

Wide-Spectrum Security of Quantum Key Distribution

Hao Tan,^{1,2,3,*} Mikhail Petrov,^{4,*} Weiyang Zhang⁵,⁵ Liying Han,^{1,2} Sheng-Kai Liao,^{1,2,5}
Vadim Makarov,^{2,4,†} Feihu Xu,^{1,2,5,‡} and Jian-Wei Pan^{1,2,5}

¹*Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, People's Republic of China*

²*Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, People's Republic of China*

³*China Telecom Quantum Information Technology Group Co., Ltd., Hefei 230088, People's Republic of China*

⁴*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*

⁵*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, People's Republic of China*



(Received 2 December 2024; revised 18 August 2025; accepted 24 September 2025; published 12 November 2025; corrected 15 May 2026)

Implementations of quantum key distribution (QKD) need vulnerability assessment against loopholes in their optical scheme. Most of the optical attacks involve injecting or receiving extraneous light via the communication channel. An eavesdropper can choose her attack wavelengths arbitrarily within the quantum channel passband to maximize the attack performance, exploiting spectral transparency windows of system components. Here we propose a wide-spectrum security evaluation methodology to achieve full optical spectrum safety for QKD systems. This technique requires transmittance characterization in a wide spectral band with a high sensitivity. We report a testbench that characterizes insertion loss of fiber-optic components in a wide spectral range of 400–2300 nm and up to 70 dB dynamic range. To illustrate practical application of the proposed methodology, we give a full Trojan-horse attack analysis for some typical QKD system configurations and discuss briefly induced-photorefractive and detector-backflash attacks. Our methodology can be used for certification of QKD systems.

DOI: [10.1103/smdh-dcpm](https://doi.org/10.1103/smdh-dcpm)

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows two remote parties to share secure keys with proven security. Although QKD is proven to be information-theoretically secure, there are gaps between the characteristics of practical devices and their theoretical models [3]. In such cases, an eavesdropper Eve might perform attacks and eavesdrop the secure key, compromising the security of QKD systems [4]. In QKD's structure, the communicating parties Alice and Bob reside in physically secure locations, and Eve cannot access them directly. However, the communication channel is controlled by Eve, and she can inject

light into Alice's and Bob's apparatuses through this channel to affect the state of internal components and also extract light reflected or emitted from them. Thus some of the most threatening strategies are light-injection and unintended-light-emission attacks [5–24].

For the transmitters of QKD systems, Eve can inject light in order to eavesdrop modulator's encoding information via reflected light [5,6,12], alter the performance of the laser [15,18,25], damage the optical devices [20,22], change the operating characteristics of phase and intensity modulators [23,24] and energy meters [13]. For the receivers of QKD systems, Eve can inject light to control the detectors [7,8,10], damage them [14], eavesdrop modulator's encoding information [12,26], or receive light emission from avalanche photon detectors leaked back into the communication channel [16,17,27].

Normally, QKD systems need to deploy additional passive optical devices, such as isolators, attenuators, and spectral filters, to mitigate the effects of these attacks [21,22,28]. However, the transmittance of these passive optical devices is typically specified only around their design wavelength, and shows significant deviations at other wavelengths, which may lead to potential spectral

*These authors contributed equally.

†Contact author: makarov@vad1.com

‡Contact author: feihuxu@ustc.edu.cn

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

side-channels. The communication channel itself, either free-space or optical fiber, is transparent in a very wide spectral range. Eve can thus choose her working wavelength arbitrarily to maximize the attack performance. For example, the reverse transmittance of isolators and circulators designed for 1550 nm rises significantly in the 1000–1400 nm wavelength range [29]. This spectral side-channel may provide a valuable “window of attack” for eavesdroppers and compromise the security of QKD systems. In another example, a Trojan-horse attack on a 1550 nm QKD receiver becomes feasible at 1924 nm [26]. An avalanche backflash is spectrally broad, spanning hundreds of nanometers [16,17]. Recently, an induced-photorefractive attack using light at 532 [24] and 405 nm [23] has been investigated, which results in significant changes in the refractive index and transmittance of lithium-niobate phase and intensity modulators. Therefore, we need to carefully analyze the vulnerability of optical components in a wide spectral range and propose appropriate countermeasures accordingly to guarantee the full-spectrum resistance to attacks in QKD systems. This will be necessary for upcoming certification of QKD [30–34]. This applies to both discrete-variable and continuous-variable systems, as the latter are also susceptible to Trojan-horse, induced-photorefractive, and other wavelength-dependent attacks [30,35,36].

Here we propose a characterization methodology to achieve this. We consider a general approach for protection of cryptographic modules and classify attacks into three cases (see Sec. II). We build an experimental testbench that can characterize transmittance of fiber-optic components in a wide spectral range of 400 to 2300 nm. We supplement the cryptographic module with a bandpass physical filter that guarantees a strong suppression of all light outside this characterization window. This allows us to find the weakest spectral spot in the protection of a QKD scheme against each attack. The information leakage is quantified at this wavelength, then if necessary the protection is improved (by, e.g., installing additional isolating components or changing the optical scheme) to a point where the attack does not impair QKD performance.

We demonstrate our methodology on examples of the Trojan-horse attack (THA), induced-photorefractive, and detector-backflash attacks. For the former, we consider three QKD source configurations and characterize each optical component in these configurations using our testbench. The optical components include isolators, circulators, variable optical attenuators, filters, and fiber coils. These devices exhibit different transmission characteristics across the wavelength spectrum. Based on these measurements, we analyze the secure key rate under THA for two QKD schemes—prepare-and-measure BB84 and measurement-device-independent—using existing security proofs and identify the source configuration that makes each scheme fully resistant to this attack.

We then consider briefly the two other types of attacks, induced-photorefractive and detector-backflash.

This paper is organized as follows. We discuss the wide-spectrum security evaluation methodology in Sec. II. Section III introduces the testbench hardware and test methodology. In Sec. IV, we discuss how to design the bandpass physical filter. We give application examples in Sec. V and conclude in Sec. VI.

II. METHODOLOGY

Eavesdropping attacks on a QKD system involve either Eve’s light injection via a quantum channel to affect a specific internal component or analysis of the system’s unintended light emission. In the first scenario, Eve controls an individual component or obtains information about it via reflected light. In the second scenario she does not inject light into the system, but only registers and analyzes the light emitted. In both scenarios, the transparency of her attack channel (i.e., that of components between the target and the quantum channel) is essential. If it is attenuating light too much, Eve is unable to affect the target component and cannot collect enough photons coming out of the system that contain secret information. Typically, QKD vulnerability is assessed only at the operating wavelength (most common in C-BAND), but it is essential to consider how transparent the attack channel is throughout the entire spectral range available via the quantum channel. A spectral transparency window allows Eve to more actively target QKD internal components or get a more intense light signal from them, and as a result, steal more information. For each possible attack scenario, the QKD vulnerability analysis involves identifying the optimal wavelength (from Eve’s viewpoint) corresponding to the maximum level of component interference or light leakage, and subsequent estimate of the maximum information leakage from the QKD devices. The analysis for a particular QKD implementation consists of several steps.

- (1) The QKD implementation is analyzed for the feasibility of all currently known attacks (similarly to Refs. [31,33]).
- (2) For each possible attack, the attack channel and list of its constituent components are defined.
- (3) The transmission of each of these components is characterized over a wide spectrum.
- (4) The total transmission spectrum of the attack channel is calculated as a product of the individual component transmittances.
- (5) The response of the target component to illumination at different wavelengths or its emission spectrum is characterized.
- (6) The maximum power of Eve’s light at the target component at the optimal wavelength for attack or total power exiting the QKD system is estimated.

- (7) From this estimate, the amount of information leakage is evaluated using existing security proofs or other experimental studies.

This wide-spectrum methodology is applicable for a very broad class of attacks on QKD systems with different protocols and internal designs. The vulnerability analysis for each specific QKD implementation should be performed individually. Every system is unique and susceptible to its own specific set of attacks [30,31,33,36]. Each has its own set of components, moreover the properties of components of the same type differ from one manufacturer to another.

More formally, the methodology is the following. To evaluate security against a light-injection or light-emission attack, one needs to know the spectral response of its target component to the attack light $S(\lambda)$ and the total transmittance of an attack channel that the light traverses inside the cryptography equipment during the attack $\gamma(\lambda)$. Both parameters are wavelength-dependent. Then, a secure key rate $R = K[S(\lambda), \gamma(\lambda)]$ is calculated. Our study is primarily concerned with the measurement of $\gamma(\lambda)$, which can be done in a uniform way. The measurement of $S(\lambda)$ and derivation of the function K are attack-specific, though we discuss some examples of these below.

From Eve's perspective, a secure cryptographic module (such as Alice or Bob) has a structure shown in Fig. 1. The target component of Eve's attack T is connected to the quantum channel, where Eve resides, via optical components P_1 to P_N and a filter F (which we explain later). Behind T , non-zero backreflections from connectors and other components always exist [5], collectively denoted by a reflection coefficient M .

An important parameter for Eve's attack is the total transmittance of the attack channel $\gamma(\lambda)$. The light suffers attenuation as it passes every component on its way. We classify Eve's attacks into three cases.

Case 1. For light-injection attacks such as laser-seeding, laser-pumping, induced-photorefractive, laser-damage, detector-efficiency-mismatch, and tampering with

a power meter, the attack channel is unidirectional from Eve to T . Then

$$\gamma(\lambda) = F(\lambda) \prod_{i=1}^N P_i^{\text{in}}(\lambda), \quad (1)$$

where P_i^{in} denotes a transmittance of component in the inward light propagation direction. While many optical components tend to have the same transmittance in both directions, some may be slightly direction-dependent or even be designed for strong non-reciprocity, such as optical isolators and circulators. For simplicity, we assume the filter's transmittance F is the same in both directions.

Case 2. Another case is a leakage of photons generated inside the cryptographic module into the communication channel, of which we currently know one example, the detector-backflash attack. In this case, the attack channel is unidirectional from T to Eve. Its total transmittance

$$\gamma(\lambda) = F(\lambda) \prod_{i=1}^N P_i^{\text{out}}(\lambda), \quad (2)$$

where P_i^{out} is the component's transmittance in the outward direction. In these two cases, reflection M is neglected.

Case 3. The third case is the Trojan-horse attack where Eve injects light and receives a fraction of it reflected back, to learn the state of the modulator. The attack channel is thus a round-trip. Then

$$\gamma(\lambda) = [F(\lambda)]^2 T^{\text{in}}(\lambda) T^{\text{out}}(\lambda) M(\lambda) \prod_{i=1}^N P_i^{\text{in}}(\lambda) P_i^{\text{out}}(\lambda), \quad (3)$$

where T^{in} and T^{out} is the transmittance of the target modulator in either direction. Estimating a reliable upper bound on M is experimentally difficult, owing to the possibility of constructive interference between multiple reflections Eve might exploit, high temporal resolution required, and possible dependence of reflections on wavelength [34]. Also, an internal reflection inside the target modulator behind its active section may contribute, excluding part of the modulator's attenuation. To avoid these challenges, it is much easier to conservatively assume $T^{\text{in}} T^{\text{out}} M = 1$ [34]. Then Eq. (3) simplifies to

$$\gamma(\lambda) = [F(\lambda)]^2 \prod_{i=1}^N P_i^{\text{in}}(\lambda) P_i^{\text{out}}(\lambda). \quad (4)$$

Since $\gamma(\lambda)$ is a product of individual transmittances (i.e., any possible interference effect involving reflections is neglected), it can be computed from transmittances of the individual optical components. We measure these with our

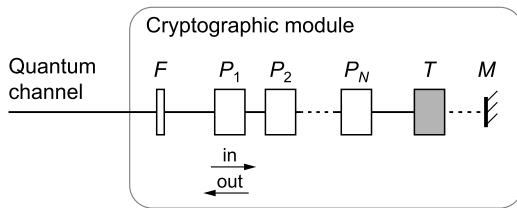


FIG. 1. General structure of a cryptographic module from Eve's point of view. An optical component T is the target of attack. It is separated from the quantum channel by other optical components P_1 to P_N and a broadband bandpass physical filter F that blocks very short and very long wavelengths. For some attacks, a backreflection M behind T should be taken into account.

testbench reported below, which covers a wide but finite spectral range. The transmittance of components remains unknown outside this characterization range. We thus need to supplement each cryptographic module with the filter F that guarantees light suppression outside this range by its design (discussed in Sec. IV).

The susceptibility of the target component itself to the attack light $S(\lambda)$ also varies with wavelength. While for treatment of the Trojan-horse attack it may reasonably (and conservatively) be assumed to be spectrally flat [28], for most attacks it varies strongly with wavelength [15,18,23,24,26]. For instance, Alice’s laser is much more responsive to seeding by light near its emission wavelength [15,18] and Bob’s avalanche photodiode emits its backflash in a broad but limited spectral band [16,17,27]. Characterizing this susceptibility and attack mechanisms is outside the scope of our present study.

Finally, the form of function K also depends on the attack. Often, Eve’s best strategy is to exploit the maximum response $\max_{\lambda}[\gamma(\lambda)S(\lambda)]$ and inject light at that single wavelength, such as, for example, in the Trojan-horse [28] and induced-photorefractive [23,24] attacks. However, some attacks may be best executed at multiple discrete wavelengths or over a certain spectrum. For instance, in the detector-backflash attack, the probability of a photon leaking into the quantum channel should be integrated over the entire emission spectrum $\int_{\lambda} \gamma(\lambda)S(\lambda) d\lambda$, where $S(\lambda)$ is the measured probability density of photon emission from the avalanche photodetector. The key rate formula K is further given by a relevant security proof that accounts for the attack or for several attacks simultaneously. In Sec. V, we give some examples of this analysis for particular attacks.

III. SPECTRAL CHARACTERIZATION TESTBENCH

Manufacturers of components typically do not document their spectral characteristics over the entire transparency range of the quantum channel that can be used by Eve. We thus have to measure the component transmittance ourselves. This measurement should have a wide dynamic range, because the component may have a low transmittance. Here we implement the testbench proposed in Ref. [31]. It consists of a wideband light source, fiber coupler, and spectrum analyzer (Fig. 2). We use a supercontinuum laser source (NKT Photonics SuperK Fianium FIU-15) that emits “white light” of about 350–2400 nm spectrum with variable pulse repetition rate of 15–78 MHz and total power of up to 7 W [37]. Compared to a previous testbench [38], the spectral coverage of our testbench is wider, facilitating the analysis of attacks in specific bands, such as the induced-photorefractive attack [23, 24]. The power can be trimmed by lowering the pulse rate. Although its output is already single-mode in a

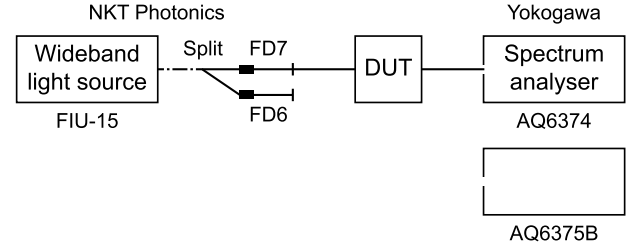


FIG. 2. Scheme of the spectral characterization testbench. DUT, device under test.

large-core-diameter fiber, it needs to be coupled into the standard single-mode fiber used by the components we test. The fiber coupler consists of a dichroic splitter (NKT Photonics SuperK Split [39]) that separates the spectrum into two 400–900 nm and 900–2400 nm outputs, each fitted with a tunable fiber coupler (NKT Photonics SuperK Connect FD7 and FD6, respectively [40]). The testbench operator manually connects the device under test (DUT) to these outputs sequentially to scan the entire wavelength range. Likewise, two spectrum analyzers are used interchangeably to cover the entire wavelength range: Yokogawa AQ6374 (350–1750 nm [41]) and AQ6375B (1200–2400 nm [42]).

We limit the total power at the input of DUT to 0.5 W, to avoid damage to fiber patchcords and the spectrum analysers. The power is lowered further for temperature-sensitive DUTs, such as variable attenuators and narrow spectral filters. Incidentally, the dichroic splitting into the two bands helps to suppress ghosts due to higher-order diffraction in the spectrometers. We limit our total characterization range to 400–2300 nm, because below 400 nm the light source has low spectral flux and the spectrometer has higher noise, and above 2300 nm the suppression of the ghost in the spectrometer is poor. To overcome the limitation of characterization wavelength range and ensure security beyond it, we design physical filters to limit Eve’s attack wavelengths, which will be discussed in Sec. IV.

Obtaining the component’s transmittance consists of a scan of the light source (done with the DUT replaced with a patchcord) followed by the same scan with the DUT in place. We have verified that the source and the rest of the setup remain stable between these scans. The DUT’s transmittance is then a ratio of the spectral flux measured with the DUT and without the DUT. In logarithmic units of spectral flux, the ratio is replaced with subtraction. The entire spectrum is covered by repeating these scans in three setup configurations and stitching them together, with the stitching point between the splitter’s outputs being at 900 nm and between the two spectrometers at 1650 nm. A typical source scan is shown in Fig. 3(a). It also shows the spectrometer dark noise level and its smoothed upper envelope obtained by a local maximum method combined with a cubic spline interpolation (function “Envelope” in OriginPro software). The difference between the measured

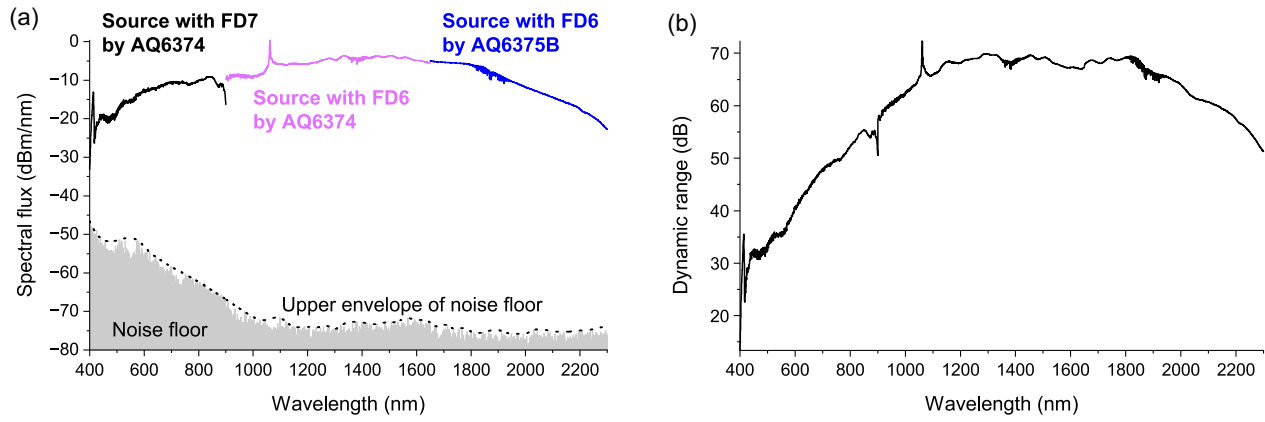


FIG. 3. Spectral performance of the testbench. (a) Spectrum of the light source (measured with the DUT replaced with a patchcord) and the analyzer's dark noise, at 1 nm resolution. (b) The resulting dynamic range of the transmittance measurement. This data is at about 0.5 W at the DUT; the dynamic range will be narrower at a lower power.

source flux and the noise envelope gives the dynamic range of our transmittance measurement, plotted in Fig. 3(b). It is above 65 dB in the central part (1100–1900 nm) and drops to 30–50 dB at the edges. When the component's insertion loss at a given wavelength is higher than that, we are unable to measure its transmittance and have to replace it with a value given by the noise envelope, for security evaluation purposes. We are thus able to guarantee the reliability of the measurement data. Although this approach is conservative, it gives adequate results when applied to typical QKD configurations, as the reader will see in Sec. V.

The spectral characterization is done with 1 nm resolution, which is sufficient for most components. If the component contains a Bragg grating filter or other structure that produces sharp spectral features, the scan resolution can be increased to 0.05 nm, at the cost of a lower dynamic range.

IV. DESIGN OF A BROADBAND BANDPASS PHYSICAL FILTER

The standard single-mode fiber may transmit light outside the characterization wavelength range of our testbench. Since the behavior of the system components there remains unknown, a supplementary filter F is needed. This filter should guarantee suppression of short- and long-wavelength light to a secure level even if all the other system components are conservatively assumed to be transparent. This completes the system certification against the attack. The suppression has to be provided by the physical design of the filter rather than by our measurement.

For long-wavelength suppression, bend loss of the fiber may be used. If the fiber is coiled with a sufficiently small radius, it loses its waveguiding properties at longer wavelengths, releasing light into the cladding where it is emitted or absorbed in the coating [43]. The smaller the bending

radius, the higher the loss of the fiber. Furthermore, light with long wavelength is more easily leaked out of the fiber at a specific radius. For example, a standard single-mode fiber exhibits high loss at longer wavelengths, see our measurement in Fig. 4. The effective cutoff wavelength depends on the bend radius, with 15 mm radius being suitable for a typical QKD system. This broadly agrees with the theory, which predicts a significant increase in bend loss at 1550 nm when the radius is less than 12 mm [43]. A previous experiment [44] shows that a single-loop coil of 15 mm radius has about 30 dB attenuation at 2250 nm and virtually no attenuation at 1550 nm, which also roughly agrees with our result. The high residual transmission observed in Fig. 4 at longer wavelengths is probably an artefact of our quick measurement, and should be verified

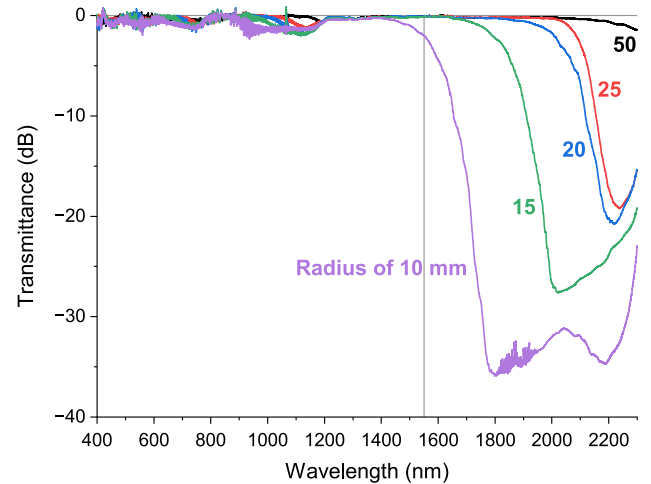


FIG. 4. Transmittance of a 2 m long single-mode fiber patchcord coiled for its entire length with different radii. The fiber is Corning SMF-28e+ with 242 μm diameter coating inside a 0.9 mm outer diameter loose jacket, made into the patchcord with FC/UPC connectors (Optizone Technology P-55-R-11-L-F-2).

in a more carefully controlled test with a different turn number and the coil being connected in series with other system components to filter out cladding modes.

For short-wavelength suppression, well-understood optical properties of bulk material may be used. For example, pure Si has an absorption coefficient $\alpha \gtrsim 10^5 \text{ cm}^{-1}$ in 250–400 nm range, while being virtually transparent ($\alpha < 1 \text{ cm}^{-1}$) past 1140 nm [45,46]. A filter can be manufactured inexpensively by inserting a several-millimeter-thick silicon optical window into a fiber-pigtailed collimator bench. Its cutoff may be shifted to a shorter wavelength by selecting a semiconductor material with a wider bandgap than that of Si (1.12 eV [47]). For example, GaAs (GaP) with the bandgap of 1.42 (2.26) eV [47] has the cutoff wavelength around 870 (550) nm.

The design of these filters should be finalized together with the system manufacturer and further verified by tests and theoretical calculations. To protect F against laser damage, it may have to be placed not at the channel entrance as shown in Fig. 1, but behind other components [22]. This is future work.

V. APPLICATION EXAMPLES

While our wide-spectrum methodology can be used for vulnerability assessments for every known attack that depends on light injection or emission, we give a few examples of its use. First, we give a full analysis (complete with the key rate calculation) of the Trojan-horse attack for some typical QKD system configurations. Then we discuss briefly how to approach two other types of attacks, induced-photorefractive and detector-backflash.

A. Trojan-horse attack

In the Trojan-horse attack, Eve sends bright light into Alice or Bob, where it passes through their modulators and gets partially reflected back into the communication channel [5,6,12,26,29]. She can then measure this reflection and learn the state of the modulator surreptitiously, without disturbing QKD operation. In fiber-optic QKD systems, the intensity of Eve's injected light is upper-bounded by a laser-induced damage threshold of the single-mode fiber comprising the channel. Given a sufficiently low $\gamma(\lambda)$, Eve receives much less than one reflected photon per qubit and the key information leakage is partial [28]. It is determined by the mean reflected photon number $\mu_{\text{out}} = N\gamma/f$, where N is the total number of photons per second Eve may inject into the channel and f is the clock rate of the QKD system.

The source in the QKD system often consists of a laser followed by modulator(s) that prepare different quantum states and variable attenuators (VOAs) that attenuate them to the required intensity. For protection against the THA, optical isolators and filters are added to the source, in order to decrease $\gamma(\lambda)$. Here we investigate three source configurations (Fig. 5), which were proposed to mitigate the

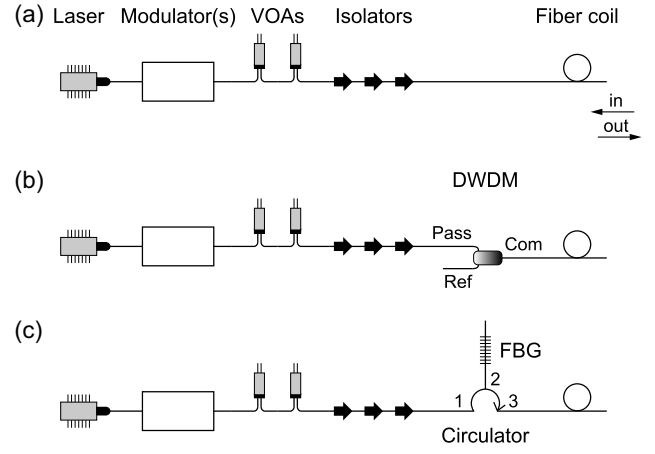


FIG. 5. Source configurations. The fiber coil is used as the broadband physical filter. The passive protection components in configuration (a) are VOAs and isolators. In configuration (b), we add a dense wavelength division multiplexer (DWDM). In configuration (c), the DWDM is replaced with a fiber Bragg grating (FBG) filter. Arrows indicate the direction of attack light transmission. Arrows in the isolator and circulator symbols indicate their forward transmission direction.

impact of THA [28] and are widely deployed in commercial QKD devices [31]. All of them use two VOAs, three isolators, and the fiber coil of 15 mm radius and 21 turns. Configuration (a) consists of only these components. The isolator transmits light at the laser wavelength in the forward direction and heavily attenuates it in the reverse direction.

In configuration (b), a dense wavelength division multiplexer (DWDM) is added. It is a three-port device that internally consists of fiber collimators and a thin-film filter. It is designed to transmit light between the ports $\text{Com} \rightleftharpoons \text{Pass}$ near the laser wavelength and $\text{Com} \rightleftharpoons \text{Ref}$ at other wavelengths within its working wavelength range.

In configuration (c), the DWDM is replaced with a filter consisting of a fiber Bragg grating (FBG) and a circulator. The fiber Bragg grating is a diffraction grating with a periodic change of refractive index in the fiber core. It transmits most light without attenuation but strongly reflects back the laser light whose wavelength matches two grating periods. The circulator transmits light from its port 1 to 2 and from port 2 to 3, and heavily attenuates light going in all the other directions. This filter thus passes laser light to the source output and heavily attenuates all other light in both directions.

In order to compute $\gamma(\lambda)$ via Eq. (4), we measure transmittance of individual components using our testbench.

1. Characterization of individual components

Isolator. We test a polarization-insensitive isolator (Optizone Technology PII-55-P-T-2-11-LL-1). Its transmittance in both forward and reverse directions is shown

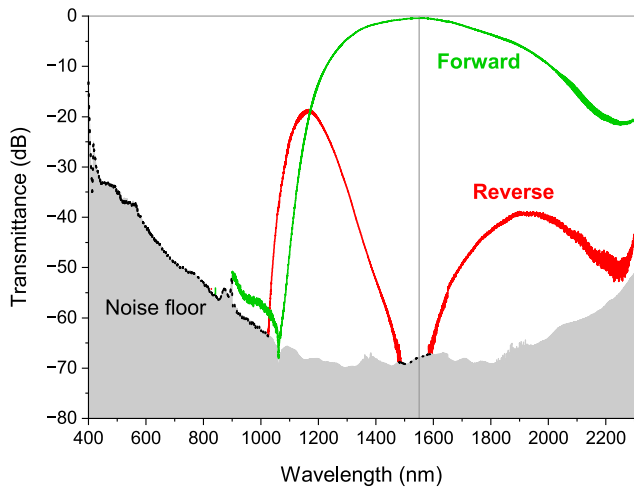


FIG. 6. Spectral characteristics of the isolator. The spectrometer noise envelope is shown as a gray area (omitted for clarity in subsequent plots) and as a black dotted line wherever it substitutes real transmittance data.

in Fig. 6. The sensitivity of our spectrometer did not allow us to measure the true transmittance in parts of the spectral range, and the noise envelope was substituted there. The forward transmittance is about -0.5 dB near the working wavelength of 1550 nm but drops far from it. The

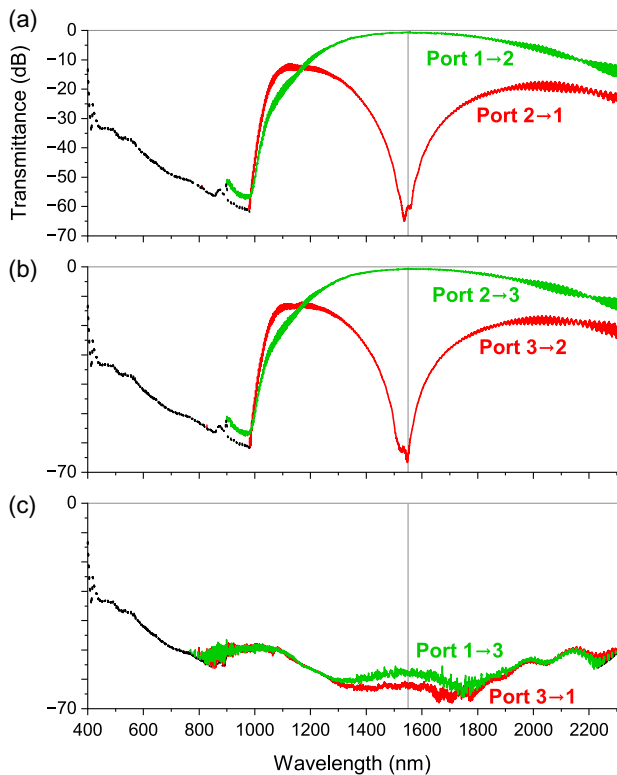


FIG. 7. Spectral characteristics of the circulator between ports (a) 1 and 2, (b) 2 and 3, and (c) 1 and 3.

isolation (defined by the reverse transmittance) is high around 1550 nm but deteriorates far from it, especially in the 1050–1300 nm range. There it drops at least 50 dB lower than at the working wavelength.

Circulator. We test a polarization-insensitive circulator (Optizone Technology FCIR-55-1-111-LLL-1) used in our source configuration (c). Its transmittance in all six possible directions is shown in Fig. 7. While the characteristics between ports $1 \rightleftharpoons 2$ and $2 \rightleftharpoons 3$ are broadly similar to those of the isolator, the attenuation between ports $1 \rightleftharpoons 3$ remains uniformly high at all wavelengths.

Variable optical attenuator. Industrial QKD systems often use inexpensive micro-electro-mechanical systems (MEMS) VOAs. We test two samples of one of these devices (Shanghai Honghui optics communication material Co., Ltd. FASRE-55SM-40BR-LS-FU-1M). It contains a mirror deflected by an externally applied dc voltage, changing its attenuation in about 1–30 dB range at 1550 nm. However, as can be seen in Fig. 8, the attenuation at longer wavelengths can be significantly lower than that set.

Dense wavelength division multiplexer. Quantum key distribution systems sometimes employ the DWDM to add separate synchronization and data channels at different wavelengths. We test one such device (Connet Fiber Optics DWDM-100G-1 $\times$ 2-C34-900-1-FA), see Fig. 9. Only one direction is shown; transmission in the opposite direction (Ref $\rightarrow$ Com and Pass $\rightarrow$ Com) is virtually identical. The device is working as designed in the 1400–1650 nm range.

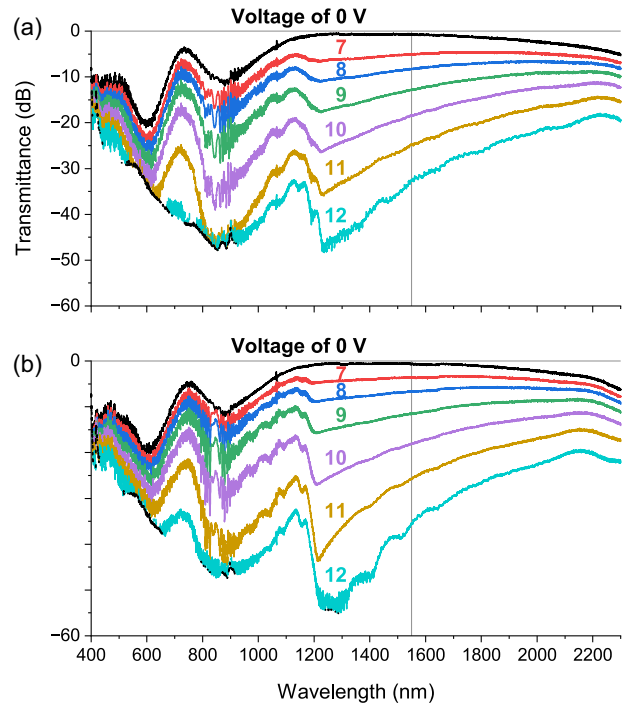


FIG. 8. Spectral characteristics of MEMS VOA at different control voltages. (a) Sample 1; (b) sample 2.

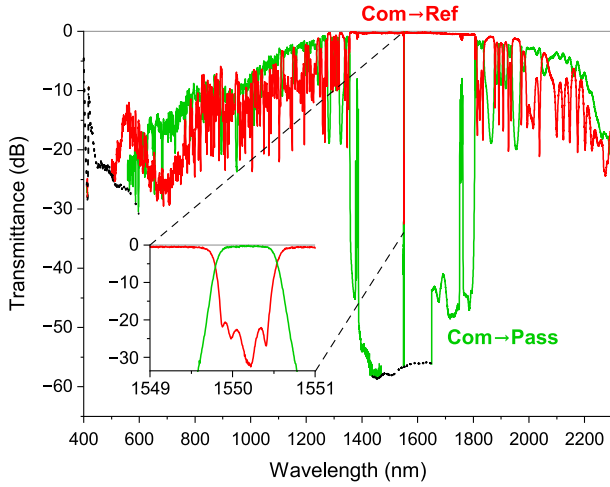


FIG. 9. Spectral characteristics of DWDM. The scan is at 1 nm resolution except its 1549–1551 nm portion scanned at 0.05 nm resolution (magnified in the inset).

Outside this range, its transmission through both port pairs becomes chaotic and generally high.

Fiber Bragg grating-based filter. The FBG filter consists of the circulator tested above and FBG (Wuxi Ruike Huatai Electronics Limited FBG-100) connected at its port 2. The other end of FBG is pigtailed with an angled connector that remains unconnected. We define the transmission from the circulator's port 1 to port 3 as the forward direction and the opposite as the reverse direction. We test this filter as a whole, see Fig. 10. Its attenuation is above 40 dB through the 750–2270 nm range in both directions, with a single narrow forward transmission peak at 1550 nm. This filter is thus wideband, unlike the other components.

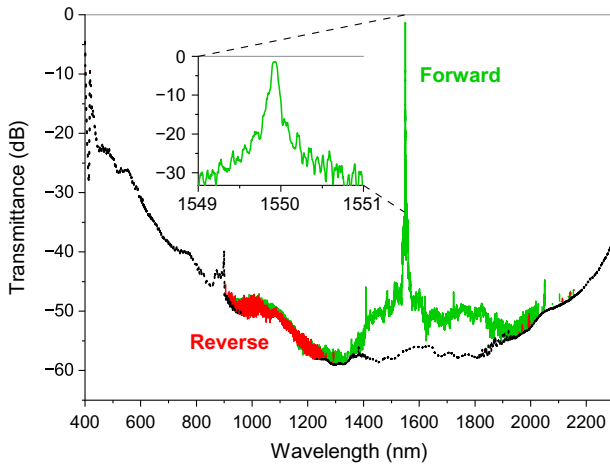


FIG. 10. Spectral characteristics of the FBG-based filter. The scan is at 1 nm resolution except its 1549–1551 nm portion scanned at 0.05 nm resolution (magnified in the inset).

2. Security evaluation

The impact of information leakage from the encoding module caused by the THA needs to be quantified. Since the target susceptibility S to THA is assumed to be wavelength-independent and need not be tested, the above measurements are sufficient for protocol security analysis [28]. The targets of the THA are the phase and intensity modulators. The former may leak the basis information under the THA, which leads to a basis-dependent problem tackled by a quantum coin method [28]. This affects the evaluation of the phase error rate

$$e_1^X = e_{1,\text{bit}}^X + 4\Delta'(1 - \Delta')(1 - 2e_{1,\text{bit}}^X) + 4(1 - 2\Delta')\sqrt{\Delta'(1 - \Delta')e_{1,\text{bit}}^X(1 - e_{1,\text{bit}}^X)}, \quad (5)$$

where $e_{1,\text{bit}}^X$ is the bit error rate and Δ' is used to quantify the basis-dependence.

The leakage of the intensity-encoding information leads to a distinguishable-decoy-states problem, treated with a trace distance method [48,49]. It introduces a deviation in the parameter estimation in the decoy-state analysis

$$\begin{aligned} |Y_n^j - [q_{nkl}Y_n^k + (1 - q_{nkl})Y_n^l]| &\leq D_{n,j,k,l}, \\ |Y_n^j e_n^j - [q_{nkl}Y_n^k e_n^k + (1 - q_{nkl})Y_n^l e_n^l]| &\leq D_{n,j,k,l}, \end{aligned} \quad (6)$$

where Y_n^j (e_n^j) is the yield (error rate) of n -photon signals under the THA given the intensities selected by Alice $j \in \{\mu, \nu, \omega\}$, $D_{n,j,k,l}$ is the trace distance, and q_{nkl} is the conditional probability to have selected the intensity setting k given that the pulse contains n photons.

We investigate the secure key rate of a decoy-state BB84 protocol [50] under the THA based on [28,48]. Its lower bound can be written as

$$R = \left\{ (\mu e^{-\mu}) Y_1^{Z,L} \left[1 - h_2(e_1^{X,U}) \right] - f_e Q_Z^\mu h_2(E_Z^\mu) \right\}, \quad (7)$$

where Q_Z^μ and E_Z^μ are the gain and QBER in Z basis; $Y_1^{Z,L}$ ($e_1^{X,U}$) is the lower (upper) bound of the single-photon yield (error rate) in Z basis (X basis); f_e is the error correction inefficiency; $h_2(x)$ is the binary entropy function. The key to calculating the secure key rate is to accurately estimate the single-photon parameters $Y_1^{Z,L}$ and $e_1^{X,U}$. We use a decoy analysis method from Ref. [50]. By introducing Eqs. (5) and (6) into the calculation of the secure key rate, we account for the THA.

We also investigate a decoy-state measurement-device-independent (MDI) QKD protocol [51]. Its secure key rate can be written as [52,53]

$$\begin{aligned} R = p_{s_A} p_{s_B} \left\{ s_A e^{-s_A} s_B e^{-s_B} Y_{11}^{X,L} \left[1 - h_2(e_{11}^{X,U}) \right] \right. \\ \left. - f_e Q_Z^{ss} h_2(E_Z^{ss}) \right\}, \end{aligned} \quad (8)$$

where p_{s_A} and p_{s_B} are the probabilities of Alice and Bob sending the signal states, Q_Z^{ss} and E_Z^{ss} are the gain and QBER in Z basis, $Y_{11}^{X,L}$ ($e_{11}^{X,U}$) is the lower (upper) bound of the single-photon yield (error rate) in X basis, and s_A and s_B are the intensities of signal states. We use a decoy analysis method from Ref. [54]. By introducing Eqs. (5) and (6) into the calculation of the secure key rate, we account for the THA.

The maximum power that can be injected within 400–2300 nm is not known precisely. Here we adopt the value of 15.6 W at 2300 nm [28]. Although this might be a slight underestimate of fiber power-carrying capability, it is in line with power levels observed to cause destructive effects in components and in the fiber [20,22,55,56], and therefore is a plausible order-of-magnitude estimate of Eve's limit. For simplicity, we set $N = 1.9 \times 10^{20}$ photon/s.

Prepare-and-measure BB84 QKD system. We calculate the secure key rate of the BB84 QKD system as detailed above, using system parameters listed in Table I and protocol specification detailed in the Appendix. Figure 11(a) shows the key rate for $\gamma = 0$ (no information leakage) and four different attenuations of Trojan photons, resulting in reduction of the maximum key generation distance to 93%, 79%, 60%, and 8%.

The actual measured attenuation of Trojan photons, calculated via Eq. (4), is shown in Fig. 11(b). The driving voltages of the two VOA samples are set here to 9 and 10 V, corresponding to attenuation of about 13 and 18 dB at 1550 nm. Their resulting attenuation of the order of 30 dB is typical for a gigahertz-rate QKD system's source [58]. These plots show that the source configuration (c) enables the QKD system to achieve over 93% maximum key generation distance under the THA over the entire wavelength range. However, configurations (a)

TABLE I. Experimental parameters [21,57] we use in the calculation of secure key rate. The previous QKD systems [21,57] had a detector efficiency of 49.5% and receiver insertion loss of 1.1 dB, resulting in the total receiver detector efficiency of 38% we use here.

Channel loss coefficient	α (dB/km)	0.2
Clock rate	f (Hz)	1.25×10^9
Background rate	Y_0	8×10^{-8}
Total misalignment error	e_d	2%
Detector efficiency	η_{det}	38%
Error correction inefficiency	f_e	1.16

and (b) both have two significant high-risk wavelength bands near 1200 and 1900 nm, where the guaranteed key generation distance drops well below 60%. Lower attenuation in these bands stems from the deficiencies in spectral characteristics of the isolator, VOA, and DWDM. The fiber Bragg grating-based filter in the configuration (c) efficiently compensates for these.

MDI-QKD system. Measurement-device-independent QKD is immune to detection-side attacks. Both Alice and Bob function as transmitters, encoding standard BB84 quantum states and sending them to an untrusted relay Charlie, where Bell-state measurements are performed. The security of the transmitter thus becomes vital. In our analysis, we assume Eve attacks both transmitters of the system simultaneously. We use system parameters listed in Table I and protocol specification detailed in the Appendix. Figure 12(a) shows the key rate for $\gamma = 0$ (no information leakage) and four different attenuations of Trojan photons, resulting in reduction of the maximum key generation distance to 93%, 79%, 60%, and 6%.

The actual measured attenuation of Trojan photons is shown in Fig. 12(b). Since this system requires higher

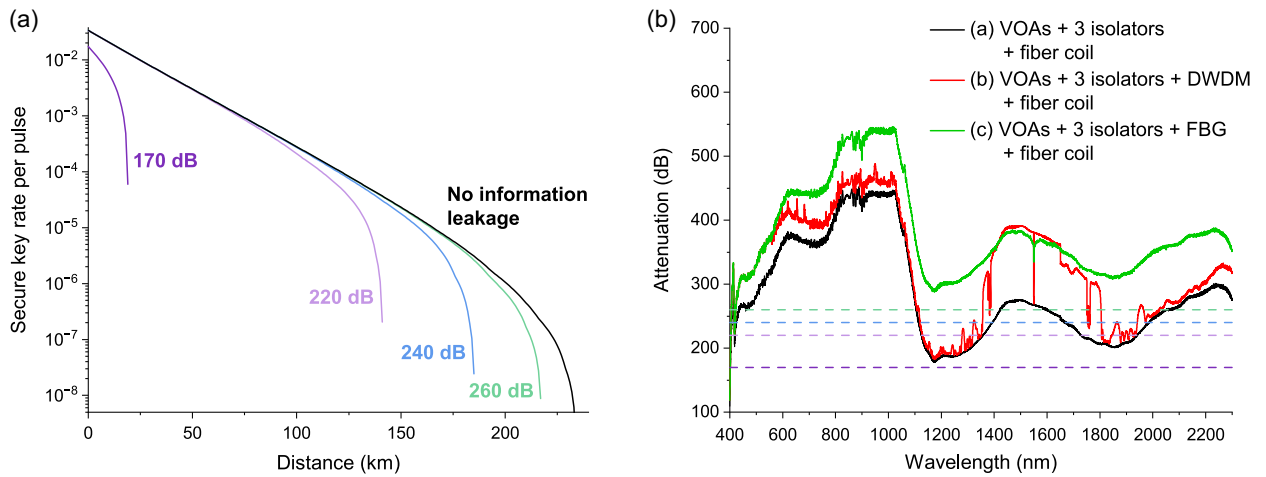


FIG. 11. Security analysis of BB84 QKD under the THA. (a) Secure key rate for different attenuations of Trojan photons. (b) Total measured attenuation of Trojan photons for the three source configurations shown in Fig. 5 under the assumption of unity backreflection.

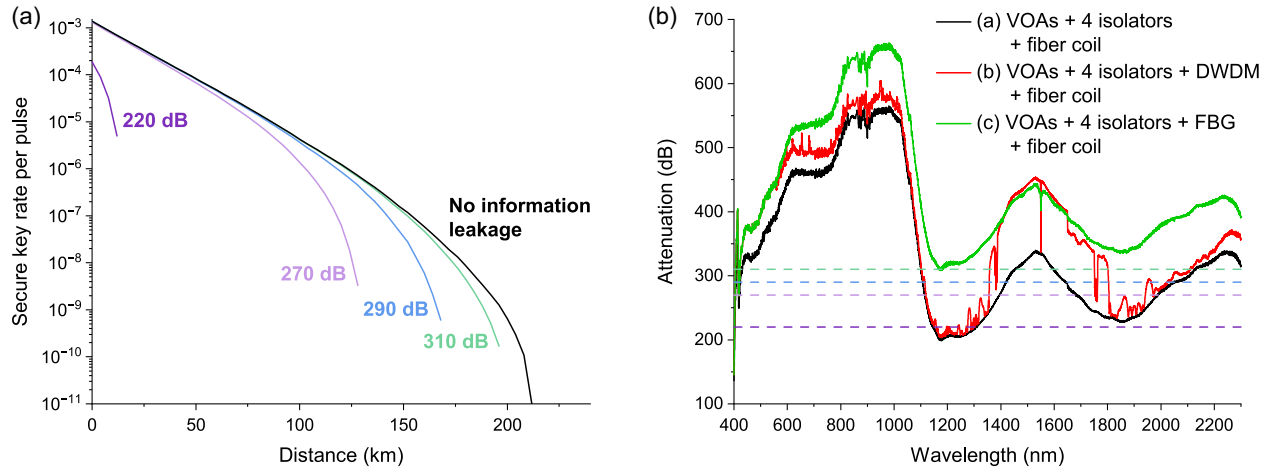


FIG. 12. Security analysis of MDI QKD under the THA. (a) Secure key rate for different attenuations of Trojan photons. (b) Total measured attenuation of Trojan photons for the three source configurations shown in Fig. 5 with four isolators in each instead of three. We conservatively assume unity backreflection.

attenuation, we have increased the number of isolators in all the source configurations to four. The settings of VOAs are the same as those in the BB84 QKD system, because the source's function is similar. Similarly to the BB84 QKD system, the source configuration (c) allows 93% maximum key generation distance under the THA over the entire wavelength range. Configurations (a) and (b) fail to guarantee key generation, owing to the high-risk band near 1200 nm.

We consider two experimental MDI-QKD systems, a free-space one [59] and fiber-optic one [60]. In both systems, the source is implemented with fiber optics. In the free-space system [59], there are two components between the modulators and the transmitter telescope: one VOA and one circulator connected via its ports $1 \rightarrow 2$. These two components provide less than 70 dB total attenuation of Trojan photons at 2000–2200 nm. This is lower than the threshold estimated in Fig. 12(a). The fiber-optic system [60] implements the intensity modulator, attenuators, and polarization modulator in an integrated-optics Si chip, followed by a single fiber-optic isolator before the communication channel. Although the integrated chip has the advantage of lower reflectivity than bulk optics, one isolator is not sufficient [21]. Therefore, both experimental systems need additional isolating and filtering components for the protection against THA in a rigorous manner.

B. Induced-photorefractive attack

In this attack, Eve injects short-wavelength light into QKD device that creates a space charge in its lithium-niobate electrooptic modulators and thus changes their photorefractive properties [23,24,61]. Illumination power at the modulator of 3 nW (400 μ W) at 405 nm (532 nm) is sufficient to induce measurable changes in its characteristics.

We can easily calculate $\gamma(\lambda)$ for the attack channel via Eq. (1) in our source configurations (Fig. 13) and upper-bound Eve's power reaching the modulators. However, the modulators' susceptibility has only been measured at the two discrete wavelengths. A general security proof that takes this imperfection into account is not available. With this limited knowledge, only a preliminary estimate of the system's security can be made.

Assuming the maximum cw power that Eve can inject into the fiber to be 15.6 W just like in the Trojan-horse attack, the power that reaches the modulators in configuration (a) at 405 nm (532 nm) is 3.3×10^{-10} W (7.2×10^{-15} W). This is 1 (11) orders of magnitude below that causing measurable effects [23,24]. Source configurations (b) and (c) provide slightly higher attenuation. The safety margin at 405 nm is small and the attenuation drops rapidly towards shorter wavelengths (Fig. 13), preventing us from drawing a reliable conclusion. If the short-wavelength

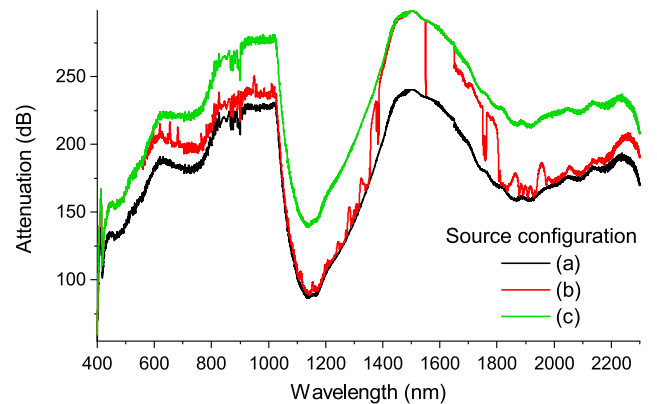


FIG. 13. Total measured attenuation of Eve's light reaching the modulators in the three source configurations shown in Fig. 5.

suppression physical filter is implemented (Sec. IV), the sources can probably be considered safe. However, we stress that the general security proof providing the secure key rate R is needed to confirm this and the modulator susceptibility $S(\lambda)$ needs to be characterized at other wavelengths. For the latter characterization, our testbench may be supplemented with a monochromator [31].

C. Detector-backflash attack

This is a passive attack, in which Eve measures the polarization or other properties of light emitted into the channel by QKD receiver device [17,27,62]. The spectrally broad emission originates in avalanche photodiodes and may identify which detector has clicked, thus leaking key information.

In a typical QKD receiver, backflash light passes several components on its way to the communication channel, such as DWDM and isolators similar to those we have characterized [31]. The transmission of attack channel $\gamma(\lambda)$ is calculated by Eq. (2). While security proofs providing R in the presence of this attack are available [17,62,63], they require as input the probability of photon emission from the receiver $\mu_{\text{leak}} = \int_{\lambda} \gamma(\lambda) S(\lambda) d\lambda$, where $S(\lambda)$ is the probability density of photon emission from the detector. The latter spectral distribution is challenging to measure, owing to high sensitivity required. The spectrometers in our testbench lack it. The characterization has to be done with a set of spectral filters or tunable filter followed by a single-photon detector [16,27,64].

VI. CONCLUSION

We have demonstrated a characterization methodology to achieve full-spectrum security of QKD systems. Since all known implementations of QKD utilize photons as information carriers, it should be applicable to most optical attacks on them. The full analysis of each attack needs data on wavelength-dependent transmission of the attack channel, target susceptibility, and security proof that accounts for these.

We have used our testbench to test passive fiber-optic components in a wide spectral range of 400–2300 nm. Our experimental results confirm that the optical device characteristics deviate significantly at different wavelengths, which may lead to potential security vulnerabilities. We have evaluated the protection of QKD sources against THA and identified that the source configuration (c) with the FBG-based filter guarantees the security of typical one-way decoy-state BB84 and MDI-QKD systems. We have outlined how to apply our methodology to induced-photonrefraction and detector-backflash attacks.

Our testbench and characterization methodology can be used for certification of QKD systems against other attacks as well. This promotes secure implementation of QKD and its standardization.

ACKNOWLEDGMENTS

We thank Anqi Huang for discussions and her help with this study.

Funding: National Key Research and Development (R&D) Plan of China (Grant No. 2020YFA0309701), National Natural Science Foundation of China (Grant No. 62031024), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300300), Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), Shanghai Academic/Technology Research Leader (21XD1403800), Shanghai Science and Technology Development Funds (22JC1402900), Key-Area Research and Development Program of Guangdong Province (2020B0303020001), Anhui Initiative in Quantum Information Technologies, and Chinese Academy of Sciences. M.P. and V.M. acknowledge funding from the Galician Regional Government (consolidation of research units: atlanTTic and own funding through the “Planes Complementarios de I+D+I con las Comunidades Autonomas” in Quantum Communication), MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1), the “Hub Nacional de Excelencia en Comunicaciones Cuánticas” funded by the Spanish Ministry for Digital Transformation and the Public Service and the European Union NextGenerationEU, the European Union’s Horizon Europe Framework Programme under Marie Skłodowska-Curie Grant No. 101072637 (project QSI) and project “Quantum Security Networks Partnership” (QSNP; Grant No. 101114043). F.X. acknowledges support from the New Cornerstone Science Foundation through the Xplorer Prize.

DATA AVAILABILITY

The data are not publicly available. The data are available from the authors upon reasonable request.

APPENDIX: QKD PROTOCOL SPECIFICATION

In the security analysis of the BB84 QKD system, we study the three-intensity decoy state BB84 QKD protocol [50]. Alice chooses her bit value uniformly at random. Then, the bases Z and X are selected with probabilities P_Z and $1 - P_Z$ and the secret key is extracted from the events whereby Alice and Bob both chose the Z basis. Each pulse is randomly prepared in one of the three intensities $\{\mu, \nu, \omega\}$ chosen with probabilities P_μ, P_ν , and $(1 - P_\mu - P_\nu)$. The intensities satisfy $\mu > \nu + \omega$ and $\mu > \nu > \omega$. Here, μ denotes the intensity of the signal state. We perform a full optimization of parameters $\{\mu, \nu, P_\mu, P_\nu, P_Z\}$. In parameter estimation, we use the analytical approaches [50,65], and consider statistical fluctuations [66] and deviations caused by THA [28,48].

In the security analysis of the MDI-QKD system, we study the four-intensity decoy state MDI-QKD protocol

[52,53]. There are three intensities $\{\mu, \nu, \omega\}$ in the X basis for the decoy-state analysis and one signal intensity $\{s\}$ in the Z basis for secret key generation. We consider a symmetric channel loss where Alice and Bob use the same parameters. Including the probabilities P for each intensity, both Alice and Bob use the same group of six parameters $\{s, \mu, \nu, P_s, P_\mu, P_\nu\}$. We perform a full optimization of parameters. In parameter estimation, we use the analytical approaches [21,54], and consider statistical fluctuations [53] and deviations caused by THA [21].

-
- [1] C. H. Bennett and G. Brassard, in *Proc. International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984), pp. 175–179.
 - [2] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
 - [4] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, *npj Quantum Inf.* **2**, 16025 (2016).
 - [5] A. Vakhitov, V. Makarov, and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, *J. Mod. Opt.* **48**, 2023 (2001).
 - [6] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Phys. Rev. A* **73**, 022320 (2006).
 - [7] 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).
 - [8] V. Makarov, Controlling passively quenched single photon detectors by bright light, *New J. Phys.* **11**, 065003 (2009).
 - [9] 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).
 - [10] 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).
 - [11] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, *Phys. Rev. A* **84**, 062308 (2011).
 - [12] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, *New J. Phys.* **16**, 123030 (2014).
 - [13] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing, *Phys. Rev. A* **91**, 032326 (2015).
 - [14] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser damage helps the eavesdropper in quantum cryptography, *Phys. Rev. Lett.* **112**, 070503 (2014).
 - [15] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, Effect of source tampering in the security of quantum cryptography, *Phys. Rev. A* **92**, 022304 (2015).
 - [16] Y. Shi, J. Z. J. Lim, H. S. Poh, P. K. Tan, P. A. Tan, A. Ling, and C. Kurtsiefer, Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes, *Opt. Express* **25**, 30388 (2017).
 - [17] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Eavesdropping and countermeasures for backflash side channel in quantum cryptography, *Opt. Express* **26**, 21020 (2018).
 - [18] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, *Phys. Rev. Appl.* **12**, 064043 (2019).
 - [19] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch, *Phys. Rev. A* **100**, 022325 (2019).
 - [20] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Laser-damage attack against optical attenuators in quantum key distribution, *Phys. Rev. Appl.* **13**, 034017 (2020).
 - [21] H. Tan, W. Li, L. Zhang, K. Wei, and F. Xu, Chip-based quantum key distribution against Trojan-horse attack, *Phys. Rev. Appl.* **15**, 064038 (2021).
 - [22] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, Protecting fiber-optic quantum key distribution sources against light-injection attacks, *PRX Quantum* **3**, 040307 (2022).
 - [23] P. Ye, W. Chen, G.-W. Zhang, F.-Y. Lu, F.-X. Wang, G.-Z. Huang, S. Wang, D.-Y. He, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Induced-photorefraction attack against quantum key distribution, *Phys. Rev. Appl.* **19**, 054052 (2023).
 - [24] L. Han, Y. Li, H. Tan, W. Zhang, W. Cai, J. Yin, J. Ren, F. Xu, S. Liao, and C. Peng, Effect of light injection on the security of practical quantum key distribution, *Phys. Rev. Appl.* **20**, 044013 (2023).
 - [25] M. Fadeev, A. Ponosova, Q. Peng, A. Huang, R. Shakhovoy, and V. Makarov, Optical-pumping attack on a quantum key distribution laser source, *Opt. Express* (in press).
 - [26] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Invisible Trojan-horse attack, *Sci. Rep.* **7**, 8403 (2017).
 - [27] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution, *Light Sci. Appl.* **6**, e16261 (2017).
 - [28] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, *Phys. Rev. X* **5**, 031030 (2015).
 - [29] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuch, Risk analysis of Trojan-horse attacks on practical quantum key distribution systems, *IEEE J. Sel. Top. Quantum Electron.* **21**, 6600710 (2015).
 - [30] ISO/IEC 23837-2:2023(en), Information security—Security requirements, test and evaluation methods for

- quantum key distribution—Part 2: Evaluation and testing methods, <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23837:-2:ed-1:v1:en>, visited 22 Nov 2023.
- [31] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A. K. Fedorov, A. Huang, E. Kiktenko, M. Petrov, A. Ponomova, D. Ruzhitskaya, A. Tayduganov, D. Trefilov, and K. Zaitsev, Preparing a commercial quantum key distribution system for certification against implementation loopholes, *Phys. Rev. Appl.* **22**, 044076 (2024).
- [32] A. Tomita, Implementation security certification of decoy-BB84 quantum key distribution systems, *Adv. Quantum Technol.* **2**, 1900005 (2019).
- [33] S. Sajed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, An approach for security evaluation and certification of a complete quantum communication system, *Sci. Rep.* **11**, 5110 (2021).
- [34] Draft ETSI GS QKD 010 V0.4.1 (2021-06), Quantum key distribution (QKD); Implementation security: protection against Trojan horse attacks, https://docbox.etsi.org/ISG/QKD/Open/GS-QKD-0010_ISTrojan_v0.4.1_OpenArea.pdf, visited 16 Mar 2025.
- [35] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: past, present, and future, *Appl. Phys. Rev.* **11**, 011318 (2024).
- [36] C. Marquardt, U. Seyfarth, S. Bettendorf, M. Bohmann, A. Buchner, M. Curty, D. Elser, S. Eul, T. Gehring, N. Jain, T. Klocke, M. Reinecke, N. Sieber, R. Ursin, M. Wehling, and H. Weier, Implementation attacks against QKD systems, BSI technical report, https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html, visited 14 Feb 2024.
- [37] NKT Photonics, SuperK Fianium supercontinuum white light fiber lasers, <https://www.nktp Photonics.com/products/supercontinuum-white-light-lasers/superk-fianium/>, visited 27 Nov 2023.
- [38] B. Nasedkin, F. Kiselev, I. Filipov, D. Tolochko, A. Ismagilov, V. Chistiakov, A. Gaidash, A. Tsyckin, A. Kozubov, and V. Egorov, Loopholes in the 1500–2100-nm range for quantum-key-distribution components: prospects for Trojan-horse attacks, *Phys. Rev. Appl.* **20**, 014038 (2023).
- [39] NKT Photonics, SuperK Split spectral splitter, <https://www.nktp Photonics.com/products/supercontinuum-white-light-lasers/superk-split/>, visited 27 Nov 2023.
- [40] NKT Photonics, SuperK Connect broadband fiber delivery, <https://www.nktp Photonics.com/products/supercontinuum-white-light-lasers/superk-connect/>, visited 27 Nov 2023.
- [41] Yokogawa, AQ6374 wide range optical spectrum analyzer, <https://tmi.yokogawa.com/solutions/discontinued/aq6374-wide-range-optical-spectrum-analyzer-350-1750-nm/>, visited 27 Nov 2023.
- [42] Yokogawa, AQ6375B wide range optical spectrum analyzer, <https://tmi.yokogawa.com/solutions/discontinued/aq6375b-optical-spectrum-analyzer/>, visited 27 Nov 2023.
- [43] Q. Wang, G. Farrell, and T. Freir, Theoretical and experimental investigations of macro-bend losses for standard single mode fibers, *Opt. Express* **13**, 4476 (2005).
- [44] W. Chen, Z. Chen, Y. Zhang, H. Li, and Y. Lian, Agarose coated macro-bend fiber sensor for relative humidity and temperature measurement at 2 μm , *Opt. Fiber Technol.* **50**, 118 (2019).
- [45] M. A. Green and M. J. Keevers, Optical properties of intrinsic silicon at 300 K, *Prog. Photovolt. Res. Appl.* **3**, 189 (1995).
- [46] M. A. Green, Self-consistent optical parameters of intrinsic silicon at 300 K including temperature coefficients, *Sol. Energy Mater. Sol. Cells* **92**, 1305 (2008).
- [47] S. Kasap and P. Kapper, (Eds.), *Springer Handbook of Electronic and Photonic Materials* (Springer, Stürtz GmbH, Würzburg, 2006), p. 54.
- [48] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, *New J. Phys.* **18**, 065008 (2016).
- [49] S. Sun and F. Xu, Security of quantum key distribution with source and detection imperfections, *New J. Phys.* **23**, 023011 (2021).
- [50] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [51] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [52] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, *Phys. Rev. A* **93**, 042324 (2016).
- [53] W. Wang, F. Xu, and H.-K. Lo, Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks, *Phys. Rev. X* **9**, 041012 (2019).
- [54] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Practical aspects of measurement-device-independent quantum key distribution, *New J. Phys.* **15**, 113007 (2013).
- [55] R. Kashyap and K. J. Blow, Observation of catastrophic self-propelled self-focusing in optical fibres, *Electron. Lett.* **24**, 47 (1988).
- [56] D. D. Davis, S. C. Mettler, and D. J. DiGiovanni, A comparative evaluation of fiber fuse models, *Proc. SPIE* **2966**, 592 (1997).
- [57] W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W.-Y. Liu, X. Jiang, S.-K. Liao, C.-Z. Peng, M. Curty, F. Xu, and J.-W. Pan, Experimental quantum key distribution secure against malicious devices, *Phys. Rev. Appl.* **15**, 034081 (2021).
- [58] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, High-rate quantum key distribution exceeding 110 Mb s⁻¹, *Nat. Photonics* **17**, 416 (2023).
- [59] Y. Cao *et al.*, Long-distance free-space measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **125**, 260503 (2020).
- [60] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics, *Phys. Rev. X* **10**, 031030 (2020).
- [61] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Hacking measurement-device-independent quantum key distribution, *Optica* **10**, 520 (2023).

- [62] A. Koehler-Sidki, J. Dynes, T. Paraïso, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. Shields, Backflashes from fast-gated avalanche photodiodes in quantum key distribution, *Appl. Phys. Lett.* **116**, 154001 (2020).
 - [63] S. Molotkov, Trojan horse attacks, decoy state method, and side channels of information leakage in quantum cryptography, *J. Exp. Theor. Phys.* **130**, 809 (2020).
 - [64] L. Marini, R. Camphausen, B. J. Eggleton, and S. Palomba, Deterministic filtering of breakdown flashing at telecom wavelengths, *Appl. Phys. Lett.* **111**, 213501 (2017).
 - [65] A. Huang, S. H. Sun, Z. Liu, and V. Makarov, Quantum key distribution with distinguishable decoy states, *Phys. Rev. A* **98**, 012330 (2018).
 - [66] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, *Phys. Rev. A* **89**, 022307 (2014).
- Correction:* An erroneous funding statement has been removed from the Acknowledgments.