applied sciences

IMPACT FACTOR 2.5

CITESCORE 5.5

Article

High-Dimensional Quantum Key Distribution with *N*-Qudits States in Optical Fibers

Jesús Liñares, Xesús Prieto-Blanco and Alexandre Vázquez-Martínez

MDPI

https://doi.org/10.3390/app16031396

applied sciences

MDPI

Article

High-Dimensional Quantum Key Distribution with *N*-Qudits States in Optical Fibers

Jesús Liñares *, Xesús Prieto-Blanco and Alexandre Vázquez-Martínez

Quantum Materials and Photonics Research Group, Optics Area, Department of Applied Physics, Institute of Materials (iMATUS) /Faculty of Physics/Faculty of Optics and Optometry, University of Santiago de Compostela, 15782 Santiago de Compostela, Galicia, Spain; xesus.prieto.blanco@usc.es (X.P.-B.); alexandre.vazquez.martinez@rai.usc.es (A.V.-M.)

* Correspondence: suso.linares.beiras@usc.es

Abstract

We present a high-dimensional quantum key distribution protocol by using *N*-qudits quantum light states—that is, product states with *N* photons, each of them in a quantum superposition of dimension *d*, which provides a high dimension d^N and, accordingly, a very high security level. We present the implementation of this protocol in different types of optical fibers, where quantum states can undergo polarization and phase perturbations under propagation in optical fibers; however, polarization perturbations can be notably reduced in a passive or active way, and, more importantly, these states can become insensitive to phase perturbations. Thus, *N*-qubits are fully robust to relative phase perturbations between any pair of 1-qubits, and therefore do not require any phase compensation, which, on the contrary, is absolutely necessary in high-dimensional QKD with 1-qudits (one photon). Likewise, quantum states also undergo attenuation, that is, some photons are lost under propagation in the optical fibers and thus $N'(<N)$-qudits are used; however, even for standard optical fiber attenuation values, high secret key rates are still obtained. Finally, we analyse the security of this high-dimensional protocol under an intercept and resend attack performed by Eve, and the resulting secure key rates are calculated, showing a significant increase with the dimension provided by number *N* of photons.

Keywords: high-dimensional QKD; *N*-qudits; optical fibers

1. Introduction

Quantum Key Distribution (QKD) is considered a key technology for future secure optical communications. The main reason for this is that the security of the present classical cryptography is based on mathematical algoritms, which will no longer be guaranteed when quantum computers become available. QKD, a branch of optical quantum communications, is a technology based on the properties of the quantum light that allows for the exchange of secure information between two users, Alice and Bob, who share a random bit series or a key transported by quantum light states. Such quantum states can not be cloned by an eavesdropper.

There are several QKD approaches, which can be classified into Discrete Variable (DV) and Continuous Variable (CV) QKD, giving rise to different local QKD protocols [1,2] and leading to the possibility of a gobal QKD netwotk [3]. DV-QKD is based on the measurement of quantum states by projective measurements, and CV-QKD is based on the measurement of the quadratures of the optical field by using, for example, a balanced

Received: 31 December 2025
Revised: 22 January 2026
Accepted: 27 January 2026
Published: 29 January 2026

homodyne detection. Furthermore, there are several types of DV-QKD protocols based on the use of one photon, such as BB84 [4], B92 [5], and so on, and on the other hand there are protocols with two photons, such as BBM92 [6], MDI-QKD [7], and so on. It is important to indicate that, in the above cases with two photons, both Alice and Bob only possess one photon. Moreover, many of the above protocols have been generalized to high-dimensional protocols by using freedom degrees of the single photons that can be implemented in both multimode optical fibers as multicore optical fibers (MCF) [8,9] or few-modes optical fibers (FMF) [10], and/or free space [11]. Likewise, the use of more than two particles has attracted attention, such as, for example, the use of an entanglement of product states (three photons) of single-photon states to implement a long-distance MDI-QKD protocol (with Bell states) [12] or the proposal of multi-user protocols (with GHZ entangled states) [13].

It is well-known that security is increased by using high-dimensional QKD, which is obtained, as noted above, by taking into account some degrees of freedom of a single photon in a multimode optical fiber, such as different linear optical momentum (LOM) in few-modes optical fibers (FMF), different paths in multicore optical fibers (MCF), different polarizations, and different orbital angular momentum (OAM) [14], that is, with 1-qudits. High-dimensional QKD protocols with a single photon require passive (autocompensation) or active methods to compensate the random changes the quantum states undergo due to the perturbations of the optical fiber. Thus, unpredictable changes in polarization (modal coupling) and the relative phases between spatial modes have to be compensated, which requires technological solutions to restore, on the one hand, the polarization and, on the other hand, the phase. In this work, we present a high-dimensional (HD) DV-QKD protocol in optical fibers by using a number N of photons, specifically N-dimensional product states formed by N single-photon states. Each photon can, in turn, be in a superposition state; therefore, we will have d^N states, that is, N-qudits, and accordingly, a HD-DV-QKD protocol will be implemented, thus achieving both greater security and a larger secure key rate. As a clarification, we will consider that spatial channels, such as the cores of a MCF, are not coupled, and, importantly, the protocol is independent of the relative phase between the single-photon states. Therefore, the main advantage of using N photons is that the relative phase perturbations between photons are no longer relevant, and thus the technological requirements of phase compensation disappear; for example, as will be shown, N-qubits of polarization excited in N single-mode fibers (SMF) do not need relative phase compensation between such SMFs, and, moreover, a fewer (passsive or active) polarization compensation systems are needed. It is interesting to note that, recently, a continuous variable QKD protocol based on the product states of weak coherent states has also been proposed [15].

On the other hand, there are some necessary requirements to produce and detect product states. One of them is the use of sources of multiple single photons. There are several possible ways to achieve these states. For example, a series of SPDC (spontaneous parametric down-conversion) sources, which emit biphotons [16], or a series of SFWM (spontaneous four-wave mixing) sources that also emit biphotons [17], and then using one of the photons as a heralding signal to obtain the states of N photons when N coincidences are detected. Another possibility is to use the spatial demultiplexation of single photons from a single-photon source [18]. By using the demultiplexing method, states with up to eight photons, and even heralded GHZ states, have been demonstrated [19], which clearly exceed the requirements of our proposed protocol. Therefore, there are enough technological possibilities to produce these kinds of product states. Likewise, measurements of quantum states have to be made using standard projective measurements, along with photon coincidences, although this last requirement of detecting coincidences would not be strictly necessary.

The plan of this paper is as follows: in Section 2 the QKD protocol with N-qudits in optical fibers is presented, considering a realistic scenario (perturbations, losses, ...). In Section 3, the different physical implementations of N-qudits in optical fibers are presented and compared with the case of 1-qudits (single photon). In Section 4, a detailed study of the quantum bit error rate (QBER) and secure key rates (SKR) is presented, where an exhaustive analysis is made ff an intercept and resend attack with losses and optical fiber perturbations. Finally, in Section 5, a discussion of the results is presented.

2. QKD Protocol with N-Qudits in Optical Fibers

In this section, we present the QKD protocol with N-qudits in optical fibers. Let us consider that N photons are excited, each of them in a quantum superposition implemented in d optical modes of optical fibers. These quantum superpositions are generated in two mutually unbiased bases (MUBs), that is, with coefficients a_{jm} in the *Basis a* and b_{jm} and the *Basis b*, where $j = 1, \ldots, d$ indicates the base vector, $m = 1, \ldots, d$ indicates the component of the vector, and consequently the following superpositions are obtained:

$$\begin{array}{cc} \textit{Basis a} & \textit{Basis b} \\ |L_{1a}\rangle = a_{11}|1_1\rangle + a_{12}|1_2\rangle + \ldots + a_{1d}|1_d\rangle & |L_{1b}\rangle = b_{11}|1_1\rangle + b_{12}|1_2\rangle + \ldots + b_{1d}|1_d\rangle \\ |L_{2a}\rangle = a_{21}|1_1\rangle + a_{12}|1_2\rangle + \ldots + a_{1d}|1_d\rangle & |L_{2b}\rangle = b_{21}|1_1\rangle + b_{12}|1_2\rangle + \ldots + b_{1d}|1_d\rangle \\ \vdots & \vdots \\ |L_{da}\rangle = a_{d1}|1_1\rangle + a_{d2}|1_2\rangle + \ldots + a_{dd}|1_d\rangle & |L_{bn}\rangle = b_{d1}|1_1\rangle + b_{d2}|1_2\rangle + \ldots + b_{dd}|1_d\rangle. \end{array} \quad (1)$$

If N photons are considered, then the following product states are obtained in the two bases, that is,

$$|L_a\rangle = |L_a^{(1)}\rangle|L_a^{(2)}\rangle \ldots |L_a^{(N)}\rangle, \quad |L_b\rangle = |L_b^{(1)}\rangle|L_b^{(2)}\rangle \ldots |L_b^{(N)}\rangle, \quad (2)$$

where $|L_a^{(i)}\rangle$ and $|L_b^{(i)}\rangle$, with $i = 1, \ldots, N$, indicate some of the superpositions of basis states, given by Equation (1), for each photon. It is obvious that we obtain a number d^N of product states in each basis, and therefore a dimension $\mathcal{N} = d^N$ is obtained.

Alice sends N-qudit states, that is, N photons in a product state of N states of 1-qudit and, more importantly, all 1-qudits (chosen in a random way) are in the same base, that is, she sends states $|L_a\rangle$ or $|L_b\rangle$. On the other hand, Bob randomly chooses the measurement base of the 1-qudits and then the state of each photon is detected by a projective measurement. Each measurement in the right basis provides a string of mN bits, where $m = \log_2 d$. Additionally, if an intercept–resend attack is performed by Eve, the QBER is related to the error in detecting the correct state, that is, since the number of product states in each basis is $\mathcal{N} = d^N$, then the QBER is given by

$$\text{QBER} \equiv e = \frac{(\mathcal{N}-1)}{2\mathcal{N}} = \frac{(d^N-1)}{2d^N}. \quad (3)$$

It is important to stress that the existence of a relative phase between states of a product state does not change the state up to a global phase. This property provides great robustness to these states. Obviously, each photon is excited in a superposition state, where perturbations in the relative phases and amplitudes are possible, and therefore some compensation technique would be required. This problem has been extensively studied in the past using both passive (plug&play) and active methods.

On the other hand, we take into account that the current optical fibers have a certain attenuation loss, which means that some photons will be lost, and therefore the N-qudits convert in $N'(\leq N)$-qudits, that is, $N-1$-qudits, $N-2$-qudits ..., 1-qudit. For that reason,

we will also have to consider this most realistic scenario. Thus, in an optical fiber, the probability P of detecting a photon at a distance L is related to the attenuation, that is,

$$P(L) = 10^{-\alpha_{att} L/10}, \tag{4}$$

where α_{att} is the attenuation coefficient in the optical fiber in dB/km. Typical values are α_{att} = 0.2–0.4 dB/km for conventional fibers; however, in this analysis we will make use of an attenuation coefficient value $\alpha_{att} \approx 0.15$ dB km^{-1}, which takes into account the new advances in fiber design technologies [20]. This value is chosen to emphasize that this protocol is feasible even without employing hollow core fibers whose coefficient is $\alpha_{att} < 0.10$ dB km^{-1} [21]. Note that if we have product states of N photons, then we obtain several effective N'-qudits under attenuation. For example, if we have $N = 3$, we obtain the following in base a (the same is true for base b):

$$\begin{aligned} |L_a\rangle &= |L_a^{(1)}\rangle|L_a^{(2)}\rangle|L_a^{(3)}\rangle \quad (N' = 3), \\ |L_a^{'}\rangle &= |0\rangle|L_a^{(2)}\rangle|L_a^{(3)}\rangle, |L_a^{(1)}\rangle|0\rangle|L_a^{(3)}\rangle, |L_a^{(1)}\rangle|L_a^{(2)}\rangle|0\rangle \quad (N' = 2), \\ L_a^{''}\rangle &= |0\rangle|0\rangle|L_a^{(3)}\rangle, |0\rangle|L_a^{(2)}\rangle|0\rangle, |L_a^{(1)}\rangle 0\rangle|0\rangle \quad (N' = 1), \end{aligned} \tag{5}$$

therefore, the probability of detecting product states with three photons is given by $P_{(3)} = P^3$, with $P \equiv P(L)$; however, the probability of detecting product states with two photons is $P_{(2)} = 3P^2(1-P)$, and the probability of detecting product states with one photon is given by $P_{(1)} = 3P(1-P)^2$. This result can be generalized to N photons, of which N' are detected, that is,

$$P_{(N')} = \binom{N}{N-N'}(1-P)^{N-N'}, \quad 0 \leq N' \leq N. \tag{6}$$

In short, the attenuation will introduce limitations to the total secure key rate and the maximum distances allowed. However, by using several photons, we can overcome this problem, significantly increasing the security. For example, let us consider the case of 1-ququart (d = 4); then, the error produced by Eve is 37.5%. However, if we use 2 or 3 photons, that is, 2 and 3-ququart respectively, we obtain an error of 46.875% or 49.92%, close to the maximum error of 50%.

3. Implementations in Optical Fibers

Different kinds of optical fibers can be used to implement the above protocol. Since non-spatial modal coupling is required, the most interesting cases correspond to the use of a set of single-mode fibers (SMF) or a multicore optical fiber (MCF) with non-coupled N cores. A first approximation would be to use two polarization modes in each core and then N-qubit states can be implemented, that is, N photons are distributed into the N cores and, therefore, polarization qubits are implemented in each core, resulting in a QKD of dimension 2^N.

Alternatively, we may employ N subsets of M cores in an MCF supporting NM spatial modes, where each photon is simultaneously excited across M cores. By exploiting polarization modes, each subset encodes a single qudit of dimension $d = 2M$. Consequently, the system represents states of N-qudits, spanning a quantum space of dimension

$$\mathcal{N} = (2M)^N = \left[(2M)^{\frac{1}{M}}\right]^{NM}. \tag{7}$$

This last expresion shows us that, for a given number of cores $C = NM$, the highest dimension $\mathcal{N} = 2^C$ is achieved for $M = 1$ (qubits) or $M = 2$ (ququarts).

A key aspect of optical fibers is that the polarization state of the quantum states is changed during their propagation, which supposes a critical caveat in the real implementation of these QKD protocols. As a consequence, we have to deal with perturbations to ensure the stability of the polarization state. To compensate the perturbations in the polarization when the states are sent from Alice to Bob, active compensation [22,23] or passive compensation (autocompensation) [10,24] techniques represent a plausible and suitable solution. Likewise, when we have several space modes using non-coupled cores, then relative phase compensation is required, and therefore we will have much more technological complexity in the case using 1-qudits than in the case using the corresponding N-qubits providing the same dimension, that is, $\mathcal{N} = d = (2)^N$.

3.1. Product States with N-Qubits with Spatial and Polarization Modes

We start with the implementation of N-qubits ($M = 1$), that is, we have N spatial modes $j = 1, \ldots N$ of an MCF or N SMFs and, in each spatial mode, we excite a single photon, and therefore N-qubits, using the polarization modes in each spatial mode. We choose, for example, the following bases: *Basis a*—X (or diagonal); and *Basis b*—Y (or circular) basis (MUBs):

$$\mathrm{X}_j = \{|1_{D_j}\rangle = \frac{1}{\sqrt{2}}(|1_{H_j}\rangle + |1_{V_j}\rangle), |1_{A_j}\rangle = \frac{1}{\sqrt{2}}(|1_{H_j}\rangle - |1_{V_j}\rangle)\}, \quad j = 1, \ldots, N, \tag{8}$$

$$\mathrm{Y}_j = \{|1_{L_j}\rangle = \frac{1}{\sqrt{2}}(|1_{H_j}\rangle + i|1_{V_j}\rangle), |1_{R_j}\rangle = \frac{1}{\sqrt{2}}(|1_{H_j}\rangle - i|1_{V_j}\rangle)\}, \quad j = 1, \ldots, N. \tag{9}$$

As an example, let us consider three photons ($N = 3$); then, we can use a three-core MCF or three SMFs. Therefore, the product states in bases X and Y are

$$\begin{aligned}\mathrm{X} \rightarrow \{&|1_{D_1}\rangle|1_{D_2}\rangle|1_{D_3}\rangle, |1_{D_1}\rangle|1_{D_2}\rangle|1_{A_3}\rangle, |1_{D_1}\rangle|1_{A_2}\rangle|1_{D_3}\rangle, |1_{D_1}\rangle|1_{A_2}\rangle|1_{A_3}\rangle,\\ &|1_{A_1}\rangle|1_{D_2}\rangle|1_{D_3}\rangle, |1_{D_1}\rangle|1_{D_2}\rangle|1_{D_3}\rangle, |1_{D_1}\rangle|1_{D_2}\rangle|1_{D_3}\rangle, |1_{A_1}\rangle|1_{A_2}\rangle|1_{A_3}\rangle\}\end{aligned} \tag{10}$$

$$\begin{aligned}\mathrm{Y} \rightarrow \{&|1_{L_1}\rangle|1_{L_2}\rangle|1_{L_3}\rangle, |1_{L_1}\rangle|1_{L_2}\rangle|1_{R_3}\rangle, |1_{L_1}\rangle|1_{R_2}\rangle|1_{L_3}\rangle, |1_{L_1}\rangle|1_{R_2}\rangle|1_{R_3}\rangle,\\ &|1_{R_1}\rangle|1_{L_2}\rangle|1_{L_3}\rangle, |1_{R_1}\rangle|1_{L_2}\rangle|1_{R_3}\rangle, |1_{R_1}\rangle|1_{R_2}\rangle|1_{L_3}\rangle, |1_{R_1}\rangle|1_{R_2}\rangle|1_{R_3}\rangle\}.\end{aligned} \tag{11}$$

The bits corresponding to the states can be, for example, $|1_{D_1}\rangle$: 0, $|1_{A_1}\rangle$: 1, $|1_{L_1}\rangle$: 0, and $|1_{R_1}\rangle$: 1. Note that, with one photon, we would need a space with eight optical modes. If we use an additional photon (four photons), we would obtain sixteen product states (with one photon, we would need a space with sixteen optical modes) and so on.

Figure 1 shows an HD-DV-QKD system for polarization qubits. First of all, Alice uses N SPDC sources to generate a pair of photons for each mode: one of them will be used as a signal and the other one as a heralding photon to obtain N-qubits by detecting coincidences. After this, using an electrooptical devices, Alice chooses a state for each signal photon, with all of them in the same basis, for example, X or Y. The photons are coupled to SMFs, and by means of a fan-in (FI), are coupled to an MCF. The quantum states travel along the MCF to Bob system where, by using a fan-out (FO), the photons are coupled to N single-core fibers in Bob's system. Finally, in Bob's quantum projective measurement system, the same base is selected with an electrooptical device. Finally, the quantum states are measured using a polarization beam splitter (PBS) for each qubit.

It is worth noting that these N-qubits (N cores or SMFs) require N polarization compensation systems and none are required for phase compensation. The corresponding 1-qudit protocol could be implemented by using 2^{N-1} cores; therefore, it requires 2^{N-1} polarization compensation systems and $(2^{N-1}-1)$ phase compensation systems—in other

words, the technological complexity with a single photon scales exponentially. For example, for 4-qubits we need four polarization compensation systems and none for phase compensation, but the corresponding 1-qudit (same dimension, $\mathcal{N} = d = 16$) requires eight polarization compensation systems and seven phase compensation systems.

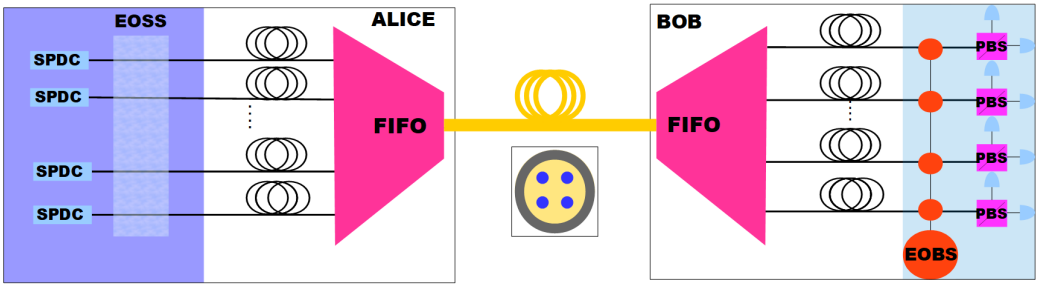

Figure 1. A HD-QKD system for N-qubits with Alice and Bob connected by a MCF. List of elements from left to right: SPDC sources, Electrooptical States Selector (EOSS), SMFs, an MCF between a fan-in and a fan-out (FIFO), an Electrooptical Base Selector (EOBS), and PBSs to perform projective measurements.

3.2. Product States with N-Qudits with Spatial and Polarization Modes

We present a case of N-qudits with N-ququarts states. Although 1-ququart requires one phase compensation system, it is obvious that N-ququarts notably increase the dimension, and therefore the security, without increasing the technological complexity. For example, 2-ququarts (where we only use two photons) would require four polarization compensation systems and two phase compensation systems; however, the corresponding 1-qudit requires, as commented above, eight and seven systems, respectively.

The ququarts states $|L\rangle$ are generated by using two spatial modes, 1 and 2 (two non-coupled cores of an MCF, or two SMFs), and the polarization modes H and V, that is, they are obtained through the following quantum superposition:

$$|L\rangle = c_{H_1}|1_{H_1}\rangle + c_{V_1}|1_{V_1}\rangle + c_{H_2}|1_{H_2}\rangle + c_{V_2}|1_{V_2}\rangle, \tag{12}$$

where the coefficients are the vectors of the two MUBs. For example, the above diagonal and circular polarization basis can be used to obtain two MUBs for 1-ququarts, that is,

$$\mathrm{X}_{12} \rightarrow \left\{ |1_{\pm D}\rangle = \frac{1}{\sqrt{2}}(|1_{D_1}\rangle \pm |1_{D_2}\rangle),\ \ |1_{\pm A}\rangle = \frac{1}{\sqrt{2}}(|1_{A_1}\rangle \pm |1_{A_2}\rangle)\right\}, \tag{13}$$

$$\mathrm{Y}_{12} \rightarrow \{ |1_{\pm L}\rangle = \frac{1}{\sqrt{2}}(|1_{L_1}\rangle \pm i|1_{L_2}\rangle),\ \ |1_{\pm R}\rangle = \frac{1}{\sqrt{2}}(|1_{R_1}\rangle \pm i|1_{R_2}\rangle)\Big\}. \tag{14}$$

If we have a second photon, then we need a second pair of spatial mode cores of MCF or SMFs 3 and 4, and so on for N-ququarts. The states in each pair of modes are again given by Equation (14). Examples of states of 2-ququarts of the first and second pairs of modes would be $|1_{+D}\rangle|1_{+D}\rangle$, $|1_{+D}\rangle|1_{-D}\rangle$, $|1_{+D}\rangle|1_{+A}\rangle$, $|1_{+D}\rangle|1_{-A}\rangle$, and so on, up to sixteen states. This can be implemented by using an MCF with four cores (two cores for each photon). A similar procedure can be followed for 3-ququarts, that is, sixty-four states. The large dimension that can be achieved is clear. Note that with a single photon we would need to use and manipulate quantum superposition states excited in sixteen or sixty-four optical modes, respectively, to achieve the same QKD dimension.

3.3. Product States with N-Qudits with Spatial and Other Optical Modes

For the sake of completeness, we present the possible use of other degrees of freedom for a single photon, that is, for other optical modes to implement N-qudits; however, we must emphasize that, in general, this will incur greater technological difficulties due to modal coupling, that is, some kind of modal coupling compensation system would be necessary. For example, we could use the modes of a few-modes optical fiber (FMF) [25], that is, with different Linear Optical Moment (LOM), or even to consider a MCF optical fiber where each core is a few-mode optical core, with LOMs $\{\hbar\beta_1, \ldots, \hbar\beta_d\}$, where $\{\beta_1, \ldots, \beta_d\}$ are the mode propagation constants. Likewise, we could consider an optical fiber with a few modes with different Orbital Angular Momentum (OAM). In fact, recent applications to QKD with one photon have been presented [26,27], and thus we could use an MCF to obtain N-qudits, where each core has a few modes with a different OAM, that is, with OAMs $\{-\hbar l, \ldots, 0, \ldots, +\hbar l\}$, where $d = 2l + 1$. A single example would be N optical fibers (or cores), with the first three modes containing OAMs $-1, 0, +1$; then, we will obtain N-qutrits, and therefore dimension $\mathcal{N} = 3^N$. The use of these 1-qudits to implement N-qudits for QKD is related to the robustness of these states before perturbations producing modal coupling and random phase changes. It is important to emphasize the possibility of using polarization maintenance optical fibers [28] because this can sometimes lead to certain technological advantages (polarization compensation would not be needed).

4. Study of Secure Key Rates

In this section, a detailed study is presented of secure key rates with the proposed protocol. We will focus our study on the product states of N-qubits and N-ququarts, although more general N-qudits could also be considered.

Obviously, qudits with $d > 4$ could be also considered qubits and ququarts provide sufficient possibilities of implementing HD-QKD. In order to evaluate the security properties of the protocol with product states, we will assume the following realistic scenario: an eavesdropper attack under imperfect channel with both losses and optical perturbations, which produce unpredictable polarization coupling and phase changes. We also assume the existence of phase and polarization compensation systems, which greatly reduce these random perturbations but do not fully eliminate them. Next, we will model the QBER model, including the aforementioned optical perturbations and Eve's presence under an intercept and resend attack. Finally, we present secure key rates with losses, that is, we will take into account the fact that quantum states can suffer from photon losses and we present new secure key rate curves under an intercept–resend attack. In particular, we prove that secure key rates are notably improved by using detections of N'(<N)-qudits, that is, employing additional detections where some photons are lost due to fiber losses.

4.1. Optical Perturbations Model

A model of optical perturbations is needed to calculate the perturbation error for N-qudits, specifically the product of N-qubits and N-ququarts states. We calculate the effect of polarization modal coupling and phase perturbations, that is, the changes in a quantum state that experiences such perturbations under propagation along optical fibers.

Let us consider a polarization 1-qubit state propagating through a core j of a multicore optical fiber (or a single-mode optical fiber j), such as an initial state $|1_{D_j}\rangle$, as shown by Equation (8), which is excited in a linear polarization diagonal mode (D_j). This becomes the following perturbated state: $|1_{D_j}\rangle_p = \cos\theta_j|1_{D_j}\rangle + \sin\theta_j e^{i\gamma_j}|1_{A_j}\rangle$. This occurs due to polarization modal coupling, described by θ_j, between diagonal (D) and anti-diagonal (A) linear modes, and phase perturbations described by γ_j. From now on, we assume statistical independence in θ_j and γ_j, and the same statistical behaviour in all cores; then, we choose

$\theta_j = \theta$ and $\gamma_j = \gamma$. Therefore, the probability of remaining in the initial state for an N-qubit state is given by

$$P_{|1_{D_1}\ldots 1_{D_N}\rangle} = \langle 1_{D_1}\ldots 1_{D_N}|1_{D_1}\ldots 1_{D_N}\rangle_p =< \cos^2\theta >^N, \tag{15}$$

where $<>$ represents an statistical average over the posible values of θ. Note that Equation (15) does not depend on the phase perturbation pertubation γ.

Analogously, let us consider 1-ququart $|1_{+D_{j,j'}}\rangle = (1/\sqrt{2})(|1_{D_j}\rangle + |1_{D_{j'}}\rangle)$ excited in the pair of cores j and j', which then, under perturbation, reaches the following perturbated state $|1_{+D_{j,j'}}\rangle_p = cos\theta_j|1_{D_j}\rangle + \sin\theta_j e^{i\gamma_j}|1_{A_j}\rangle + e^{i\varphi_j}(\cos\theta_{j'}|1_{D_{j'}}\rangle + \sin\theta_{j'}e^{i\gamma_{j'}}|1_{A_{j'}}\rangle)$. By assuming statistical independence in $\theta_{j(j')}$, $\gamma_{j(j')}$ and φ_j, and the same statistical behaviour ($\varphi_j = \varphi$), it can be easily observed that the probability of an initial N-ququart state $|1_{+D_{1,1'}}\ldots 1_{+D_{N,N'}}\rangle$ remaining unperturbed is given by

$$P_{|1_{+D_{1,1'}}\ldots 1_{+D_{N,N'}}\rangle} = \langle 1_{+D_{1,1'}}\ldots 1_{+D_{N,N'}}|1_{+D_{1,1'}}\ldots 1_{+D_{N,N'}}\rangle_p =$$

$$=< \cos^2\theta >^N \frac{< 1+\cos\varphi >^N}{2^N}. \tag{16}$$

Next, we calculate the statistical average of the previously obtained functions, that is, $< \cos^2\theta >$ and $< 1+\cos\varphi >$ in Equations (15) and (16), over normalized Gaussian probability densities of variances $\alpha_c L$ (polarization modal coupling) and $\alpha_p L$ (phase), respectively, where L is the length and α_c and α_c are the coefficients that characterize the strength of the residual (non-compensated) perturbations.Therefore, we write

$$< \cos^2\theta >= \int_{-\infty}^{\infty} \cos^2\theta \frac{1}{\sqrt{\pi\alpha_c L}} e^{-\frac{\theta^2}{\alpha_c L}} d\theta = \frac{1+e^{-\alpha_c L}}{2}, \tag{17}$$

$$\frac{< 1+\cos\varphi >}{2} = \frac{1}{2}\int_{-\infty}^{\infty} (1+\cos\varphi)\frac{1}{\sqrt{\pi\alpha_p L}} e^{-\frac{\varphi^2}{\alpha_p L}} d\varphi = \frac{1+e^{-\frac{1}{4}\alpha_p L}}{2}, \tag{18}$$

where we use the interval $(-\infty, \infty)$ because we assume that θ and φ can take values over the entire real line (unwrapped angles), although in our case, this is also justified due to the small variances obtained under the compensation methods of these perturbations. Finally, for N-qubits and N-ququarts, we obtain

$$P_{Nqb} = P_{|1_{1D}\ldots 1_{ND}\rangle} = \left(\frac{1+e^{-\alpha_c L}}{2}\right)^N, \tag{19}$$

$$P_{Nqq} = P_{|1_{D_{1,1'}}\ldots 1_{D_{N,N'}}\rangle} = \left(\frac{1+e^{-\alpha_c L}}{2}\right)^N \left(\frac{1+e^{-\frac{1}{4}\alpha_p L}}{2}\right)^N. \tag{20}$$

Note that the probabilities given by Equation (20) strongly depend on α_c and α_p; therefore, N-qubits would be more easily implemented in practical systems because they only undergo the polarization coupling pertubation—that is, only polarization compensation systems would be needed. In the case of 1-ququarts, they also undergo phase perturbations, and if a phase compensation system is used, then high-dimensional N-ququarts protocols with a high performance could also be implemented. As commented, from a technological point of view, the use of 1-qudits with $d \geq 4$ would experience greater implementation difficulties due to the fragility of these states to optical phase perturbations.

Finally, we must stress that the values of α_c and α_p without compensation are very high; when compensation systems are used, we can assume the same expression for the probabilities of their remaining in the initial states but with effective coefficients $\tilde{\alpha}_c$ and $\tilde{\alpha}_p$ in Equation (19) and Equation (20), respectively.

4.2. QBER with Perturbations

In order to calculate the QBER, we have to take into account the sources of errors due to Eve's attack and the aforementioned optical perturbations. The first can be written as ae_E, where a is the fraction of attack, that is, the rate of bits intercepted by Eve, and e_E is Eve's QBER. It is known that intercept–resend attack is the most direct QKD attack. We use this attack to describe the security properties of the QKD protocol with product states. As usual, Eve has to choose a measurement basis and, because she makes a wrong choice, the QBER is given by Equation (3): $e_E = (d^N - 1)/2d^N$.

Next, we will calculate Bob's QBER e_B equations for N-qbits and N-ququarts. If we consider errors due to optical perturbations e_p, then we can define an error $e_B = A + BP'$, with $P' = P'_{Nqb} = 1 - P_{Nqb}$ if we send qubit states or $P' = P'_{Nqq} = 1 - P_{Nqq}$ for ququarts. This represents the probability of receiving a mistaken bit due to perturbations. A and B are constants that are determined by boundary conditions $e_B(L = 0) = ae_E$, where $e_E = (\mathcal{N} - 1)/2\mathcal{N}$ is the error due to Eve's attack, and $e_B(L = \infty) = (\mathcal{N} - 1)/\mathcal{N}$; therefore, we obtain the following expressions for coefficients A and B:

$$A = ae_E, \quad B = 1 - \frac{\mathcal{N}}{\mathcal{N} - 1}(ae_E). \tag{21}$$

Note that for qubits, $\mathcal{N} = 2^N$, and for ququarts, $\mathcal{N} = 4^N$. Using this result, we write down the expressions for Bob's QBER:

$$\textit{Qubits}$$
$$e_B = ae_E + (1 - \tfrac{\mathcal{N}}{\mathcal{N}-1}\, ae_E)(1 - (\frac{1 + e^{-\alpha_c L}}{2})^N), \tag{22}$$

$$\textit{Ququarts}$$
$$e_B = ae_E + (1 - \tfrac{\mathcal{N}}{\mathcal{N}-1}\, ae_E)(1 - (\frac{1 + e^{-\alpha_c L}}{2})^N (\frac{1 + e^{-\frac{1}{4}\alpha_p L}}{2})^N). \tag{23}$$

For illustrative purpose, we will choose, if compensation is used, the following value for modal coupling, $\tilde{\alpha}_c \approx 5 \cdot 10^{-4}$ km^{-1}; in fact, when polarization compensation techniques are applied, then values quite close to this value can be inferred [29–31]. On the other hand, a very optimistic value for the phase dispersion (without compensation) is given by $\alpha_p = 5 \cdot 10^{-2}$ km^{-1}, although it is only valid for a short period of a few minutes [32]. Moreover, under phase compensation, the coefficient $\tilde{\alpha}_p$ has values equal to several times $\tilde{\alpha}_c$ because of the larger technological difficulties in compensating for phase perturbations; specifically, we take $\tilde{\alpha}_p \approx 4 \cdot 10^{-3}$ km^{-1} [33], that is, $\tilde{\alpha}_p \approx 8\tilde{\alpha}_c$, and therefore both perturbations provide similar statistical properties.

4.3. Secure Key Rate with $N'(\leq N)$-Qudits Under Attack in Line

As commented, we will consider that Eve is present and that the channel has an optical attenuation (attenuation coefficient $\alpha_{att} \approx 0.15$ dB km^{-1}). The secure key rate R, obtained using N-qudits, can be calculated by taking into account the GLLP security analysis [34], and therefore using the mutual information I_{AB} between A and B with $\mathcal{N} = d^N$ states, where the information lost during error correction is $f\, H(x)$, with $H(x)$ being the Shannon entropy, x the total QBER, and f the reconciliation efficiency. Therefore, under a fraction of attack a, rate R can be written as follows:

$$R_{(d,N)}(\mathcal{N}) = I_{AB} - f\, H(e_B) - I_{AE}(e_E) =$$
$$= \frac{1}{2}\big(\log_2(\mathcal{N}) + f\big[(1 - e_B)\log_2(1 - e_B) + e_B \log_2(\frac{e_B}{\mathcal{N} - 1})\big] - a\frac{\log_2(\mathcal{N})}{2}\big) \tag{24}$$

where the second term term on the right side represents the information loss by Bob due to channel error and the presence of Eve, and the third term is the mutual information I_{AE} [35] multiplied by the attack fraction a, where, as usual, it is assumed that Eve has all the technology needed to eliminate classical errors. From now on, we will use an acceptable value $f \approx 1.15$ [36].

As commented above, we have to consider the possible lost photons, which were therefore not detected by Bob, which means that despite the channel losses, the remaining photons, that is, the remaining qudits of lower $N' < N$ dimensions, can still be employed to produce a secret key. Using the probabilities given in Section 2, we can weigh the secret key rates given by Equation (24) according to the number of lost photons: $0, 1, \ldots, N-1$, that is, $R'_{(d,N)}(d^N) = P_{(N)} R_{(d,N)}(d^N)$, $R'_{(d,N-1)}(d^{N-1}) = P_{(N-1)} R_{(d,N-1)}(d^{N-1}), \ldots, R'_{(d,2)}(d) = P_{(2)} R_{(d,2)}(d^2)$, $R'_{(d,1)}(d) = P_{(1)} R_{(d,1)}(d)$. Consequently, the total secure key rate $R'_{dT}(d^N)$ is the sum of these ponderated secure key rates, that is,

$$R'_{dT}(d^N = \mathcal{N}) = R'_{(d,N)}(d^N) + R'_{(d,N-1)}(d^{N-1}) + \ldots + R'_{(d,2)}(d^2) + R'_{(d,1)}(d). \tag{25}$$

Next we present a detailed analysis without and with an attack for some N-qudits with a certain practical interest.We calculate, for the purpose of illustration, examples of secure key rates for the case of 1-, 2-, and 3-qubits (dimensions $\mathcal{N} = 2, 4, 8$), that is, $R'_{2T}(\mathcal{N})$, and 1-ququart (dimension $\mathcal{N} = 4$), that is, $R'_{4T}(\mathcal{N})$. The ponderated sums of these secure keys rates are given by the following expressions for 1-qubit, 2-qubits, and 3-qubits:

$$R'_{2T}(2) = P R_{2,1}(2), \quad R'_{2T}(4) = P^2 R_{(2,2)}(4) + 2P(1-P) R_{(2,1)}(2),$$

$$R'_{2T}(8) = P^3 R_{2,3}(8) + 3P^2(1-P) R_{(2,2)}(4) + 3P(1-P)^2 R_{(2,1)}(2) \tag{26}$$

and the following expression is used for the total secure key rate when 1-ququart, 2-ququarts, and 3-ququarts are used:

$$R'_{4T}(4) = P R_{(4,1)}(4), \quad R'_{4T}(16) = P^2 R_{(4,2)}(16) + (2P(1-P)) R_{(4,1)}(4)$$

$$R'_{4T}(64) = P^3 R_{(4,3)}(64) + (3P^2(1-P)) R_{(4,2)}(16) + (3P(1-P)^2) R_{(4,1)}(4) \tag{27}$$

Note, for example, that the total secure key rate $R'_{2T}(8)$ for 3-qubits consists of the weighted contribution of the secure key rates from a tri-photon channel, three bi-photon channels, and another three single-photon channels, which is equivalent to detecting one triple coincidence (tri-photon channel), three double coincidences (bi-photon channels), and three single detections (single-photon channels). Analogously, similar considerations can be made for the remaining cases. On the other hand, we must note that the losses in the optical fiber give rise to a small amount of N photon coincidences, which suggests that such coincidences could be used to check whether Eve is tapping. The main argument is that although the N photons coincidences are very unlikely in longer distances, and therefore their contribution to the total secure key is very small, they can be used to quickly detect the presence of Eve because of their greater contribution to Bob's quantum bit error rate (QBER), which increases with dimension. Moreover, dimensionality implies a longer distance is reached and secure key is gained for the protocol.

4.4. Results Without Phase Compensation

Next we present numerical results for QBERs and SKRs. First of all, let us consider the case of 2-qubits and 1-ququart, that is, a protocol of dimension $\mathcal{N} = 4$, with only polarization compensation in both cases. As noted above, we will use $\tilde{\alpha}_c = 5 \cdot 10^{-4}$ km^{-1}

(under polarization compensation), and an optimistic value for the non-compensated phase perturbation in the case of 1-ququart, that is, $\alpha_p = 5 \cdot 10^{-2}$ km^{-1}.

We start by comparing two SKR curves vs. L for 2-qubits and 1-ququart for an attack rate of $a = 0.55$ and an attenuation coefficient $\alpha = 0.15$ dB km^{-1}. The curves are shown in Figure 2 and correspond to the SKR functions $R'_{2T}(4)$ for 2-qubits, given in Equation (26), and $R'_{4T}(4)$ for 1-ququart, given by Equation (27). It is very clear that the 1-ququart protocol is completely inefficient; however, 2-qubit presents an excellent key rate without using phase compensation. In the inset, the QBER is presented, with the distance for both cases; it is also clear that when phase is not compensated, the QBER is very high, and in the case of 2-qubits, the QBER is low because it is non sensitive to phase perturbations. Obviously, these results would be much more pronounced if we compared 3-qubits with a 1-qudit $d = 8$ (with only polarization compensation), because the phase perturbations would be increased; in fact, it would be necessary to compensate three relative phases of this 1-qudit.

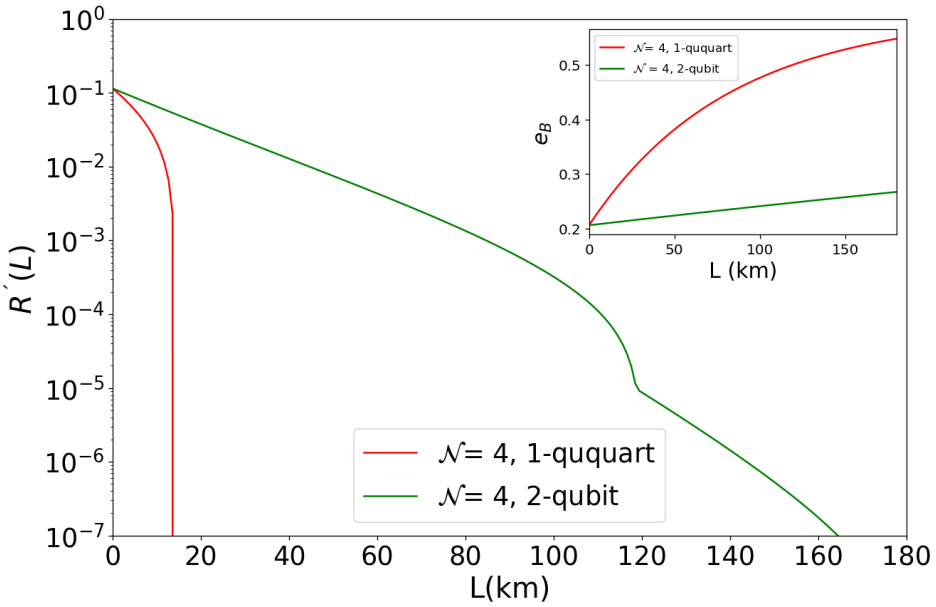

Figure 2. Semilog SKR curves vs. L (km) for 2-qubits and 1-ququart. Parameters: $\alpha = 0.15$ dB km^{-1}; $\tilde{\alpha}_c = 5 \cdot 10^{-4}$ km^{-1}; $\alpha_p = 5 \cdot 10^{-2}$ km^{-1} (for 1-ququart) and $a = 0.55$. QBERs (e_B) are shown in inset.

In Figure 3, we present the results for QBERs and SKRs for 1-, 2-, and 3-qubits. For comparison purposes, we also present one (1-qubit), two, and three channels, since they are also insensitive to phase perturbations; note that the use of one channel or several independent channels would correspond to the standard high-dimensional protocol with one photon in each channel and several degrees of freedom.

Note that 2- and 3-qubits increase SKR and security (see QBERs), as expected. It is also interesting to note that a simple inspection shows that several independent single-photon channels provide lower secure key rates, that is, $2R(2) < R(4)$, $3R(2) < R(8)$ for qubits, and moreover, much less security. Finally, the SKRs sums the results in the small downward spikes in higher-dimension curves; these are located at the distances at which multiple-photon coincidences become less probable than coincidences with a lower number of photons.

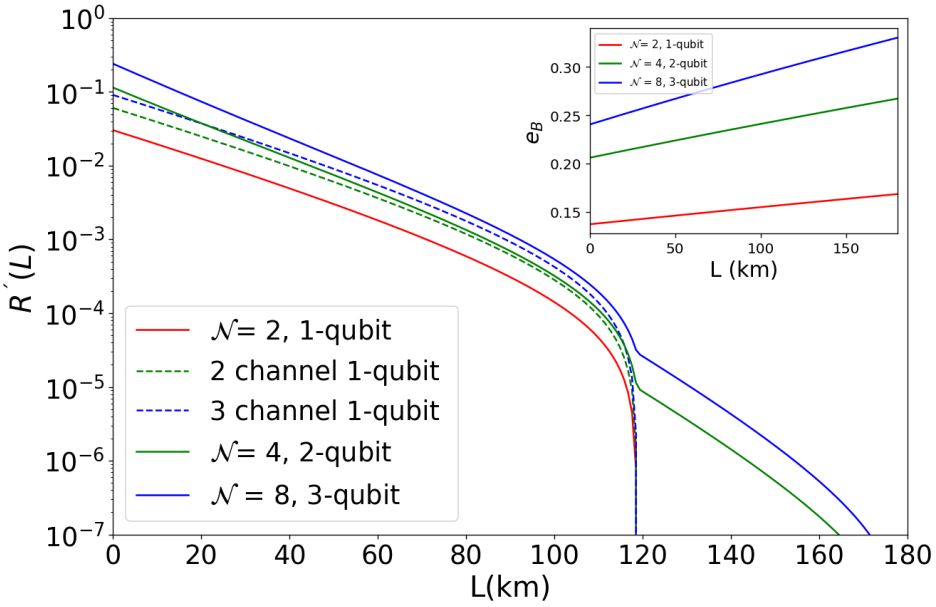

Figure 3. Semilog SKR curves vs. L (km) for 1-, 2-, and 3-qubits (solid lines) and 1-, 2-, and three 1-qubit channels (dashed lines). Parameters: $\alpha = 0.15$ dB km^{-1}; $\tilde{\alpha}_c = 5 \cdot 10^{-4}$ km^{-1}; and $a = 0.55$. Likewise, SKR for one (1-qubit), two, and three channels is shown for comparison purposes. QBERs (e_B) are also presented in the inset.

4.5. Results with Phase Compensation

Finally, we present, in Figure 4, the results for SKR and QBER with phase compensation, specifically, for 1-, 2-, and 3-ququarts. Again, we obtain that several single-photon channels (dashed lines) provide lower secure key rates than 1-, 2-, and 3-ququarts (solid lines), that is, $2R(4) < R(16)$, $3R(4) < R(64)$. Likewise, higher QBERs, along with higher SKRs, are obtained, that is, a greater security key rate and a very high security is obtained; moreover, SKRs sum results once more in the small downward spikes in higher-dimension curves; such spikes are located where multiple-photon coincidences become less probable, that is, when one photon is lost.

However, remember that although phase compensation technology is required, its complexity is remarkably reduced; indeed, 3-ququarts ($\mathcal{N} = 64$) require six polarization compensation systems and three phase compensation systems, while the corresponding 1-qudit with $d = \mathcal{N} = 64$ requires thirty-two polarization compensation systems and thirty-one phase compensation systems. Finally, it is worth comparing the 2-qubit SKR curve shown in Figure 3, which uses only polarization compensation, with the 1-ququart SKR curve shown in Figure 4, which uses both polarization and phase compensation; we note that 2-qubits provide similar or even better results than a phase-compensated 1-ququart. We must stress that both the 1-qubit, or several channels of 1qubit, and 1-ququart, or several channels of 1-ququart, show results of the same order as the standard ones with phase compensation [8,9,30,33,37]; therefore, we can conclude that protocols with N-qudits will provide better SKRs and QBERs without the complex technological requirements of phase compensation.

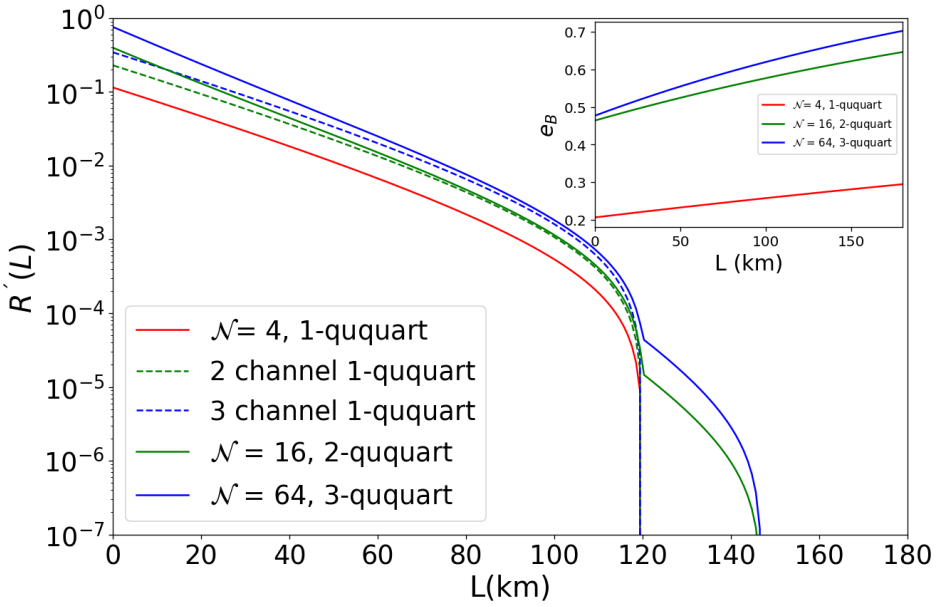

Figure 4. Semilog SKR curves vs. L (km) for 1-, 2-, and 3-ququarts (solid lines) and 1-, 2-, and three 1-ququart channels (dashed lines). Parameters: $\alpha = 0.15$ dB km^{-1}, $\tilde{\alpha}_c = 5 \cdot 10^{-4}$ km^{-1}; $\tilde{\alpha}_p = 4 \cdot 10^{-3}$ km^{-1}; and $a = 0.55$. Likewise, SKR for one (1-ququart), two, and three channels is shown for comparison purposes. QBERs (e_B) are also presented in the inset.

5. Discussion

In this work, a high-dimensional discrete variable QKD protocol based on product states was proposed, using N-qudits states formed by the product state of N photons, each of them in a 1-qudit state. The results for N-qubits and N-ququarts were presented and analysed. The QKD state measurements combine projective measurements with photon coincidences, although such coincidences would not be strictly necessary. Since losses are considered, we obtain a total secure key rate as the weighted sum of secure key rates for $N'(\leq N)$-qudits ($N' = N, N-1, \ldots, 1$). Moreover, the states with a maximum number of N photons, that is, the least probable states, could be used to check the security of the quantum channel. For the two types of product states that were analysed in detail, that is, N-qubits and N-ququarts, the results show that security key rates improve notably when compared to the use of N single-photon channels. Furthermore the main advantage of using N-qudits is that we can use modal configurations where a exponential reduction in the phase compensation technological complexity is obtained; this reduction is the maximum possible when N-qubits of polarization are used to implement high-dimensional QKD. Additionally, if phase compensation is used, then the high-dimensional results with several photons are scaled exponentially.

Author Contributions: Conceptualization, J.L., X.P.-B. and A.V.-M.; methodology, J.L., X.P.-B. and A.V.-M.; validation, J.L., X.P.-B. and A.V.-M.; formal analysis, J.L., X.P.-B. and A.V.-M.; investigation, J.L., X.P.-B. and A.V.-M.; writing—original draft preparation, J.L., X.P.-B. and A.V.-M.; writing—review and editing, J.L., X.P.-B. and A.V.-M.; supervision, J.L. and X.P.-B.; project administration, J.L. and X.P.-B.; funding acquisition, J.L. and X.P.-B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the MICIN, European Union NextGenerationEU under Grant PRTR-C17.I1, and in part by the Galician Regional Government through Planes Complementarios de I+D+I con las Comunidades Autónomas in Quantum Communication. It was also funded by MCIU/AEI/10.13039/501100011033/FEDER, UE under project PID2023-152607NB-I00.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

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

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distribution
DV	Discrete variable
CV	Continuous variable
DV-QKD	Discrete-variable quantum key distribution
CV-QKD	Continuous-variable quantum key distribution
BB84	Bennet–Brassard 1984 protocol
B92	Bennet 1992 protocol
BBM92	Bennet–Brassard–Mermin 1992 protocol
MDI-QKD	Measurement-device-independent quantum key distribution
GHZ	Greenberger–Horne–Zeilinger state
LOM	Linear optical momentum
FMF	Few-modes optical fibers
MCF	Multicore optical fibers
OAM	Orbital angular momentum
HD	High-dimensional
HD-DV-QKD	High-dimensional discrete-variable quantum key distribution
SPDC	Spontaneous parametric down-conversion
SFWM	Spontaneous four-wave mixing
MUB	Mutually unbiased bases
QBER	Quantum bit error rate
SMF	Single-mode fibers
PL	Photonic lantern
EOSS	Electrooptical state selector
EOBS	Electrooptical basis selector
PBS	Polarization beam-splitter
GLLP	Gottesman–Lo–Lutkenhaus–Preskill

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
2. 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. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
3. Zhang, H.; Zhu, H.; He, R.; Zhang, Y.; Ding, C.; Hanzo, L.; Gao, W. Towards global quantum key distribution. *Nat. Rev. Electr. Eng.* **2025**, *2*, 806–818. [CrossRef]
4. Bennet, 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*; IEEE: New York, NY, USA, 1984; pp. 175–179.
5. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef]
6. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef]
7. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
8. Cañas, G.; Vera, N.; Cariñe, J.; González, P.; Cardenas, J.; Connolly, P.W.R.; Przysiezna, A.; Gómez, E.S.; Figueroa, M.; Vallone, G.; et al. High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. *Phys. Rev. A* **2017**, *96*, 022317. [CrossRef]
9. Ding, Y.; Bacco, D.; Dalgaard, K.; Cai, X.; Zhou, X.; Rottwitt, K.; Oxenlowe, L. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf.* **2017**, *3*, 25. [CrossRef]

10. Balado, D.; Liñares, J.; Prieto-Blanco, X.; Barral, D. Phase and polarization autocompensating N-dimensional quantum cryptography in multicore optical fibers. *J. Opt. Soc. Am. B* **2019**, *36*, 2793–2803. [CrossRef]
11. Zheng, X.T.; Zhang, Q.F.; Ling, J.; Guo, G.C.; Han, Z.F. Free-space continuous-variable quantum key distribution under high background noise. *npj Quantum Inf.* **2025**, *11*, 52. [CrossRef]
12. Xu, F.; Qi, B.; Liao, Z.; Lo, H.K. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Appl. Phys. Lett.* **2013**, *103*, 061101. [CrossRef]
13. Hua, X.; Hu, M.; Guo, B. Multi-User Measurement-Device-Independent Quantum Key Distribution Based on GHZ Entangled State. *Entropy* **2022**, *24*, 841. [CrossRef]
14. Huang, H.; Milione, G.; Lavery, M.P.J.; Xie, G.; Ren, Y.; Cao, Y.; Ahmed, N.; An Nguyen, T.; Nolan, D.A.; Li, M.J.; et al. Mode division multiplexing using an orbital angular momentum mode sorter and MIMO-DSP over a graded-index few-mode optical fibre. *Sci. Rep.* **2015**, *5*, 14931. [CrossRef]
15. Vázquez-Martínez, A.; Prieto-Blanco, X.; Mateo, E.; Liñares, J. High-dimensional autocompensating discrete modulation CV-QKD protocol in optical fibers. *arXiv* **2025**, arXiv:2508.10442.
16. Collins, M.J.; Xiong, C.; Rey, I.H.; Vo, T.D.; He, J.; Shahnia, S.; Reardon, C.; Krauss, T.F.; Steel, M.J.; Clark, A.S.; et al. Integrated spatial multiplexing of heralded single-photon sources. *Nat. Commun.* **2013**, *4*, 2582. [CrossRef]
17. Koefoed, J.G.; Friis, S.M.M.; Christensen, J.B.; Rottwitt, K. Spectrally pure heralded single photons by spontaneous four-wave mixing in a fiber: Reducing impact of dispersion fluctuations. *Opt. Express* **2017**, *25*, 20835–20849. [CrossRef]
18. Münzberg, J.; Draxl, F.; Covre da Silva, S.F.; Karli, Y.; Manna, S.; Rastelli, A.; Weihs, G.; Keil, R. Fast and efficient demultiplexing of single photons from a quantum dot with resonantly enhanced electro-optic modulators. *APL Photonics* **2022**, *7*, 070802. [CrossRef]
19. Cao, H.; Hansen, L.M.; Giorgino, F.; Carosini, L.; Zahálka, P.; Zilk, F.; Loredo, J.C.; Walther, P. Photonic Source of Heralded Greenberger-Horne-Zeilinger States. *Phys. Rev. Lett.* **2024**, *132*, 130604. [CrossRef]
20. Hasegawa, T.; Tamura, Y.; Sakuma, H.; Kawaguchi, Y.; Yamamoto, Y.; Koyano, Y. The first 0.14-dB/km ultra-low loss optical fiber. *SEI Tech. Rev.* **2018**, *86*, 18–22.
21. Petrovich, M.; Fokoua, E.; Chen, Y.; Sakr, H.; Adamu, A.; Hassan, R.; Wu, D.; Ando, R.; Papadimopoulos, A.; Sandoghchi, S.; et al. Broadband optical fibre with an attenuation lower than 0.1 decibel per kilometre. *Nat. Photonics* **2025**, *19*, 1203–1208. [CrossRef]
22. Chen, W.; Han, Z.; Mo, X.; Xu, F.; Wei, G.; Guo, G. Active phase compensation of quantum key distribution system. *Chin. Sci. Bull.* **2008**, *53*, 1310–1314. [CrossRef]
23. Yuan, Z.; Shields, A. One-way quantum key distribution system with active phase compensation. In *Proceedings of the 2005 European Quantum Electronics Conference, Munich, Germany, 12–17 June 2005*; IEEE: New York, NY, USA, 2005; p. 306. [CrossRef]
24. Bethune, D.S.; Risk, W.P. Autocompensating quantum cryptography. *New J. Phys.* **2002**, *4*, 42. [CrossRef]
25. Sillard, P.; Bigot-Astruc, M.; Molin, D. Few-Mode Fibers for Mode-Division-Multiplexed Systems. *J. Light. Technol.* **2014**, *32*, 2824–2829. [CrossRef]
26. Wang, J.; Zhang, X. Orbital Angular Momentum in Fibers. *J. Lightwave Technol.* **2023**, *41*, 1934–1962. [CrossRef]
27. Li, J.; Wang, X.; Yu, H.; Tang, J.; Liu, Y.; Cao, Y.; Deng, Z.; Wu, D.; Hu, H.; Wang, Y.; et al. State-dependent misalignment and turbulence effects on high-dimensional quantum key distribution with orbital angular momentum. *New J. Phys.* **2024**, *26*, 053034. [CrossRef]
28. Fu, S.; Wang, Y.; Cui, J.; Mo, Q.; Chen, X.; Chen, B.; Tang, M.; Liu, D. Panda Type Few-Mode Fiber Capable of Both Mode Profile and Polarization Maintenance. *J. Light. Technol.* **2018**, *36*, 5780–5785. [CrossRef]
29. Liñares, J.; Prieto-Blanco, X.; Balado, D.; Carral, G.M. Fully autocompensating high-dimensional quantum cryptography by quantum degenerate four-wave mixing. *Phys. Rev. A* **2021**, *103*, 043710. [CrossRef]
30. Chen, J.; Wu, G.; Li, Y.; Wu, E.; Zeng, H. Active polarization stabilization in optical fibers suitable for quantum key distribution. *Opt. Express* **2007**, *15*, 17928–17936. [CrossRef] [PubMed]
31. Park, S.; Baek, J.; Lee, M.H.; Lee, S.; Moon, G. Long-term polarization stabilization of a polarization maintaining fiber via dynamic temperature control. *Curr. Appl. Phys.* **2025**, *72*, 51–55. [CrossRef]
32. Mazur, M.; Fontaine, N.K.; Ryf, R.; Dallachiesa, L.; Chen, H.; Neilson, D.T.; Marotta, A.; Hayashi, T.; Nagashima, T.; Nakanishi, T.; et al. Characterization of phase stability and core-to-core delays in a field-deployed uncoupled-core multi-core fiber cable. In *Proceedings of the 49th European Conference on Optical Communications (ECOC 2023)*; IET: Stevenage, UK, 2023; Volume 2023, pp. 952–955. [CrossRef]
33. Minář, J.; de Riedmatten, H.; Simon, C.; Zbinden, H.; Gisin, N. Phase-noise measurements in long-fiber interferometers for quantum-repeater applications. *Phys. Rev. A* **2008**, *77*, 052325. [CrossRef]
34. Gottesman, D.; Lo, H.K.; Lutkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. In *Proceedings of the International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*; IEEE: New York, NY, USA, 2004; p. 136. [CrossRef]
35. Bourennane, M.; Karlsson, A.; Björk, G.; Gisin, N.; Cerf, N.J. Quantum key distribution using multilevel encoding: Security analysis. *J. Phys. A Math. Gen.* **2002**, *35*, 10065. [CrossRef]

36. Elkouss, D.; Martinez-Mateo, J.; Martin, V. Information reconciliation for quantum key distribution. *Quantum Inf. Comput.* **2011**, *11*, 226–238.
37. Zhang, Y.; Zhao, H.; Wu, T.; Gao, Z.; Ge, L.; Feng, L. High-Dimensional Quantum Key Distribution by a Spin-Orbit Microlaser. *Phys. Rev. X* **2025**, *15*, 011024. [CrossRef]