entropy

MDPI

Article

Practical Security of High-Dimensional Quantum Key Distribution with Intensity Modulator Extinction

Yang Wang [1,2,3,*], Ge-Hai Du [2,3], Yang-Bin Xu [2,3], Chun Zhou [2,3], Mu-Sheng Jiang [2,3], Hong-Wei Li [2,3] and Wan-Su Bao [2,3]

1 National Laboratory of Solid State Microstructures, School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China
2 Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, China; dgh@qiclab.cn (G.-H.D.); xyb@qiclab.cn (Y.-B.X.); zc@qiclab.cn (C.Z.); jms@qiclab.cn (M.-S.J.); lhw@qiclab.cn (H.-W.L.); bws@qiclab.cn (W.-S.B.)
3 Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
* Correspondence: wy@qiclab.cn

Abstract: Quantum key distribution (QKD) has attracted much attention due to its unconditional security. High-dimensional quantum key distribution (HD-QKD) is a brand-new type of QKD protocol that has many excellent advantages. Nonetheless, practical imperfections in realistic devices that are not considered in the theoretical security proof may have an impact on the practical security of realistic HD-QKD systems. In this paper, we research the influence of a realistic intensity modulator on the practical security of HD-QKD systems with the decoy-state method and finite-key effects. We demonstrate that there is a certain impact in the secret key rate and the transmission distance when taking practical factors into security analysis.

Keywords: quantum key distribution; high-dimensional; practical security; intensity modulator extinction

Citation: Wang, Y.; Du, G.-H.; Xu, Y.-B.; Zhou, C.; Jiang, M.-S.; Li, H.-W.; Bao, W.-S. Practical Security of High-Dimensional Quantum Key Distribution with Intensity Modulator Extinction. *Entropy* **2022**, *24*, 460. https://doi.org/10.3390/e24040460

Academic Editors: Leong Chuan Kwek, Xiang-Bin Wang and Cong Jiang

Received: 10 January 2022
Accepted: 25 March 2022
Published: 26 March 2022

1. Introduction

Quantum key distribution (QKD) [1,2] initiates a novel routine of secret key sharing between two distant parties (usually called Alice and Bob) in the presence of an eavesdropper (called Eve). Since the proposal of the first QKD protocol—BB84 protocol [1]—QKD has become the focus point of quantum information technology [3,4]. The unconditional security of QKD, which is guaranteed by the laws of quantum mechanics, has already been proved via different methods [5–7]. After the traditional BB84 protocol, various types of new QKD protocols have been proposed. Among these, high-dimensional quantum key distribution (HD-QKD) has garnered much attention due to its excellent capacity of encoding multiple bits on one single photon and strong tolerance to channel noise. In high-dimensional quantum key distribution systems, information is encoded on high dimensional degree of freedom of quantum state, such as time-energy entanglement [8–10], time-bin encoding [11,12], path [13,14] and orbital angular momentum [15–17]. Security proof for the HD-QKD protocol has also been established [18–20]. With the technological development of high-dimensional quantum state preparation and measurement, different HD-QKD schemes have achieved a number of record-breaking results in recent years [21–23]. Thereinto, time-bin based HD-QKD scheme [11,23] has realized a record high secret key rate and can offer security against general coherent attacks.

Unfortunately, practical devices in realistic QKD systems often present imperfections and rarely conform to theoretical security models [24,25]. Therefore, there is always a gap between the theory and practice of QKD. During the past decades, the practical security of QKD systems has been researched extensively. The eavesdropper can steal

secret key information between Alice and Bob by seeking and utilizing side-channels introduced by different imperfect devices. For example, an imperfect phase modulator would introduce phase-remapping attacks [26], a realistic fiber beam splitter may provide convenience to wavelength attacks [27], and practical single photon detectors (SPDs) could be affected by time-shift attacks [28], faked state attacks [29] and detection blinding attacks [30,31]. Fortunately, efforts have been focused on proposing corresponding feasible countermeasures [32–34], and robust QKD protocols have been proposed, which are immune against detection-side-channel attacks, e.g., measurement-device-independent QKD (MDI-QKD) [35,36] and twin-field QKD (TF-QKD) [37–40]. On this account, it is of great significance to analyze how imperfections in realistic transmitters influence the practical security of QKD. Since the practical intensity modulators (IMs), which have been used in practical transmitters, are band limited, electrical signal distortion may cause intensity fluctuations of pulses and other phenomena [41,42]. Therefore, it is important to quantitatively evaluate the imperfections in IMs for the security certification of practical QKD systems.

Analogously, there is also a deviation between theoretical security and practical performance in HD-QKD systems. Although theoretical security analysis for HD-QKD protocol is exhaustive, its practical feasibility is far from sufficient. Toward this end, research on the practical security analysis of HD-QKD protocol is ongoing. In realistic experimental implementations, the requirement for single photon sources is not easily satisfied, the weak coherent source is employed instead. This kind of source contains multi-photon signals and the eavesdropper can carry out the photon number-splitting (PNS) attack [43,44] to steal secret keys. Zhang et al. [45] applied decoy-state methods [46–48] to the HD-QKD protocol to defeat the PNS attack with an infinite number of decoy states and proved its security against collective attacks. Afterwards, the security analysis of the HD-QKD protocol employing a practical number of decoy states is followed [49]. In addition, the number of transmitted signals is always finite in practical QKD processes. This would bring in another practical issue: finite-key problem. There exists fluctuations between practical measurement output and theoretical estimation and the secret key rate would be calculated by mistake. Scarani et al. [50] and Tomamichel et al. [51] analyzed the practical finite-key security of the BB84 protocol under collective attacks and coherent attacks at the first step. Following the methods proposed in refs. [50,51], the practical security of decoy-state HD-QKD protocol against collective attacks [52] and coherent attacks [53] in the finite-key scenario is established. In decoy-state methods, the intensities of signal state and decoy states should be stable and controllable. Nonetheless, an unstable source would lead to intensity fluctuations in practical QKD systems. When there exist intensity fluctuations, the original characterization of the decoy-state method needs further improvement [54,55]. The effects of both intensity fluctuations of sources and statistical fluctuations have been discussed [56], and the results on the secret key rate were then further improved [57]. Following the approach to describing the intensity fluctuations proposed by Wang et al. [55,56], tight finite-key analysis for practical decoy-state QKD protocols with unstable sources is proposed [58–60]. To guarantee its practical performance, the practical security analysis of HD-QKD protocol needs further investigations.

In realistic implementations, the intensity modulator on Alice's side is used to attenuate the light intensity and filter out some redundant light pulses. One important parameter of IM is the extinction ratio, which appears as a fixed finite value (ranging from 20 dB to 40 dB usually). In ref. [61], the finite extinction of imperfect intensity modulators in the BB84 system was investigated. It is surprising that the extra noise caused by realistic IM reduces Eve's information. The secret key rate is increased and practical security is enhanced. To investigate the practical security of the HD-QKD protocol, we focus our attention on the impact of this realistic imperfection on practical HD-QKD systems in this work. We characterize a model of extinction ratio and derive a new expression of quantum bit error rates for HD-QKD. Then, the maximal tolerable quantum bit error rate and secret key rate are calculated for HD-QKD with the single photon state and the decoy-state

method, respectively. The combined effect of the finite extinctions of intensity modulator and intensity fluctuations of the source in the finite-key scenario is analyzed as well.

The rest of this paper is organized as follows. In Section 2, we present a brief introduction on the state preparation and transmission processes of the HD-QKD system and establish the model characterization of the extinction ratio. In Section 3, we analyze the practical security of HD-QKD system with the single-photon source and the decoy-state method, respectively. Some further discussions on the combined influence of the finite extinction and intensity fluctuations on the practical security of HD-QKD system were also put forward. Simulation results are depicted in Section 4 and some conclusive comments are summarized in Section 5.

2. Model Characterization of the Extinction Ratio

Without a loss of generality, we take the four-dimensional time-bin HD-QKD scheme [11] for example. As illustrated in Figure 1, Alice employs two intensity modulators and one phase modulator controlled by a field programmable gate array (FPGA) to fabricate time-bin states $|t_n\rangle$ and phase states $|f_n\rangle$, which are the discrete Fourier transforms of time-bin states where $|f_n\rangle = \frac{1}{2}\sum_{m=0}^{3} exp(\frac{\pi inm}{2})|t_m\rangle, n = 0, 1, 2, 3$. Alice modulates a periodic chain of optical pulses produced by the laser source with IM1 to determine these pulses for either time-bin states or phase states. Each state consists of four time-bins and each time-bin contains one light pluse. For time-bin states, three light pulses out of four that we do not need are filtered out with IM1. Afterwards, IM2 is used to adjust the amplitude of phase states relative to the primary time-bin states and the phase modulator is used to encode different phase states. An attenuator is used to reduce the photon states to single-photon levels. In a realistic setup, the extinction ratio of the intensity modulator is not infinite; hence, light pulses cannot be attenuated to zero intensity and are filtered out thoroughly. Because phase states are not required to be attenuated to zero intensity, only the finite extinction of IM1 will have impact on the final security of the system.

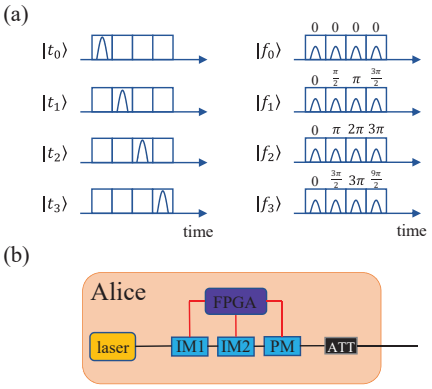

Figure 1. (Color online) Schematic diagram of the four-dimensional time-bin HD-QKD system. (**a**) Representation of time-bin states (left) and phase states (right). (**b**) Diagram of producing time-bin states and phase states on Alice's side, where laser means Alice produces periodic light pluses with a laser source, FPGA is the field-programmable gate array, IM1 and IM2 are intensity modulators, PM is the phase modulator, and ATT is the attenuator. See more details in ref. [11].

Due to the electro-optic effect, we can apply different voltages on the intensity modulator to control the intensity of the passing light. Then, we can define the state of IM1 as "off" when it has high attenuation and "on" when it has nearly no attenuation. The light intensity is attenuated by a factor of $\sqrt{P_{off}}$ or $\sqrt{P_{on}}$ when the state of IM1 is off or on, and the intensity of the output light is $I_{off} = P_{off} I_0$ or $I_{on} = P_{on} I_0$, respectively, where I_0 is the

intensity of the input light. Therefore, we can define the extinction ratio of the intensity modulator as follows.

$$r = \frac{I_{on}}{I_{off}}. \tag{1}$$

Supposing that Alice prepares the signal state $|t_0\rangle$, high attenuation will be applied to the second, third and fourth time-bins. Let $a = \sqrt{P_{on}}$ and $b = \sqrt{P_{off}}$, the signal state transmitted out of IM1 can be written as follows:

$$\begin{aligned}
\rho_0 &= a^2|t_0\rangle\langle t_0| + b^2(|t_1\rangle\langle t_1| + |t_2\rangle\langle t_2| + |t_3\rangle\langle t_3|) \\
&= (a^2 - b^2)|t_0\rangle\langle t_0| + 4b^2 \cdot \frac{|t_0\rangle\langle t_0| + |t_1\rangle\langle t_1| + |t_2\rangle\langle t_2| + |t_3\rangle\langle t_3|}{4} \\
&= (a^2 + 3b^2)(\frac{a^2 - b^2}{a^2 + 3b^2}|t_0\rangle\langle t_0| + \frac{4b^2}{a^2 + 3b^2} \cdot \frac{\hat{I}}{4}) \\
&= (a^2 + 3b^2)(\frac{a^2 - b^2}{a^2 + 3b^2}\rho_{ideal} + \frac{4b^2}{a^2 + 3b^2}\rho_{noise})
\end{aligned} \tag{2}$$

where ρ_{ideal} denotes the pure signal state ($|t_0\rangle\langle t_0|$, $|t_1\rangle\langle t_1|$, $|t_2\rangle\langle t_2|$ or $|t_3\rangle\langle t_3|$), and $\rho_{noise} = \frac{\hat{I}}{4}$ denotes the density matrix of the extra noise introduced by the finite extinction ratio of IM1. After normalization, Equation (2) can be generally written as follows:

$$\rho_{signal} = \frac{r-1}{r+3}\rho_{ideal} + \frac{4}{r+3}\rho_{noise} \tag{3}$$

since $r = \frac{I_{on}}{I_{off}} = \frac{P_{on}}{P_{off}} = \frac{a^2}{b^2}$. Similarly, we can extend the discussion above to arbitrary d-dimensional time-bin QKD systems. By calculation, the equation of state transmission can be written as follows.

$$\rho_{signal} = \frac{r-1}{r+d-1}\rho_{ideal} + \frac{d}{r+d-1}\rho_{noise}. \tag{4}$$

By using this method, we can notice that (3) is of the same form as Equation (3) in ref. [61]. This is because, in the polarization coding BB84 protocol, X and Z basis states are generated and detected in the same manner and can transform mutually into each other. All four states are affected by the finite extinction of intensity modulators. On the other hand, in the time-bin HD-QKD protocol, time-bin states $|t_n\rangle$ and phase states $|f_n\rangle$ are neither generated nor detected in the same manner [11]. One basis cannot transform into the other mutually either. More importantly, only four time-bin states are affected by the finite extinction of intensity modulator in the state preparation process.

3. Security Analysis

In this section, we analyze the practical security of the time-bin HD-QKD system described above. We firstly analyze the practical security in the case of the HD-QKD system with the ideal single photon source. Then, we generalize our analysis to the HD-QKD system combined with the decoy-state method. The combined effect of intensity fluctuations in the laser source and the finite extinction of the intensity modulator is discussed in the end.

3.1. HD-QKD with the Single Photon State

Here, we discuss the universal situation for arbitrary d-dimensional HD-QKD protocol. The secret key rate of d-dimensional QKD system in asymptotic infinite-key scenario can be written as follows:

$$R_\infty = \log_2 d - H(e) - H(e_p) \tag{5}$$

where e is the quantum bit error rate (QBER) caused by noises and $H(x) = -x\log_2(\frac{x}{d-1}) - (1-x)\log_2(1-x)$ is the d-dimensional Shannon entropy [19]. After key sifting processes,

Alice and Bob should perform classical post-processing, which consists of error correction and privacy amplification. The fractions $H(e)$ of the sifted key bits are sacrificed to perform error correction, and the fractions $H(e_p)$ of the sifted key bits are sacrificed to perform privacy amplification. [62].

Since the finite extinction of IM1 will bring in some extra noises, QBER can be modified into the following.

$$\begin{aligned} e^{'} &= \frac{r-1}{r+d-1}e + \frac{d}{r+d-1}\cdot\frac{d-1}{d} \\ &= (1-\frac{d}{r+d-1})e + \frac{d-1}{r+d-1}. \end{aligned} \tag{6}$$

The first term of the right hand side of (6) is caused by the noises introduced by Eve when she attempts to steal secret key information on the quantum channel via some attacking strategies. In addition, the second term of the right hand side is attributed to a probability of $\frac{d-1}{d}$ of an incorrect alphabet resulting from ρ_{noise}. Since the identity matrix remains unchanged under all unitary operations, Eve cannot achieve any useful information by performing any operation on ρ_{noise}. Therefore, the privacy amplification process is not required for the part of ρ_{noise}, and only a fraction $(1-\frac{d}{r+d-1})$ of sifted key bits need to perform privacy amplification [62]. Certainly, all error bits should undergo error correction process and the the QBER is $e^{'}$ now. Therefore, (5) turns into the following.

$$\begin{aligned} R_{\infty}^{'} &= \log_2 d - H(e^{'}) - (1-\frac{d}{r+d-1})H(e) \\ &= \log_2 d - H(e^{'}) - (1-\frac{d}{r+d-1})H(\frac{e^{'}-\frac{d-1}{r+d-1}}{1-\frac{d}{r+d-1}}). \end{aligned} \tag{7}$$

3.2. HD-QKD with the Decoy-State Method

In this subsection, we only consider four-dimensional time-bin QKD systems with finite-key analysis. Islam et al. [11] applied decoy state methods to a four-dimensional time-bin QKD scheme and bounded the secret key length (denoted by l) as follows:

$$l \leq max\lfloor 2\tilde{s}_{T,0} + \tilde{s}_{T,1}[c - H(\lambda^U)] - leak_{EC} + \Delta_{FK}\rfloor \tag{8}$$

where $\tilde{s}_{T,0}$ and $\tilde{s}_{T,1}$ are the vacuum and single-photon detection counts in the temporal basis, respectively. c is defined as $c := -\log_2 max_{i,j}|\langle f_i|t_j\rangle|^2$, and λ^U is an upper bound of the single-photon phase error rate. $leak_{EC} = 1.16H(x)$ is the number of secret key bits sacrificed for error correction processes, and Δ_{FK} is the finite-key estimation item. The detailed expressions of $\tilde{s}_{T,0}$, $\tilde{s}_{T,1}$ and λ^U are given by the following:

$$\begin{aligned} \tilde{s}_{T,0} &:= max\{\lfloor \frac{\tau_0}{\mu_2-\mu_3}(\frac{\mu_2 e^{\mu_3} n^{-}_{T,\mu_3}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^{+}_{T,\mu_2}}{p_{\mu_2}})\rfloor, 0\}, \\ \tilde{s}_{T,1} &:= max\{\frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3)-(\mu_2^2-\mu_3^2)}[\frac{e^{\mu_2} n^{-}_{T,\mu_2}}{p_{\mu_2}} \\ &- \frac{e^{\mu_3} n^{+}_{T,\mu_3}}{p_{\mu_3}} + \frac{\mu_2^2-\mu_3^2}{\mu_1^2}(\frac{\tilde{s}_{T,0}}{\tau_0} - \frac{e^{\mu_1} n^{+}_{T,\mu_1}}{p_{\mu_1}})], 0\}, \\ \lambda^U &:= \frac{\tilde{v}_{F,1}}{\tilde{s}_{F,1}} + \sqrt{\frac{(\tilde{s}_{T,1}+\tilde{s}_{F,1})(\tilde{s}_{F,1}+1)}{\tilde{s}_{T,1}(\tilde{s}_{F,1})^2} ln\frac{2}{\beta}} \end{aligned} \tag{9}$$

where $\tilde{v}_{F,1} = \frac{\tau_1}{\mu_2-\mu_3}(\frac{e^{\mu_2} m^{+}_{F,\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} m^{-}_{F,\mu_3}}{p_{\mu_3}})$ and $\tau_n = \sum_{k\in K} e^{-k}\frac{k^n p_k}{n!}$, while $\tilde{s}_{F,1}$ has a similar form to $\tilde{s}_{T,1}$. One signal state and two decoy states are denoted as $K := \{\mu_1, \mu_2, \mu_3\}$ (chosen with probabilities p_{μ_1}, p_{μ_2} and $p_{\mu_3} := 1 - p_{\mu_1} - p_{\mu_2}$, respectively) where $\mu_1 > \mu_2 + \mu_3$ and

$\mu_1 \geq \mu_2 \geq \mu_3 \geq 0$. More details are depicted in ref. [11]. In the finite-key scenario, there are statistical fluctuations in the parameter estimation procedure. Therefore, we employ the improved Chernoff bound to estimate the upper and lower bounds for $n_{T,k}$, which represents the total number of detection events in the temporal basis. For the improved Chernoff bound [63], the upper and lower bounds for the measurement outcome $n_{T,k}$ can be expressed as follows:

$$\begin{aligned} n_{T,k} &\leqslant \frac{n_{T,k}}{1-\delta_C^U(n_{T,k},\varepsilon_C)} = n_{T,k}^+ \\ n_{T,k} &\geqslant \frac{n_{T,k}}{1+\delta_C^L(n_{T,k},\varepsilon_C)} = n_{T,k}^- \end{aligned} \tag{10}$$

with probability of at least $1-2\varepsilon_C$, where ε_C is the correctness parameter. For $\delta_C^U(x,y)$ and $\delta_C^L(x,y)$, a simplified analytical approximation is given by [63] the following.

$$\delta_C^U(x,y) = \delta_C^L(x,y) = \frac{-3ln(\frac{y}{2}) + \sqrt{[ln(\frac{y}{2})]^2 - 8xln(\frac{y}{2})}}{2x + 2ln(\frac{y}{2})}. \tag{11}$$

Substituting (10) and (11) into (9), we can derive a lower bound on the secret key's length.

Because only the imperfections of IM1 have an effect on the practical security of this system and IM1 only acts on time-bin states, only error events in the temporal basis in (8) should append the consideration of the finite extinction of the intensity modulator. As discussed above, $leak_{EC} = 1.16H(x) = 1.16H(E_t)$, where $E_t = \frac{m_{T,\mu_1}+m_{T,\mu_2}+m_{T,\mu_3}}{n_{T,\mu_1}+n_{T,\mu_2}+n_{T,\mu_3}}$. In this fraction, $m_{T,k} = p_{\mu_k}p_T^2N(e_d(1-e^{-\eta\mu_k}) + 0.75P_d)$ ($K \in \{\mu_1,\mu_2,\mu_3\}$) represents error events in the temporal basis, while $n_{T,k}$ is defined as $n_{T,k} = p_{\mu_k}p_T^2N(1-e^{-\eta\mu_k} + P_d)$. Here, p_T is the preparation probability of time-bin states, η is the overall system transmittance and P_d denotes the dark count rate of single photon detectors. e_d is the error bit rate caused by the misalignment of the system, which includes the error bit rate introduced by the imperfect IM and can be obtained from the field test experiments. With another form of (6), i.e., $e = \frac{e' - \frac{d-1}{r+d-1}}{1-\frac{d}{r+d-1}}$, we can set $d = 4$ and transform e_d into the following.

$$e_d \to \frac{e_d' - \frac{3}{r+3}}{1-\frac{4}{r+3}}. \tag{12}$$

Substituting (12) into (8), we can obtain a modified formula of secret key length while considering the finite extinction of the practical intensity modulator. Taking the number of transmitted signals N and state preparation rate into account, we can obtain the final secret key rate.

3.3. HD-QKD with Both Intensity Fluctuations and the Finite Extinction

Last but not least, we should mention that we carry out our security analysis with the assumption that there is no intensity fluctuations in the light exiting from the laser source. In reality, intensity fluctuations in practical QKD systems always exist and have deep influence on the performance of the HD-QKD system [58,59]. Taking both intensity fluctuations resulted from the unstable source and finite extinction of intensity modulator into consideration in the security analysis, we can figure out how these two issues affect the practical performance of the HD-QKD system simultaneously in a realistic setup. When conducting security analysis, we should employ Azuma's inequality [64] instead of the improved Chernoff bound to estimate the statistical fluctuations caused by intensity fluctuations. This is because the intensity fluctuations would break the independent condition for independent random samples and Azuma's inequality can hold with dependent random samples by the square. In greater detail, we use Azuma's inequality to quantify the fluctua-

tion ranges in $\tilde{s}_{T,0}$, $\tilde{s}_{T,1}$ and λ^U in (9). With Azuma's inequality, the observed values of the number of detection events and the observed number of errors for the case with intensity fluctuations in the temporal basis $n^*_{T,k}$ and $m^*_{T,k}$ satisfy the following:

$$|n^*_{T,k} - n_{T,k}| \leq \delta(n_T, \beta) \tag{13}$$

and

$$|m^*_{T,k} - m_{T,k}| \leq \delta(m_T, \beta) \tag{14}$$

with probability of at least $1 - 2\beta$ where $\delta(x, y) = \sqrt{2xln(\frac{1}{y})}$. Then, we find the following:

$$\begin{aligned} n^*_{T,k} &\leq n_{T,k} + \delta(n_T, \beta) = n^+_{T,k}, \\ n^*_{T,k} &\geq n_{T,k} - \delta(n_T, \beta) = n^-_{T,k}, \\ m^*_{T,k} &\leq m_{T,k} + \delta(m_T, \beta) = m^+_{T,k}, \\ m^*_{T,k} &\geq m_{T,k} - \delta(m_T, \beta) = m^-_{T,k} \end{aligned} \tag{15}$$

and they are the upper and lower bounds of $n^*_{T,k}$ and $m^*_{T,k}$ for all values of k, which appear in (9). Values for phase basis $n^*_{F,k}$ and $m^*_{F,k}$ hold a similar form to (13)–(15).

According to refs. [58,59], we assume that the fluctuation ranges of intensity $k \in (k^-, k^+)$ is known to Alice and Bob. We can present a detailed decoy-state analysis with intensity fluctuations. For $k \in \mu_1, \mu_2, \mu_3$, we also assume that $\mu_1 > \mu_2 + \mu_3$ and $\mu_1 \geq \mu_2 \geq \mu_3 \geq 0$. When considering intensity fluctuations, we can obtain the lower bound for the number of vacuum events, and it is given by the following:

$$\tilde{s}_{T,0} := max\{\lfloor \frac{\tau_0}{\mu_2^- - \mu_3^+} (\frac{\mu_2^- e^{\mu_3^+} n^-_{T,\mu_3}}{p_{\mu_3}} - \frac{\mu_3^+ e^{\mu_2^-} n^+_{T,\mu_2}}{p_{\mu_2}}) \rfloor, 0\}, \tag{16}$$

and the lower bound for the number of single-photon events can be expressed as follows.

$$\begin{aligned} \tilde{s}_{T,1} := max\{ &\frac{\mu_1^- \tau_1}{\mu_1^-(\mu_2^+ - \mu_3^-) - ((\mu_2^+)^2 - (\mu_3^-)^2)} [\frac{e^{\mu_2^+} n^-_{T,\mu_2}}{p_{\mu_2}} \\ &- \frac{e^{\mu_3^-} n^+_{T,\mu_3}}{p_{\mu_3}} + \frac{(\mu_2^+)^2 - (\mu_3^-)^2}{(\mu_1^-)^2} (\frac{\tilde{s}_{T,0}}{\tau_0} - \frac{e^{\mu_1^-} n^+_{T,\mu_1}}{p_{\mu_1}})], 0\}. \end{aligned} \tag{17}$$

Substituting (9) and (15)–(17) into (8), we can derive the modified secret key rate formula by considering intensity fluctuations and the finite extinction of the intensity modulator simultaneously.

4. Simulation Results

Figure 2 is the numerical simulation result of (7) where $e^{'}$ is the observed quantum bit error rate. The extinction ratio r is selected as 500 (27 dB), which is a typical parameter value of practical devices.

As illustrated in Figure 2 and Table 1, we find that there is an increase in the maximal tolerable QBER when taking the finite extinction of the intensity modulator into account. Furthermore, this increase is more obvious for higher dimension d. This is because systematic noises come from two parts: Eve's attacking behaviour and the imperfection of the practical intensity modulator, as illustrated in (6). When performing the error correction, all errors are considered to be introduced by Eve and Eve will lose more information than Alice and Bob. As a consequence, Alice and Bob can distill more secret keys, and the secret key rate is increased. We should also notice that three full curves in Figure 2 do not start from zero on the horizontal axis. This is because there exist intrinsic noises of $\frac{d-1}{r+d-1}$ caused by the imperfection of the practical intensity modulator when setting $e = 0$ in (6).

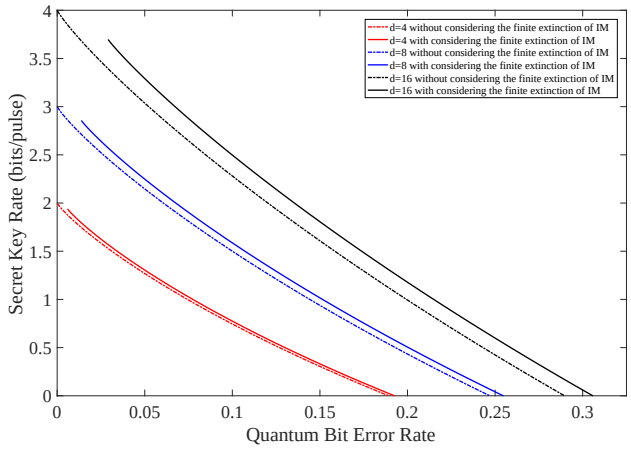

Figure 2. (Color online) The secret key rate vs. observed quantum bit error rate with and without considering the finite extinction of intensity modulator.

Table 1. The maximal tolerable QBER with and without considering the finite extinction of intensity modulator for different dimensions.

Dimension	Maximal Tolerable QBER	
	without Considering the Finite Extinction of IM	**with Considering the Finite Extinction of IM**
d = 4	18.93%	19.27%
d = 8	24.71%	25.47%
d = 16	28.97%	30.58%

Figure 3 shows the simulation results of the secret key rate with and without considering the finite extinction of the intensity modulator when Alice transmits different numbers of signals N's. The simulation parameters are selected as follows. The average intensities of one signal state and two decoy states are selected to be 0.66, 0.16 and 0.002, respectively. The probabilities of sending these three states are 0.8, 0.1 and 0.1, respectively. Time-bin and phase states are prepared with probabilities of 0.90 and 0.10, which are p_T and p_F. The quantum channel is described by a loss $\eta_{ch} = 10^{-\alpha L/10}$, where $\alpha = 0.2$ dB/km is the loss coefficient of the fiber, and L (km) is the transmission distance. We also assume that the dark count rate $P_d = 10^{-8}$ and two correctness parameters $\beta = 1.72 \times 10^{-10}$, $\varepsilon_C = 10^{-12}$ from ref. [11]. As shown in Figure 3, we can see that when considering the finite extinction of the intensity modulator, the transmission distance increases about 1km for different N's. For $N = 6.25 \times 10^{11}$, there is an increase of 9-11% in the secret key rate, as illustrated in Table 2.

Furthermore, the influence of different extinction ratios on the practical performance of the HD-QKD system is investigated. We again employ the parameters of four-dimensional time-bin QKD system mentioned above and the number of transmitted signals is set to be $N = 6.25 \times 10^{11}$. The secret key rate results when considering different extinction ratios are depicted in Figure 4. It is beyond expectation that the lower extinction ratio can result in a higher secret key rate. This is because that the quantum bit error rate results from two parts: the imperfection of the practical intensity modulator and the channel noises. Different extinction ratios will make error rates resulting from these two factors make up different accounts for the total quantum bit error rate. For the HD-QKD system with lower extinction ratios, the intrinsic noises caused by the imperfection of practical intensity modulator appear higher. On the basis of the discussion above, Eve would lose more information during classical data post-processing. Therefore, the secret key rate becomes higher as a result. It should be noted that this conclusion can only be drawn when the total

quantum bit error rate remains unchanged. HD-QKD systems with different quantum bit error rate values cannot be compared with each other.

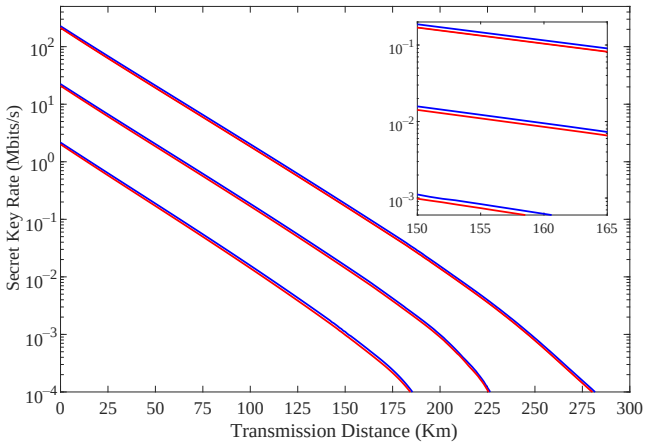

Figure 3. (Color online) The final secret key rate vs. transmission distance with (blue curves) and without (red curves) considering the finite extinction of intensity modulator for $N = 6.25 \times 10^x$ with x = 9, 10, 11 (curves from bottom to top).

Table 2. The secret key rate calculated with and without considering the finite extinction of intensity modulator in units of Mbps.

Transmission Distance (km)	without Considering the Finite Extinction of IM	with Considering the Finite Extinction of IM
30	49.54	54.09
80	4.703	5.171
130	0.4417	0.4869
180	0.03927	0.04348
230	0.0027	0.00297

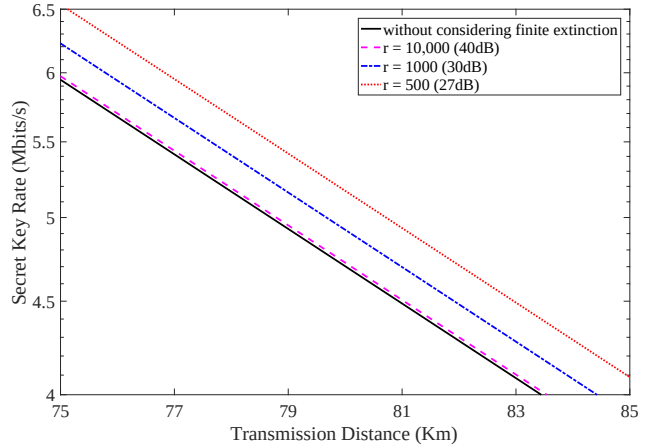

Figure 4. (Color online) The secret key rate vs. transmission distance considering different extinction ratios.

The combined effect of finite extinction of intensity modulator and intensity fluctuation in laser source is illustrated in Figure 5. The number of transmitted signals is set to be $N = 6.25 \times 10^{11}$. We find that there is always an increase in the secret key rate when taking the finite extinction into consideration. Moreover, this improvement is more obvious when

the intensity fluctuation increases. Table 3 shows different secret key rate results at a fixed transmission distance when considering different intensity fluctuations with and without considering the finite extinction of the intensity modulator.

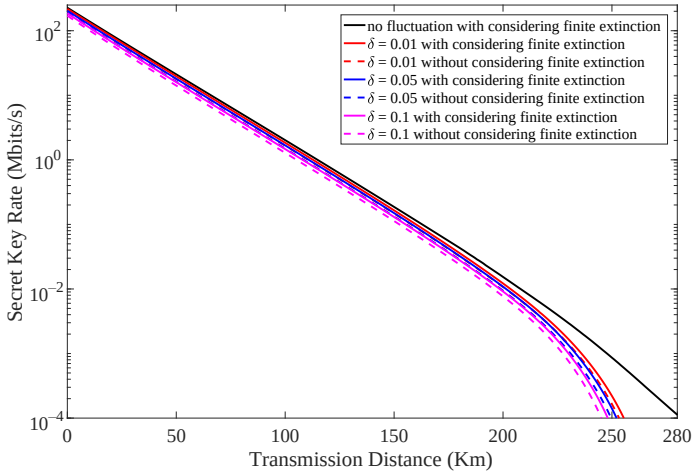

Figure 5. (Color online) The secret key rate vs. transmission distance when considering different intensity fluctuations (δ = 0.01, 0.05, 0.1) with and without considering finite extinction of intensity modulator.

Table 3. The secret key rate results calculated with and without considering the finite extinction of intensity modulator for different intensity fluctuations when the transmission distance is 50 km in units of Mbps.

Intensity Fluctuation	0.01	0.05	0.1
Secret key rate without considering the finite extinction of IM	17.87	16.22	14.13
Secret key rate with considering the finite extinction of IM	19.67	18.03	15.96
Improvement	10.07%	11.16%	12.96%

5. Conclusions

In summary, we analyze the influence of the realistic intensity modulator on the practical security of high-dimensional quantum key distribution systems. We present finite-key analysis of HD-QKD with extinction ratios and intensity fluctuations. In our analysis, we improved the lower bounds of the secret key rate for the HD-QKD system with both the single photon state and the decoy-state method. We should also mention that different extinction ratios and intensity fluctuations have deep influences on the practical security of the HD-QKD protocol, and these issues are worthy of deep consideration when building realistic HD-QKD systems.

Furthermore, we should note that we conduct our analysis only in the time-bin HD-QKD system, and our method can be extended to HD-QKD systems by employing other different photonic degrees of freedom. Last but not least, our research has opened up a new path for the security analysis of practical HD-QKD systems. Analysis on other practical issues can follow the routine we proposed in this paper.

Author Contributions: Conceptualization, Y.W.; methodology, Y.W. and G.-H.D.; writing—original draft preparation, Y.W. and G.-H.D.; writing—review and editing, Y.-B.X., C.Z., M.-S.J. and H.-W.L.; supervision, W.-S.B.; project administration, Y.W.; funding acquisition, W.-S.B., Y.W., C.Z., M.-S.J. and H.-W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Grant Nos. 62101597, 61605248, 61675235 and 61505261), the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the China Postdoctoral Science Foundation (Grant

No. 2021M691536), the Natural Science Foundation of Henan (Grant Nos. 202300410534 and 202300410532) and the Anhui Initiative in Quantum Information Technologies.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef]
3. 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]
4. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [CrossRef]
5. Lo, H.-K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef]
6. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
7. Renner, R. Security of Quantum Key Distribution. Ph.D. Dissertation, Department of Physics, Swiss Federal Insititute of Technology (ETH), Zürich, Switzerland, 2005.
8. Ali-Khan, I.; Broadbent, C.J.; Howell, J.C. Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States. *Phys. Rev. Lett.* **2007**, *98*, 060503. [CrossRef]
9. Mower, J.; Zhang, Z.; Desjardins, P.; Lee, C.; Shapiro, J.H.; Englund, D. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A* **2013**, *87*, 062322. [CrossRef]
10. Wang, Y.; Bao, W.S.; Bao, H.Z.; Zhou, C.; Jiang, M.S.; Li, H.W. High-dimensional quantum key distribution with the entangled single-photon-added coherent state. *Phys. Lett. A* **2017**, *381*, 1393–1397. [CrossRef]
11. Islam, N.T.; Lim, C.C.W.; Cahall, C.; Kim, J.; Gauthier, D.J. Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **2017**, *3*, e1701491. [CrossRef]
12. Vagniluca, I.; Lio, B.D.; Rusca, D.; Cozzolino, D.; Ding, Y.; Zbinden, H.; Zavatta, A.; Oxenløwe, L.K.; Bacco, D. Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Phys. Rev. Appl.* **2020**, *14*, 014051. [CrossRef]
13. Lio, B.D.; Cozzolino, D.; Biagi, N.; Ding, Y.; Rottwitt, K.; Zavatta, A.; Bacco, D.; Oxenløwe, L.K. Path-encoded high-dimensional quantum communication over a 2-km multicore fiber. *NPJ Quantum Inf.* **2021**, *7*, 63. [CrossRef]
14. Ding, Y.; Bacco, D.; Dalgaard, K.; Cai, X.; Zhou, X.; Rottwitt, K.; Oxenløwe, L.K. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *NPJ Quantum Inf.* **2017**, *3*, 25. [CrossRef]
15. Wang, Q.K.; Wang, F.X.; Liu, J.; Chen, W.; Han, Z.F.; Forbes, A.; Wang, J. High-dimensional quantum cryptography with hybrid orbital-angular-momentum states through 25 km of ring-core fiber: A proof-of-concept demonstration. *Phys. Rev. Appl.* **2021**, *15*, 064034. [CrossRef]
16. Cozzolino, D.; Bacco, D.; Lio, B.D.; Ingerslev, K.; Ding, Y.; Dalgaard, K.; Kristensen, P.; Galili, M.; Rottwitt, K.; Ramachandran, S.; et al. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Phys. Rev. Appl.* **2019**, *11*, 064058. [CrossRef]
17. Sit, A.; Bouchard, F.; Fickler, R.; Gagnon-Bischoff, J.; Larocque, H.; Heshami, K.; Elser, D.; Peuntinger, C.; Günthner, K.; Heim, B.; et al. High-dimensional intracity quantum cryptography with structured photons. *Optica* **2017**, *4*, 1006–1010. [CrossRef]
18. Cerf, N.J.; Bourennane, M.; Karlsson, A.; Gisin, N. Security of Quantum Key Distribution Using d-Level Systems. *Phys. Rev. Lett.* **2002**, *88*, 127902. [CrossRef]
19. Sheridan, L.; Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **2010**, *82*, 030301. [CrossRef]
20. Coles, P.J.; Metodiev, E.M.; Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nat. Commun.* **2016**, *7*, 11712. [CrossRef]
21. Wang, S.; Yin, Z.Q.; Chau, H.F.; Chen, W.; Wang, C.; Guo, G.C.; Han, Z.F. Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme. *Quantum Sci. Technol.* **2018**, *3*, 025006. [CrossRef]
22. Lee, C.; Bunandar, D.; Zhang, Z.; Steinbrecher, G.R.; Dixon, P.B.; Wong, F.N.C.; Shapiro, J.H.; Hamilton, S.A.; Englund, D. Large-alphabet encoding for higher-rate quantum key distribution. *Opt. Express* **2019**, *27*, 17539–17549. [CrossRef]
23. Islam, N.T.; Lim, C.C.W.; Cahall, C.; Qi, B.; Kim, J.; Gauthier, D.J. Scalable high-rate, high-dimensional time-bin encoding quantum key distribution. *Quantum Sci. Technol.* **2019**, *4*, 035008. [CrossRef]
24. Lo, H.-K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **2014**, *8*, 595–604. [CrossRef]
25. Diamanti, E.; Lo, H.-K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 16025. [CrossRef]

26. 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]
27. Li, H.; Wang, S.; Huang, J.; Chen, W.; Yin, Z.; Li, F.; Zhou, Z.; Liu, D.; Zhang, Y.; Guo, G.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **2011**, *84*, 062308. [CrossRef]
28. Qi, B.; Fung, C.H.F.; Lo H.K.; Ma, X.F. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **2007**, *7*, 73–82. [CrossRef]
29. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705. [CrossRef]
30. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **2010**, *4*, 686–689. [CrossRef]
31. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349. [CrossRef]
32. Zhang, G.; Primaatmaja, I.W.; Haw, J.Y.; Gong, X.; Wang, C.; Lim, C.C.W. Securing Practical Quantum Communication Systems with Optical Power Limiters. *PRX Quantum* **2021**, *2*, 030304. [CrossRef]
33. Qian, Y.J.; He, D.Y.; Wang, S.; Chen, W.; Yin, Z.Q.; Guo, G.C.; Han, Z.F. Robust countermeasure against detector control attack in a practical quantum key distribution system. *Optica* **2019**, *6*, 1178–1184. [CrossRef]
34. Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Avoiding the blinding attack in QKD. *Nat. Photon.* **2010**, *4*, 800–801. [CrossRef]
35. Lo, H.-K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
36. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
37. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
38. Wang, X.-B.; Yu, Z.-W.; Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
39. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
40. Cui, C.; Yin, Z.Q.; Wang, R.; Chen, W.; Wang, S.; Guo, G.C.; Han, Z.F. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **2019**, *11*, 034053. [CrossRef]
41. Yoshino, K.; 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]
42. Lu, F.; Lin, X.; Wang, S.; Fan-Yuan, G.; Ye, P.; Wang, R.; Yin, Z.; He, D.; Chen, W.; Guo, G.; et al. Intensity modulator for secure, stable, and high-performance decoy-state quantum key distribution. *NPJ Quantum Inf.* **2021**, *7*, 75. [CrossRef]
43. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef] [PubMed]
44. Lütkenhaus, N.; Jahma, M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J. Phys.* **2002**, *4*, 44.
45. Zhang, Z.; Mower, J.; Englund, D.; Wong, F.N.C.; Shapiro, J.H. Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry. *Phys. Rev. Lett.* **2014**, *112*, 120506. [CrossRef] [PubMed]
46. Hwang, W.-Y. Quantum key distribution with high loss: Towards global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
47. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef] [PubMed]
48. Lo, H.-K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
49. Bunandar, D.; Zhang, Z.; Shapiro, J.H.; Englund, D.R. Practical high-dimensional quantum key distribution with decoy states. *Phys. Rev. A* **2015**, *91*, 022336. [CrossRef]
50. Scarani, V.; Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **2008**, *100*, 200501. [CrossRef]
51. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef]
52. Bao, H.-Z.; Bao, W.-S.; Wang, Y.; Zhou, C.; Chen, R.-K. Finite-key analysis of a practical decoy-state high-dimensional quantum key distribution. *J. Phys. A Math. Theor.* **2016**, *49*, 205301. [CrossRef]
53. Niu, M.Y.; Xu, F.; Shapiro, J.H.; Furrer, F. Finite-key analysis for time-energy high-dimensional quantum key distribution. *Phys. Rev. A* **2016**, *94*, 052323. [CrossRef]
54. Wang, X.B. Decoy-state quantum key distribution with large random errors of light intensity. *Phys. Rev. A* **2007**, *75*, 052301. [CrossRef]
55. Wang, X.-B.; Peng, C.-Z.; Zhang, J.; Yang, L.; Pan, J.-W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **2008**, *77*, 042311. [CrossRef]
56. Wang, X.-B.; Yang, L.; Peng, C.-Z.; Pan, J.-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **2009**, *11*, 075006. [CrossRef]

57. Chi, H.-H.; Yu, Z.-W.; Wang, X.-B. Decoy-state method of quantum key distribution with both source errors and statistics fluctuations. *Phys. Rev. A* **2012**, *86*, 042307. [CrossRef]
58. Wang, Y.; Bao, W.-S.; Zhou, C.; Jiang, M.-S.; Li, H.-W. Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources. *Phys. Rev. A* **2016**, *94*, 032335. [CrossRef]
59. Gan, Y.H.; Wang, Y.; Bao, W.S.; Zhou, C.; Jiang, M.S.; Li, H.W. Finite-key analysis for high-dimensional quantum key distribution with intensity fluctuations. *J. Phys. B At. Mol. Opt.* **2018**, *51*, 245502. [CrossRef]
60. Wang, Y.; Bao, W.-S.; Zhou, C.; Jiang, M.-S.; Li, H.-W. Finite-key analysis of practical decoy-state measurement-device-independent quantum key distribution with unstable sources. *J. Opt. Soc. Am. B* **2019**, *36*, B83–B91. [CrossRef]
61. Huang, J.Z.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Han, Z.F. Effect of intensity modulator extinction on practical quantum key distribution system. *Eur. Phys. J. D* **2012**, *66*, 159. [CrossRef]
62. Gottesman, D.; Lo, H.-K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **2004**, *4*, 325–360.
63. Zhang, Z.; Zhao, Q.; Razavi, M.; Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **2017**, *95*, 012333. [CrossRef]
64. Azuma, K. Weighted sums of certain dependent random variables. *Tohoku Math. J.* **1967**, *19*, 357–367. [CrossRef]