Loopholes in the 1500–2100-nm Range for Quantum-Key-Distribution Components: Prospects for Trojan-Horse Attacks

Boris Nasedkin,[1,2,*] Fedor Kiselev,[2,3] Ilya Filipov,[2] Darya Tolochko,[2] Azat Ismagilov,[1] Vladimir Chistiakov,[1,2] Andrei Gaidash,[1,3,4] Anton Tcypkin,[1] Anton Kozubov,[1,3,4] and Vladimir Egorov[2,3]

[1] *Laboratory of Quantum Processes and Measurements, ITMO University, 3b Kadetskaya Line, Saint Petersburg 199034, Russia*

[2] *Laboratory for Quantum Communications, ITMO University, 3b Kadetskaya Line, Saint Petersburg 199034, Russia*

[3] *SMARTS-Quanttelecom LLC, Saint Petersburg 199178, Russia*

[4] *Department of Mathematical Methods for Quantum Technologies, Steklov Mathematical Institute of Russian Academy of Sciences, 8 Gubkina St, Moscow 119991, Russia*

(Received 1 December 2022; revised 26 April 2023; accepted 16 June 2023; published 18 July 2023)

Vulnerabilities of components used in quantum-key-distribution systems affect its implementation security and must be taken into consideration during system development and security analysis. In this paper, we investigate transmission of fiber optical elements, which are commonly used in quantum-key-distribution systems for designing countermeasures against Trojan-horse attacks, in the 1500–2100-nm range. As a result, we find loopholes in their transmission spectra that open possibilities for eavesdropping. We also consider a simple passive countermeasure based on the violation of total internal reflection in a single-mode fiber, that provides additional insertion losses of at least 60 dB for double-pass Trojan-horse probe pulses for wavelengths longer than 1830 nm.

DOI: 10.1103/PhysRevApplied.20.014038

I. INTRODUCTION

One of the interesting applications of quantum technology is quantum key distribution (QKD), which allows two legitimate parties (Alice and Bob, sender and receiver, respectively) to generate private symmetrical bit sequences secured by laws of quantum physics. That means that an illegitimate user, or eavesdropper (Eve), has no possibility of obtaining the secret key information while staying undetected by legitimate users, because any intermediate measurement in the quantum channel would affect the quantum bit error rate (QBER) [1–3], the excess noise level [4], or detection statistics [5–7] depending on the given QKD protocol. One of the main problems in practical QKD is to prove theoretical security of the given protocol.

However, even when the QKD system is designed based on a theoretically secure protocol, its technical implementation might still remain vulnerable to a vast number of attacks based on imperfections of real-life optical components, e.g., Refs. [8–12], known as quantum hacking. For instance, part of the mentioned approaches concentrate their attention on heating of optical elements. That leads to the change of their properties or disables them completely [13,14] resulting in a loophole for an attack. Other approaches, such as the Trojan-horse attack (also known as "large pulse attack") [15–19], detector blinding attack [20–22] and attacks where detector blinding is a necessary component [5,6], use high-transmission spectral regions of optical elements to illegitimately interact with Alice's and Bob's hardware via optical probing.

This paper is focused on the Trojan-horse attack (THA). To implement the THA, an eavesdropper directs intense optical pulses to Alice's or Bob's optical outputs or inputs, respectively, into inner components of their modules. These pulses propagate through the optical elements used in quantum state generation and detection and interacts with them. A fraction of these probe pulses is reflected back to the channel, similar to optical time-domain reflectometry (OTDR) [23], and may be registered by Eve, who uses suitable registration techniques, such as homodyne detection for phase-coded states. Despite the limitations on utilized by Eve optical power of probes are individual for various QKD systems, we may estimate them as follows. The THA clearly has an upper bound of the source power used for the attack; higher power may destroy optical fiber before light reaches optical elements, or cause a destructive fiber fuse effect [24]. The latter limits the highest probing power at approximately 10 W, according to Ref. [13] for continuous-wave lasers, while for pulsed sources the latter value is reduced even more with the decrease of

*banasedkin@itmo.ru

pulse duration. Even though in theory the optical probe, depending on its wavelength and power, may be sensed by monitoring and single-photon detectors installed in the QKD system, discovering this possibility is beyond the scope of the paper, and we leave it for future work, focusing here only on THA. Logically we presume that at high power levels THA and detector blinding might be used simultaneously, which does not contradict the main results of this work. Thus, we use 10-W power as an upper bound on the probing power in our estimations. The lower bound for the power used for the attack is limited by the high enough probability of information extraction (arbitrarily close to unity, depending on an eavesdropping model) from back reflected light.

To ensure the security of QKD systems against quantum hacking, and THA in particular, additional optical elements are introduced into QKD modules in order to limit detection of optical pulses sent by the eavesdropper. Such elements include attenuators, filters, isolators, circulators, monitor photodiodes, etc. However, these devices, in turn, have their own flaws that were previously investigated in Refs. [25,26] in the 1000–1800-nm range. In practice, the THA is feasible for wavelengths longer than 1250 nm in the case of a single-mode fiber. However, it is limited by distinguishability of the measured states and the absorption of a fiber. Moreover, the THA may be quite effective at wavelengths longer than 1750 nm; its possibility was previously demonstrated for 1924 nm [27]. Therefore, measuring transmission of QKD system elements both in forward and backward directions for ranges beyond 1000–1800 nm constitute a practical problem. In addition, optical probing in a wide spectral range can potentially be used in other quantum hacking techniques, e.g., detector blinding implementations. However, spectral measurements of fiber optical elements in a wide range is a challenging problem that requires precise hardware. Results of discussed wide-ranged measurements should be then taken into consideration during the full security analysis.

There are two methods of measuring transmission and reflectance of fiber optical elements. The first one is to use tunable lasers, which allow achieving higher power for a single wavelength measurement without damaging the system and consequently expand the dynamic range of the measurement [28]. The drawback of the approach is the discrete spectra. Another way is to use broadband sources, such as thermal or supercontinuum sources [25,29]. However, the main drawback of broadband sources is high integral power and low power near a single wavelength compared to tunable lasers.

In this work, we investigate transmittance of several optical elements conventionally used in QKD in the 1500–2100-nm range in the search of potential loopholes for quantum hackers that utilize an optical probing technique. It is worthwhile to note that the range from 1800 to 2100 nm has never been completely investigated before. Additionally, this range is of interest regarding the THA due to the fact that some detectors have significantly lower sensitivity if any [30] and potentially scanning THA pulses can be invisible for legitimate parties. As a complement to our results, we propose a passive countermeasure that reduces the possibility of the THA in the spectral range and could be simply integrated into QKD systems.

It was mentioned before that countermeasures against quantum hacking are dependent on the protocol and therefore, on its hardware implementation, especially its optical components. The measurements as well as their impact on the security evaluation described in the paper are performed for a discrete-variable subcarrier wave (SCW) QKD system, see Ref. [31]. In this system, the discrete set of phases is utilized in Alice's and Bob's modules, thus leaving both of them potentially vulnerable to THA. However, it should be emphasized that the proposed method can be easily generalized or adapted for various implementations of QKD protocols; the basic principles remain the same despite altering the optical scheme in both quantitative or qualitative manner.

II. PRIMARY GOAL

A. Problem

In order to estimate possible THA efficiency in the spectral range of interest, we should identify the part of the optical setup Eve would be probing and has access to. On the one hand, since any optical elements introduce losses, in the case of the optimal attack, Eve would monitor reflection of the probe as close to the start and the end of the quantum channel (for Alice and Bob, respectively) as possible. On the other hand, in order to gather the information about the signal states, a probe should interact with the phase modulator (PM). Therefore, we presume that Eve would monitor the optical parts that are located between the quantum channel entrance and the further facet of the PM, which has significant reflectance. To illustrate that, the examined parts of Alice's and Bob's optical schemes of the SCW QKD implementation are shown in Fig. 1.

It is imperative to elucidate that our analysis solely focuses on the backward reflection emitted from the adjacent optical bulkhead connector towards the phase modulator, under the assumption that the remaining connectors provide significantly lower impact on the overall output power. Additionally, the fundamental objective of this paper is to meticulously examine the transmittance spectra of individual optical components separately. As an illustrative example, we provide an approximate evaluation of the composite transmittance. It may be considered as the first-order approximation and regarding strict security evaluation of a QKD system one may perform additional measurements and consider them by the analogy.

To calculate the transmittance in the investigated parts of Alice's and Bob's modules (without any

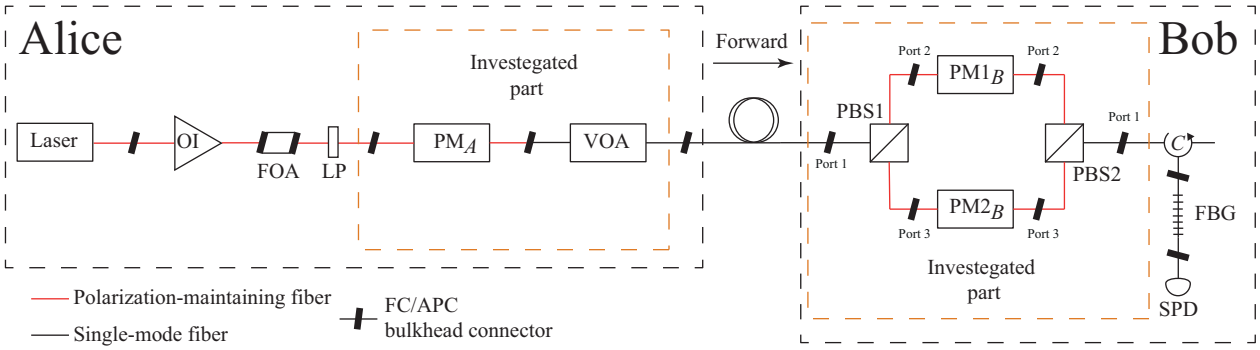

FIG. 1. Principal scheme of the SCW QKD optical setup. Investigated parts of Alice's and Bob's optical schemes are highlighted by orange-dashed rectangles. OI is an optical isolator, FOA is a fixed optical attenuator, LP is a linear polarazer, PM_A and PM_B are phase modulators in Alice's and Bob's schemes, respectively, VOA is a variable attenuator, PBS is a polarizing beam splitter, C is an optical circulator, FBG is a fiber Bragg grating, and SPD is a single-photon detector.

passive countermeasures against quantum hacking) we sum up transmittances of each measured optical element:

$$T_A \approx T_{\mathrm{VOA}f} + T_{\mathrm{PM}f} + \mathrm{Ref} + T_{\mathrm{PM}b} + T_{\mathrm{VOA}b}, \quad (1)$$

$$T_B \approx T_{\mathrm{PBS1}_{12}} + T_{\mathrm{PM1}_f} + T_{\mathrm{PBS2}_{23}} + T_{\mathrm{PM2}_b} + T_{\mathrm{PBS1}_{31}}, \quad (2)$$

where T_A and T_B are transmittance in Alice's and Bob's studied optical paths, respectively. T_{VOA}, T_{PBS1}, T_{PBS2}, T_{PM1}, and T_{PM2} are measured transmittance of variable optical attenuator, polarizing beam splitter and phase modulator, respectively. Indices f and b mark forward and backward directions, and indices 12, 23, and 31 mark PBS ports. $T_{\mathrm{PBS2}_{23}}$ denotes transmittance of PBS2 between ports 2 and 3 for Bob's scheme. Ref should be reflectance of PM's rear end, however we could not measure its value precisely, because it was beyond the noise level of the photodiode in our experimental setup. The latter is shown in Fig. 2. Therefore, we overestimate Ref value using the noise level of the photodiode in our experimental setup, which is higher and lies between −(40–50) dB (see Fig. 2) compared to the scanning power of supercontinuum for Alice's scheme. One should keep in mind that there are more possible ways to implement the THA for Bob's system (e.g., see Appendix A) and decision should be based on higher reflectance and transmittance of elements and possibility of extracting additional information compared to alternative ways, e.g., considering possible interference, time-multiplexing issues, etc. We choose the one with all measurable transmittances possible for your experimental setup and potentially the most conservative case as an explicit example to demonstrate the technique.

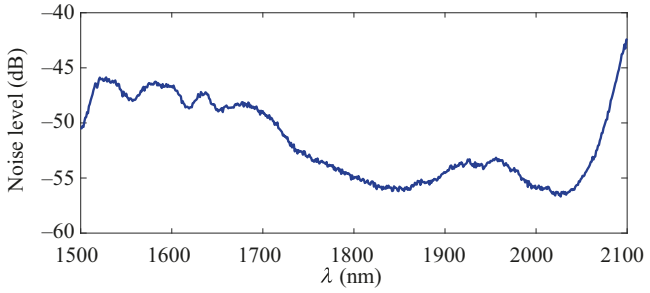

FIG. 2. Photodiode noise level compared to the scanning power of supercontinuum.

B. Experimental setup

In our experimental setup (Fig. 3) we use a pulsed supercontinuum generator (SC, Avesta EFOA) as a broadband light source with integral power of 150 mW [32]. Light from the source is guided into a single-mode optical fiber (OF) to investigate different fiber optical elements under test (EUT). Then, transmitted light is collimated into the free-space monochromator (MC, Action 2500) and measured by a calibrated photodiode (D, Hamamatsu). One of the problems with measurements in the optical spectrum beyond the telecommunication range is the lack of equipment with high dynamic range. To solve this issue, transmitted light is attenuated utilizing two conventional neutral spectral filters (F, NS10 and NS11) with known attenuation in the broadband spectral range. Since the dynamic range of utilized photodiodes is low (approximately 30 dB), we measure lower optical powers by removing the filters. Then, the transmittance is recalculated according to the following expression:

$$T_{\mathrm{dB}} = -10\log_{10}(P_{\mathrm{ref}} * T_f / P_{\mathrm{mes}}), \quad (3)$$

where P_{ref} is measured power without an element under test, P_{mes} is measured power with an element under test, T_f is filter transmission. Details regarding error calculations may be found in Appendix B.

As mentioned before, in our experiment we use the SCW QKD testbed described in Ref. [31]. To collect the

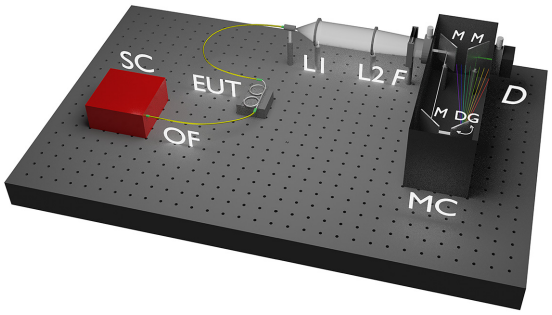

FIG. 3. Experimental setup for measurement of optical fiber elements' transmittance in the 1500–2100-nm range. SC is the supercontinuum source, OF is optical fiber, EUT is an element under test, L1 and L2 are lenses, *F* are neutral spectral filters, MC is monochromator, *M* is mirror, DG is diffraction grating, *D* is photodiode detector.

data needed for evaluation of the security against the THA, we measure individual transmittance of optical elements included in the system in forward and backward directions. To find overall transmittance for Alice's and Bob's setups, we sum up the transmittances of individual elements. Final results are averaged by ten measurements, and errors are calculated (for more information regarding error estimation, see Appendix B). It should be emphasized, we measure only optical elements placed before the phase modulator; this decision is based on the assumption, that maximal reflection of the eavesdropper's optical probe, that contains information of the chosen phase shift, is right after the modulator.

III. EXPERIMENTAL RESULTS

A. Phase modulator

Phase modulator is present in any QKD system with phase encoding, e.g., SCW QKD, and is also the main aim of the THA for quantum hackers. The key PM component is a lithium niobate electro-optical crystal [33,34]. Transmittance for the tested PM is shown in Fig. 4.

PM transmittance increases with the wavelength growth, which may be attributed to the modulator crystal absorption. Considering errors in the insertion-loss measurements for forward and backward directions, these measurements are almost identical. According to the datasheet, losses at 1550 nm are −3 dB, which is consistent with the obtained result. Losses at longer wavelengths may negatively affect the possibility of the THA. The maximum value of additional losses is −52 dB at, 2075 nm in a double-pass scheme.

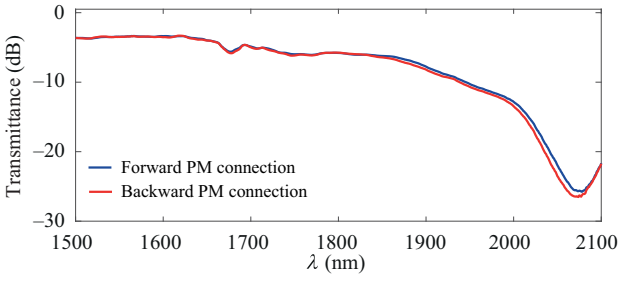

FIG. 4. Measured phase modulator (PM) transmittance. Blue line denotes transmittance in forward direction, red line denotes transmittance in backward direction.

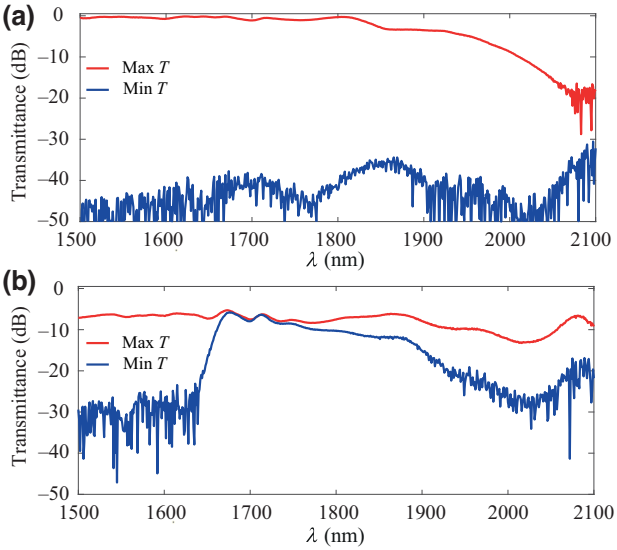

FIG. 5. Measured transmittance of (a) electromechanical VOA and (b) electro-optical VOA. Red and blue lines correspond to transmittance at minimal and maximal attenuation settings, respectively.

B. Variable optical attenuators

The second investigated component is a variable optical attenuator (VOA), which is used in Alice's module for setting quasi-single-photon power level (i.e., mean photon number during the time between phase shifts is less than one) in the quantum channel. Therefore, altered VOA functionality may lead to a severe security breach. We have measured the properties of two VOAs with different switching time and internal structure; in this paper, we refer to them as electro-optical VOA, and electromechanical VOA. The measurements are preformed at two VOA settings: at maximum and minimum transmittance. Transmittance value may be changed by altering the control voltage. The results of our measurements are shown in Fig. 5.

Transmittance of the electromechanical VOA are relatively stable in a wide spectral range for both minimum and maximum attenuation settings. The level of attenuation dependent on the voltage settings is consistent with its datasheet. Electro-optical VOA transmittance is also consistent with the datasheet in telecommunication range, but it has an unexpected transmission window with

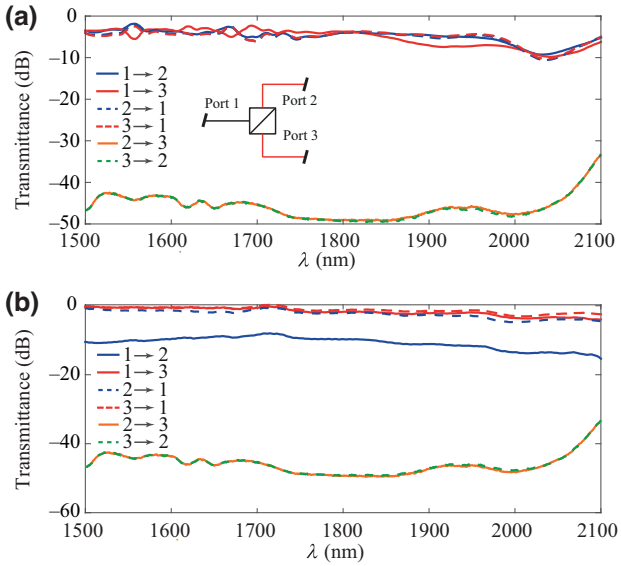

FIG. 6. Measured transmittance for polarizing beam splitter by (a) unpolarized source and (b) polarized source. Solid blue, red and orange lines correspond to the transmittance from port 1 to port 2, from port 1 to port 3, and from port 2 to port 3, respectively. Dashed blue, red, and green lines correspond to the transmittance from port 2 to port 1, from port 3 to port 1, and from port 3 to port 2, respectively.

low attenuation beyond this range. For the supplied voltage correspondent to minimal attenuation, electro-optical VOA did not insert any significant losses at 1650–1750 nm. For longer wavelengths, the attenuation level is lower compared with the datasheet values given for the telecom range.

C. Polarizing beam splitter

Polarizing beam splitter (PBS) is a key optical element for the implementation of some countermeasures. PBS is also placed in Bob's module of SCW QKD to divide polarization components of the signal for their independent modulation. The measurement results are shown in Fig. 6.

Transmittance measurements of the PBS for unpolarized source are almost the same for each arm and direction: around −5 dB in a wide range from 1500 to 2000 nm [Fig. 6(a)]. Transmittance between port 2 and port 3 is nonzero and increased with wavelength. This may be potentially used by Eve for the THA realization due to higher reflectance.

To measure transmittance by the polarized source, we use an additional PBS, which is located prior to the investigated one. The results of these measurements are presented in Fig. 6(b). For the wavelength range 1500–1700-nm transmittance is in a good agreement with the PBS datasheet (its values are within −0.5 dB deviation). For longer wavelengths (up to 1994 nm) minimal transmittance is at least −4.7 dB. Transmittance between port 2 and port 3 is higher in that case compared to unpolarized source measurements. Transmittance from ports 2 and 3 to port 1 are similar, because after the first PBS, signal polarization is aligned with the same axis of polarization-maintaining fiber.

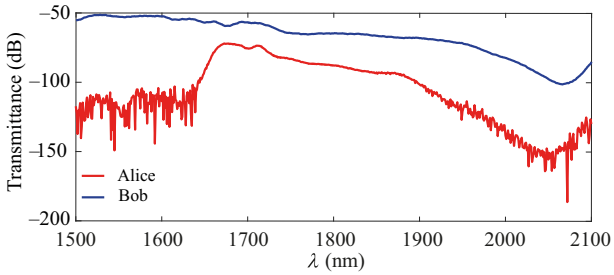

FIG. 7. Integral transmittance of Alice's (red line) and Bob's (blue line) optical schemes, shown in Fig. 1.

IV. COUNTERMEASURES

In the section, we consider possible countermeasures against THA in the wide spectral rage, since some conventional countermeasures have loopholes beyond telecom range that should be taken into account. According to Eqs. (1) and (2), we may estimate the integral transmittance of the studied parts of Alice's and Bob's optical schemes, respectively; they are shown in Fig. 7. To show possible loopholes beyond telecom range we choose elements with higher transmittance in order to ensure the best outcomes for Eve, i.e., the worst case scenario for legitimate users. For example, for determining Alice's transmittance, we use experimental data for the PM and electro-optical VOA with maximal attenuation. We find maximum transmittance for Alice's system to be −71 dB at 1673 nm. The minimum is −185 dB at 2072 nm. VOA mostly affects transmission of Alice's system beyond telecom range, but its effect is balanced by the change in the transmittance of PM. For Bob's system, we use PBS transmittance measured for a polarized source. We should note that after the PBS, the light is aligned with the slow axis for ports 2 and 3, according to the datasheet. This allowed us to use transmittance between ports 2 and 3 as maximal reflectance in Eq. (2), denoted as Ref. Transmittance beyond the telecom range decreases with the wavelength growth. The maximum is at 1801 nm and the minimum is at 2066 nm, with the values −64 dB and −101 dB, respectively. Overall, we may conclude that the investigated scheme requires additional countermeasures beyond telecom range.

There are several ways of preventing the THA, such as utilization of fiber filters based on various filtering principles, circulators, watchdog detectors, and other possible solutions, e.g., Refs. [35–37]. However, not all of them are efficient for a longer wavelength region, in particular

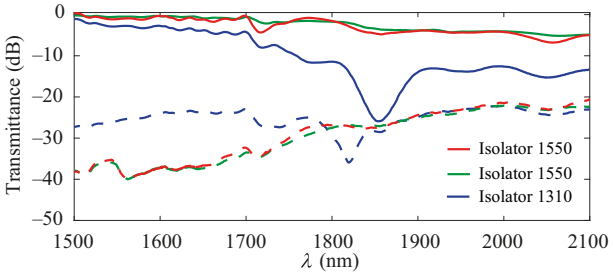

FIG. 8. Measured transmittance of isolators in forward (straight lines) and backward directions (dashed lines), where red and green colors denote results for 1550-nm isolators and blue colors denote results for the 1310-nm isolator.

beyond 1800 nm. For that reason, we investigate transmission spectra of several optical elements, which are conventionally used as quantum hacking countermeasures.

A. Isolators

In many QKD systems, isolators ensure a decrease of outcoming optical power, such as backscattered light or probe pulses used for the THA. Most of the manufacturers usually indicate the value of backward attenuation for the telecom range, but the THA is possible for longer wavelengths. However, the isolator is an example of a fiber optical element with altering properties beyond its normal operational range [14]. That leads to a necessity of measuring their transmittance in a wider spectral range.

In this study, we measure transmittance of three different isolators: two isolators from the same manufacturer (but different batches) with operational range at 1550 nm and one from another manufacturer with operational range at 1310 nm. Results are shown in Fig. 8.

For isolators with operational range at 1550 nm, we find that transmittance in forward direction decreases slowly up to approximately −7 dB. For the isolator with operational range at 1310-nm transmittance decreases rapidly and reaches the minimum at 1853 nm, however within telecom range its attenuation is consistent with datasheet. Backward transmittance for each isolator increases with the growth of scanning wavelength, which is consistent with other experimental [28] and theoretical research [38].

B. WDM components

Another way of additional losses introduction to Eve's probing signals is installation of wavelength-division multiplexing (WDM) components that would cut off wavelengths not used by legitimate users. In the paper, we measure transmittance of coarse WDM (CWDM) and dense (DWDM) components.

CWDM elements from two different manufacturers are studied. We have two samples from one of the manufacturers: CWDM1 and CWDM2 are from different batches;

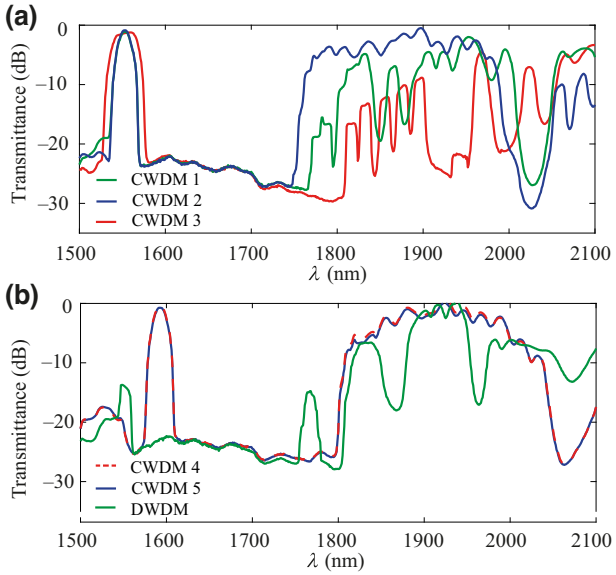

FIG. 9. Measured transmittance of WDM components. (a) Blue and green lines denote results for the same CWDM components from different batches, the red line denotes the result for the CWDM component of another manufacturer; (b) blue line and red dashed line denote results for CWDM components from the same batch, green line corresponds to DWDM component.

CWDM3 came from another manufacturer. Operational wavelength for these CWDMs is 1550 nm. We also have samples CWDM4 and CWDM5 that came from the first manufacturer and from the same batch. However, their operational wavelength is 1590 nm. Results of their measurements are shown in Fig. 9. As can be seen from the figures, each investigated component has wide transmission windows beyond the telecom range. Surprisingly, even though WDM components from the same batch have identical transmittance, components from different batches have noticeably distinct transmission spectra. These peculiarities could be attributed to production technology of thin film filters [39]. This may potentially affect the security of QKD system and should be always considered. The measured DWDM filter spectrum can also be seen in Fig. 9(b) (DWDM) and is similarly characterized by wide transmission windows in 1800–2100-nm range.

Collected data clearly indicates that isolators and WDM filters cannot be implemented as sufficient countermeasures in the investigated spectral region and should be carefully considered and experimentally studied during QKD design.

C. Fiber windings

We therefore suggest using fiber windings in QKD modules as a simple and passive countermeasure to prevent quantum hacking at longer wavelengths. It is known that macrobending losses in a single-mode fiber increase with wavelength. Thus, a section of fiber with a certain length

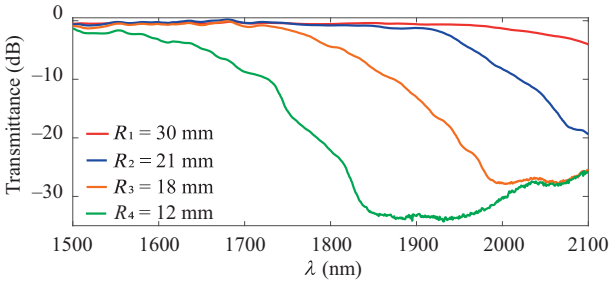

FIG. 10. Single-mode fiber transmission with different winding radii.

bent at a certain radius can act as a spectral filter. To demonstrate this, we install 1 m of single-mode optical fiber with different windings in our QKD modules to measure their transmittance. The results can be seen in Fig. 10.

The windings have low effect on transmission at 1550 nm, QKD system operating wavelength. At the same time, for the longer wavelengths, in particular beyond 1830 nm, it introduces up to 30-dB loss in one direction for the bending radius of 12 mm. As a result, this simple technique is a promising countermeasure against optical probing beyond standard telecommunication wavelength range.

D. Implementation

To analyze the impact of any single element used as a countermeasure (isolator, CWDM component, and fiber windings) we may individually add its transmission values in forward and backward directions to Eqs. (1) and (2). Then we can suggest a combination of these elements to close the THA loophole for the investigated system, as shown in Fig. 11.

Comparing the efficiency of isolators and fiber windings, one can see that an isolator has a higher impact in the telecom range. However, beyond that range the fiber windings provide approximately 30 dB more attenuation than the isolator. CWDM component provides noticeable attenuation in the telecom range except the region around its working wavelength. Moreover, one can see that no single component provides sufficient attenuation against the THA (see the next section), so a combination of elements should be used to achieve that. In our scheme we propose to use one isolator, one CWDM, and one set of fiber windings with 12-mm radius for Alice, which is similar to the countermeasures described in Ref. [36]; the same countermeasures fit for Bob's scheme, but including two isolators. These schemes take into account the disadvantages of each element separately and allows attenuating Eve's scanning signal output to an acceptable level.

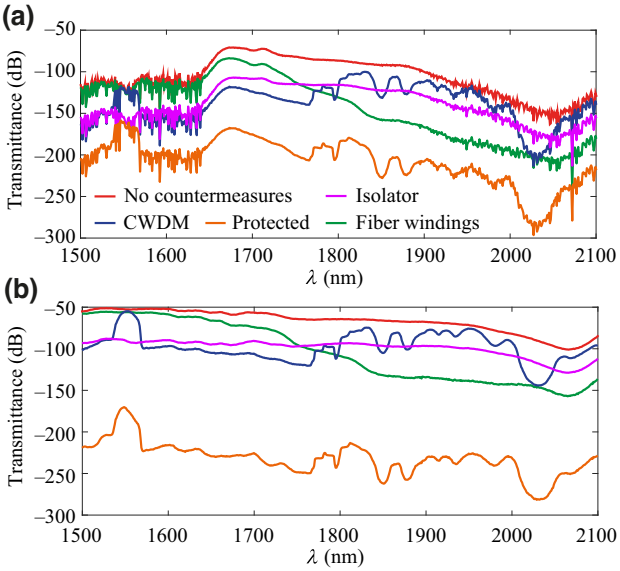

FIG. 11. Application of countermeasures to (a) Alice's system, (b) Bob's system. "No countermeasures" marks Alice's and Bob's transmissions calculated by Eqs. (1) and (2) without any countermeasures, "fiber windings" marks the system's transmission with additionally inserted one fiber windings set, "CWDM" marks the system's transmission with additionally inserted one CWDM-component", "isolator" marks the system's transmission with additionally inserted one isolator, "protected" marks the combination of all described countermeasures against the THA in the system.

V. THEORETICAL CALCULATIONS AND ANALYSIS

As a result of the THA, an eavesdropper can receive information in addition to the attacks on quantum channel. To analyze the eavesdropper's advantage given by the considered attack, we need to estimate the output power from both Alice and Bob. Depending on it, we can calculate the efficiency of the attack. The maximum amount of information that can be obtained from the output can be easily evaluated after reconciliation step using Holevo bound as follows:

$$\chi = S\left(\sum_k p_k \rho_k\right) - \sum_k p_k S(\rho_k), \tag{4}$$

where $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$ is von Neumann entropy, ρ_k is the density matrix of one state from the set and p_k denotes *a priori* probability of the kth state. This quantity may be utilized as the upper bound on additional information; a tighter bound may be found, but this question is out of scope for the paper. However, since we consider the SCW QKD system and the set of pure states, Eq. (4) can be

rewritten as shown in Ref. [40] as follows:

$$\chi(\mu) = h\left(\frac{1-\langle\psi(0)|\psi(\pi)\rangle}{2}\right) \approx h\left(\frac{1-e^{-2\mu}}{2}\right), \quad (5)$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is a binary entropy function, $|\psi(\phi)\rangle$ is a quantum state modulated with a harmonic electrical signal that has phase ϕ, and μ is the mean photon number of all sidebands in the spectrum.

The upper bound on tolerated radiation power in an optical fiber is approximately 10 W, because above this point, a laser can initiate fiber fuse [13,24,41]. We use this value as the upper bound of the input power by an eavesdropper. This amount of power should be scaled by total transmittance T and then converted to the mean number of photons in order to obtain the mean number of photons of output light. For example, 12.8-pW power at 1550-nm wavelength corresponds to 1 mean photon number at 100-MHz repetition (phase change) rate. Also, one should keep in mind that in SCW QKD only sidebands contain information about chosen by legitimate party phase, hence ratio $M < 1$ of the sidebands power to all optical power should be taken into account. Thus, mean photon number of an output probe beam can be estimated by

$$\mu_p = \frac{M \times 10 \times 10^{\frac{T}{10}}}{12.8 \times 10^{-12}} \approx M \times 10^{\frac{T}{10}+11.93}. \quad (6)$$

For further numerical estimations, we assume $M = 0.1$. Then it is straightforward that $\chi(\mu_p)$ is an upper-bound estimation on eavesdropper's information that should be taken into account at the step of privacy amplification. In Fig. 12 dependence of $\chi(\mu_p)$ on the total transmittance T is shown. For $T > -110$ dB, an eavesdropper may obtain almost all key information, while obtained information is rather small for $T < -140$ dB. One may compare these values to the ones shown in Figs. 11(a) and 11(b), where transmittance is not higher than negative 140–150 dB (see "Protected" case, i.e., with all necessary countermeasures applied). The latter values of transmittance correspond to $\chi < 10^{-2}$, which should be taken into consideration at the privacy amplification step.

VI. CONCLUSION

In this paper we experimentally investigate the spectral properties of several conventional QKD components: phase modulators, variable attenuators, isolators, CWDM, and DWDM filters in a spectral range of 1500–2100 nm. We show that transmission of various fiber optical elements beyond telecommunication range (especially 1800 nm and beyond) should be taken into account during QKD system design and development due to the possibility for realization of the THA, as we demonstrate in the brief theoretical analysis. Moreover, even identical optical components from the same manufacturer may have varying optical spectra beyond their normal operational range. We also suggest a simple passive countermeasure against the THA in 1800–2100-nm range based on the violation of total internal reflection in a bent optical fiber. This technique introduces up to 30-dB additional loss at each passing for the winding radius of 12 mm and inserts low losses at 1550 nm.

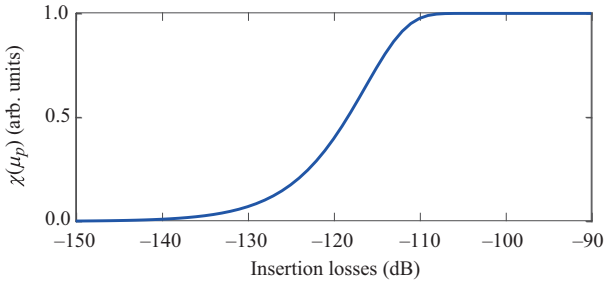

FIG. 12. Holevo bound (5) evaluated for mean photon number of an output probe beam μ_p (6) dependence on transmittance.

Combined countermeasures allow us to achieve a "secure" region at negative 140–150-dB transmittance, where upper-bound estimation on the eavesdropper's information (additional to attacks in a quantum channel) is rather low, $\chi < 10^{-2}$. Derived expression $\chi(\mu_p)$, composed by Eqs. (5) and (6) (or analogous expression suitable for different QKD systems), may be utilized in order to make express estimations on eavesdropper's information that should be additionally taken into consideration at the privacy amplification step. As an alternative, derived expression $\chi(\mu_p)$ may be utilized for a QKD system optical design, where one may determine insertion-loss threshold for keeping χ considerably low.

ACKNOWLEDGMENTS

The study is partially funded by the Ministry of Education and Science of the Russian Federation (Passport No. 2019-0903).

APPENDIX A: ALTERNATIVE SCHEMES

There are various possible scenarios for the implementation of the THA. The other options should be considered for a rigorous security estimations when analyzing the possibility of implementing the attack. Due to the features of the system under consideration, an eavesdropper can potentially implement one of the following options as an alternative to the one described by Eq. (2):

$$T_{B1} \approx T_{\mathrm{PBS1}_{12}} + T_{PM1_f} + \mathrm{Ref}_{\mathrm{port2}} + T_{PM1_b} + T_{\mathrm{PBS1}_{21}}, \quad (A1)$$

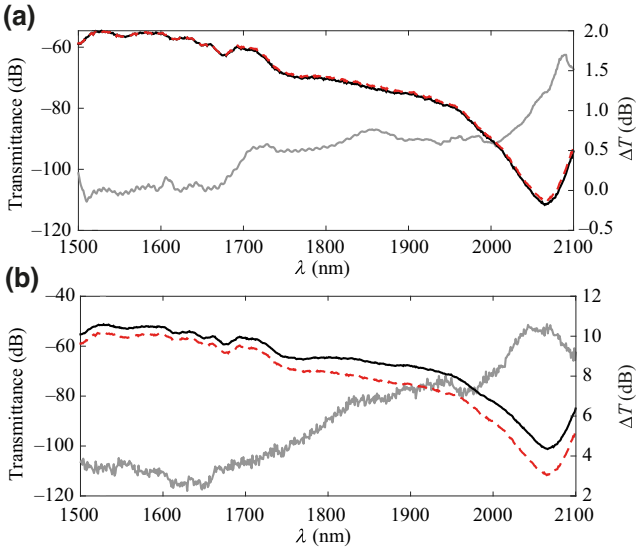

FIG. 13. Integrated transmittance of Bob's optical scheme: (a) red dashed line corresponds to Eq. (A1), black line corresponds to Eq. (A2), and gray line corresponds to the difference between them; (b) red dashed line corresponds to Eq. (A1), black line corresponds to Eq. (2), and gray line corresponds to difference between them. The left scale is for the calculated transmittance and the right scale for the difference between them.

or

$$T_{B2} \approx T_{\mathrm{PBS1}_{13}} + T_{PM2_f} + \mathrm{Ref}_{\mathrm{port3}} + T_{PM2_b} + T_{\mathrm{PBS1}_{31}}, \tag{A2}$$

or an intermediate option, in which part of the radiation of the probing pulses is divided between the ports of the beam splitter according to the power ratio of the polarization components and the characteristics of the polarization beam splitter used. For such a case, each arm of the scheme under consideration will also be described by Eqs. (A1) and (A2), taking into account the correction term related to what part of the initial power of the probing pulses propagated into the corresponding arm. A limitation of the maximum power that can be used to implement the THA and cannot exceed 10 W remains, which will not allow implementing additional polarization multiplexing in order to increase the power used. After passing through the polarization beam splitter, polarization states in ports 2 and 3 are aligned with the slow axis of the polarization maintaining fiber, which is a feature of the polarization beam splitter used; this is necessary for the effective operation of phase modulators. It should be noted that the phase modulators in the scheme operate simultaneously and apply the same phase shift. After reflection from the connector, the radiation goes back to the polarization beam splitter, where the polarization multiplexing of the reflected pulses takes place. In the case of simultaneous arrival of pulses, their interference is possible due to imperfections of the polarization beam splitter, which negatively affects the extracting of the phase of the reflected pulses by an eavesdropper. Thus, it seems optimal for an eavesdropper to use only one of the arms to extract information. The calculated transmissions for Eqs. (A1) and (A2) are shown in Fig. 13(a). From the figures, it can be concluded that the data slightly differ.

Next, we may compare the data obtained for Eq. (2) with the data for Eq. (A1) from the main body of the paper in Fig. 13(b). It can be seen that in the entire wavelength range, the calculated transmission as considered in the main body of the paper is greater than for the case considered here.

It implies that the former is optimal for analyzing the possibility of implementing the THA and allows a more conservative assessment of the system security in the first approximation. We emphasize, for the case of a detailed study of the system, it is necessary to consider all possible options for the transmission of the system upon reflection from various elements and select those that correspond to the minimum introduced attenuation of scanning pulses and allows extracting additional information.

APPENDIX B: ERROR CALCULATIONS

We repeat all measurements 10 times and then estimate the mean transmitted power as follows:

$$\bar{P} = \frac{\sum_{i=1}^{n} P_i}{n}. \tag{B1}$$

The standard deviation can be expressed as follows:

$$S_P = \sqrt{\frac{\sum_{i=1}^{n} (\bar{P} - P_i)^2}{n(n-1)}}. \tag{B2}$$

Then we may calculate the measurement error as follows:

$$\Delta P = t S_P, \tag{B3}$$

where t is the Student coefficient. We use $t = 2.764$, which corresponds to 99% confidence interval for ten measurements.

We calculate the transmittance as follows:

$$T_{\mathrm{dB}} = -10 \log_{10}(P_{\mathrm{ref}} * T_f / P_{\mathrm{mes}}), \tag{B4}$$

where P_{ref} is the mean measured power without an element under test, P_{mes} is the mean measured power with an element under test, T_f is filter transmission.

We have calculated the error as follows:

$$\Delta T_{\mathrm{dB}} = \sqrt{\left(\frac{\partial T_{\mathrm{dB}}}{\partial P_{\mathrm{ref}}} \Delta P_{\mathrm{ref}}\right)^2 + \left(\frac{\partial T_{\mathrm{dB}}}{\partial P_{\mathrm{mes}}} \Delta P_{\mathrm{mes}}\right)^2}, \tag{B5}$$

where ΔP_{ref} is the calculated error for P_{ref} and ΔP_{mes} is the calculated error for P_{mes}. Errors are shown in Fig. 14.

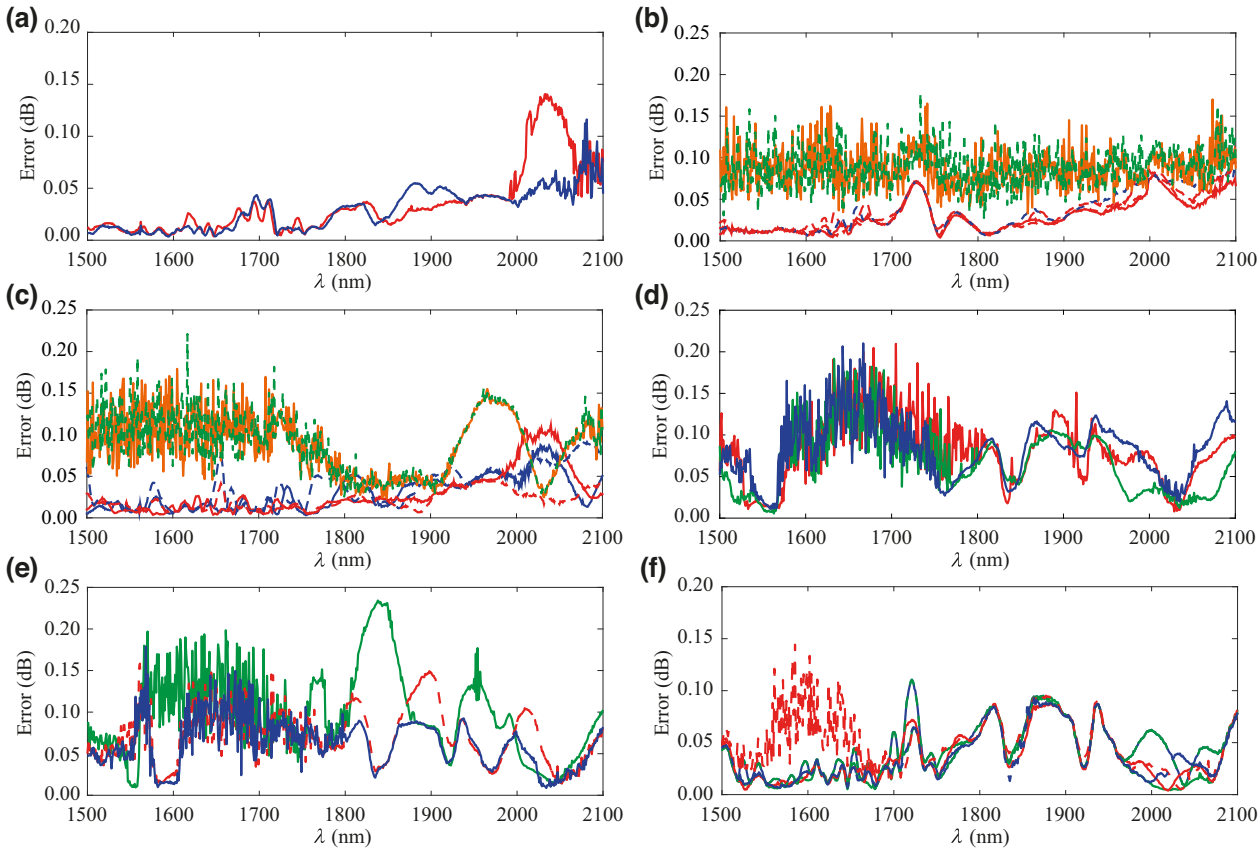

FIG. 14. Calculated errors for (a) phase modulator, where the blue line is for forward connection and the red line is for backwards connection. (b) PBS with unpolarized source, where the blue line is transmittance from port 1 to port 2, the red line is transmittance from port 1 to port 3, and dashed lines are for reverse connections. (c) PBS with polarized source, where the blue line is transmittance from port 1 to port 2, the red line is transmittance from port 1 to port 3, the red dashed line is transmittance from port 2 to port 1, the blue dashed line is transmittance from port 3 to port 1, the orange line is transmittance from port 2 to port 3, the green dashed line is transmittance from port 3 to port 2. (d) Isolators, where red and green lines are for 1550-nm isolators (straight lines in forward direction and dashed in backwards), green lines are for the 1310-nm isolator. (e) CWDM components, where the green line is for CWDM1, the blue line is for CWDM2, and the red line is for CWDM3; (f) CWDM and DWDM components, where the red dashed line is for CWDM5, blue is for CWDM6, and the green line is for DWDM.

[1] Artur K. Ekert, in *Quantum Measurements in Optics*, p. 413. Springer, 1992.

[2] Charles H. Bennett, Gilles Brassard, and N. David Mermin, Quantum Cryptography Without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[3] Peter W. Shor and John Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[4] Nitin Jain, Hou-Man Chin, Hossein Mani, Cosmo Lupo, Dino Solar Nikolic, Arne Kordts, Stefano Pirandola, Thomas Brochmann Pedersen, Matthias Kolb, and Bernhard Ömer, *et al.*, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 1 (2022).

[5] Andrei Gaidash, George Miroshnichenko, and Anton Kozubov, Subcarrier wave quantum key distribution with leaky and flawed devices, JOSA B **39**, 577 (2022).

[6] Anton Kozubov, Andrei Gaidash, and George Miroshnichenko, Quantum control attack: Towards joint estimation of protocol and hardware loopholes, Phys. Rev. A **104**, 022603 (2021).

[7] 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).

[8] Yi Zhao, Chi-Hang Fred Fung, Bing Qi Christine Chen, and Hoi-Kwong Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[9] 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).

[10] 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).

[11] S. N. Molotkov, K. A. Balygin, A. N. Klimov, and S. P. Kulik, Active sensing and side channels of information leakage in quantum cryptography, Laser Phys. **29**, 124001 (2019).
[12] Paulo Vinicius Pereira Pinheiro, Poompong Chaiwongkhot, Shihan Sajeed, Rolf T. Horn, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov, Eavesdropping and countermeasures for back-flash side channel in quantum cryptography, Opt. Express **26**, 21020 (2018).
[13] Anqi Huang, Ruoping Li, Vladimir Egorov, Serguei Tchouragoulov, Krtin Kumar, and Vadim Makarov, Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution, Phys. Rev. Appl. **13**, 034017 (2020).
[14] Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhot, Vladimir Egorov, Vadim Makarov, and Anqi Huang, Protecting Fiber-Optic Quantum Key Distribution Sources Against Light-Injection Attacks, PRX Quantum **3**, 040307 (2022).
[15] Artem Vakhitov, Vadim Makarov, and Dag R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. **48**, 2023 (2001).
[16] Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).
[17] Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New J. Phys. **16**, 123030 (2014).
[18] 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).
[19] Yaxi Pan, Ling Zhang, and Duan Huang, Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution, Appl. Sci. **10**, 7788 (2020).
[20] Vadim Makarov, Controlling passively quenched single photon detectors by bright light, New J. Phys. **11**, 065003 (2009).
[21] Lars Lydersen, Mohsen K. Akhlaghi, A. Hamed Majedi, Johannes Skaar, and Vadim Makarov, Controlling a superconducting nanowire single-photon detector using tailored bright illumination, New J. Phys. **13**, 113042 (2011).
[22] Vladimir Chistiakov, Anqi Huang, Vladimir Egorov, and Vadim Makarov, Controlling single-photon detector ID210 with bright light, Opt. Express **27**, 32253 (2019).
[23] M. K. Barnoski, M. D. Rourke, S. M. Jensen, and R. T. Melville, Optical time domain reflectometer, Appl. Opt. **16**, 2375 (1977).
[24] Raman Kashyap, The fiber fuse-from a curious effect to a critical issue: A 25th year retrospective, Opt. Express **21**, 6422 (2013).
[25] Nitin Jain, Birgit Stiller, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs, Risk analysis of trojan-horse attacks on practical quantum key distribution systems, IEEE J. Sel. Top. Quantum Electron. **21**, 168 (2014).
[26] Ivan S. Sushchev, Diana M. Guzairova, Andrey N. Klimov, Dmitriy A. Dvoretskiy, Sergey A. Bogdanov, Klim D. Bondar, and Anton P. Naumenko, in *Emerging Imaging and Sensing Technologies for Security and Defence VI*, volume 11868, p. 57. SPIE, 2021.
[27] Shihan Sajeed, Carter Minshull, Nitin Jain, and Vadim Makarov, Invisible trojan-horse attack, Sci. Rep. **7**, 1 (2017).
[28] A. V. Borisova, B. D. Garmaev, I. B. Bobrov, S. S. Negodyaev, and I. V. Sinil'shchikov, Risk analysis of countermeasures against the trojan-horse attacks on quantum key distribution systems in 1260–1650 nm spectral range, Opt. Spectrosc. **128**, 1892 (2020).
[29] B. A. Nasedkin, I. M. Filipov, A. O. Ismagilov, V. V. Chistiakov, F. D. Kiselev, A. N. Tsypkin, and V. I. Egorov, Analyzing transmission spectra of fiber-optic elements in the near ir range to improve the security of quantum key distribution systems, Bull. Russ. Acad. Sci.: Phys. **86**, 1164 (2022).
[30] K. D. Stock and R. Heine, Spectral characterization of InGaAs trap detectors and photodiodes used as transfer standards, Metrologia **37**, 449 (2000).
[31] Shihan Sajeed, Poompong Chaiwongkhot, Anqi Huang, Hao Qin, Vladimir Egorov, Anton Kozubov, Andrei Gaidash, Vladimir Chistiakov, Artur Vasiliev, and Artur Gleim, *et al.*, An approach for security evaluation and certification of a complete quantum communication system, Sci. Rep. **11**, 1 (2021).
[32] Anton V. Tausenev, Petr Georgievich Kryukov, Mikhail Mikhailovich Bubnov, Mikhail Evgen'evich Likhachev, E. Yu Romanova, Mikhail Viktorovich Yashkov, Vladimir Fedorovich Khopin, and M. Yu Salganskii, Efficient source of femtosecond pulses and its use for broadband supercontinuum generation, Quantum Electron. **35**, 581 (2005).
[33] Ashutosh Rao and Sasan Fathpour, Heterogeneous thin-film lithium niobate integrated photonics for electrooptics and nonlinear optics, IEEE J. Sel. Top. Quantum Electron. **24**, 1 (2018).
[34] Ed L. Wooten, Karl M. Kissa, Alfredo Yi-Yan, Edmond J. Murphy, Donald A. Lafaw, Peter F. Hallemeier, David Maack, Daniel V. Attanasio, Daniel J. Fritz, and Gregory J. McBrien, *et al.*, A review of lithium niobate modulators for fiber-optic communications systems, IEEE J. Sel. Top. Quantum Electron. **6**, 69 (2000).
[35] Nitin Jain and Gregory S. Kanter, Upconversion-based receivers for quantum hacking-resistant quantum key distribution, Quantum Inf. Process. **15**, 2863 (2016).
[36] 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).
[37] Gong Zhang, Ignatius William Primaatmaja, Jing Yan Haw, Xiao Gong, Chao Wang, Charles Ci, and Wen Lim, Securing Practical Quantum Communication Systems with Optical Power Limiters, PRX Quantum **2**, 030304 (2021).
[38] Michał Berent, Andon A. Rangelov, and Nikolay V. Vitanov, Broadband Faraday isolator, JOSA A **30**, 149 (2013).

[39] Pei-fu Gu and Zhen-rong Zheng, Design of non-polarizing thin film edge filters, J. Zhejiang Univ.-Sci. A **7**, 1037 (2006).

[40] 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).

[41] Donald D. Davis Jr, Stephen C. Mettler, and David J. DiGiovanni, in *Laser-Induced Damage in Optical Materials: 1996*, volume 2966, p. 592. SPIE, 1997.