entropy

MDPI

Article

Efficient High-Dimensional Quantum Key Distribution with Hybrid Encoding

Yonggi Jo [1,2], Hee Su Park [3], Seung-Woo Lee [4] and Wonmin Son [1,*]

1 Department of Physics, Sogang University, Seoul 04107, Korea; starult@gmail.com
2 Research Institute for Basic Science, Sogang University, Seoul 04107, Korea
3 Korea Research Institute of Standards and Science, Daejeon 34113, Korea; hspark@kriss.re.kr
4 Quantum Universe Center, Korea Institute for Advanced Study, Seoul 02455, Korea; swleego@gmail.com
* Correspondence: sonwm@physics.org

Received: 26 December 2018; Accepted: 14 January 2019; Published: 17 January 2019

Abstract: We propose a schematic setup of quantum key distribution (QKD) with an improved secret key rate based on high-dimensional quantum states. Two degrees-of-freedom of a single photon, orbital angular momentum modes, and multi-path modes, are used to encode secret key information. Its practical implementation consists of optical elements that are within the reach of current technologies such as a multiport interferometer. We show that the proposed feasible protocol has improved the secret key rate with much sophistication compared to the previous 2-dimensional protocol known as the detector-device-independent QKD.

Keywords: quantum cryptography; quantum key distribution; high-dimensional quantum states

1. Introduction

Quantum key distribution (QKD) is a novel scheme to distribute a symmetric secret key between two distant authorized parties, Alice, and Bob, by exploiting quantum mechanical phenomena. The protocol provides an information-theoretic security under potential attacks of a malicious eavesdropper, conventionally called Eve. Since its first seminal proposal called BB84 protocol [1], many relevant or extended versions of QKD protocols have been proposed and studied based on quantum principles [2–8].

In recent QKD studies, the security defects due to device imperfections have been emerging as an important issue. It has been shown that Eve can hack into the QKD system by exploiting the imperfection of devices. This is known as a side channel attack including photon number splitting (PNS) attack [9], faked-state attack [10], detector efficiency mismatch attack [11], detector blinding attack [12,13], time-shift attack [14], and laser damage attack [15]. In this background, measurement-device-independent QKD (MDI-QKD) was proposed to overcome the problems coming from imperfections of measurement devices [16]. In MDI-QKD, the Bell state measurement (BSM) of two photons [17] is an essential task. However, the success probability of BSM with linear optics on single photons is upper bounded by 50% [18,19]. Recent advanced schemes of BSM require multi-photon encoding of 2-dimensional quantum states, called qubits, to beat the limit with linear optics [20–24]. Then, detector-device-independent QKD (DDI-QKD) was proposed [25–27] to simplify the scheme of MDI-QKD, exploiting two different degrees-of-freedoms (DoFs) in a single photon and single-photon interference instead of two-photon interference. In its protocol, Alice encodes her information into one DoF of a single photon and sends it to Bob, who encodes his information into another DoF of the single photon. The measurement result of the single photon reveals correlation of two DoFs in the single photon. The implementation of DDI-QKD requires only measurements on single photons and is thus less challenging than BSM performed on two photons. As its scheme is

similar to the process of BSM used in MDI-QKD, it was conjectured that DDI-QKD guarantees the same security level with MDI-QKD. However, it has been shown that not all the side channel attacks are protected with DDI-QKD [28,29], and an assumption of the trusted measurement setup is necessary for ensuring its security.

In another branch of QKD research, there has been significant effort to improve the secret key rate, for example, using d-dimensional quantum states, called qudits. There are several advantages to using qudits as a generalized information carrier. For example, qudits ($d > 2$) can naturally carry more classical information than qubits. Compared to qubit operations, qudits has been shown to be more robust against quantum cloning (i.e., a possible eavesdropping) [30–32]. It has been also found that the efficiency of key distribution increases with qudits in an ideal situation [32–36]. Various high-dimensional QKD protocols have been proposed such as a generalized version of BB84, a multipartite high-dimensional QKD [37], and MDI-QKDs using high-dimensional quantum states [38–40]. Moreover, QKD protocols using qudits have been implemented experimentally in various quantum system, for instance, energy-time eigenstates [41–45] and orbital angular momentum (OAM) mode of a single photon [46–50].

In this article, we propose a schematic configuration of high-dimensional QKD based on hybrid encoding over two different DoFs. We demonstrate that the secret key rate is improved with our scheme over previous 2-dimensional QKD based on two different DoFs of a single photon. We also present its implementation with current optical technologies, by exploiting the OAM mode of a single photon as a high-dimensional information carrier. We evaluate the secret key rate of our scheme with respect to the experimental parameters and identify the regime where our scheme is more secure than the original DDI-QKD. In addition, we also compare the security of our scheme with that of high-dimensional MDI-QKD (for the case of $d = 3$).

We note that our protocol is more secure than the original BB84 protocol against a side channel attack (but less secure than MDI-QKD). For example, it can detect the basic detector blinding attack [12] from double clicks of detectors [28,29]. On the other hand, the attained key rate with our protocol is comparable with BB84 protocol, while MDI-QKD has a half of signal sifting rate of BB84 protocol due to the 50% limit of the success probability of the BSM. Although DDI-QKD is not as secure as MDI-QKD and requires trusted elements in BSM setup, the main idea of employing two different DoFs motivated by DDI-QKD still merits consideration for practical usage in some secure communications e.g. quantum secret sharing [51]. As we demonstrate in this article, it is possible to improve the security as well as the efficiency over the original DDI-QKD in high-dimensional approach. In addition, we here propose a feasible high-dimensional QKD scheme with OAM of a single photon, while a high-dimensional MDI-QKD may be hard to realize due to the difficulty in implementing high-dimensional BSM on two photons with linear optical elements [19].

This article is organized as follows. A schematic description of the d-dimensional QKD (d-QKD) with hybrid encoding is presented in Section 2, and its practical implementation is in Section 3. In Section 4, we analyze the secure key rate of our protocol. Finally, conclusion on the efficiencies is drawn in Section 5.

2. Schematic Description

In this section, we describe a schematic setup of d-QKD with hybrid encoding. As an example, the schematic setup of 3-dimensional QKD (3d-QKD) with hybrid encoding is shown in Figure 1. In d-QKD with hybrid encoding, we exploit OAM mode and multipath mode of a single photon as a information carrier, since the OAM mode is known to be suitable for quantum communication as it is resilient against perturbation effects [52].

As a first step of the protocol, Alice generates d-dimensional information randomly. Subsequently, Alice randomly chooses a encoding basis between two mutually unbiased bases (MUBs) which are written as $\{|l_x\rangle\}$ and $\{|\bar{l}_x\rangle\}$ where $x \in \{0, 1, 2, ..., d-1\}$. The relation between the two MUBs is

described as the d-dimensional discrete Fourier transformation on the d OAM modes which is shown in Equation (1):

$$|\bar{l}_x\rangle = \frac{1}{d}\sum_{k=0}^{d-1}\omega^{xk}\,|l_k\rangle \tag{1}$$

where $\omega = \exp(2\pi i/d)$. Alice encodes her d-dimensional information in OAM modes of a single photon [53]. For example, when $d = 3$, Alice's classical information x_3 would be one of the dimensional integers, $x_3 \in \{0,1,2\}$, and she generates a quantum state denoted as $|l_{x_3}\rangle$ whose OAM value is $(x_3 - 1)$.

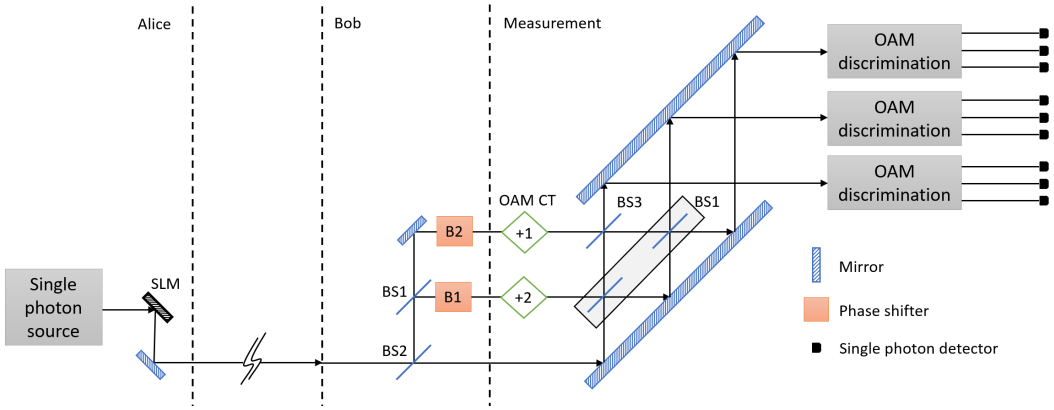


Figure 1. A schematic setup of 3-dimensional quantum key distribution (QKD) with hybrid encoding. Alice uses orbital angular momentum (OAM) modes of a single photon, and Bob controls the phase of each path to encode their information in the single photon. The encoded photon enters into a 3-port interferometer. After single photon interference, a OAM value and existing path of the single photon is measured. SLM: spatial light modulator; BS1: 50:50 beam splitter; BS2: beam splitter of which transmissivity is 1/3; BS3: beam splitter of which transmissivity is 2/3; OAM CT: cyclic transformation of OAM modes.

Subsequently, Alice sends the encoded photon to Bob, who encodes his d-dimensional information in multipath modes of the single photon. Bob also uses two MUBs that are described as $\{|p_y\rangle\}$ and $\{|\bar{p}_y\rangle\}$. $|p_y\rangle$ denotes a single photon state in the optical path p_y where $y \in \{0,1,2,...,d-1\}$. Similarly with Alice's bases, the relation between Bob's two bases is given as the d-dimensional discrete Fourier transformation of the d path modes. Figure 2 shows a schematic setup of Bob's encoding systems. Bob randomly chooses one basis between path modes and bar path modes, which are MUBs of the path modes. If Bob uses a path mode, he selects one optical path among $\{p_0, p_1, p_2\}$ corresponding to his information. If he chooses a bar path mode, he encodes his information by selecting a phases set $\{B1, B2\}$ in Figure 2b among $\{1,1\}$, $\{\omega, \omega^2\}$, and $\{\omega^2, \omega\}$.

After Bob's encoding, the two qudits encoded in the single photon, which can be written as $|l_x, p_y\rangle$, go into a cyclic transformation of OAM modes. A transformed OAM value of the single photon in path p_y is obtained with the following rule: $x \rightarrow x + d - y \pmod d$. Subsequently, a single photon interference is performed by recombining d-path via beam splitters that have different transmissivity. The unitary transformation on path modes operated by multi-port interferometer,

called tritter [54], is defined as the d-dimensional discrete Fourier transformation on the d path modes as shown in Equation (2):

$$\hat{U}_d = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{d-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(d-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(d-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & \omega^{3(d-1)} & \cdots & \omega^{(d-1)(d-1)} \end{pmatrix}. \tag{2}$$

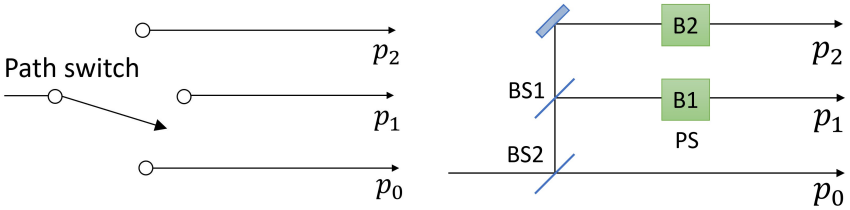
Subsequently, a OAM value of the single photon is measured in each output port of the tritter. The result of the measurement is obtained from click of a single photon detector. A click in one of the d^2 detectors corresponds to a projection into one of the following two qudits encoded in a single photon written in Equation (3):

$$|\Phi_{di+j}\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} \omega^{jx} |l_x, p_{x+i}\rangle, \tag{3}$$

where $i, j \in \{0, 1, 2, ..., d-1\}$, and (mod d) is omitted in the subscript of p. Since the states have the similar form to the d-dimensional Bell states, it is expected that the states can be used to distribute a secret key between Alice and Bob. The relation between two qudits encoded in a single photon that enters into the tritter and its corresponding detector click event is shown in Equation (4):

$$|\Phi_{di+j}\rangle \rightarrow D(l_{d-i}, p_{d-j}) \tag{4}$$

where $i, j \in \{0, 1, 2, ..., d-1\}$, and we label a click event of a single photon detector as $D(l_x, p_y)$ corresponding to the single photon whose OAM value is l_x and path mode is p_y after the tritter operation. Since there are d^2 orthonormal states in Equation (3), the measurement setup should include d^2 single photon detectors for one-to-one correspondence of the states and the detectors.



(**a**) Path mode encoding (**b**) Bar path mode encoding

Figure 2. Schematic setups of Bob's two encoding systems. (**a**) Bob chooses one path to encode his information by using optical switch; (**b**) Bob encodes his information by control phase shifters, B1 and B2. Details are described in the maintext. BS1 : 50:50 beam splitter; BS2 : beam splitter of which transmissivity is 1/3; PS : phase shifter

In order to share a secret key, it is necessary to retrieve Bob's information based on the basis choice of Alice and Bob, and the result of the measurement. For restoration, Alice sends her basis choice to Bob. The method of the restoration is shown in Table 1 as an example when 3d-QKD with hybrid encoding is performed. Bob announces only the basis matching information through classical communication, not the result of the measurement. Alice does not need to know the measurement outcome, since Bob already retrieved his encoded information by using the result.

Table 1. An example of Bob's operation on his encoded information when $d = 3$ and the result of the measurement is $|\Phi_{3i+j}\rangle$. According to their bases choice and the measurement result, it is necessary to retrieve his information for sharing the same information.

Bases	Bob's Operation ($\|\Phi_{3i+j}\rangle$)
bases 1 (l_x, p_y)	$y \to y - i$ (mod 3)
bases 2 ($\bar{l}_x$, $\bar{p}_y$)	$1 \leftrightarrow 2$ for $j = 0$ $0 \leftrightarrow 2$ for $j = 1$ $0 \leftrightarrow 1$ for $j = 2$

3. Experimental Implementation

We investigate a practical implementation of experimental elements that can construct d-QKD with hybrid encoding. Alice can generate a single photon OAM state by means of a spatial light modulator (SLM) [55]. SLMs usually have a limited frame rate of around 60 Hz, for fast generation of various OAM values, a digital micromirror device(DMD) is more desirable [56]. An OAM sorter based on liquid crystal devices can also generate photonic OAM states [57,58].

Bob's path encoding system is realizable with an optical switch over d-port, and a schematic setup is shown in Figure 2a. Bob's bar path encoding system can be changed from Figure 2b by using an optical d-port switch and a d-port tritter, whose operation on path modes is the d-dimensional discrete Fourier transformation as shown in Equation (2). With the tritter, Bob can choose bar path mode by selecting an input port of the tritter rather than controlling the phase shifters in Figure 2b.

After Bob's encoding, cyclic transformations of OAM modes are performed in the each port. Figure 3 shows a schematic setup of three-fold OAM cyclic transformation $(+1)$ of OAM values $\{-1, 0, 1\}$. The setup consists of OAM holograms, mirrors, beam splitters and OAM beam splitters (OAM BSs). An OAM BS, composed of a Mach-Zehnder interferometer with a Dove prism in each arm, sorts individual photons based on their OAM value [59]. α is defined from relative angle $\alpha/2$ between the two Dove prisms and relative phase between photons in the two arms is given by $\exp(il\alpha)$. The three-fold OAM cyclic transformation $(+1)$ consists of three OAM BSs whose α are π, $\pi/2$, and $-\pi$. The first OAM BS ($\alpha = \pi$) and the final OAM BS ($\alpha = -\pi$) change the direction of propagation of a photon whose OAM value is odd and even, respectively. The second OAM BS ($\alpha = \pi/2$) spatially separates photons whose OAM value is 0 and 2. Photons are separated and combined spatially by using the OAM BSs according to their OAM value. With OAM holograms on each arm, the three-fold cyclic transformation of OAM modes $\{-1, 0, 1\}$ is accomplished as it is shown in Figure 3. The experimental setup of the four-fold and five-fold cyclic transformation of OAM modes were proposed and demonstrated as well [60–63]. While theoretical efficiency of the four-fold cyclic transformation is 100%, fidelity of 4-dimensional Bell state transformation using the four-fold cyclic transformation setup was reported as roughly 91.5% due to reflectivity of optical elements and misalignment [61].

Subsequently, d-port single photon interference is performed by using the tritter shown in Equation (2). The tritter can be implemented with only linear optical elements which are beam splitters, mirrors, and phase shifters. After the interference, an OAM value of the single photon is measured. Direct measurements of an OAM value of a single photon have been studied recently, for instance, by using refractive optical elements that convert OAM modes into transverse momentum modes [64,65], refractive optical elements that give spatial separation of OAM modes [66], sequential weak and strong measurements [67,68], spectrum analysis based on the rotational Doppler effect [69], and interferogram analysis with a multipixel camera [70].

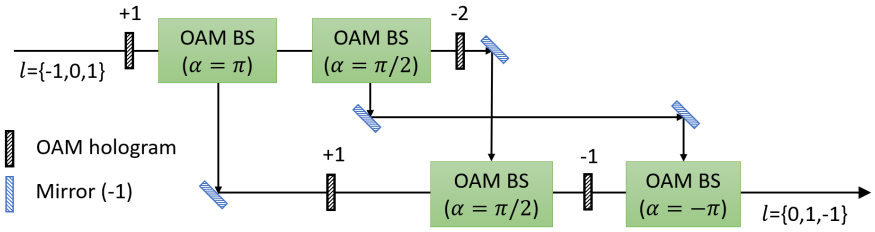


Figure 3. A schematic diagram of experimental setup of three-fold cyclic transformation of OAM modes. There are OAM beam splitters (OAM BSs) which consist of a Mach-Zehnder interferometer with Dove prisms. $\alpha/2$ means relative angle between the two Dove prisms. The first OAM BS ($\alpha = \pi$) and the final OAM BS ($\alpha = -\pi$) change a direction of propagation of a photon whose OAM value is odd and even, respectively. The second OAM BS ($\alpha = \pi/2$) separates a photon whose OAM value is 0 and 2. With OAM holograms, the three-fold cyclic transformation of OAM modes $\{-1, 0, 1\}$ is accomplished.

There has been an experimental demonstration of the prepare-and-measure qudit QKD using seven OAM values of a single photon, which includes DMD for fast generation of single photon OAM states and spatial separation of OAM modes proposed in for OAM mode detection [56,66]. In the experiment, it was reported that the efficiency of OAM mode separation was 93%. It is expected that an experimental demonstration of d-QKD with hybrid encoding is possible by using above technologies as well as the prepare-and-measure qudit QKD.

4. Security Analysis

Before we analyze security of d-QKD with hybrid encoding, we need to assume constraints to construct secure d-QKD with hybrid encoding as it is studied in [28]: (i) Alice's and Bob's random number generators and their classical post-processing should be trusted. (ii) Alice's and Bob's encoding systems should be fully characterized and not be influenced by Eve. (iii) Eve cannot physically access to the output ports of the interferometer, in our protocol, the tritter. (iv) The detectors may have some imperfections, but the defects is not from Eve. The first assumption is essential for all QKD schemes to ensure security. The first and second assumptions are necessary for MDI-QKD as well. The third and final assumptions are different from the scenario of MDI-QKD. They are necessary to prevent particular classes of side channel attacks [28,29]. The third assumption can be considered not impractical, since d-QKD with hybrid encoding has the similar experimental situation to prepare-and-measure QKD protocols like original BB84. In the situation, Bob can have full measurement setup in his room and he can block access from the outside.

Let us consider several side channel attacks against d-QKD with hybrid encoding. Since its similarity of principles to the original DDI-QKD, the security of d-QKD with hybrid encoding against side channel attacks is comparable to that of the original DDI-QKD studied in [28,29]. Faked-state attack [10], detector efficiency mismatch attack [11], and time-shift attack [14] are not compatible with assumption (iv) since the attacks require a prior knowledge of imperfections of the single photon detectors. Trojan-horse attack based on back reflection [71–73] is considerable. In Trojan-horse attack based on back reflection, Eve sends multi-photon states into Alice's(Bob's) encoding system. The photons are reflected at the elements in the encoding system. Then Eve can obtain information about a generated single photon state by analyzing the reflected beam. The attack can be prevented by using frequency filters and isolators like in MDI-QKD case. Trojan-horse attack proposed in [74] is forbidden by assumption (iv), since the detectors in the measurement setup should be manufactured by Eve to accomplish this attack.

Detector blinding attack can threaten QKD systems as well. An essential procedure of the detector blinding attack is that Eve shines strong classical light onto detectors, avalanche photodiodes, to change their mode from Geiger mode to linear mode [12]. In the linear mode, a detection signal can be generated by the strong light pulse that exceeds a threshold. This means that Eve can control a detector

click by regulating amplitude of the light pulse. If a threshold of the all detectors is identical, the basic detector blinding attack can be detected by Bob. Let us define the threshold μ. Then the amplitude of Eve's light pulse should be larger than μ when it arrives at detectors. Eve intercepts Alice's signal and resends a strong light corresponding to the measured quantum state. When Eve's and Bob's bases are matched, for example OAM modes and path modes, the amplitude of Eve's light pulse should be larger than $d\mu$ to make a detector click since the tritter splits the light pulse into four output ports identically. In the situation, Bob can notice the detector blinding attack since d detectors are clicked simultaneously. Bob can make an error rate be affected by the attack by assigning random number when more than two detectors are clicked. If there are differences among the threshold of detectors, it is possible that Eve generates one detector click. The clicked detector must have the lowest threshold among the detectors. This means that Eve cannot generate a click of the other detectors independently. So the attack can be found by analyzing statistics of detector clicks.

Detector blinding attack with various blinding power [13] can threaten d-QKD with hybrid encoding as well as the original DDI-QKD [29]. However, since the attack requires a prior knowledge about the detectors, it is not compatible with assumption (iv). So we can conclude that without the assumptions which are not necessary in MDI-QKD, the security of d-QKD with hybrid encoding cannot be guaranteed against all detector side channel attacks.

To detect Eve's side channel attacks, we introduce a random tritter operation of Bob. The tritter operation written in Equation (2) is performed on path modes after Bob's encoding. It is possible that Bob chooses one of tritter operation among d different operations ratter than a fixed operation. For example, Bob can chooses one operation among the operations shown in Equation (5):

$$\hat{U}_{3,0} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \hat{U}_{3,1} = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega^2 & 1 & \omega \\ 1 & 1 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}, \quad \hat{U}_{3,2} = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega^2 & \omega & 1 \\ \omega & \omega^2 & 1 \\ 1 & 1 & 1 \end{pmatrix} \tag{5}$$

for $3d$-QKD with hybrid encoding. The operations can be implemented by using $3d$-tritter and phase shifters.

Let us consider the case that Bob chooses path mode $|\bar{p}_0\rangle$ and Eve tries detector blinding attack with strong pulse whose OAM mode is $|\bar{l}_0\rangle$. If Bob chooses t, where $t \in \{0, 1, 2\}$, and performs the tritter operation $\hat{U}_{3,t}$, the pulse goes to output port p_t of the tritter. For a successful attack, Eve must find the pulse intensity and that one detector in the output port is clicked and the other detectors are not, regardless of Bob's choice of tritter operation. Also, Eve should perform detector blinding attacks with various blinding power and find at least three different blinding powers, since Bob monitors statistics of outcomes. For instance, Bob can check whether $|\bar{l}_0, \bar{p}_0\rangle$ is projected onto $|\Phi_0\rangle$, $|\Phi_3\rangle$, and $|\Phi_6\rangle$ equally or not. Therefore, Eve should prepare at least three different pulse intensities, which occur click events of different detectors on the same output port, to pass Bob's statistics check.

For a large dimension, we expect that such attack is improbable with the assumption (iv), i.e., with trusted devices. Since click thresholds of different detectors are very similar but randomly fluctuated, it is difficult to find blinding powers and pulse intensities that satisfy the successful attack conditions. For a successful attack, Eve should find the powers and intensities that only one detector is clicked while the other $d-1$ detectors in the port are not clicked, and the attack does not influence Bob's outcome statistics regardless of Bob's choice of tritter operation $\hat{U}_{d,t}$, where $t \in \{0, 1, 2, ..., d-1\}$. Therefore, we expect that side channel attacks are probably detected for a high-dimensional QKD using hybrid encoding, if Bob applies the random choice of tritter operation and a countermeasure of a side channel attack, such as the random-detector-efficiency protocol [75,76]. Compared to this, prepare-and-measure QKD protocols using high-dimensional systems are threatened by the first proposal of detector blinding attack [12], and the original DDI-QKD was breached by the combined attack of the detector blinding attack with various blinding power and detector efficiency mismatched attacks even with the random-detector-efficiency protocol [13]. Therefore, we can conclude that the complexity of a successful side channel attack becomes higher by exploiting the proposed protocol

compared to prepare-and-measure d-QKDs and the original DDI-QKD, although the proposed protocol does not provide the detector-device-independent security.

It is necessary to analyze security of d-QKD with hybrid encoding to evaluate the usefulness of the protocol. The analysis of the security is able to be made through the inspection of the equivalent protocol using the entanglement distillation process (EDP) [4–6]. The idea of the method is that, if Alice and Bob share the maximally entangled state, Eve cannot generate correlation between her state and the shared maximally entangled state of Alice and Bob [77]. In the method, we can analyze the security of the proposed protocol with the amount of distributed maximally entangled states. In order to use the method, an equivalent protocol of which Alice and Bob share an entangled state at the end should be introduced. Note that the equivalent protocol is employed only for the security analysis, so its experimental efficiency is not significant. However, it is important that the equivalent protocol is physically realizable, since any security analysis of QKD should be valid under quantum mechanics. Therefore, we will briefly introduce possible implementations of the equivalent protocol to show that it is physically reasonable.

At first, Alice and Bob generate the three-photon entangled state shown in Equation (6):

$$|\Psi\rangle_{ABD} = \frac{1}{d}\sum_{m,n=0}^{d-1} |l_m\rangle_A \, |l=0, p_n\rangle_B \, |l_m, p_n\rangle_D \,, \tag{6}$$

where the subscript $A(B)$ means Alice's (Bob's) single photon state and the subscript D means a single photon that goes to tritter and OAM measurement setup. Generation of this state is possible, in principle, by using two cascade spontaneous parametric down-conversion (SPDC) crystals, spatial discrimination elements of the OAM mode, and relabelling of the OAM and path values. For a 4-dimensional system, the generation of 4-dimensional OAM mode entangled states [78] and 4-dimensional path mode entangled states [79,80] using SPDC crystals was demonstrated . Alice and Bob keep their photons, and Bob measures the photon D using the measurement setup. Based on the result, Bob performs the corresponding unitary operation to share the maximally entangled state shown in Equation (7) :

$$\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} |l_k\rangle_A \otimes |p_k\rangle_B \,. \tag{7}$$

Alice (Bob) chooses her (his) measurement basis randomly between OAM (path) modes and bar OAM (path) modes. After the measurement, Alice and Bob share their measurement bases and discard if the two bases are not matched. If the two bases are matched, their measurement outcomes are always identical if there is no error and no Eve.

Since the maximally entangled state is distributed to Alice and Bob, security of the protocol becomes the same with that of a d-dimensional entanglement based QKD. Security of a QKD using d-dimensional maximally entangled states was studied against individual attacks [33] (Eve monitors state separately), and against collective attacks [34,35] (Eve monitors several states jointly). According to the results, secret key rate of QKD using d-dimensional quantum states against collective attack is evaluated as shown in Equation (8):

$$r = \log_2 d + 2Q\log_2\left(\frac{Q}{d-1}\right) + (1-Q)\log_2(1-Q)\,. \tag{8}$$

The unit of the secret key rate is (bits/sifted signal). Q is state error rate obtained from Equation (9):

$$Q = \sum_{i\neq j} \langle l_i, p_j| \, \rho \, |l_i, p_j\rangle \,, \tag{9}$$

where ρ is the density matrix of the state shared by Alice and Bob, and $i, j \in \{0, 1, 2, ..., d-1\}$. In the ideal case, no error and no Eve, since the distributed state is the state described in Equation (7), the error rate becomes trivial, $Q = 0$.

Now, we investigate an improvement of a secret key rate of d-QKD with hybrid encoding compared with the original DDI-QKD. Secret key rates per sifted signal, r, of d-QKD with hybrid encoding are plotted in Figure 4. Figure 4a shows the secret key rate of the original DDI-QKD (black dotted line), 3d- (red dashed line), 4d- (blue dot-dashed line), and 5d-QKD with hybrid encoding (orange solid line) in the ideal situation. QKD with hybrid encoding using higher dimensional quantum states has a higher secret key rate than the original DDI-QKD at same error rate, since a quantum system in high-dimension can carry more information per single quanta and qudit has enhanced robustness against an optimal cloning and eavesdropping.

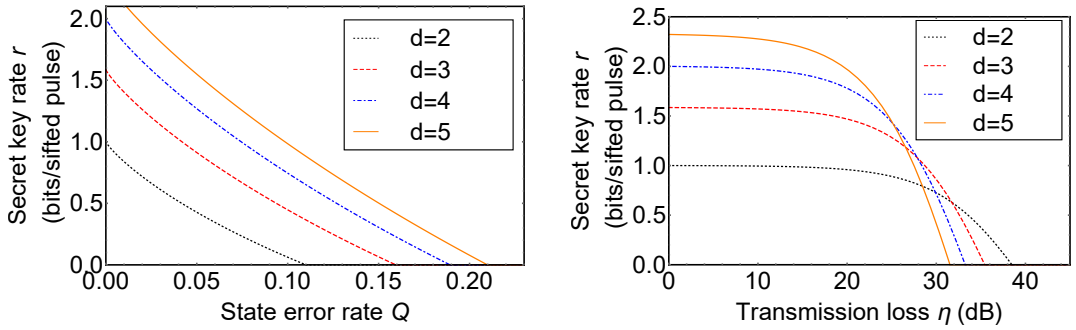


Figure 4. The secret key rate of the original detector-device-independent QKD (DDI-QKD) (black dotted line), 3d- (red dashed line), 4d- (blue dot-dashed line), and 5d-QKD with hybrid encoding (orange solid line). (**a**) Plot of the secret key rate r (bits/sifted pulse) vs. state error rate Q; (**b**) Plot of the secret key rate r (bits/sifted pulse) vs. transmission loss η (dB). Dark count rate of single photon detectors is assumed as 10^{-5} per pulse.

In Figure 4b, we simulate secret key rates of d-QKD with hybrid encoding and the original DDI-QKD with a change of the realistic experimental factors, transmission loss η and dark count rate of single photon detectors. When a photon propagates through an optical fiber or atmosphere, there is transmission loss. So transmission efficiency is approximately proportional to the distance between Alice and Bob that QKD is able to be achieved. For a single photon detector, since it is very sensitive in order to detect a very weak pulse, a single photon, it is possible to be clicked by background noise even if there is no received photon. The event is called dark count. If there is no Eve, the probability of the detector click corresponding to the state $|\Phi_0\rangle$ when Alice encodes x and Bob encodes y in a single photon is able to be described as follows:

$$p(x,x) = \frac{1}{d}(1-\eta)(1-\nu)^{(d^2-1)} + \eta\nu(1-\nu)^{(d^2-1)} \tag{10}$$

$$p(x,y) = \eta\nu(1-\nu)^{(d^2-1)} \tag{11}$$

where $x, y \in \{0, 1, 2, ..., d-1\}$, $x \neq y$, d is the dimension of quantum states used in d-QKD with hybrid encoding, and ν is the dark count rate per pulse. The first term in Equation (10) denotes the case when the single photon arrives at a detector and it triggers off the detector, while there is no dark count in the other detectors. The second term in Equation (10) denotes that the single photon detector is clicked due to the dark count when the single photon is lost in channel and the other detectors are not clicked. In the ideal case, no Eve and no state error, $p(x, y)$ should be zero since the state cannot be projected on $|\Phi_0\rangle$. The only case that the detector is clicked is that the single photon is lost and the detector is

clicked due to the dark count. The error rate in this situation is evaluated from the equation described as follows:

$$Q = \frac{\sum_{i \neq j} p(i,j)}{\sum_{x,y=0}^{d-1} p(x,y)}, \tag{12}$$

where $i, j \in \{0, 1, 2, ..., d-1\}$. The dark count rate, ν, is assumed as 10^{-5} per pulse in Figure 4b. In the plot, it is shown that a secret key rate becomes higher, as the dimension of quantum states used in d-QKD with hybrid encoding increases in low transmission loss regime. When the transmission loss is high, the secret key rate decreases more rapidly as d increases. QKD with hybrid encoding using higher dimensional quantum states is more influenced by the dark count of detectors, since the number of the single photon detector used in d-QKD with hybrid encoding is lager than the original DDI-QKD. Therefore, when a single photon is lost, the error rate of QKD with hybrid encoding using higher dimensional quantum states increases rapidly compared with that of the original DDI-QKD.

Now, we compare 3d-QKD with hybrid encoding with MDI-QKD using 3-dimensional quantum states (3d-MDI-QKD). 3d-MDI-QKD was proposed to increase a secret key rate of original MDI-QKD [38]. In its key rate analysis, it is assumed that 3-dimensional BSM used in 3d-MDI-QKD includes six single photon detectors and the 3-dimensional BSM setup can discriminate only three 3-dimensional Bell states among nine ones. Figure 5 shows the secret key rate of 3d-MDI-QKD (red dashed line) and 3d-QKD with hybrid encoding (black solid line). Secret key rate per total pulse can be obtained from (signal sifting rate) $\times$ (secret key rate per sifted key r). The signal sifting rate is obtained from (the probability that Alice and Bob used the same bases) in d-QKD with hybrid encoding, and (the probability that Alice and Bob used the same bases) $\times$ (the success probability of a BSM) in MDI-QKD. Since a success probability of BSM with linear optics cannot be 100% [18,19], MDI-QKD always has a lower secret key rate per total signal than prepare-and-measure QKD protocols and QKD with hybrid encoding.

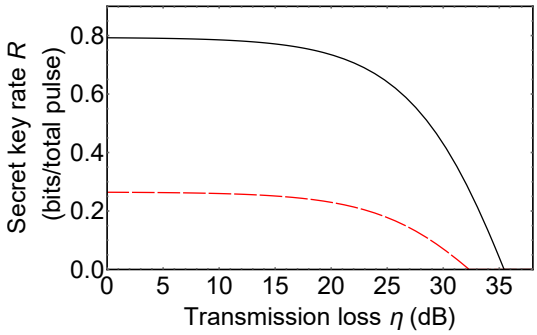


Figure 5. The secret key rate of 3d-measurement-device-independent QKD (MDI-QKD) (red dashed line) and 3d-QKD with hybrid encoding (black solid line). Plot of the secret key rate R (bits/total pulse) vs. transmission loss η (dB). The secret key rate per total signal is obtained from (the secret key rate per sifted key)$\times$(the signal sifting rate). Details are described in maintext. Dark count rate of single photon detectors is assumed as 10^{-5} per pulse.

Furthermore, it was proven that a generalized BSM in a high-dimensional two-photon state cannot be implemented by means of linear optical elements [19]. The scheme using multi-photon interference with linear optics can be adopted to implement MDI-QKD using qudits [81], however, the secret key rate R of the protocol is always lower than original MDI-QKD, since the signal sifting rate of the protocol is given as $1/(2d^2)$. There is another scheme in which the ideal signal sifting rate can reach $1/(2d)$ by exploiting nonlinear effects, however, because of the nonlinearity, experimental efficiency of the scheme is much lower than that of the setup with linear optical elements [82]. Also, it was shown that a secret key rate of MDI-QKD using qudits ($d > 4$) cannot exceed that of qubit MDI-QKD at low error rate even if a signal sifting rate of a d-dimensional BSM setup reaches $1/(2d)$ [82]. Therefore,

it can be claimed that QKD with hybrid encoding is more suitable to exploit qudits than MDI-QKD in its implementation, although it needs additional assumptions to guarantee the security level of MDI-QKD.

Here, we compare key generation efficiency of d-QKD with hybrid encoding with that of existing d-QKDs. First, compared with entanglement-based d-QKDs [43–45], our protocol has an advantage in that generation of an entangled state is not necessary. A high-dimensional time-energy entangled state is generated from spontaneous parametric down-conversion (SPDC), and entangled state generation efficiency of SPDC is not comparable with a single photon OAM mode encoder.

Key generation efficiency of prepare-and-measure d-QKDs [47–50,83] are comparable with that of our protocol. Our protocol is vulnerable to photon loss noise compared with prepare-and-measure d-QKDs, as it is shown in Figure 6. Our protocol employs d^2 detectors in the measurement setup, while prepare-and-measure d-QKDs have $2d$ detectors. Because of this reason, an effect of a dark count of detectors in our protocol is larger than that in prepare-and-measure d-QKDs. This means that growth in an error rate of our protocol is higher than that of prepare-and-measure d-QKDs when a single photon is lost. However, as it is shown in the security analysis, our protocol can prevent certain kinds of side channel attacks against detectors, while security of prepare-and-measure d-QKDs is threatened even by the first proposal of a detector blinding attack. In consideration of this, the gap between the two secret key rates shown in Figure 6 is not significant.

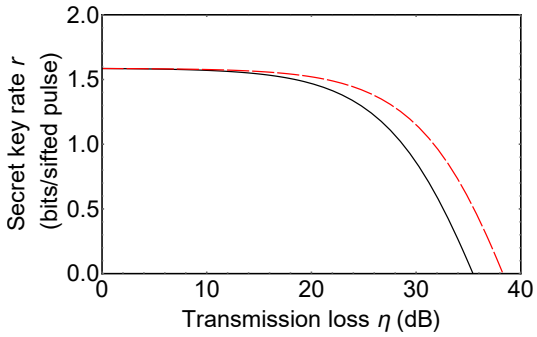


Figure 6. The secret key rate of $3d$-QKD hybrid encoding (black solid line) and a prepare-and-measure $3d$-QKD (red dashed line). Dark count rate of single photon detectors is assumed as 10^{-5} per pulse.

Finally, we note that it is possible to employ state-of-the-art techniques in our protocol, since our protocol is constructed with general experimental elements. For example, in d-QKD using partial MUBs of OAM [49], they proposed using special single photon OAM modes in their protocol for noise robustness. It is expected that the setups used in the protocol are exploited in our protocol for the same purpose as well.

5. Conclusions

In this paper, we proposed a schematic configuration of d-dimensional QKD based on hybrid encoding over two different DoFs. Qudits are exploited in the setup to improve a secret key rate, since a qudit can carry more classical information and it has enhanced robustness against eavesdropping compared with a qubit. We investigated possible practical implementations of the proposed QKD protocol with current optical technologies. OAM modes of a single photon is exploited as a high-dimensional information carrier. OAM modes are suitable for quantum communication because of their resilience against perturbation effects. We showed that a cyclic transformation of OAM modes can be implemented within the reach of current technologies as well. We analyzed security of the proposed protocol and showed there is improvement compared with original qubit protocol in an ideal situation. We found the condition that d-QKD with hybrid encoding has a higher secret key rate than the original DDI-QKD in the consideration of realistic experimental parameters as well.

Finally we compared our protocol with existing d-QKDs and showed our protocol has advantages regarding the prevention of side channel attacks against detectors and experimental feasibility.

Author Contributions: Y.J. designed and analysed the protocols. H.S.P. and S.-W.L. provided guidance. W.S. supervised the whole project. All authors reviewed the manuscript.

Funding: This work was supported by the R&D Convergence Program of the National Research Council of Science and Technology (NST) (Grant No. CAP-15-08-KRISS) of Republic of Korea.

Acknowledgments: Yonggi Jo thanks to the Agency for Defense Development (ADD) for their graduate student scholarship program. Wonmin Son acknowledges the University of Oxford and the Korea Institute for Advanced Study (KIAS) for their visitorship program.

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. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
3. Deutsch, D.; Ekert, A.; Jozsa, R.; Macchiavello, C.; Popescu, S.; Sanpera, A. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.* **1996**, *77*, 2818–2821. [CrossRef] [PubMed]
4. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351–406. [CrossRef]
5. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]
6. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **2005**, *461*, 207–235. [CrossRef]
7. Koashi, M. Unconditional security of quantum key distribution and the uncertainty principle. *J. Phys. Conf. Ser.* **2006**, *36*, 98–102. [CrossRef]
8. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **2009**, *11*, 045018. [CrossRef]
9. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef]
10. Makarov, V.; Hjelme, D.R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **2005**, *52*, 691–705. [CrossRef]
11. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313. [CrossRef]
12. 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]
13. Huang, A.; Sajeed, S.; Chaiwongkhot, P.; Soucarros, M.; Legre, 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]
14. Qi, B.; Fung, C.F.; Lo, H.; Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **2007**, *7*, 73–82.
15. 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] [PubMed]
16. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
17. Żukowski, M.; Zeilinger, A.; Horne, M.A.; Ekert, A.K. "Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **1993**, *71*, 4287–4290. [CrossRef] [PubMed]
18. Lütkenhaus, N.; Calsamiglia, J.; Suominen, K.A. Bell measurements for teleportation. *Phys. Rev. A* **1999**, *59*, 3295–3300. [CrossRef]
19. Calsamiglia, J. Generalized measurements by linear elements. *Phys. Rev. A* **2002**, *65*, 030301. [CrossRef]

20. Grice, W.P. Arbitrarily complete Bell-state measurement using only linear optical elements. *Phys. Rev. A* **2011**, *84*, 042331. [CrossRef]
21. Zaidi, H.A.; van Loock, P. Beating the One-Half Limit of Ancilla-Free Linear Optics Bell Measurements. *Phys. Rev. Lett.* **2013**, *110*, 260501. [CrossRef] [PubMed]
22. Lee, S.W.; Jeong, H. Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits. *Phys. Rev. A* **2013**, *87*, 022326. [CrossRef]
23. Lee, S.W.; Park, K.; Ralph, T.C.; Jeong, H. Nearly Deterministic Bell Measurement for Multiphoton Qubits and its Application to Quantum Information Processing. *Phys. Rev. Lett.* **2015**, *114*, 113603. [CrossRef] [PubMed]
24. Lee, S.W.; Park, K.; Ralph, T.C.; Jeong, H. Nearly deterministic Bell measurement with multiphoton entanglement for efficient quantum-information processing. *Phys. Rev. A* **2015**, *92*, 052324. [CrossRef]
25. Lim, C.C.W.; Korzh, B.; Martin, A.; Bussières, F.; Thew, R.; Zbinden, H. Detector-device-independent quantum key distribution. *Appl. Phys. Lett.* **2014**, *105*, 221112. [CrossRef]
26. Liang, W.Y.; Li, M.; Yin, Z.Q.; Chen, W.; Wang, S.; An, X.B.; Guo, G.C.; Han, Z.F. Simple implementation of quantum key distribution based on single-photon Bell-state measurement. *Phys. Rev. A* **2015**, *92*, 012319. [CrossRef]
27. González, P.; Rebón, L.; Ferreira da Silva, T.; Figueroa, M.; Saavedra, C.; Curty, M.; Lima, G.; Xavier, G.B.; Nogueira, W.A.T. Quantum key distribution with untrusted detectors. *Phys. Rev. A* **2015**, *92*, 022337. [CrossRef]
28. Boaron, A.; Korzh, B.; Houlmann, R.; Boso, G.; Lim, C.C.W.; Martin, A.; Zbinden, H. Detector-device-independent quantum key distribution: Security analysis and fast implementation. *J. Appl. Phys.* **2016**, *120*, 063101. [CrossRef]
29. Sajeed, S.; Huang, A.; Sun, S.; Xu, F.; Makarov, V.; Curty, M. Insecurity of Detector-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2016**, *117*, 250505. [CrossRef]
30. Navez, P.; Cerf, N.J. Cloning a real *d*-dimensional quantum state on the edge of the no-signaling condition. *Phys. Rev. A* **2003**, *68*, 032313. [CrossRef]
31. Bouchard, F.; Fickler, R.; Boyd, R.W.; Karimi, E. High-dimensional quantum cloning and applications to quantum hacking. *Sci. Adv.* **2017**, *3*. [CrossRef]
32. 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] [PubMed]
33. Durt, T.; Kaszlikowski, D.; Chen, J.L.; Kwek, L.C. Security of quantum key distributions with entangled qudits. *Phys. Rev. A* **2004**, *69*, 032313. [CrossRef]
34. Sheridan, L.; Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **2010**, *82*, 030301. [CrossRef]
35. Ferenczi, A.; Lütkenhaus, N. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A* **2012**, *85*, 052310. [CrossRef]
36. Coles, P.J.; Metodiev, E.M.; Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nat. Commun.* **2016**, *7*, 11712. [CrossRef] [PubMed]
37. Pivoluska, M.; Huber, M.; Malik, M. Layered quantum key distribution. *Phys. Rev. A* **2018**, *97*, 032312. [CrossRef]
38. Jo, Y.; Son, W. Key-rate enhancement using qutrit states for quantum key distribution with askew aligned sources. *Phys. Rev. A* **2016**, *94*, 052316. [CrossRef]
39. Hwang, W.Y.; Su, H.Y.; Bae, J. N-dimensional measurement-device-independent quantum key distribution with N + 1 un-characterized sources: zero quantum-bit-error-rate case. *Sci. Rep.* **2016**, *6*, 30036. [CrossRef]
40. Dellantonio, L.; Sørensen, A.S.; Bacco, D. High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. *Phys. Rev. A* **2018**, *98*, 062301. [CrossRef]
41. Bechmann-Pasquinucci, H.; Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **2000**, *61*, 062308. [CrossRef]
42. 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]
43. 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]

44. Nunn, J.; Wright, L.J.; Söller, C.; Zhang, L.; Walmsley, I.A.; Smith, B.J. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express* **2013**, *21*, 15959–15973. [CrossRef] [PubMed]
45. 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]
46. Gröblacher, S.; Jennewein, T.; Vaziri, A.; Weihs, G.; Zeilinger, A. Experimental quantum cryptography with qutrits. *New J. Phys.* **2006**, *8*, 75. [CrossRef]
47. Mirhosseini, M.; Magaña-Loaiza, O.S.; O'Sullivan, M.N.; Rodenburg, B.; Malik, M.; Lavery, M.P.J.; Padgett, M.J.; Gauthier, D.J.; Boyd, R.W. High-dimensional quantum cryptography with twisted light. *New J. Phys.* **2015**, *17*, 033033. [CrossRef]
48. Sit, A.; Bouchard, F.; Fickler, R.; Gagnon-Bischoff, J.; Larocque, H.; Heshami, K.; Elser, D.; Peuntinger, C.; Günthner, K.; Heim, B.; Marquardt, C.; Leuchs, G.; Boyd, R.W.; Karimi, E. High-dimensional intracity quantum cryptography with structured photons. *Optica* **2017**, *4*, 1006–1010. [CrossRef]
49. Wang, F.; Zeng, P.; Wang, X.; Gao, H.; Li, F.; Zhang, P. Towards practical high-speed high dimensional quantum key distribution using partial mutual unbiased basis of photon's orbital angular momentum. *arXiv* **2018**, arXiv:quant-ph/1801.06582.
50. Bouchard, F.; Heshami, K.; England, D.; Fickler, R.; Boyd, R.W.; Englert, B.G.; Sánchez-Soto, L.L.; Karimi, E. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2018**, *2*, 111. [CrossRef]
51. Yang, X.; Wei, K.; Ma, H.; Liu, H.; Yin, Z.; Cao, Z.; Wu, L. Detector-device-independent quantum secret sharing with source flaws. *Sci. Rep.* **2018**, *8*, 5728. [CrossRef]
52. Erhard, M.; Fickler, R.; Krenn, M.; Zeilinger, A. Twisted photons: New quantum perspectives in high dimensions. *Light Sci. Appl.* **2018**, *7*, 17146. [CrossRef]
53. Mair, A.; Vaziri, A.; Weihs, G.; Zeilinger, A. Entanglement of the orbital angular momentum states of photons. *Nature* **2001**, *412*, 313–316. [CrossRef] [PubMed]
54. Żukowski, M.; Zeilinger, A.; Horne, M.A. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Phys. Rev. A* **1997**, *55*, 2564–2579. [CrossRef]
55. Bazhenov, V.; Soskin, M.; Vasnetsov, M. Screw Dislocations in Light Wavefronts. *J. Mod. Opt.* **1992**, *39*, 985–990. [CrossRef]
56. Mirhosseini, M.; na Loaiza, O.S.M.; Chen, C.; Rodenburg, B.; Malik, M.; Boyd, R.W. Rapid generation of light beams carrying orbital angular momentum. *Opt. Express* **2013**, *21*, 30196–30203. [CrossRef] [PubMed]
57. Larocque, H.; Gagnon-Bischoff, J.; Bouchard, F.; Fickler, R.; Upham, J.; Boyd, R.W.; Karimi, E. Arbitrary optical wavefront shaping via spin-to-orbit coupling. *J. Opt.* **2016**, *18*, 124002. [CrossRef]
58. Larocque, H.; Gagnon-Bischoff, J.; Mortimer, D.; Zhang, Y.; Bouchard, F.; Upham, J.; Grillo, V.; Boyd, R.W.; Karimi, E. Generalized optical angular momentum sorter and its application to high-dimensional quantum cryptography. *Opt. Express* **2017**, *25*, 19832–19843. [CrossRef] [PubMed]
59. Leach, J.; Padgett, M.J.; Barnett, S.M.; Franke-Arnold, S.; Courtial, J. Measuring the Orbital Angular Momentum of a Single Photon. *Phys. Rev. Lett.* **2002**, *88*, 257901. [CrossRef]
60. Krenn, M.; Malik, M.; Fickler, R.; Lapkiewicz, R.; Zeilinger, A. Automated Search for new Quantum Experiments. *Phys. Rev. Lett.* **2016**, *116*, 090405. [CrossRef]
61. Schlederer, F.; Krenn, M.; Fickler, R.; Malik, M.; Zeilinger, A. Cyclic transformation of orbital angular momentum modes. *New J. Phys.* **2016**, *18*, 043019. [CrossRef]
62. Babazadeh, A.; Erhard, M.; Wang, F.; Malik, M.; Nouroozi, R.; Krenn, M.; Zeilinger, A. High-Dimensional Single-Photon Quantum Gates: Concepts and Experiments. *Phys. Rev. Lett.* **2017**, *119*, 180510. [CrossRef] [PubMed]
63. Chen, D.X.; Liu, R.F.; Zhang, P.; Wang, Y.L.; Li, H.R.; Gao, H.; Li, F.L. Realization of quantum permutation algorithm in high dimensional Hilbert space. *Chin. Phys. B* **2017**, *26*, 060305. [CrossRef]
64. Lavery, M.P.J.; Robertson, D.J.; Berkhout, G.C.G.; Love, G.D.; Padgett, M.J.; Courtial, J. Refractive elements for the measurement of the orbital angular momentum of a single photon. *Opt. Express* **2012**, *20*, 2110–2115. [CrossRef] [PubMed]
65. Lavery, M.P.J.; Robertson, D.J.; Sponselli, A.; Courtial, J.; Steinhoff, N.K.; Tyler, G.A.; Willner, A.; Padgett, M.J. Efficient measurement of an optical orbital-angular-momentum spectrum comprising more than 50 states. *New J. Phys.* **2013**, *15*, 013024. [CrossRef]

66. Mirhosseini, M.; Malik, M.; Shi, Z.; Boyd, R.W. Efficient separation of the orbital angular momentum eigenstates of light. *Nat. Commun.* **2013**, *4*, 1–6. [CrossRef] [PubMed]
67. Malik, M.; Mirhosseini, M.; Lavery, M.P.J.; Leach, J.; Padgett, M.J.; Boyd, R.W. Direct measurement of a 27-dimensional orbital-angular-momentum state vector. *Nat. Commun.* **2014**, *5*, 3115. [CrossRef] [PubMed]
68. Shi, Z.; Mirhosseini, M.; Margiewicz, J.; Malik, M.; Rivera, F.; Zhu, Z.; Boyd, R.W. Scan-free direct measurement of an extremely high-dimensional photonic state. *Optica* **2015**, *2*, 388–392. [CrossRef]
69. Zhou, H.L.; Fu, D.Z.; Dong, J.J.; Zhang, P.; Chen, D.X.; Cai, X.L.; Li, F.L.; Zhang, X.L. Orbital angular momentum complex spectrum analyzer for vortex light based on the rotational Doppler effect. *Light Sci. Appl.* **2017**, *6*, e16251–e16251. [CrossRef]
70. Kulkarni, G.; Sahu, R.; Magaña-Loaiza, O.S.; Boyd, R.W.; Jha, A.K. Single-shot measurement of the orbital-angular-momentum spectrum of light. *Nat. Commun.* **2017**, *8*, 1054. [CrossRef]
71. 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]
72. 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]
73. Jain, N.; Stiller, B.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 168–177. [CrossRef]
74. Qi, B. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Phys. Rev. A* **2015**, *91*, 020303. [CrossRef]
75. Da Silva, T.F.; do Amaral, G.C.; Xavier, G.B.; Temporão, G.P.; von der Weid, J.P. Safeguarding Quantum Key Distribution Through Detection Randomization. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 159–167. [CrossRef]
76. Lim, C.C.W.; Walenta, N.; Legré, M.; Gisin, N.; Zbinden, H. Random Variation of Detector Efficiency: A Countermeasure Against Detector Blinding Attacks for Quantum Key Distribution. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 192–196. [CrossRef]
77. Coffman, V.; Kundu, J.; Wootters, W.K. Distributed entanglement. *Phys. Rev. A* **2000**, *61*, 052306. [CrossRef]
78. Wang, F.; Erhard, M.; Babazadeh, A.; Malik, M.; Krenn, M.; Zeilinger, A. Generation of the complete four-dimensional Bell basis. *Optica* **2017**, *4*, 1462–1467. [CrossRef]
79. Lee, H.J.; Choi, S.K.; Park, H.S. Experimental Demonstration of Four-Dimensional Photonic Spatial Entanglement between Multi-core Optical Fibres. *Sci. Rep.* **2017**, *7*, 4302. [CrossRef]
80. Lee, H.J.; Park, H.S. Generation and measurement of arbitrary four-dimensional spatial entanglement between photons in multicore fibers. *Photon. Res.* **2019**, *7*, 19–27. [CrossRef]
81. Goyal, S.K.; Boukama-Dzoussi, P.E.; Ghosh, S.; Roux, F.S.; Konrad, T. Qudit-Teleportation for photons with linear optics. *Sci. Rep.* **2014**, *4*, 4543. [CrossRef]
82. Jo, Y.; Son, W. Enhanced Bell state measurement for efficient measurement-device-independent quantum key distribution using 3-dimensional quantum states. *Sci. Rep.* **2019**, in press.
83. 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]