entropy

MDPI

Review

A Review of Security Evaluation of Practical Quantum Key Distribution System

Shihai Sun[1,*] **and Anqi Huang** [2,*]

[1] School of Electronics and Communication Engineering, Sun Yat-Sen University, Shenzhen 518107, China
[2] Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China
* Correspondence: sunshh8@mail.sysu.edu.cn (S.S.); angelhuang.hn@gmail.com (A.H.)

Abstract: Although the unconditional security of quantum key distribution (QKD) has been widely studied, the imperfections of the practical devices leave potential loopholes for Eve to spy the final key. Thus, how to evaluate the security of QKD with realistic devices is always an interesting and opening question. In this paper, we briefly review the development of quantum hacking and security evaluation technology for a practical decoy state BB84 QKD system. The security requirement and parameters in each module (source, encoder, decoder and detector) are discussed, and the relationship between quantum hacking and security parameter are also shown.

Keywords: quantum cryptography; quantum communication; quantum key distribution; practical security; security evaluation

Citation: Sun, S.; Huang, A. A Review of Security Evaluation of Practical Quantum Key Distribution System. *Entropy* **2022**, *24*, 260. https://doi.org/10.3390/e24020260

Academic Editor: Gregg Jaeger

Received: 21 December 2021
Accepted: 1 February 2022
Published: 10 February 2022

1. Motivation

Quantum key distribution (QKD) provides an approach to share a *key* between two remote parties via an insecure channel with information-theoretic security (or called the unconditional security). Since the first QKD protocol, BB84, was proposed by Bennett and Brassard in 1983 [1], various types of QKD protocols based on the discrete variables [2–4] or the continuous variables [5,6] have been proposed, which have been applied to different situations according to their characteristics. Remarkably, QKD-based quantum networks are also available in many countries [7–9]. For example, an integrated space-to-ground quantum communication network over 4600 km was implemented in China [10].

However, the unconditional security of the final key still might be broken because the imperfections of the practical devices could be exploited by Eve to bypass the security assumptions of QKD. For example, in the standard BB84 protocol, Alice is required to encode her information in the single-photon pulse. Nevertheless, instead of the single-photon source (SPS), the weak coherent source (WCS) that includes the multi-photon portion is widely used in most practical QKD systems. Then, Eve can perform the photon-number-splitting (PNS) attack by exploiting these multi-photon pulses [11,12]. So far, many quantum attack strategies have been discovered (see Table 1 in Section 5 for the detailed information, and Ref. [13] for a review).

In order to overcome the practical security threat, at least two solutions have been proposed. One is the new QKD protocol in which the loopholes of practical devices can be partially removed. For example, all loopholes in the detection part can be removed by the measurement-device-independent (MDI-) QKD protocol [14]. Moreover, by introducing Bell's inequality [15,16], the unconditional security of device-independent (DI-) QKD can be proven with just a few basic assumptions. The other solution is security patching. The patches to certain known attacks are employed in a QKD system. By measuring or monitoring the parameters of the QKD system, the leaked information can be estimated. The security patching plays an important role to guarantee the security of a QKD system with imperfect devices. First, a security evaluation is necessary for most of the practical

QKD system, even for MDI- and DI-QKD. Second, by monitoring the parameters of the QKD system, Alice and Bob can make sure that Eve cannot perform some quantum attacks, and then the performance of a QKD system can be improved.

In this paper, we review the development of security evaluation technology for QKD. Although there are many different QKD protocols based on both the discrete variables and the continuous variables, we focus our main attention on the decoy state BB84 protocol [17–19] here since it is the widely used protocol in many practical applications. In Section 2, we introduce the communication model of a typical QKD system, which can be divided into five modules (source, encoder, channel, decoder, and detector). Then, the basic security requirement for each module is introduced. In Section 3, by reviewing the main quantum hacking strategies in each module (The quantum channel is totally controlled by Eve, and the unconditional security of QKD is proven under the general coherent attack; thus the practical imperfections of the quantum channel only reduce the efficiency of the QKD system, but do not break its security.), it is clearly shown that, once some security requirements introduced in Section 2 are broken (due to the imperfection of the practical optical and electrical devices), the unconditional security of the final generated key will be compensated. In Section 4, we review the security model and show how to define the security parameter, which describes the deviation between the theoretical security requirement (introduced in Section 2) and the practical implementation (which could be exploited by Eve in Section 3). In Section 5, we introduce the security evaluation technology, and show the relationship between quantum hacking and security parameters.

2. Communication Model and Security Requirement

According to a general communication model [20], a QKD system also can be divided as five parts (Figure 1): source, encoder, channel, decoder and detector. Now, we give the detail definition and security requirement of each module for a typical decoy state BB84 protocol.

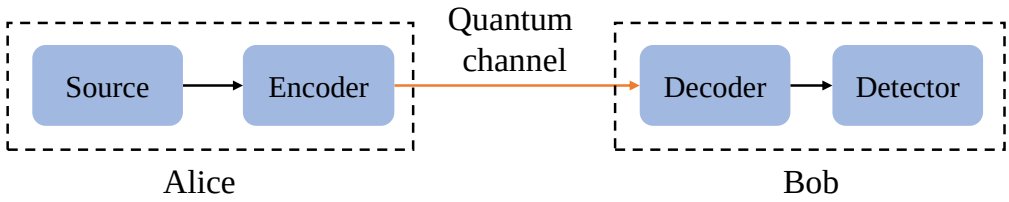

Figure 1. The concept communication model of a QKD system, which includes five modules: source, encoder, channel, decoder and detector. The source generates the required optical pulse, single photon pulse for BB84, or the weak coherent pulses with different average intensities. The encoder and decoder transform two classical bits into quantum states, back and forth. The detector absorbs the photon and registers the click of SPDs. The detailed definition and security requirement for each module are given in the main text.

Source: In this module, a required optical pulse is generated, such as a single-photon pulse for the standard BB84 protocol. However, a perfect SPS is still unavailable for a practical QKD system, due to the complexity, stability, cost, and so on. Thus, for a practical decoy state BB84 protocol, the source generates a weak optical pulse with stable average intensity and known photon number distribution (PND). The most widely used source in a practical QKD system is the laser diode combining with an attenuator, which generates the weak coherent pulses following the Poisson distribution with an average intensity of $\mu \approx 0.1$.

Although the security of QKD is compensated by the multi-photon pulse in the WCS, the decoy state method [17–19] can be used to estimate the contribution of the single photon pulse. In other words, with the help of the decoy state method, the laser diode combined with an attenuator can be considered a SPS with finite-generation efficiency (the contribution of the multi-photon pulse could be removed from the total gain and bit error).

In order to guarantee the security of a decoy state BB84 QKD system, at least three basic assumptions are required [17–19]: (1) the average intensity and the PND of the source should be exactly stable and known; (2) the phase of each optical pulse should be uniformly randomized from 0 to 2π; (3) the decoy states should be indistinguishable in any dimensions except for the average intensity.

Encoder: In this module, Alice transforms her two random classical bits (one is called *basis bit* and the other one *information bit*) into the quantum state. Then, one of four encoded quantum states is randomly generated by modulating the photon emitted by the sources. The two classical bits should be generated by a true random number generator (TRNG), such as the quantum random number generator [21,22]. The transformation from classical bits to quantum states is performed by a modulator, which is the core part of the encoder module and should be carefully protected to remove the existence of Eve. In order to make sure that Eve cannot distinguish the encoded quantum state, at least three assumptions are required [23–25]: (1) Eve does not have any information about the random number used by Alice (the random number used by Alice should be random and secure); (2) the encoded quantum state should perfectly match the standard quantum state required by the BB84 protocol (perfect quantum state preparing phase); and (3) the encoded quantum state should not be distinguished in any dimensions, except for the encoded degree (no information is leaked from the side channel).

Quantum channel: In this module, the quantum state of Alice is transmitted to Bob. The fiber and free space are two typical quantum channels for QKD (the security of the classical channel used for the post-processing and device calibration is not considered here). In the security model of QKD, the quantum channel is assumed to be totally controlled by Eve, who can perform any operation admitted by the quantum mechanics. Thus, there are no security requirements for the quantum channel. However, the loss and noise of the quantum channel should amplify the flaws of the source and encoder [23], then limit the final key rate. Thus, a quantum channel with lower loss and noise is always necessary to improve the performance of the practical QKD system.

Decoder: In this module, by measuring the optical pulse coming from the quantum channel, Bob could transform the quantum state into two classical bits (also called *basis bit* and *information bit*) again. The *basis bit* could be actively chosen with a T-RNG or passively registered with a beam splitter. The *information bit* is registered according to the click of SPDs. Since the optical pulse measured by Bob is totally controlled by Eve, the click of SPDs is determined by three parts, the encoded state of Alice, the operation of Eve and the measurement of Bob. In other words, the decoder module can be considered a box with one input and four outputs (although, in some QKD systems, Bob actively chooses his basis, and there are only two outputs in the decoder, but, theoretically speaking, we can consider the two basis one by one). For each optical pulse going into the box, it will output from one of the four outputs (presenting the two classical bits). Therefore, the following assumptions are required for the decoder module [24,25]: (1) the basis of Bob should be random, which cannot be controlled or known by Eve; (2) for each basis, Eve cannot control the output of the decoder box by manipulating the parameters of each optical pulse, such as the time, wavelength, and so on; and (3) no optical or electrical signal is leaked to the quantum channel from the decoder module. Since the decoder is the most weak part of the QKD system, we give a detailed discussion about it here. The first two assumptions above mean that Eve cannot control the probability $P(i|\lambda)$ $(i = 0, 1, 2, 3)$, which is the conditional probability that a photon outputs from the i-port of the decoder box given the hidden variable parameter λ controlled by Eve. Here, we remark that both the two phases that Bob randomly chooses as his basis and analyses of Alice's information bit are included in "*Decoder*" in this review. The main advantage here is that a part of the imperfection of the SPDs can be included in the *basis bit* and *information bit*. For example, the SPD blinding attack [26] for a polarization-encoding QKD system can be considered such that Eve can set the probability $P(i|\lambda)$ as $P(i|I, Pol.) = p\delta_{ik}$ for each optical pulse. Here, I ($Pol.$) is the intensity (polarization) of

Eve's optical pulse, k is the index of SPD that should click if Eve is absent, and p is the probability that a optical pulse should be detected by Bob when Eve is absent.

Detector: In the detector module, Bob measures the decoded optical pulse with SPDs and registers which SPD clicks (according to the security analysis, if more than one SPD click, Bob should randomly register one). Based on the *Decoder* module above, four SPDs are required. For the QKD system with only two SPDs, another two virtual SPDs that have the same parameters as that of the two factual SPDs can be introduced. Then, two virtual SPDs are used to measure the optical pulse for one basis and two factual SPDs for the other basis.

Thus, for the detector module, the following assumptions are required [27]: (1) all the clicks of the detectors can be registered by Bob; (2) no active optical or electrical signal is leaked to Eve from the detector.

3. Quantum Hacking

In this section, we briefly introduce the quantum attacks to show that Eve can exploit the imperfections of the practical devices to break parts of the required security requirements in Section 2, then compensate for the unconditional security of the final generated key. Here we should remark that, most of these attacks can be removed by taking the security parameters into the security model or monitoring the security parameters to remove Eve's attack. The security parameter and the evaluation technology are discussed in next two sections. The detailed definitions of these security parameters are discussed in Section 4, which characterize the deviation between the theoretical requirement and the practical implement. The relationship between the quantum hacking and the security parameters is discussed in Section 5.

3.1. Source

The phase randomization is a core assumption for a QKD with WCS. However, it has been shown that the phase might be unrandomized, due to imperfect implementation, which gives Eve a chance to distinguish the states and learn the secret keys [23]. Specifically, Eve can apply the unambiguous state discrimination (USD) measurement to distinguish decoy states and signal states if the phase is fully non-random [28]. With the help of homodyne detection, the encoded quantum state can be distinguishable when the phase of the source is just partially randomized [29]. Furthermore, the distribution of the phase can be tampered from uniform to Gaussian via the laser-injection attack [30] (see Figure 2a,b for detail).

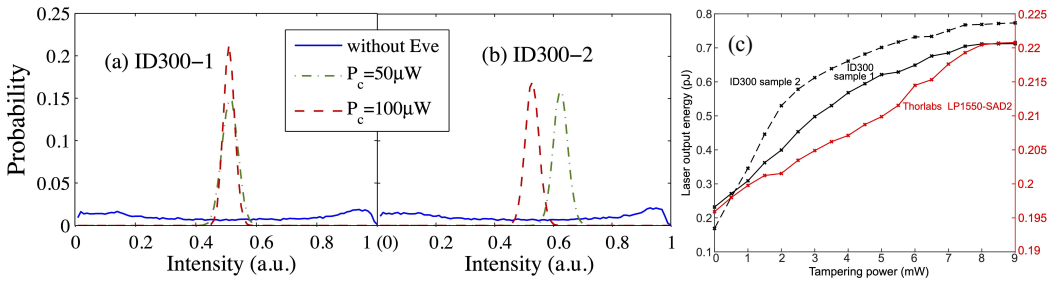

Figure 2. The phase distribution and intensity with and without Eve's laser-injection attack, reprinted from Refs. [30,31]. (**a**,**b**) Phase distribution of Alice's adjacent pulses tested from two samples of ID300 lasers. Without Eve's attack, the phase is random. However, under 50 μW or 100 μW of Eve's injected light, the phase follows a Gaussian distribution. (**c**) The increased intensity under laser-injection attack.

The shape of the optical pulses is another type of vulnerability. If one drives the laser diode with different amounts of electrical current to generate decoy states and signal states, this driving mode may result in various lasering times and a lasting period for decoy states and signal states [32], as shown in Figure 3a. To exploit this loophole, Eve carefully chooses

two observing windows, W_d and W_s, to distinguish the signal state and decoy state [32] as shown in Figure 3a. The configuration of the multiple laser diodes may disclose the variation of the decoy states and signal states in the timing, spectral, and intensity degrees of freedom [33], which is shown in Figure 3b.

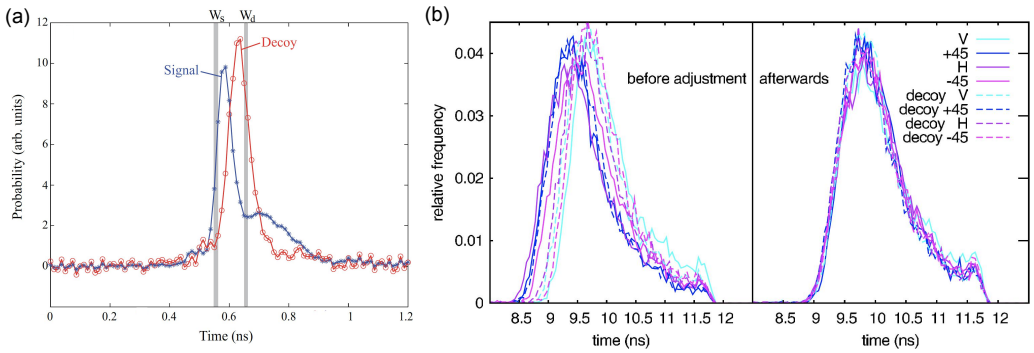

Figure 3. The experimental measurement of distinguishable states. (**a**) The pulse shapes of the decoy state and the signal state driven by electrical current. Reprinted from Ref. [32]. (**b**) Four encoded signal states and decoy states generated by individual laser diodes. Reprinted from Ref. [33].

Time and spectrum are two other typical side channels. Intersymbol interference in time is usually disclosed in a high-speed QKD system [34]. The distorted driving signal for the intensity modulator may result in the intensity correlation between neighboring pulses in the time degree of freedom as shown in Figure 4, which breaks the assumption about independent and identical distribution. By actively shifting the arriving time of pulses to an intensity modulator, the spectrum of optical pulses can be correlated with the intensity of the light in a plug-and-play QKD system [35].

In the decoy-state BB84 protocol, the intensities of decoy states and signal states are preset to be optimal values, maximizing the key rate. However, these preset intensities might be manipulated by the laser-injection attack during the operating phase of a QKD system [30,31,36]. This is because Eve can lock Alice's laser diode by injecting a bright light into it. As shown in Figure 2c, the intensity of Alice's laser is increased to 3.07 times as the maximum with the raise of Eve's injected power, which is not noticed by Alice and Bob. As a result, they may incorrectly estimate the contribution of the single photon pulse.

The intensity of Alice's pulse also can be actively manipulated by Eve with the laser-damage attack on the optical attenuator [37,38]. Eve's injected high-power light from the quantum channel first reaches the optical attenuator [39–41] and decreases the attenuation value [38]. Figure 5 illustrates the typical results of decreased attenuation after the attenuator being shined by 2.8 W laser for 10 s, which increases the intensity of Alice's pulses.

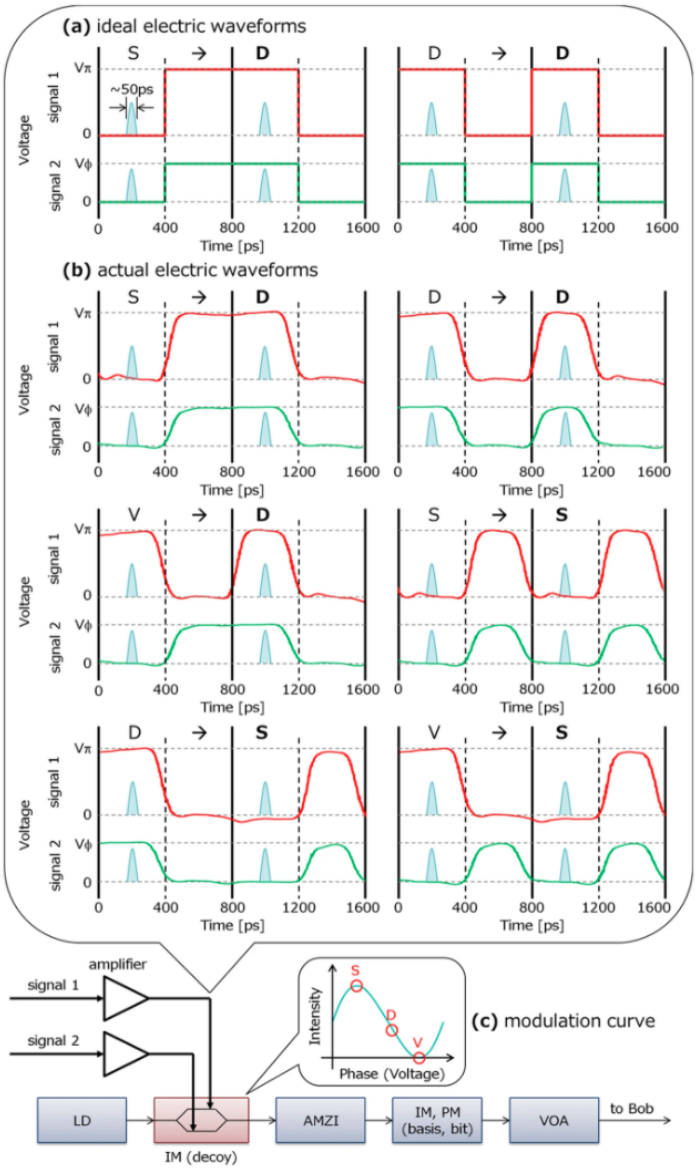

Figure 4. The typical testing result of intersymbol interference, which shows the intensity correlation between neighboring pulses. Reprinted from Ref. [34].

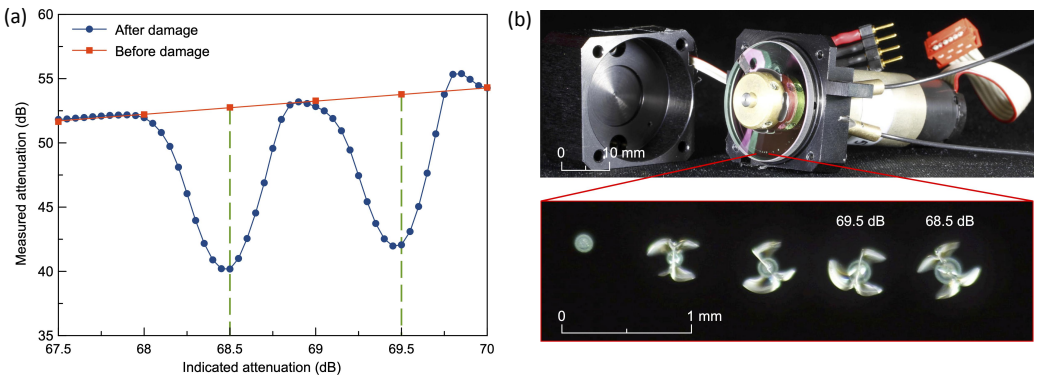

Figure 5. The testing results of the laser damage attack on attenuator. (**a**) The attenuation values before and after the laser damage attack. (**b**) The attenuator with the damaged areas. Reprinted from Ref. [38].

3.2. Encoder

The encoder is always the target of Eve's attack, since the quantum states is modulated here to represent the secret information. The security vulnerabilities of the encoder module come from both the encoding and non-encoding degrees of freedom.

For the encoding degrees of freedom, an imperfect encoder module may prepare non-orthogonal states. For example, in a phase-encoding QKD, the encoder is assumed to generate a state with one of four phases in $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. However, the actual phase modulated on the optical pulse may deviate from the required one, which allows Eve to partially distinguish the states [42]. Furthermore, the precision of modulation can be manipulated by modifying the arriving time of the pulses. For example, in a phase-encoding plug-and-play QKD system, Eve may remap the encoded phase of Alice by controlling the time that the optical pulse arrives at Alice's modulator [43].

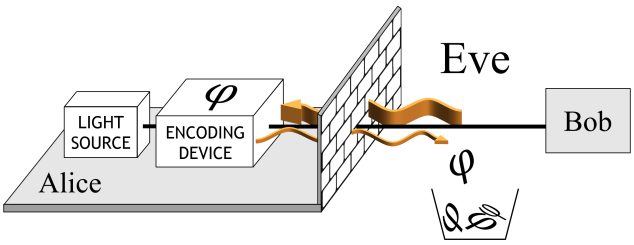

Figure 6. The working principle of Trojan horse attack. Reprinted from Ref. [44].

The non-encoding degrees of freedom also reveal side channels to Eve. For instant, in the Trojan horse attack [45], Eve actively sends optical pulses into Alice's encoder from the quantum channel, a portion of which may be modulated by Alice and return to the channel again as shown in Figure 6. Since the reflected photon is measured by Eve and not transmitted to Bob, it does not increase the error rate and interrupt the QKD system. Therefore, Eve can silently learn the secret key.

It is notable that all the imperfections and attacks discussed in the source, Section 3.1, and the encoder, Section 3.2, not only affect the security of a decoy-state BB84 QKD system, but also may compromise the security of a MDI-QKD system that is immune to all attacks on the measurement unit. Since the MDI-QKD is out of the scope of this review, we will not discuss the security threat of it in detail here.

3.3. Decoder

At Bob's side, the decoder module shall randomly choose the basis bit and the information bit as introduced in 2. In practice, these random choices may be known or controlled by Eve via the following attacks.

Regarding the basis bit, Bob may actively choose his basis with a modulator. Therefore, similar to the encoder, the choice of Bob's basis may be eavesdropped by the Trojan horse attack on the modulator [46]. However, to reduce the probability that the Trojan horse light is detected by Bob's SPDs, Eve may employ a hacking laser with a wavelength out of the SPDs' sensitive range [47], which helps Eve hide her attack.

Another configuration of basis selection, named passive choice of measurement basis, is realized by a 50:50 beam splitter (BS). The randomness of the basis bit relays on the coupling ratio of the BS at the working wavelength, such as 1550 nm for a fiber-based QKD system. However, Eve may perform the wavelength-dependent attack [48]. Eve intercepts Alice's state and resends a faked state whose wavelength depends on its basis. As shown in Figure 7, the different wavelengths may result in highly unbalanced coupling ratio of the BS, such as 99:1 or 1:99, which almost certainly determines the selection of the measurement basis.

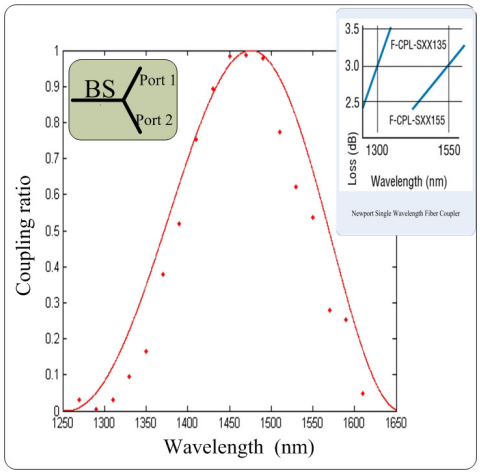

Figure 7. The change of coupling ratio depending on the wavelength, which can be exploited by Eve to conduct the wavelength-dependent attack. Reprinted from Ref. [48].

The information bit is registered by the click from one of two Bob's SPDs in the same basis. This result shall be fully determined by the randomness of Alice's quantum state. However, in practice, Eve also can control the click of Bob's SPDs, which breaks the randomness of the information bit (see Section 2 for the details). For example, Eve may exploit the loopholes of the SPDs to control the information bit. These types of attacks have been discovered the most so far, in which Eve tailors the arriving time, the intensity, the phase, or the polarization of the hacking pulses.

There are various types of attacks controlling the detection results by manipulating the arriving time of the hacking pulses, such as the time-shift attack [49], the efficiency mismatch attack [50,51], the dead-time attack [52], the after-gate attack [53], and the super-linearity attack [54].

A typical detection efficiency curve is shown in Figure 8a, in which two detectors present a mismatch at point A and B. Then Eve can conduct the time-shift attack [49] by controlling the transmission delay of Alice's pulse. Once the pulse passes through the shorter arm (Figure 8b) and arrives at moment A (Figure 8a), '"Detector 0" clicks with a higher probability than that of '"Detector 1", and vice versa.

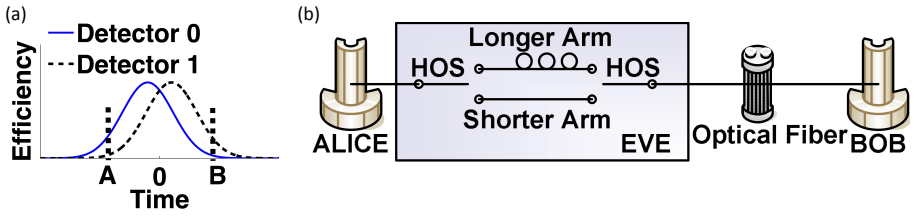

Figure 8. The working principle of time-shift attack. (**a**) The typical mismatched curves of detection efficiency. (**b**) The scheme of experimental demonstration. Reprinted from Ref. [49].

Another typical time-related attack is the dead-time attack [52]. Instead of tampering the signal state, Eve sends a faked state with multiple photons, for example $|-\rangle$ in Figure 9a, slightly before the signal state. The faked state triggers D_H, D_-, and D_V click, following a period of dead time τ_D, during which these three detectors are not sensitive to incoming photons. Only when the signal state of Alice is orthogonal to the faked state ($|+\rangle$), Bob registers a valid click on D_+. To avoid extra QBER, Eve's faked state must be out of the detection time window Δ_{tw}, while the signal state must be in the dead time period as shown in Figure 9b.

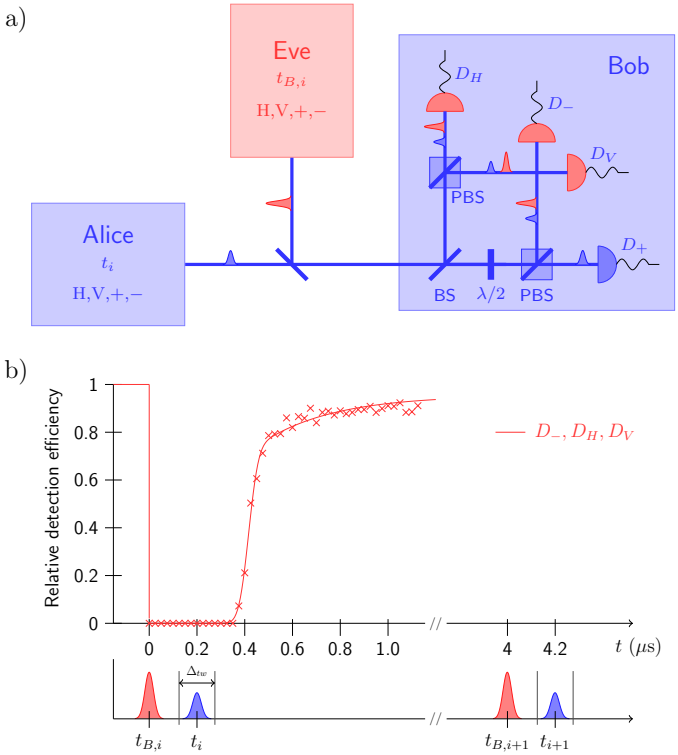

Figure 9. The illustration of dead-time attack. Reprinted from Ref. [52]. (**a**) The scheme of the dead-time attack; (**b**) the timings of faked pulses and signal pulses with detection efficiency of signal pulses under dead-time attack.

By tailoring the intensity of the faked state, Eve also can control the information bit via the blinding attack [26,55,56]. Specifically, Eve first applies a strong continuous wave or pulsed light to transfer the SPD from the Geiger mode to the linear mode, then the SPD is no longer sensitive to a single photon. This is because, as shown in Figure 10a, the resistor R_bias reduces the voltage across the APD to be lower than the breakdown voltage (Figure 10b), once a bright light illuminates at the APD. Then the blinded detector is employed in the "fake-state" attack. Eve intercepts Alice's state and resends a faked state with a well-designed intensity to the blinded detector. The faked state triggers a click with high probability, even 100%, once Bob and Eve choose the same basis. Otherwise, Bob's SPD almost does not click.

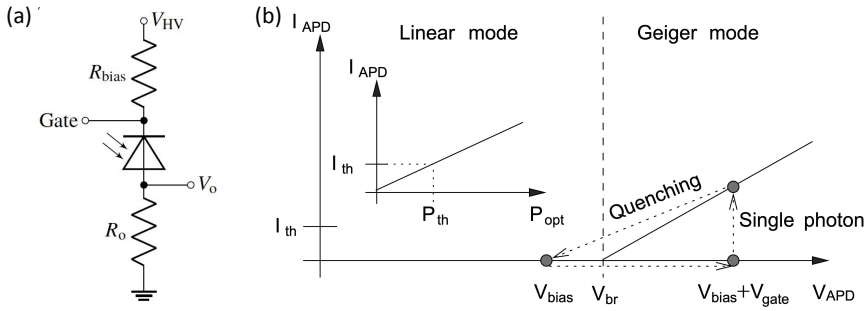

Figure 10. The illustration of the blinding attack. (**a**) The equivalent circuit related to the APD in a detector, reprinted from [56]; (**b**) the working modes of a APD, reprinted from Ref. [26].

By increasing the power of the hacking light, Eve can conduct the laser damage attack to actively engineer multiple loopholes of a well-characterized detector [37]. A bright light with power 0.3 to 0.5 W can reduce the detection efficiency of the SPD by 80%–90%. This hacking light with a certain encoded state would permanently decrease the

detection efficiency of a target SPD, which creates an efficiency mismatch between SPDs in Bob. Moreover, increasing the hacking power in the range from 1.2 to 1.7 W, the SPD is permanently blinded into the linear mode. Then, Eve performs the same as the blinding attack mentioned above, and the detector is fully controllable. In terms of the other power level, Eve may also change the characteristics of the detector, but there seems to be no help for Eve [37]. When the power of the hacking laser is over a threshold, 2 W in this case, the detector is catastrophically damaged.

3.4. Detector

The side channels of the detectors may leak the result of the detection, even though the decoder module randomly decodes the basis bit and the information bit. For example, the backflash attack takes advantage of the phenomenon that an APD has a chance to emit photons back to the channel after each detection [57]. The backflashed photon may be varied in the polarization, reflection time, and so on, depending on which SPD it comes from. Therefore, Eve can tell the clicked detector to learn the secret information. Another possible side channel in the detector is in the timing domain. Since the optical path to each detector or the response time of each detector may be slightly different, the registration time of detection might be varied depending on different detectors. If Eve has access to this timing side channel, she can derive the secret information [58].

4. Security Model and Parameters

According to the discussion above, Eve can break some security requirements and perform quantum hacking by exploiting the imperfections of practical devices. In this section, we show how to define the main security parameters in each module to describe the deviation between the theoretical requirement and the practical implementation. Before the main text, we give some discussions about the security parameter here. First, although the main security parameters are shown, the final key rate is not discussed in this paper. This is because it is still an open and very difficult question to calculate the final key rate by taking all the security parameters in one general security model. In some previous works [59,60], the flaws in the source and encoder were analyzed together, but most of flaws in the decoder and detector are still excluded. Second, these security parameters are measurable, and thus the legitimate parties can measure these parameters in the security evaluation phase, then evaluate the practical security and performance. In fact, by taking these security parameters into the key rate or monitoring them in real time, almost all of the discovered quantum hacking can be efficiently defeated.

4.1. Source

4.1.1. The Intensity and Photon Number Distribution

Generally speaking, in order to estimate the contribution of the single-photon pulses, Alice should know the PND of her source $\{P_n\}$. However, the PND varies in the practical systems due to the fluctuation of the average intensity of the optical pulse [61], or Eve's active attacks [30,31]. Thus, Alice should estimate the upper and lower bounds of the probability for each n-pulse, which is defined as

$$P_n \in [P_n^L, P_n^U]. \tag{1}$$

Strictly speaking, Alice should measure the PND for the source with a photon number resolving detector. However, it is still quite experimentally challenging to achieve because only a few photons can be probably distinguished for some state-of-the-art detectors [62,63]. Thus, a reasonable assumption for Alice is that the source is a coherent state (any other source with a known PND in theory, such as the heralded single photon source [64], also can be analyzed with the same method given above) which is widely used in practical systems, and the variability of the PND can be estimated by the fluctuation of the average intensity of the source [38,61].

With the assumption given above, the deviation of the average intensity of the source is a proper parameter to bound the PND [61]. When Alice sends an optical pulse with average intensity μ, the factual intensity is bounded by

$$\mu \in \{\mu_L, \mu_U\}. \tag{2}$$

Then, Alice can redefine the average intensity of the optical pulses and the deviation of intensity, which are given by [61]

$$\begin{aligned} \overline{\mu} &= (\mu_U + \mu_L)/2, \\ \varepsilon_\mu &= |\mu_U - \overline{\mu}|. \end{aligned} \tag{3}$$

Thus, for the WCS, the bounds of the probability for each $n-$photon pulse are given by

$$P_n^L = \frac{(\overline{\mu} - \varepsilon_\mu)^n}{n!} e^{-(\overline{\mu}-\varepsilon_\mu)}, \qquad P_n^U = \frac{(\overline{\mu} + \varepsilon_\mu)^n}{n!} e^{-(\overline{\mu}+\varepsilon_\mu)}. \tag{4}$$

4.1.2. The Random Phase of Source

In order to estimate the yield and error rate of the single photon pulses in the decoy state method, the source should be considered a mixed state of all photon number states. This assumption is valid only when the phase of the WCS is uniformly randomized within $[0, 2\pi]$. Then the density matrix of the WCS can be written as

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi} |\sqrt{\mu} e^{i\theta}\rangle\langle\sqrt{\mu} e^{i\theta}| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n.| \tag{5}$$

Here, μ is the average intensity of the source, $|n\rangle$ is the Fock state with $n-$photon. Note that the security of BB84 also can be guaranteed with the discrete-phase-randomized WCS by modifying the post processing [65].

However, the phase-random assumption should be broken by Eve's active attacks [28,29,66] as described in Section 3. Thus, the practical density matrices for each encoded state should be rewritten as

$$\rho_{\alpha_i} = \int_0^{2\pi} d\theta P(\theta) |\alpha_i e^{i\theta}\rangle\langle\alpha_i e^{i\theta}|, \tag{6}$$

where $\alpha = z, x$ is the basis, $i = 0, 1$ is the bit for each basis, and $P(\theta)$ is the probability distribution of phase θ. The detailed expression of $|\alpha_i e^{i\theta}\rangle$ depends on the encoding of the QKD protocol. For example, $|\alpha_i e^{i\theta}\rangle = |\alpha e^{i\theta}\rangle$ for the polarization encoding, and $|\alpha_i e^{i\theta}\rangle = |\alpha e^{i(\theta+\varphi_i)}\rangle_s |\alpha e^{i\theta}\rangle_r$ for the phase encoding. Here, φ_i is the encoded phase, and the subscript $s(r)$ means the signal (reference) pulse.

For the given state of Equation (6), the virtual entanglement states between Alice and Bob can be written as

$$\begin{aligned} \rho_z &= \frac{1}{2}(|z_0\rangle\langle z_0| \otimes \rho_{z_0} + |z_1\rangle\langle z_1| \otimes \rho_{z_1}), \\ \rho_x &= \frac{1}{2}(|x_0\rangle\langle x_0| \otimes \rho_{x_0} + |x_1\rangle\langle x_1| \otimes \rho_{x_1}). \end{aligned} \tag{7}$$

Here, $|z_{0(1)}\rangle$ and $|x_{0(1)}\rangle$ are the ideal quantum states required by the BB84 protocol. When the phase of the source is not uniformly randomized, the measured bit error in the x-basis does not equal the phase error in the z-basis. The phase error can be bounded by the measured bit error and the following parameter [23]

$$\varepsilon_{RP} = \frac{1}{2}[1 - F(\rho_z, \rho_x)], \tag{8}$$

where $F(\rho, \sigma)$ is the fidelity between ρ and σ.

4.1.3. The Distinguishability of the Decoy States

For the discrete variable QKD with a non-single-photon source, the decoy state method [17–19] is considered one of the best ways to defeat photon-number-dependent attacks [11,12]. One of the basic assumptions for the decoy state method is that all the decoy states should be indistinguishable, except for the intensity. However, this assumption is hard to be guaranteed for some practical systems, due to the active attacks of Eve or passive side channels of Alice's source [32,67].

When the side channels are taken into account, the density matrix of the decoy state with intensity μ_i can be written as

$$\rho_{\mu_i}(\omega) \equiv \rho_{\mu_i}(t, \lambda, w, \cdots), \tag{9}$$

where, ω includes all the side channels that can be exploited by Eve to distinguish the decoy states, such as time t, wavelength λ, waveform w, and so on. According to the analysis of Refs. [32,67], the distinguishability of the decoy states can be defined as

$$\varepsilon_{DS} = \max_{i,j} \varepsilon_{DS}^{ij} \equiv \max_{i,j} \frac{1}{2} D(\rho_{\mu_i}, \rho_{\mu_j}), \tag{10}$$

here, $D(\rho, \sigma)$ is the trace distance of ρ and σ.

4.2. Encoder

4.2.1. The Inaccuracy of the Encoded State

Due to the finite extinction ratio of practical optical devices or Eve's active attacks [43], the practical encoded states of Alice may be different from the ideal states required by the QKD protocol. For example, Alice wants to send a quantum state $|H\rangle$, but the practical state sent by her may be $\cos\theta|H\rangle + \sin\theta|V\rangle$ with a small angle deviation $\theta \neq 0$. The density matrix of the practical encoded state can be written as $\rho_{\alpha_i}^{en}$. Simply, if we assume that the encoded state of Alice is pure, then

$$\rho_{\alpha_i}^{en} = P[\cos\theta_{\alpha_1}|\alpha_0\rangle + \sin\theta_{\alpha_1}|\alpha_1\rangle] \tag{11}$$

where $P[|a\rangle] = |a\rangle\langle a|$ is the project operator. Then the deviation of the encoded state can be written as

$$\varepsilon_{EN} = \max_{\alpha_i,\beta_j} \varepsilon_{EN}^{\alpha_i,\beta_j} = \max_{\alpha_i,\beta_j} \frac{1}{2}[1 - F(\rho_{\alpha_i}^{en}, \rho_{\beta_j}^{en})]. \tag{12}$$

Here, we consider the worst case by maximizing $\varepsilon_{EN}^{\alpha_i,\beta_j}$ for all $\alpha, \beta = x, z$ and $i, j = 0, 1$.

4.2.2. The Side Channel of Encoder

The encoded states of Alice may be distinguishable in the non-encoded degrees of freedom, whose examples are given in Section 3. Then the practical density matrix of the encoded state should be written as

$$\rho_{\alpha_i}^{si} = (\omega) = \rho_{\alpha_i}^{si}(t, \lambda, w, \cdots) \tag{13}$$

where ω includes all the side channels that can be exploited by Eve to distinguish the encoded state. The distinguishability of the side channels can be defined as

$$\varepsilon_{SI} = \max_{\alpha_i,\beta_j} \varepsilon_{SI}^{\alpha_i,\beta_j} = \max_{\alpha_i,\beta_j} \frac{1}{2}\left[1 - F(\rho_{\alpha_i}^{si}, \rho_{\beta_j}^{si})\right] \tag{14}$$

In all the side channels, the Trojan horse attack plays an important role since it is one of the most well-known attacks in both classical and quantum communication. Here, we only consider the optical Trojan horse attack in QKD processing. When an optical pulse

with intensity μ is reflected from Alice's zone, the quantum state of such a Trojan horse photon can be written as

$$|\sqrt{\mu_{\alpha_i}^{th}}\rangle, \tag{15}$$

where the subscription α_i means the encoded state of Alice, and the superscription th means the Trojan horse pulse. We assume that the quantum state above is pure to maximize Eve's information. Thus, the deviation of the Trojan horse photon belonging to each α_i can be defined as

$$\varepsilon_{TH} = \max_{\alpha_i,\beta_j} \varepsilon_{TH}^{\alpha_i,\beta_j} = \max_{\alpha_i,\beta_j} \frac{1}{2}\left[1 - \left|\langle\sqrt{\mu_{\alpha_i}^{th}}|\sqrt{\mu_{\beta_j}^{th}}\rangle\right|^2\right] \tag{16}$$

4.3. Channel

In the security model of QKD, it is assumed that the channel is totally controlled by Eve who can do any operation and measurement admitted by the quantum mechanics. Thus, generally speaking, the imperfections of the quantum channel will not break the security of the generated key. However, the performance of the QKD system is compensated by the loss of the quantum channel. First, the final key rate is directly reduced by the loss and noise of the quantum channel. Second, the flaws of source could be amplified by the loss of the quantum channel [23].

For a quantum channel with transmittance η, the total count rate is the function of the loss, $Q = Q(\eta)$. The deviation of source flaws (ε_{EN}, ε_{SI}, and ε_{TH}) should be rewritten as [23]

$$\varepsilon_\gamma \to \varepsilon_\gamma / Q(\eta), \tag{17}$$

where $\gamma = EN, SI, TH$. Obviously, the deviation is large for long-distance communication. In order to overcome this problem, by introducing the "qubit" assumption, the loss-tolerant protocol was proposed by Tamaki et al. [68]. However, because of the side channels of the encoder [45] described in the next subsection, the "qubit" assumption is hard to be guaranteed in practical systems. Thus, the loss-tolerant protocol is not analyzed here.

4.4. Decoder

When the encoded states are flying into Bob's zone, he randomly measures it with one of two bases. That is, the basis bit is randomly chosen by Bob (actively or passively). In each basis, the photon arrives at one of two SPDs to decide the value of Bob's information bit. Strictly speaking, both the basis bit and the information bit should be totally random. However, due to the imperfection of the decoder, they could be controlled by Eve, such as the wavelength-dependent attack [48] and the detection efficiency mismatch attack [49] described in Section 3.

The weak randomness of Bob's basis bit (x_0) and information bit (x_1) can be analyzed by introducing two hidden variables λ_0^{de} and λ_1^{de} [24,25]. By controlling λ_0^{de} and λ_1^{de}, Eve can determine x_0 and x_1 for each pulse. Setting $k, k' \in \{0, 1\}$ as the value of x_0 and x_1, the probabilities that Bob obtains $x_0 = k$ and $x_1 = k'$ are respectively given by

$$\begin{aligned} p(x_0 = k) &= \sum_i p(\lambda_0 = i) p(x_0 = k | \lambda_0 = i) \\ p(x_1 = k') &= \sum_j p(\lambda_1 = j) p(x_1 = k' | \lambda_1 = j), \end{aligned} \tag{18}$$

where $\sum_i p(\lambda_0 = i) = \sum_j p(\lambda_1 = j) = 1$. $p(x_0 = k|\lambda_0 = i)$ is the conditional probability that Bob obtains $x_0 = k$, given the hidden variable $\lambda_0 = j$, and $p(x_1 = k'|\lambda_1 = j)$ has the same definition. Obviously, Eve can determine the basis-bit and information-bit for each pulse by controlling the probability $p(\lambda_0 = i)$ and $p(\lambda_1 = j)$. Thus, the conditional probabilities

$p(x_0 = k|\lambda_0 = i)$ and $p(x_1 = k'|\lambda_1 = j)$ represent Bob's basis bit and information bit leaked to Eve. In other words, the deviation of the decoder can be defined as [24,25]

$$\begin{aligned} \varepsilon_{DE}^{basis} &= \max_i \varepsilon_{DE}^{basis,i} = \max_i |p(x_0 = k|\lambda_0 = i) - 1/2| \\ \varepsilon_{DE}^{bit} &= \max_j \varepsilon_{DE}^{bit,j} = \max_j |p(x_1 = k'|\lambda_1 = j) - 1/2|. \end{aligned} \tag{19}$$

Here we remark that in Equation (19), the deviation of basis bit (x_0) and information bit (x_1) are analyzed independently. However, generally speaking, Eve can control x_0 and x_1 at the same time with a joint hidden variable λ. Then Equation (19) should be rewritten as

$$\varepsilon_{DE} = \max_\lambda \varepsilon_{DE}^{\lambda} = \max_\lambda |p(x_0 = k, x_1 = k'|\lambda) - 1/4|. \tag{20}$$

4.5. Detector

In the BB84 protocol, two or four SPDs are required by Bob to register the photon of Alice. There are two major imperfections for these SPDs. One is that the efficiency of these SPDs may depend on the parameters of the optical pulse, such as the time, wavelength, polarization, photon number (or intensity), and so on. The other one is the side channels, such as the reflection light [27,57,69].

For the first one, since each SPD represents the basis bit or information bit, it can be considered the flaw of the decoder (see Equation (19)). In this subsection, only the second one should be analyzed. The density matrix of the photon emitted into the quantum channel from Bob's zone can be written as $\rho_{\alpha_i}^{Det}$. Then, Eve can guess which SPD clicks for each pulse by measuring the leakage signal. Thus, the deviation of the side channels can be defined as

$$\varepsilon_{Det} = \max_{\alpha_i,\beta_j} \varepsilon_{Det}^{\alpha_i,\beta_j} = \max_{\alpha_i,\beta_j} D(\rho_{\alpha_i}^{Det}, \rho_{\beta_j}^{Det}), \tag{21}$$

where $D(a, b)$ is the trance distance between a and b.

5. Security Evaluation and Standardization

The implementation of QKD systems, especially decoy-state BB84 ones, continues to mature. Commercial QKD products based on the decoy-state BB84 protocol are available in the market. Moreover, large-scale QKD networks all over the world are being deployed. During the commercialization and globalization of QKD, the reliability in use is essential for practical QKD systems, which highly depends on the security performance of the practical QKD system. However, as discussed in Section 3, the violation of the security requirement may be exploited by Eve to perform quantum hacking and then may threaten the practical security of a QKD system. In order to close the possible security loopholes (quantum attacks) and support the reliable use, one shall conduct the evaluation to verify the practical security of a QKD system. Generally speaking, in the evaluation phase, all the security parameters given in Section 4 should be carefully measured to guarantee that they are lower than the given threshold. Moreover, the optical and electrical signal also should be carefully monitored in the key-exchange phase to make sure that the evaluated security parameters are valid in practical situations. In other words, the evaluation phase provides the confidence to the QKD users and broadens the deployed range of QKD systems (if a QKD system passes through the evaluation test, it is secure even if there exist flaws).

To evaluate the security performance of a QKD system, the tester mimics as a quantum hacker to attack the QKD system under test, which may disclose the security vulnerabilities or show the defense against the attacks. For each testing item, the testing procedure follows the steps of conducting a certain quantum attack. Then, the corresponding behavior of the QKD system under attack shall be judged by a quantified criteria with a pass/failure threshold. For the decoy-state BB84 QKD system considered in this paper, most of the attacks described in Section 3 can be tested. Furthermore, the testing results can be quantified by the security parameters defined in Section 4.

The typical attacks and the corresponding security parameters are summarized in Table 1. According to Table 1, the attacks affecting the same security parameter in each module are classified, which indicates that fully characterizing a parameter requires multiple tests. The more tests are conducted, the better one knows about the practical performance of a QKD system. Generally, all the security parameters are considered in the final key rate. However, it is still a big challenge to take all of them into account in one security model at the same time.

Table 1. The main quantum attacks and security parameters.

Target	Attacks	Exploited Imperfections	Security Parameters
Source	Source attack [28,29]	Nonrandom phase	ε_{RP}
	Laser injection [30]	Nonrandom phase under laser injection	ε_{RP}
	Distinguishable decoy states [32]	Pump-current intensity modulation	ε_{DS}
	Side channels in free-space Alice [33]	Multiple laser diodes	ε_{DS}
	Intersymbol effect [34]	Intensity correlation between neighboring pulses	$\overline{\mu}$, ε_{μ}
	Wavelength-selected [35]	Intensity-related change in wavelength	$\overline{\mu}$, ε_{μ}
	Laser injection [31]	Increased intensity under laser injection	$\overline{\mu}$, ε_{μ}
	Laser damage [38]	Reduced attenuation under high-power illumination	$\overline{\mu}$, ε_{μ}
Encoder	Source flaw [42]	Inaccurate state modulation	ε_{EN}
	Phase remapping [43]	Incorrect encoding among transition edges of modulation	ε_{EN}
	Trojan horse [44,45]	Reflection photon from injected laser	ε_{SI} (ε_{TH})
Decoder	Trojan horse [46,47]	Reflection photon from injected laser	ε_{DE}^{basis}
	Phase remapping [43]	Incorrect decoding among transition edge of modulation	ε_{DE}^{basis}
	Wavelength-dependent [48]	Wavelength-dependent coupling ratio of BS	ε_{DE}^{basis}
	Time shift [49]	Mismatched detection efficiencies	ε_{DE}^{bit}
	Efficiency mismatch [50,51]	Mismatched detection efficiencies	ε_{DE}^{bit}
	Dead time [52]	Individual dead time of each detector	ε_{DE}^{bit}
	After gate [53]	Linear mode of SPD	ε_{DE}^{bit}
	Superlinearity attack [54]	Superlinear response of SPD among transition edges	ε_{DE}^{bit}
	Detector blinding [26,55,56]	Linear mode of SPD	ε_{DE}^{bit}
	Laser damage [37]	Mismatched detection efficiencies and linear mode of SPD	ε_{DE}^{bit}
Detector	Backflash attack [57]	Backward-transmitted photons	ε_{Det}
	Timing side channel [58]	Detector-related detection timing tag	ε_{Det}

This methodology of evaluation is possible to be standardized to serve as a third party certification for all decoy-state BB84 systems. The standardized verification provides a person-independent evaluation outcome, helping the customers build confidence and trust in QKD products. Most importantly, the security standard also guides the commercial company to produce the QKD products with high security performance, which promotes global deployment and enhances their application in various situations. The security evaluation standards are established by many organizations [70–72].

However, we should note that setting the thresholds for these security parameters is still an open question in practical application since a general security model including all the parameters is still unavailable; the final key rate may be rapidly reduced by parts of parameters, making the QKD system unusable. Therefore, a practical choice for the security evaluation and standard is to divide all the security parameters as two parts; one is considered in the security model (called *analyzed parameter*), and the other one is monitored (called *monitored parameter*). If a security parameter is analyzed in a security model, and some quantum hacking strategies by exploiting this loophole are discovered, this security parameter can be called an *analyzed parameter*. For these analyzed parameters, the QKD system is secure, no matter which threshold is set (the threshold only determine the final key rate). If a security parameter is not included in the security model, or no efficient hacking strategy is discovered by exploiting this loophole, this security parameter is called a *monitored parameter*. For these monitored parameters, the threshold should be carefully set to make sure that Eve's potential attack can be removed within the current technology.

Author Contributions: S.S. wrote the paper for Section Sections 1, 2 and 4, and A.H. wrote the paper for Section Sections 3 and 5. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China (grants number 62171485, 61901483 and 62061136011), the National Key Research and Development Program of China (grant number 2019QY0702), and the Youth Talent Lifting Project (grant number 20-JCJQ-QT-045).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All the data are available by contracting the authors.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distribution
PND	Photon number distribution
PNS	Photon number splitting attack
SPS	Single photon source
SPD	Single photon detector
WCS	Weak coherent source

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and con tossing. In Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
2. Inoue, K.; Waks, E.; Yamamoto, Y. Differential Phase Shift Quantum Key Distribution. *Phys. Rev. Lett.* **2002**, *89*, 037902. [CrossRef] [PubMed]
3. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. [CrossRef]
4. Branciard, C.; Gisin, N.; Scarani, V. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New J. Phys.* **2008**, *10*, 013031. [CrossRef]
5. Cerf, N.J.; Lévy, M.; Assche, G.V. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311. [CrossRef]

6. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
7. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef] [PubMed]
8. Stucki, D.; Legré, M.; Buntschu, F.; Clausen, B.; Felber, N.; Gisin, N.; Henzen, L.; Junod, P.; Litzistorf, G.; Monbaron, P.; et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **2011**, *13*, 123001. [CrossRef]
9. Wang, S.; Chen, W.; Yin, Z.Q.; Li, H.W.; He, D.Y.; Li, Y.H.; Zhou, Z.; Song, X.T.; Li, F.Y.; Wang, D.; et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **2014**, *22*, 21739–21756. [CrossRef]
10. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef]
11. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef] [PubMed]
12. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
13. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
14. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
15. Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501. [CrossRef] [PubMed]
16. Pironio, S.; Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Scarani, V. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **2009**, *11*, 045021. [CrossRef]
17. Hwang, W.Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
18. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
19. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
20. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
21. Ma, X.; Yuan, X.; Cao, Z.; Qi, B.; Zhang, Z. Quantum random number generation. *Npj Quantum Inf.* **2016**, *2*, 16021. [CrossRef]
22. Herrero-Collantes, M.; Garcia-Escartin, J.C. Quantum random number generators. *Rev. Mod. Phys.* **2017**, *89*, 015004. [CrossRef]
23. Lo, H.K.; Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quantum Info. Comput.* **2007**, *7*, 431–458. [CrossRef]
24. Li, H.W.; Yin, Z.Q.; Wang, S.; Qian, Y.J.; Chen, W.; Guo, G.C.; Han, Z.F. Randomness determines practical security of BB84 quantum key distribution. *Sci. Rep.* **2015**, *5*, 16200. [CrossRef] [PubMed]
25. Sun, S.H.; Tian, Z.Y.; Zhao, M.S.; Ma, Y. Security evaluation of quantum key distribution with weak basis-choice flaws. *Sci. Rep.* **2020**, *10*, 18145. [CrossRef] [PubMed]
26. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
27. Pinheiro, P.V.P.; Chaiwongkhot, P.; Sajeed, S.; Horn, R.T.; Bourgoin, J.P.; Jennewein, T.; Lütkenhaus, N.; Makarov, V. Eavesdropping and countermeasures for backflash side channel in quantum cryptography. *Opt. Express* **2018**, *26*, 21020–21032. [CrossRef]
28. Tang, Y.L.; Yin, H.L.; Ma, X.; Fung, C.H.F.; Liu, Y.; Yong, H.L.; Chen, T.Y.; Peng, C.Z.; Chen, Z.B.; Pan, J.W. Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **2013**, *88*, 022308. [CrossRef]
29. Sun, S.H.; Gao, M.; Jiang, M.S.; Li, C.Y.; Liang, L.M. Partially random phase attack to the practical two-way quantum-key-distribution system. *Phys. Rev. A* **2012**, *85*, 032304. [CrossRef]
30. Sun, S.H.; Xu, F.; Jiang, M.S.; Ma, X.C.; Lo, H.K.; Liang, L.M. Effect of source tampering in the security of quantum cryptography. *Phys. Rev. A* **2015**, *92*, 022304. [CrossRef]
31. Huang, A.; Navarrete, A.; Sun, S.H.; Chaiwongkhot, P.; Curty, M.; Makarov, V. Laser-Seeding Attack in Quantum Key Distribution. *Phys. Rev. Appl.* **2019**, *12*, 064043. [CrossRef]
32. Huang, A.; Sun, S.H.; Liu, Z.; Makarov, V. Quantum key distribution with distinguishable decoy states. *Phys. Rev. A* **2018**, *98*, 012330. [CrossRef]
33. Nauerth, S.; Fürst, M.; Schmitt-Manderbach, T.; Weier, H.; Weinfurter, H. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **2009**, *11*, 065001. [CrossRef]
34. Yoshino, K.i.; Fujiwara, M.; Nakata, K.; Sumiya, T.; Sasaki, T.; Takeoka, M.; Sasaki, M.; Tajima, A.; Koashi, M.; Tomita, A. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *Npj Quantum Inf.* **2018**, *4*, 8. [CrossRef]
35. Jiang, M.S.; Sun, S.H.; Li, C.Y.; Liang, L.M. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys. Rev. A* **2012**, *86*, 032310. [CrossRef]

36. Pang, X.L.; Yang, A.L.; Zhang, C.N.; Dou, J.P.; Li, H.; Gao, J.; Jin, X.M. Hacking quantum key distribution via injection locking. *Phys. Rev. Appl.* **2020**, *13*, 034008. [CrossRef]
37. Bugge, A.N.; Sauge, S.; Ghazali, A.M.M.; Skaar, J.; Lydersen, L.; Makarov, V. Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.* **2014**, *112*, 070503. [CrossRef]
38. Huang, A.; Li, R.; Egorov, V.; Tchouragoulov, S.; Kumar, K.; Makarov, V. Laser damage attack against optical attenuators in quantum key distribution. *Phys. Rev. Appl.* **2020**, *13*, 034017. [CrossRef]
39. Takesue, H.; Nam, S.W.; Zhang, Q.; Hadfield, R.H.; Honjo, T.; Tamaki, K.; Yamamoto, Y. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photonics* **2007**, *1*, 343–348. [CrossRef]
40. Yuan, Z.; Dixon, A.; Dynes, J.; Sharpe, A.; Shields, A. Practical gigahertz quantum key distribution based on avalanche photodiodes. *New J. Phys.* **2009**, *11*, 045019. [CrossRef]
41. Tang, Y.L.; Yin, H.L.; Chen, S.J.; Liu, Y.; Zhang, W.J.; Jiang, X.; Zhang, L.; Wang, J.; You, L.X.; Guan, J.Y.; et al. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **2014**, *113*, 190501. [CrossRef]
42. Xu, F.; Sajeed, S.; Kaiser, S.; Tang, Z.; Qian, L.; Makarov, V.; Lo, H.K. Experimental quantum key distribution with source flaws and tight finite-key analysis. *Phys. Rev. A* **2015**, *92*, 032305. [CrossRef]
43. Fung, C.H.F.; Qi, B.; Tamaki, K.; Lo, H.K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* **2007**, *75*, 032314. [CrossRef]
44. Lucamarini, M.; Choi, I.; Ward, M.; Dynes, J.; Yuan, Z.; Shields, A. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Phys. Rev. X* **2015**, *5*, 031030. [CrossRef]
45. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **2006**, *73*, 022320. [CrossRef]
46. Jain, N.; Anisimova, E.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **2014**, *16*, 123030. [CrossRef]
47. Sajeed, S.; Minshull, C.; Jain, N.; Makarov, V. Invisible Trojan-horse attack. *Sci. Rep.* **2017**, *7*, 8403. [CrossRef]
48. Li, H.W.; Wang, S.; Huang, J.Z.; Chen, W.; Yin, Z.Q.; Li, F.Y.; Zhou, Z.; Liu, D.; Zhang, Y.; Guo, G.C.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **2011**, *84*, 062308. [CrossRef]
49. Zhao, Y.; Fung, C.H.F.; Qi, B.; Chen, C.; Lo, H.K. Quantum: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **2008**, *78*, 042333. [CrossRef]
50. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. erratum ibid. **78**, 019905 (2008). [CrossRef]
51. Sajeed, S.; Chaiwongkhot, P.; Bourgoin, J.P.; Jennewein, T.; Lütkenhaus, N.; Makarov, V. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* **2015**, *91*, 062301. [CrossRef]
52. Weier, H.; Krauss, H.; Rau, M.; Fürst, M.; Nauerth, S.; Weinfurter, H. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2011**, *13*, 073024. [CrossRef]
53. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New J. Phys.* **2011**, *13*, 013043. [CrossRef]
54. Lydersen, L.; Jain, N.; Wittmann, C.; Marøy, Ø.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A* **2011**, *84*, 032320. [CrossRef]
55. Huang, A.; Sajeed, S.; Chaiwongkhot, P.; Soucarros, M.; Legré, M.; Makarov, V. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption. *IEEE J. Quantum Electron.* **2016**, *52*, 8000211. [CrossRef]
56. Wu, Z.; Huang, A.; Chen, H.; Sun, S.H.; Ding, J.; Qiang, X.; Fu, X.; Xu, P.; Wu, J. Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination. *Opt. Express* **2020**, *28*, 25574–25590. [CrossRef] [PubMed]
57. Kurtsiefer, C.; Zarda, P.; Mayer, S.; Weinfurter, H. The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? *J. Mod. Opt.* **2001**, *48*, 2039–2047. [CrossRef]
58. Lamas-Linares, A.; Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **2007**, *15*, 9388–9393. [CrossRef]
59. Pereira, M.; Curty, M.; Tamaki, K. Quantum key distribution with flawed and leaky sources. *Npj Quantum Inf.* **2019**, *5*, 62. [CrossRef]
60. Sun, S.; Feihu, X. Security of quantum key distribution with source and detection imperfections. *New J. Phys.* **2021**, *23*, 023011. [CrossRef]
61. Wang, X.B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **2007**, *75*, 052301. [CrossRef]
62. Jahanmirinejad, S.; Frucci, G.; Mattioli, F.; Sahin, D.; Gaggero, A.; Leoni, R.; Fiore, A. Photon-number resolving detector based on a series array of superconducting nanowires. *Appl. Phys. Lett.* **2012**, *101*, 072602. [CrossRef]
63. Jönsson, M.; Björk, G. Evaluating the performance of photon-number-resolving detectors. *Phys. Rev. A* **2019**, *99*, 043822. [CrossRef]
64. Wang, Q.; Chen, W.; Xavier, G.; Swillo, M.; Zhang, T.; Sauge, S.; Tengner, M.; Han, Z.F.; Guo, G.C.; Karlsson, A. Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source. *Phys. Rev. Lett.* **2008**, *100*, 090501. [CrossRef]

65. Cao, Z.; Zhang, Z.; Lo, H.K.; Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.* **2015**, *17*, 053014. [CrossRef]
66. Kobayashi, T.; Tomita, A.; Okamoto, A. Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser. *Phys. Rev. A* **2014**, *90*, 032320. [CrossRef]
67. Tamaki, K.; Curty, M.; Lucamarini, M. Decoy-state quantum key distribution with a leaky source. *New J. Phys.* **2016**, *18*, 065008. [CrossRef]
68. Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **2014**, *90*, 052314. [CrossRef]
69. Meda, A.; Degiovanni, I.P.; Tosi, A.; Yuan, Z.; Brida, G.; Genovese, M. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. *Light. Sci. Appl.* **2017**, *6*, e16261–e16261. [CrossRef]
70. Marco, L.; Andrew, S.; Romain, A.; Christopher, C.; Degiovanni, I.; Gramegna, M.; Atilla, H.; Bruno, H.; Rupesh, K.; Andrew, L.; et al. Implementation Security of Quantum CryptographyIntroduction, Challenges, Solutions | ETSI White Paper No. 27. 2018. Available online: http://hdl.handle.net/11696/59931 (accessed on 20 December 2021).
71. ISO/IEC CD 23837-1.2: Information Technology Security Techniques—Security Requirements, Test and Evaluation Methods for Quantum Key Distribution—Part 1: Requirements. Available online: https://www.iso.org/standard/77097.html (accessed on 20 December 2021).
72. ISO/IEC CD 23837-2.2: Information Technology Security Techniques—Security Requirements, Test and Evaluation Methods for Quantum Key Distribution—Part 2: Evaluation and Testing Methods. Available online: https://www.iso.org/standard/77309.html (accessed on 20 December 2021).