (20 dB) likely corresponds to when this ceramic material is darkened under the high temperature generated by the illumination.

C. MEMS-based variable attenuator

The third type is a variable optical attenuator (VOA) based on a MEMS element. The MEMS VOA is voltage adjustable from a maximum of 31–34 dB to a minimum of approximately 1 dB. Its physical disassembly shows two parallel input and output fibers facing a reflector-lens assembly (Fig. 4). The voltage controls the tilt of the reflector mirror via electrostatic force, and thus changes the amount of coupling between the input and output fiber. During the tests, the attenuation of the samples is set within a range that might be used in the QKD system that employs this attenuator.

1. Preliminary tests on individual attenuators

We test eight samples of MEMS VOAs in an unpowered state, in which they have their maximum attenuation value. Out of these tested, three samples exhibit an average change of −3 dB after optical damage, as shown in Fig. 5, which is confirmed to be permanent with subsequent measurements after several hours and days. The permanent decrease in attenuation occurs near laser power of 4 W (36 dBm). Near this damage threshold, the attenuation fluctuates when measured after turning off the EDFA, steadily decreases, and stabilizes after a few minutes. This is likely due to thermal effects. If the failure threshold is exceeded, the optical attenuator sustains catastrophic damage and its attenuation is permanently increased to >70 dB.

2. Further tests on assembled attenuator boards

Following the initial confirmation that MEMS VOAs are especially vulnerable to the laser-damage attack and exhibit a permanent attenuation drop after optical damage, subsequent experiments are done using complete

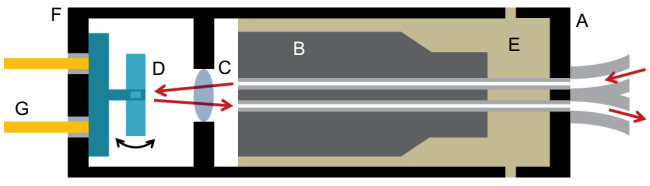

FIG. 4. Simplified schematic of MEMS variable optical attenuator, with parts labeled (not to scale). A, metal cap holding the input and output single-mode fibers; B, glass sheath; C, collimating lens; D, voltage adjustable MEMS mirror on torsion mount; E, adhesive filler; F, metal body; G, electrical leads.

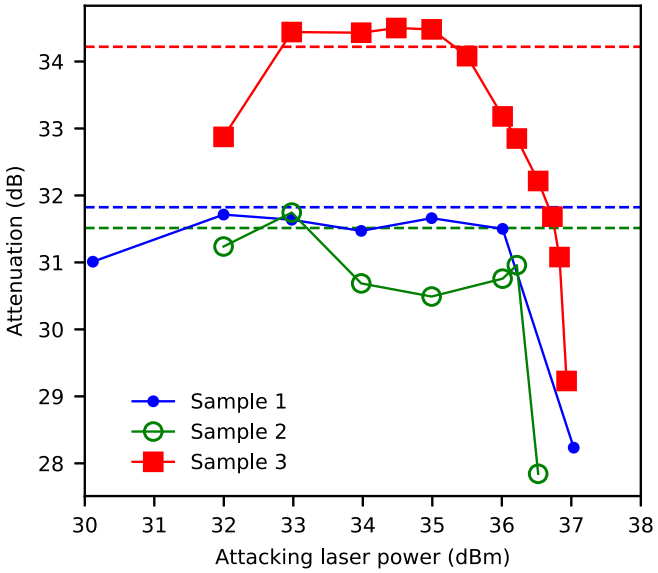

FIG. 5. Selected samples of MEMS VOA with permanent decrease in attenuation after laser damage. The attenuation decreases abruptly near 4 W (36 dBm). Horizontal lines indicate the initial measured attenuation before the application of high power. The leftmost point shown is the first application of high power to each sample.

printed-circuit-board (PCB) mounted-attenuator assemblies received from industry, shown in Fig. 6. The attenuators are from two different manufacturers but are nearly identical in their construction, here labeled subtype A or B, and are attached using a soft silicone glue to the PCB, providing a thermally accurate representation of their use in the QKD system.

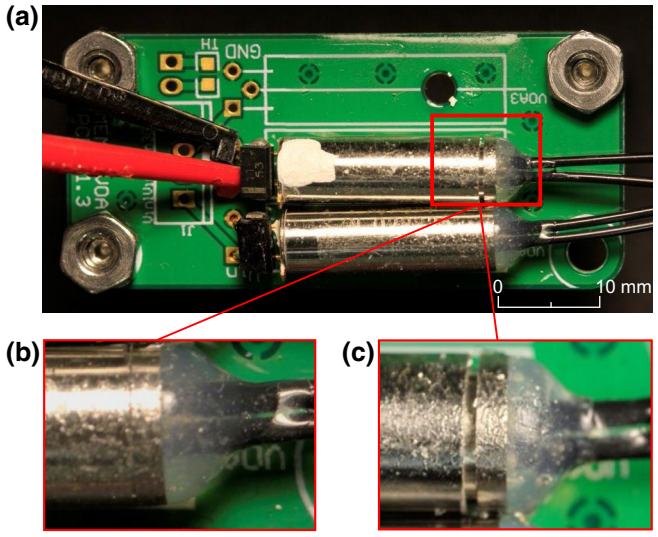

FIG. 6. MEMS VOAs mounted on (a) PCB. (b) Initially, the end cap is tightly inserted into the body. (c) Catastrophic structural damage in MEMS VOA sample 3 at 5.6 W (37.5 dBm). The cap is displaced.

TABLE II. Optical damage results for complete MEMS VOA assemblies. Testing voltage is the attenuator control voltage at which high power is applied. Δ is the change in attenuation observed at the testing voltage.

Sample	Subtype	Testing voltage (V)	Attenuation before (dB)	Attenuation after (dB)	Δ (dB)	Attack threshold (dBm)
1	A	12.0	33.05	35.44	+2.39	36.5
2	A	12.0	33.88	32.95	−0.93	37.0
3	A	11.5	32.81	64.28	+31.47	37.5 (failure)
4	B	14.0	38.79	32.32	−6.47	35.5
5	B	14.5	≈68[a]	58.82	≈−9.2	36.0
6	B	13.5	31.21	22.29	−8.92	34.5

[a]Measurement near the minimum power range of the power meter.

Our results are summarized in Table II. At the testing voltage chosen, corresponding to an attenuation of approximately 30 dB, four out of the six attenuators tested exhibit a permanent drop in attenuation. Furthermore, for five out of the six attenuators, there exists an attenuation range with a decrease in attenuation postdamage, as shown by the shaded area in Fig. 7. The response curve of the attenuation within the shaded area is shown for all successfully damaged attenuators in Fig. 8. We can deem the optical damage attack to be successful within this voltage range. The range at which there is a clear drop in attenuation is almost always at the higher attenuation settings, and Fig. 7 shows a typical behavior for the successfully attacked sample.

Attenuator sample 3 has exhibited a near-total failure, where the attenuation after the optical damage is dramatically increased over its normal value. Effectively, this is similar to a component becoming an open circuit in electronics, corresponding to the optical component blocking light. This sample represents a case of critical failure, which is an undesirable outcome for Eve resulting in denial of service in QKD.

Attenuator sample 5 is peculiar. When we initially measure its attenuation-voltage curve (before applying high optical power), the attenuation value has become latched at 14.5 V. A subsequent voltage change down to 0 V did not change this measured attenuation. The 14.5-V voltage, however, does appear to be in the working range for the other attenuators from manufacturer B. Since the applied voltage is close to the maximum voltage specified, it is likely that the latching observed at this voltage is from some inherent variability in the working voltage range between components, or a manufacturing defect. However, despite this unexpected malfunction, a permanent decrease in attenuation after laser damage is still observed in this sample.

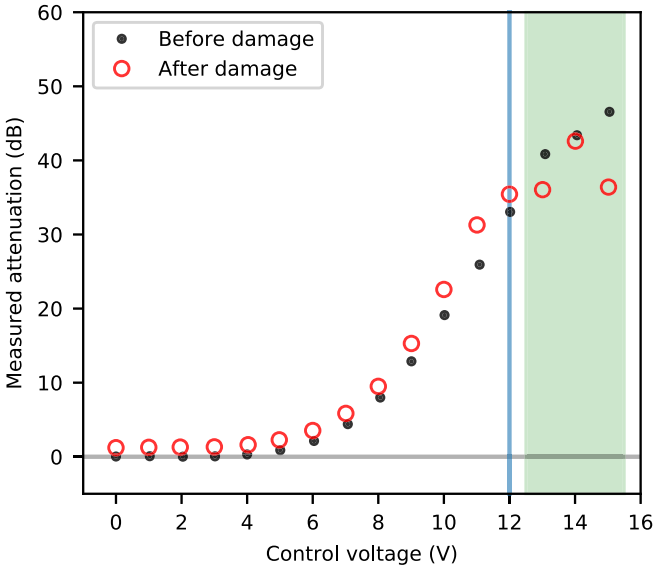

FIG. 7. Typical voltage-attenuation curve of a successfully compromised sample 1 of MEMS VOA. Blue vertical line denotes the voltage setting at which the laser damage is done. The shaded area denotes the range where permanent attenuation drop is observed.

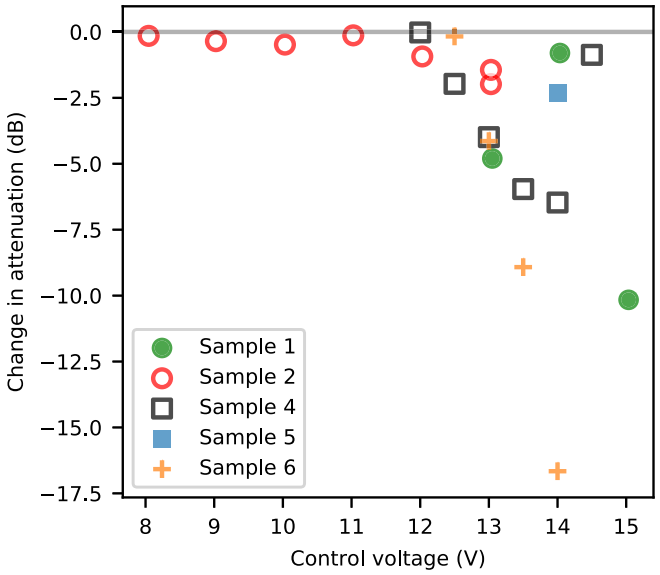

FIG. 8. Attenuation change after optical damage for successfully compromised MEMS VOA samples. For clarity, only control voltage points for which the attenuation has decreased are plotted. That is, the plotted data points correspond to points within the shaded area in Fig. 7.

3. Possible damage mechanisms

During the application of high power near the damage threshold, the cap holding the input and output fibers bulges outwards (Fig. 6), possibly pulling the fiber inside the VOA out of alignment with the collimating lens. In a catastrophic damage scenario at approximately 5.6 W (37.5 dBm), the cap detaches itself from the attenuator casing and a puff of smoke emits from the opening. Figure 9 shows the thermal profile of the attenuator under high-power laser recorded using an uncooled microbolometer-based thermal camera (FLIR E60). As the images show, the highest temperature occurs near the front end of the VOA casing where the input and output fibers are inserted. Since the process of coupling a beam of light into a single-mode fiber is highly dependent on relative positions of the involved optical elements [59], we hypothesize that structural deformation under high temperature is a likely cause for the observed change in attenuation.

Another possible cause is that for typical MEMS materials used (Si, SiN, SiC, etc.) [60], the operating temperature can induce lattice strain and change its spring constant [61]. The ductility of polycrystalline Si is reported to increase at temperatures near 500 °C [61]. Since the MEMS micromirror used in the VOA is fixed using a torsion mount, the amount of deflection induced by a given voltage may change with temperature. The voltage-attenuation curve might be different once the VOA heats up and exceeds its proper operating temperature range, which may either result in a drop in attenuation or an increase, depending on the exact material behavior under high temperature. Our observations using the thermal camera show that the outer casing of the VOA reached 120 °C at the attack threshold power. The internal temperature is likely to be much higher. However, from the observations and physical disassembly, it appears that the area near the fiber end of the VOA is visibly more affected by thermal damage, and not the mirror facet, which attributes some doubt to this mechanism of damage.

D. Variable-density metal-coating variable attenuator

The fourth type is a programmable VOA (FOD 5418) whose active element is a glass disk covered with variable-density metal coating (VDMC), see Fig. 10. Collimated light from the input fiber passes through VDMC, the glass, gets reflected from a dielectric mirror deposited at the back surface of the disk, then passes the glass and VDMC again. It then enters another collimator coupling it to the output fiber. An externally controlled motor rotates the glass disk to expose different coating density to the beam, adjusting attenuation in 0–80-dB range.

This VDMC VOA is used in a QKD system developed at ITMO University. The latter is based on a subcarrier-wave architecture with phase protocol and typical mean photon number around 0.2 [62,63]. At the time of the experiments described here, the attenuator is the last component before Alice's output [50,51], thus potentially allowing Eve to attack it.

1. Testing results

We test one VDMC VOA with a total of 25 measurements over different points of the active element corresponding to its different attenuation value settings, as summarized in Table I. During seven of these measurements done at laser power ≤1.95 W (≤32.9 dBm), neither permanent nor temporary change in attenuation has been

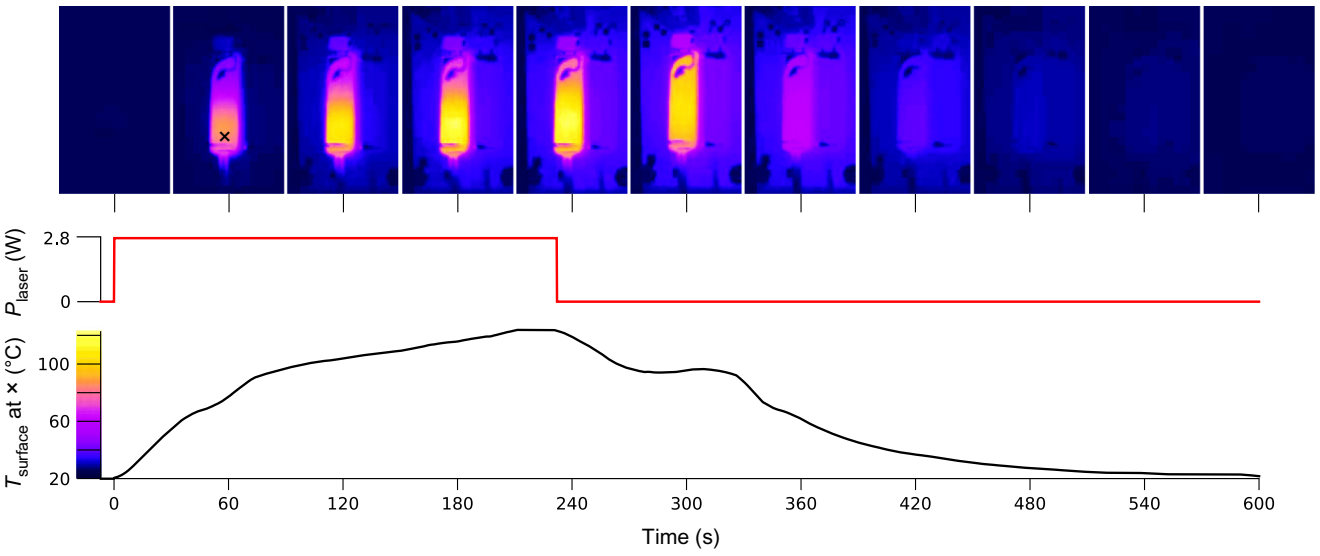

FIG. 9. Temperature profile of VOA sample 6 at the attack threshold, taken at a single point (marked ×) near the cap of the VOA. The high-power laser is set to 2.8 W (34.5 dBm) and turned on from time 0 through 232 s.

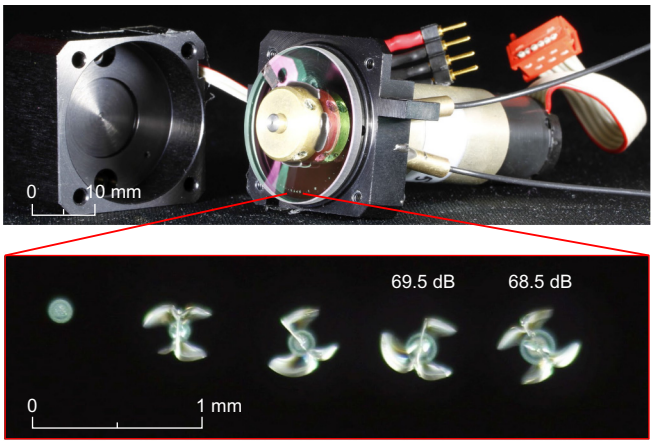

FIG. 10. Variable-density metal-coating variable attenuator opened with the glass-disk active element visible. Small dots around the disk edge correspond to irradiated areas. Magnified view of five damaged spots is given in the inset. The two rightmost spots are those shown in Fig. 11.

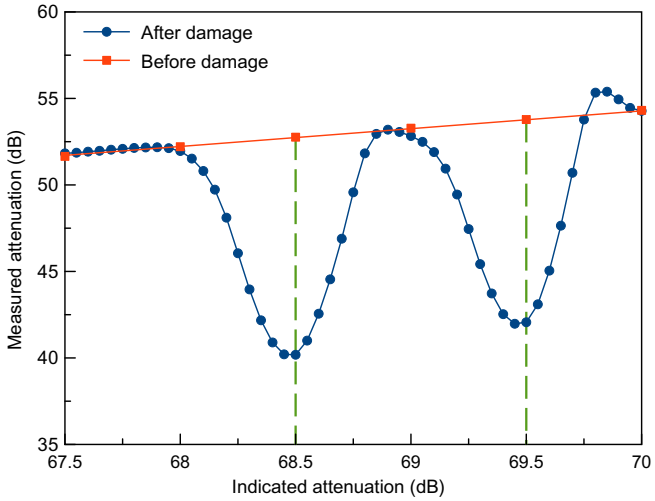

FIG. 11. Typical attenuation curve of successfully compromised VDMC VOA. Green vertical lines denote the attenuation settings at which optical damage is done. The high-power laser applied 2.8 W (34.5 dBm) for 10 s.

observed. All the remaining sample points have been successfully "hacked," demonstrating a permanent decrease in attenuation with mean change of −9.59 dB. None of the points are critically damaged when we apply up to 6.8 W (38.3 dBm) over up to 15-min duration. This is the maximum power available in our test setup at the time of this last experiment, because the EDFA has aged.

The successful attack threshold for VDMC VOA sample points depends on exposure time. In order to avoid destruction of its active element (due to heat-induced cracking of the glass disk) in our tests, we chose reasonably low exposure time of 10 s. After every 10 s of exposure we switch off the EDFA for another 10 s in order to cool down the sample and then resume our testing at the initial power level. We can, therefore, observe the added effects of high-power exposure on the metal coating with a minimal risk of sample destruction. In this subsection and in Table III, the total heat duration is calculated as the sum of all 10-s intervals of high-power exposure, disregarding the cooling time. Our goal is to define optimal conditions in terms of repeatability and minimal total exposure (i.e., both irradiation time and optical power). The latter would potentially decrease the probability of catastrophic sample damage or uncovering Eve's operation. We find that a minimum power level that leads to the successful attack is 2.0 W (33.0 dBm) for 200-s exposure time. At 2.2 W (33.4 dBm) the effect is achieved at shorter times varying from 30 to 50 s. Finally, exposure for only 10 s at 2.8 W (34.5 dBm) has led to a steadily repeatable result over nine sample points, therefore this power value may be considered a consistent attack threshold.

Typical attenuation curves before and after successful attacks are shown in Fig. 11. "Indicated attenuation" represents the programmed VOA setting [64]. An area of lowered attenuation has appeared around each affected sample point as the result of laser damage. Optical loss gradually increases around the point and returns to normal after 0.5-dB shift in either direction. Figure 12 illustrates consequences of choosing suboptimal laser-damage conditions.

TABLE III. Optical damage results for several VDMC VOA sample points.

Sample point	Attenuation before (dB)	Attenuation after (dB)	Δ (dB)	Power (W)	Total heat duration (s)
1	5.29	3.0	−2.29	2.81	10
2	9.86	4.21	−5.65	2.81	20
3	27.29	12.78	−14.51	2.81	50
4	49.56	38.71	−10.85	2.22	30
5	52.76	40.18	−12.58	2.81	10
6	55.88	46.27	−9.61	2.50	20
7	56.98	44.45	−12.53	2.50	100
8	57.99	45.42	−12.57	2.50	10
9	60.09	52.87	−7.22	2.22	50
10	62.21	50.46	−11.75	1.98	200

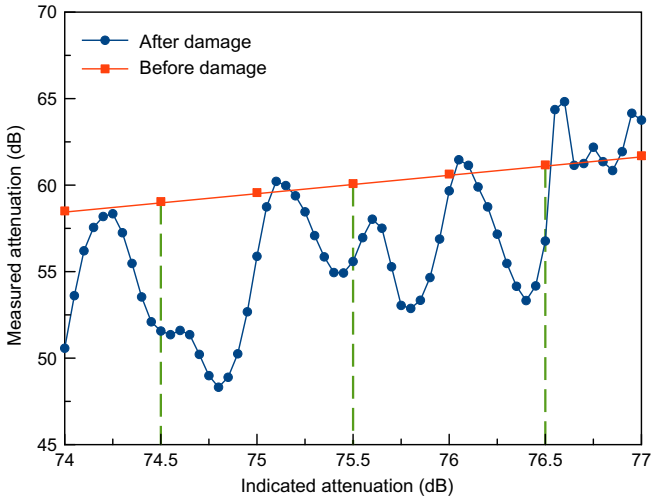

FIG. 12. Attenuation curve of VDMC VOA compromised in suboptimal conditions. Green vertical lines denote the attenuation settings at which optical damage is done. High-power exposure parameters are given in the text.

When the optical power goes below 2.8 W (e.g., 74.5-dB point, 2.5 W for 10 s), the curve structure becomes asymmetric and attenuation is not minimized at the point of damage. This effect is countered by increasing the exposure time. However, the damage outcome is more sensitive to power than time, as can be seen at the second point in Fig. 12 (75.5-dB point, 2.2 W for 50 s), where the asymmetry becomes even more prominent. Finally, lowered power and increased exposure time (76.5-dB point, 2.2 W for 30 s) sometimes results in increased loss value around the damaged area and/or a slight shift of the attenuation minimum from the point of damage. We attribute these effects to structural damage of the sample such as the glass surface cracking or the metal coating detaching owing to continuous local overheating.

As explained earlier, the light beam passes through the VDMC twice. We verify that damaged areas from different sample points never overlap, ensuring no interference between them in this experiment. To do so, before taking each measurement we check that attenuator losses coincide with their initial level defined during calibration. Also, the damage observed in most samples is only at the first passage point.

Table III summarizes laser-damage conditions and attenuation decrease over ten selected sample points damaged under different conditions. A local minimum value is given for each sample, even when the measurement point did not perfectly coincide with the point of damage (see Fig. 12). During a realistic attack Eve cannot control the VOA setting in the source to access this local minimum. Nevertheless, since our experiments indicate that in suboptimal irradiation conditions the acquired attenuation value randomly fluctuates around the damage point, it is reasonable to consider the worst-case scenario when the minimum randomly aligns with the VOA setting. Maximum attenuation decrease in optimal conditions (2.8 W, 10 s) is −12.58 dB. Over all 18 sample points, −9.54 dB mean change is observed. Minimum change in attenuation (−2.29 dB) is observed in the area of very low initial losses (5.29 dB).

2. Destructive testing and damage mechanism

After collecting all the data, we perform a destructive test at the programmed setting of 63 dB (measured 46.9 dB). Increasing power between 2.8 W and 4.4 W over 10 s did not affect attenuation any further. Subsequently raising it to 4.5 W (36.5 dBm) initiated fiber fuse at the flat-connector (FC) interface between VDMC VOA output and the beamsplitter arm. As a result, the beamsplitter-side fiber is burnt while VDMC VOA output connector remained seemingly undamaged. After resplicing the damaged section, cleaning the connector and repeating the experiment we observe the fuse again. Therefore, this power setting may be considered a limit in realistic conditions. In order to study high-exposure effects on the active element itself, we proceed with the tests, this time directly splicing the beamsplitter arm to VDMC VOA output. Repeatedly applying to the same spot 4.5–6.8 W for 10 s (with a roughly 0.5-W step) resulted in dramatic drop in attenuation of −20.7 dB in addition to the previous −11.3 dB, totaling a −32 dB decrease from the initial value. After this point, 6.8-W power is repeatedly applied for 30, 60, 180, 300, and 600 s without switching off the EDFA. Measurements made after the first two pulses indicated further slight decremental changes (−1.25 and −1.07 dB), the third and the fourth had virtually no effect (< -0.1 dB), while the last led to a slight attenuation increase (0.48 dB) probably due to structural damage of the glass-disk surface. Neither of these tests resulted in breaking the active element and causing denial of service.

Mechanically disassembling VDMC VOA and analyzing the effects on the active element confirmed the expected damage mechanism of partial metal-coating ablation during laser damage. As can be seen in Fig. 10, concentric structures appear at the damage points after high power exposure. A closer look reveals that they consist of darker central parts and several brighter outer rings. Formation of such structures is typical for laser-ablation processes in glasses with metal films or nanoparticles in the near-surface layer [65–67]. They appear when glass and metal particles are evaporated and melted away from the center of the affected area to cooler outer regions. We also observe cracks on the glass surface around some of the damaged regions (look like X-wing starfighters in Fig. 10), caused by overheating and local surface defects. The proposed mechanism explains why attenuation decrease is less pronounced at the sample regions with lower

attenuation, where the metal film is initially much thinner (see Table III). The minimal achieved loss is limited by insertion loss of the glass disk and other attenuator components, whose experimentally measured value is 1.7 dB.

V. STATISTICAL-RISK ESTIMATE

It would be common to say at the conclusion of this study that other QKD systems may be vulnerable to the laser-damage attack as the results of this paper make clear. However, is this a practically significant risk or not? A more precise statistical statement can be made using methods that are not familiar to most readers in the physics field, but are much more common in other fields that study complex systems. In these fields, the likelihood of outcomes is often estimated without a detailed understanding of the underlying processes. Clinical trials of new drugs and prediction of the magnitude and frequency of natural disasters are examples. Here we make an observation that the laser-damage attack on QKD is a similar setting, and attempt to make a relevant statistical prediction using the methodology borrowed from outside the quantum physics field.

The laser damage belongs to a class of attacks that are not based on a clear physical model. The outcome of such an attack on a particular QKD system—either denial of service or security breach—depends on a multitude of factors difficult to predict in advance, and is only possible to ascertain by experimental testing. (Other examples of attacks in this class are detector control attacks [6,12,20–27] and timing attacks [3–5,8,15]. To give a contrary example, a photon number splitting attack [37,38] has a well understood physical model, and its outcome can be predicted theoretically based on system design and specifications.)

In this setting, a risk prediction for untested QKD systems can be made by Bayesian analysis [68] after testing a small subset of the systems. A crucial assumption here is that this subset is chosen among the entire system population at random. This assumption is currently not possible to enforce with industrial QKD systems, because many of them would not be made available for testing if requested by us. However, we feel that our choice of the samples for testing has been sufficiently wide ranging, and we do not exclude any system from the testing based on our expectations or its design. With this caveat, we apply the Bayesian analysis.

After two QKD systems are tested and compromised by the laser-damage attack in Ref. [13], a statistical prediction is made that a significant fraction ($>20\%$) of remaining untested QKD implementations are almost certain (99.0% probability) to contain similar unpatched loopholes. This is a practically relevant prediction: if one fifth of the existing systems are almost certain to be vulnerable to the attack, then this is a serious security risk, and the community needed to worry about this attack.

The outcome of our present study is consistent with this prediction. We remark that we only test one component (optical attenuator) in one half of each QKD system (the source) against one type of laser illumination (<9 W cw at 1550 nm). Eve could, in principle, try higher power, pulsed illumination regimes, and different wavelengths to improve her attack, and she could try attacking the receiver side as well. Even with our restricted testing, we observe at least two attenuator types and thus QKD systems that use them are compromised.

Let us update the Bayesian analysis prediction, taking into account the additional outcomes from our present study. For the sake of this discussion, we give the QKD system containing the fixed attenuator a big benefit of doubt, and assume the outcome to be the denial of service. The systems containing the MEMS and VDMC VOAs are considered to be compromised. The system with the manual VOA is excluded from the statistics so far, because a higher laser power is needed to complete its testing. This leaves us (taking the two original data points [13] into account) with five systems tested to date, out of which one denial of service and four security-compromise outcomes are observed. The Bayesian analysis prediction then gives 99.5% probability that $>20\%$ of the remaining untested systems are vulnerable [69]. This confirms that the laser-damage attack on today's QKD implementations should be taken very seriously.

VI. COUNTERMEASURES

Our testing shows that none of the attenuators is confidently robust against the high-power laser-damage attack (the test of manual VOA is inconclusive owing to the insufficient power of our EDFA). Thus, countermeasures to this attack need to be developed and tested. A straightforward countermeasure, a watchdog monitor, might not be sufficient, as the monitor itself can be destroyed under high power [13]. Instead, passive countermeasures like optical isolators and circulators are used in some QKD systems (including commercial ones) to add isolation between the vulnerable attenuator and the quantum channel [70,71]. While this may protect the vulnerable attenuator from the laser-damage attack, the isolators and circulators also need to be tested for laser damage. This follow-up study is under way [72].

Alternatively we propose to add a special passive component, an optical fuse, at the source's output. The optical fuse will only tolerate a certain amount of laser power, and will permanently disconnect itself once injected power crosses a threshold. In this way, this fuse physically interrupts the injected high power and protects the system from the laser-damage attack. Such a device has been previously proposed using a TeO_2 soft-glass segment inserted inline a standard fiber, which prevents pulses higher than approximately 1 W (with duration approximately 1 s) from passing

through [73]. Adopting this or a similar technique into a QKD system could be another future study.

VII. CONCLUSION

In this work, four types of fiber-optic attenuators commonly used in QKD implementations are tested under high-power cw laser. The manual variable attenuator exhibits minimal change during testing. The fixed attenuator exhibits a temporary drop in attenuation at 2.5 W (34 dBm) of optical power. The MEMS VOA and VDMC VOA both show a permanent and large—several decibel—decrease in attenuation. The decreased attenuation results in the increased intensity of transmitted states, which can be exploited by Eve to compromise the security of QKD. This shows that the mean photon number can be tampered with, which effectively breaks the fundamental assumption about the mean photon number crucial in a QKD system with a weak coherent source [35,74]. Our study also confirms earlier statistical predictions about the danger of the laser-damage attack on QKD.

The demonstrated attack shows one more way to break the fundamental assumption about mean photon numbers in the QKD security proofs, in addition to a laser-seeding attack [40]. A detailed analysis of its effect on decoy-state BB84 and MDI QKD protocols is given in Ref. [40]. We hope our work encourages the development of nonleaky state preparation in MDI and device-independent QKD systems.

ACKNOWLEDGMENTS

We thank our industry collaborators for their cooperation. We thank J.-P. Bourgoin for recalculating the Bayesian analysis. This work is funded by NSERC of Canada (programs Discovery and CryptoWorks21), CFI, MRIS of Ontario, the National Natural Science Foundation of China (Grants No. 61901483, No. 61601476, and No. 61632021), the National Key Research and Development Program of China (Grant No. 2019QY0702) and the Ministry of Education and Science of Russia (programs 5-in-100 and NTI center for quantum communications). A.H. is supported by China Scholarship Council. This work is funded by Government of Russian Federation (Grant No. 08-08).

A.H., R.L., and V.E. conducted the experiments and analyzed the data. S.T. designed and built the custom EDFA, and K.K. the fiber fuse monitor. A.H., R.L., V.E., and V.M. wrote the paper. V.M. supervised the study.

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

[2] C. H. Bennett, Quantum Cryptography Using Any 2 Nonorthogonal States, Phys. Rev. Lett. **68**, 3121 (1992).

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

[4] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, Information leakage via side channels in freespace BB84 quantum cryptography, New J. Phys. **11**, 065001 (2009).

[5] 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).

[6] 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).

[7] 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).

[8] 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).

[9] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang Fred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan, Source attack of decoy-state quantum key distribution using phase information, Phys. Rev. A **88**, 022308 (2013).

[10] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M. Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov, Laser Damage Helps the Eavesdropper in Quantum Cryptography, Phys. Rev. Lett. **112**, 070503 (2014).

[11] 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).

[12] Anqi Huang, Shihan Sajeed, Poompong Chaiwongkhot, Mathilde Soucarros, Matthieu Legré, and Vadim Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, IEEE J. Quantum Electron. **52**, 8000211 (2016).

[13] Vadim Makarov, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagné, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legré, Carter Minshull, and Shihan Sajeed, Creation of backdoors in quantum communications via laser damage, Phys. Rev. A **94**, 030302 (2016).

[14] Shihan Sajeed, Anqi Huang, Shihai Sun, Feihu Xu, Vadim Makarov, and Marcos Curty, Insecurity of Detector-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **117**, 250505 (2016).

[15] Anqi Huang, Shi-Hai Sun, Zhihong Liu, and Vadim Makarov, Quantum key distribution with distinguishable decoy states, Phys. Rev. A **98**, 012330 (2018).

[16] Xiao-Ling Pang, Ai-Lin Yang, Chao-Ni Zhang, Jian-Peng Dou, Hang Li, Jun Gao, and Xian-Min Jin, Hacking quantum key distribution via injection locking, arXiv:1902.10423 [quant-ph].

[17] Vladimir Chistiakov, Anqi Huang, Vladimir Egorov, and Vadim Makarov, Controlling single-photon detector id210 with bright light, Opt. Express **27**, 32253 (2019).

[18] Gaëtan Gras, Nigar Sultana, Anqi Huang, Thomas Jennewein, Félix Bussières, Vadim Makarov, and Hugo Zbinden, Optical control of single-photon negative-feedback avalanche diode detector, arXiv:1911.12742 [quant-ph].

[19] Poompong Chaiwongkhot, Katanya B. Kuntz, Yanbao Zhang, Anqi Huang, Jean-Philippe Bourgoin, Shihan Sajeed, Norbert Lütkenhaus, Thomas Jennewein, and Vadim Makarov, Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence, Phys. Rev. A **99**, 062315 (2019).

[20] 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).

[21] 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).

[22] 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).

[23] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors, New J. Phys. **13**, 073024 (2011).

[24] 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).

[25] 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).

[26] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, Controlling an actively-quenched single photon detector with bright light, Opt. Express **19**, 23590 (2011).

[27] 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).

[28] 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).

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

[30] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).

[31] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[32] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan, Field test of measurement-device-independent quantum key distribution, IEEE J. Sel. Top. Quantum Electron. **21**, 6600407 (2015).

[33] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over Untrustful Metropolitan Network, Phys. Rev. X **6**, 011024 (2016).

[34] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[35] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[36] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[37] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[38] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses, J. Mod. Opt. **48**, 2009 (2001).

[39] Jason Pereira and Stefano Pirandola, Hacking alice's box in continuous-variable quantum key distribution, Phys. Rev. A **98**, 062319 (2018).

[40] Anqi Huang, Álvaro Navarrete, Shi-Hai Sun, Poompong Chaiwongkhot, Marcos Curty, and Vadim Makarov, Laser-Seeding Attack in Quantum Key Distribution, Phys. Rev. Appl. **12**, 064043 (2019).

[41] Yi Zheng, Peng Huang, Anqi Huang, Jinye Peng, and Guihua Zeng, Practical security of continuous-variable quantum key distribution with reduced optical attenuation, Phys. Rev. A **100**, 012313 (2019).

[42] Yi Zheng, Peng Huang, Anqi Huang, Jinye Peng, and Guihua Zeng, Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack, Opt. Express **27**, 27369 (2019).

[43] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, Nat. Photonics **1**, 343 (2007).

[44] Kyo Inoue and Yuuki Iwai, Differential-quadrature-phase-shift quantum key distribution, Phys. Rev. A **79**, 022319 (2009).

[45] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Practical gigahertz quantum key distribution based on avalanche photodiodes, New J. Phys. **11**, 045019 (2009).

[46] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[47] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over 200 km, Phys. Rev. Lett. **113**, 190501 (2014).

[48] Chao Wang, Xiao-Tian Song, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Chun-Mei Zhang, Guang-Can Guo, and Zheng-Fu Han, Phase-Reference-Free Experiment of Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **115**, 160502 (2015).

[49] Yao Fu, Hua-Lei Yin, Teng-Yun Chen, and Zeng-Bing Chen, Long-Distance Measurement-Device-Independent Multiparty Quantum Communication, Phys. Rev. Lett. **114**, 090501 (2015).

[50] A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller, Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference, Opt. Express **24**, 2619 (2016).

[51] A. V. Gleĭm, V. V. Chistyakov, O. I. Bannik, V. I. Egorov, N. V. Buldakov, A. B. Vasilev, A. A. Gaĭdash, A. V. Kozubov, S. V. Smirnov, S. M. Kynev, S. É. Khoruzhnikov, S. A. Kozlov, and V. N. Vasil'ev, Sideband quantum communication at 1 Mbit/s on a metropolitan area network, J. Opt. Technol. **84**, 362 (2017).

[52] Roger M. Wood, *Laser-Induced Damage of Optical Materials* (CRC Press, Boca Raton, 2003).

[53] S. Yanagi, S. Asakawa, and R. Nagase, Characteristics of fibre-optic connector at high-power optical incidence, Electron. Lett. **38**, 977 (2002).

[54] R. Kashyap and K. J. Blow, Observation of catastrophic self-propelled self-focusing in optical fibres, Electron. Lett. **24**, 47 (1988).

[55] Raman Kashyap, The fiber fuse – from a curious effect to a critical issue: A 25th year retrospective, Opt. Express **21**, 6422 (2013).

[56] Donald D. Davis, Stephen C. Mettler, and David J. DiGiovanni, in *Proc. SPIE* (International Society for Optical Engineering, Washington, 1997), Vol. 2966, p. 592.

[57] Richard G. Smith, Optical power handling capacity of low loss optical fibers as determined by stimulated Raman and Brillouin scattering, Appl. Opt. **11**, 2489 (1972).

[58] Govind P. Agrawal, *Nonlinear Fiber Optics* (Academic Press, Berlin, 2007).

[59] James Matthew Martin, Master's thesis, University of Central Florida, USA, 1979.

[60] Geoffrey Kotzar, Mark Freas, Phillip Abel, Aaron Fleischman, Shuvo Roy, Christian Zorman, James M Moran, and Jeff Melzak, Evaluation of MEMS materials of construction for implantable medical devices, Biomaterials **23**, 2737 (2002).

[61] W. N. Sharpe, Jr., in *Advances in Experimental Mechanics IV*, Appl. Mech. Mater. (Trans Tech Publications, Stafa-Zurich, 2005), Vol. 3, p. 59.

[62] A. Gaidash, A. Kozubov, and G. Miroshnichenko, Countermeasures for advanced unambiguous state discrimination attack on quantum key distribution protocol based on weak coherent states, Phys. Scr. **94**, 125102 (2019).

[63] G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, and D. B. Horoshko, Security of subcarrier wave quantum key distribution against the collective beam-splitting attack, Opt. Express **26**, 11292 (2018).

[64] Prior to the experiment, we performed a manual calibration of the VOA measuring its actual attenuation versus the programmed setting over its typical operating region, 20 to 80 dB, with 0.5-dB step. We found that the attenuation curve of our device sample is initially shifted (Fig. 11), probably due to a mechanical rotational misalignment of the active element, while it is otherwise a stable and fully functioning device. As the reader may understand, we choose this out-of-calibration device sample for our destructive tests, because it had limited value for other purposes. Our conclusions are not affected by the device being out of calibration.

[65] M. Domke, L. Nobile, S. Rapp, S. Eiselen, J. Sotrop, H. Huber, and M. Schmidt, Understanding thin film laser ablation: The role of the effective penetration depth and the film thickness, Phys. Procedia **56**, 1007 (2014).

[66] V. I. Egorov, I. V. Zvyagin, D. A. Klyukin, and A. I. Sidorov, The formation of silver nanoparticles on the surface of silver-containing glasses when they are irradiated with nanosecond laser pulses, J. Opt. Technol. **81**, 270 (2014).

[67] V. I. Egorov, A. V. Nashchekin, and A. I. Sidorov, Formation of an ensemble of silver nanoparticles in the process of surface evaporation of glass optical waveguides doped with silver ions by the radiation of a pulsed CO_2 laser, Quantum Electron. **45**, 858 (2015).

[68] Andrew Gelman, John B. Carlin, Hal S. Stern, David B. Dunson, Aki Vehtari, and Donald B. Rubin, *Bayesian Data Analysis* (CRC Press, Boca Raton, 2014), 3rd ed.

[69] The probability is given by beta cumulative function [Eq. (12) in Ref. [75] but integrated from 0 to t, where t is the fraction of untested samples that can be safe to the attack while having at least $1-t$ of untested samples vulnerable]. We assume the entire population comprises 50 QKD systems. We assume Jeffreys prior, although with five outcomes the choice of prior affects the prediction already very little.

[70] Marco Lucamarini, Iris Choi, Martin B. Ward, James F. Dynes, Z. L. Yuan, and Andrew J. Shields, Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

[71] Technical documents provided by Quantum CTek Co., Ltd. (2019).

[72] Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhot, Vladimir Egorov, Vadim Makarov, and Anqi Huang, manuscript in preparation.

[73] Shin-ichi Todoroki and Satoru Inoue, Observation of blowing out in low loss passive optical fuse formed in silica glass optical fiber circuit, Jpn. J. Appl. Phys. **43**, L728 (2004).

[74] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[75] K. P. Murphy, Bayesian statistics: A concise introduction (2007), https://www.cs.ubc.ca/~murphyk/Teaching/CS340-Fall07/reading/bayesStat.pdf, visited 6 Jan 2019.