entropy

MDPI

Article

High-Dimensional and Multi-Intensity One-Photon-Interference Quantum Secure Direct Communication

Yu-Ting Lei [1,†], Xiang-Jie Li [2,†], Xing-Bo Pan [1], Yun-Rong Zhang [1] and Gui-Lu Long [1,3,4,5,*]

[1] State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China
[2] Future Research Lab, China Mobile Research Institute, Beijing 100053, China
[3] Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[4] Frontier Science Center for Quantum Information, Beijing 100084, China
[5] Beijing National Research Center for Information Science and Technology, Beijing 100084, China
* Correspondence: gllong@mail.tsinghua.edu.cn
† These authors contributed equally to this work.

Abstract: As a novel paradigm in quantum communication, quantum secure direct communication (QSDC) enables secure, reliable, and deterministic information transmission, leveraging the principles of quantum mechanics. One-photon-interference QSDC is particularly attractive because it mitigates the vulnerabilities in measurement devices while extending transmission distances. In this paper, we propose a high-dimensional one-photon-interference QSDC protocol that exploits the advantages of high-dimensional encoding in the phase of weak coherent pluses to further enhance transmission distances and improve secrecy channel capacity. The security of this protocol is analyzed using quantum wiretap channel theory, and its resistance to common quantum threats is discussed. Numerical simulations demonstrate that our protocol outperforms its predecessor in terms of its secrecy capacity and extends the maximum communication distance achievable up to 494 km, which is over 13% longer than the two-dimensional case, effectively doubling the transmission length of traditional protocols. These improvements highlight the protocol's potential for use in quantum communication applications in this era of frequent data breaches and information leaks.

Keywords: quantum information; quantum communication; quantum secure direct communication; one-photon-interference quantum communication

check for updates

Academic Editor: Ivo Pietro Degiovanni

Received: 31 January 2025
Revised: 6 March 2025
Accepted: 20 March 2025
Published: 22 March 2025

Citation: Lei, Y.-T.; Li, X.-J.; Pan, X.-B.; Zhang, Y.-R.; Long, G.-L. High-Dimensional and Multi-Intensity One-Photon-Interference Quantum Secure Direct Communication. *Entropy* **2025**, *27*, 332. https://doi.org/10.3390/e27040332

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The last two decades have witnessed the rapid development of quantum communication, which has garnered extensive attention due to its high security, guaranteed by the laws of quantum physics. One typical form of quantum communication is quantum key distribution (QKD), which provides secure key agreements between remote parties. Starting with Bennett and Brassard's pioneering BB84 scheme [1] and the very first entanglement-based protocols, E91 [2] and BBM92 [3], QKD has evolved significantly over the years, and its security has been theoretically proven [4–6]. Early efforts aimed to bridge the gap between theoretical security promises and practical implementations, exemplified by the decoy-state method [7–9], which mitigates photon-number-splitting (PNS) attacks and enables a high secret key rate even with a practical weak coherent source instead of an ideal single-photon source. To address vulnerabilities arising from detector-side loopholes, a measurement-device-independent QKD (MDI-QKD) [10–12] has been proposed to eliminate the security

risks associated with measurement-device imperfections in legitimate users. On the other hand, quantum secure direct communication (QSDC) has rapidly become a key paradigm of quantum cryptography. It originates from the seminal work by Long and Liu [13], which demonstrated the possibility of direct secret transmission in quantum channels, while subsequent protocols have extended their framework to incorporate various quantum resources, including polarizations in back-and-forth single photons [14]; orbital angular momentum states [15]; hyperentangled states [16]; high-dimensional optical degrees of freedom in both time and phase [17]; quadrature components, which are commonly used in continuous-variable (CV) protocols [18]; and so on. In facing the threats posed by attacks targeting experimental devices, the advent of MDI [19–21] and device-independent (DI) [22–24] techniques has further enhanced QSDC's security by incorporating realistic and imperfect implementations into its theoretical framework. QSDC also has the advantage of compatibility with existing Internet infrastructure [25], and simplifies its deployment by trimming the need for the management of pre-distributed keys. Numerous experimental demonstrations in recent years have proved the feasibility of these QKD [26–30] and QSDC [31–35] protocols, thereby increasing their potential for application in future scenarios requiring high levels of security.

The security of QSDC is based on the quantum wiretap channel theory [36,37], taking advantage of channel parameters such as the yield and error rate in transmission. As long as the secrecy channel capacity is non-zero, then there must exist a classical encoding scheme that ensures the secure and reliable transmission of information over a noisy and eavesdropping channel, according to Wyner's theory [38–40].

To further increase the key generation rate and extend the distance of communication, Lucamarini et al. put forward the twin-field QKD (TF-QKD) [41], which replaces the two-photon Bell state measurements in MDI-QKD with single-photon interferences. This allows the key rate to scale with the square root of the channel transmittance, effectively doubling the secure transmission distance compared to prior protocols, and can break the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound [42], which was once considered to be unfeasible without quantum repeaters. Thus, this novel feature has led to many research endeavors [43–48]. The essential mechanism behind TF-QKD is to exploit the one-photon interference. Inspired by this, one-photon-interference QSDC (OPI-QSDC) [49] is proposed to enhance the practicality and performance of QSDC protocols, while forgoing the need for either ideal single-photon sources, entangled light sources, or quantum memory. Meanwhile, it also possesses the MDI characteristic that mitigates the vulnerabilities in measurement devices.

However, OPI-QSDC employs only two phases for encoding secret information onto weak coherent pulses, leaving room for additional performance enhancement. High-dimensional quantum states not only increase the transmission rate but also enhance the probability of detecting eavesdropping [17,20,26]. In the meantime, by introducing additional bases into the encoding mode when preparing the quantum states to be transmitted, significant reductions in information leakage can be achieved over long distances [47]. Following these works, a high-dimensional one-photon-interference QSDC (HDOPI-QSDC) protocol is proposed in this paper.

The rest of this paper is organized as follows: Section 2 presents a detailed description of the protocol. In Section 3, we analyze the security of the protocol utilizing Wyner's wiretap theory, and discuss its resistance to several common quantum threats. Section 4 is dedicated to a numerical simulation of our scheme to evaluate its performance compared with two other typical QSDC protocols. A short summary and outlook is given at the end, in Section 5.

2. Our Protocol

We assume that Alice and Bob use weak laser pulses with phase locking and have agreed upon a reasonable number of total base slices M before completing the following steps. Charlie, an untrusted third party, is in between them, as illustrated in Figure 1. The steps of the HDOPI-QSDC protocol are as follows.

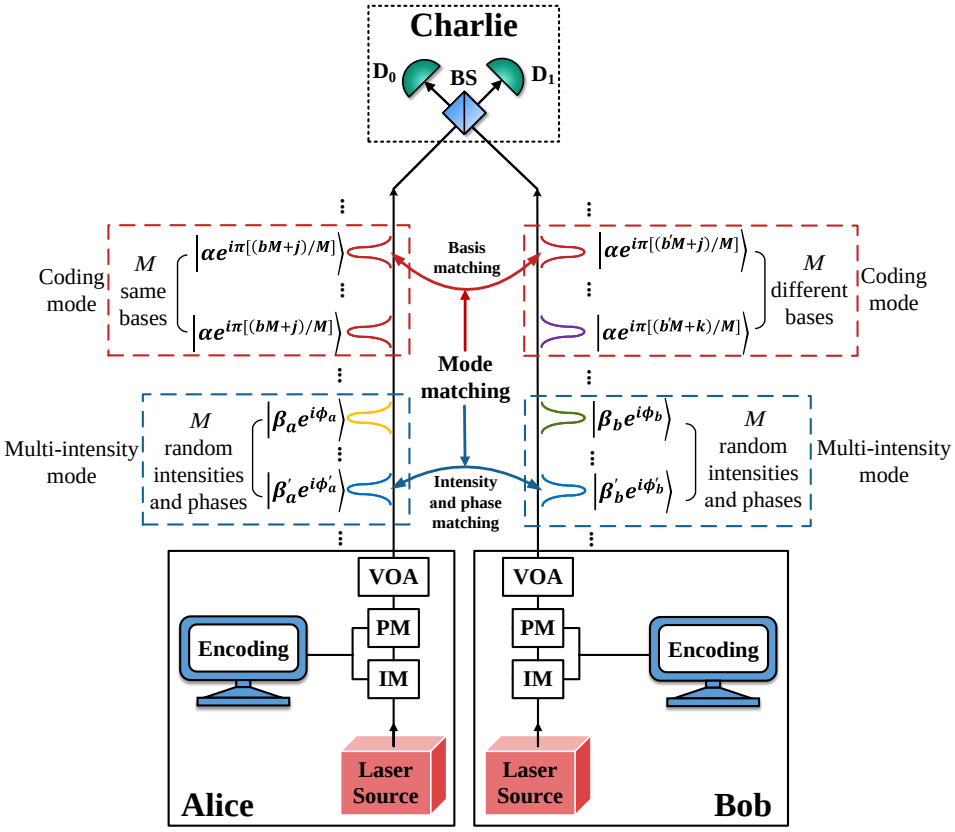


Figure 1. Schematic diagram of the HDOPI-QSDC protocol. BS, 50:50 beam splitter; D_0 and D_1, single-photon detectors; VOA, variable optical attenuator; PM, phase modulator; IM, intensity modulator. Red dashed boxes represent the coding modes, and blue dashed boxes represent the multi-intensity modes. In coding modes, Alice's pulses contain M same bases, while Bob's contain M different bases, and the order of these bases is random as well. In multi-intensity modes, Alice and Bob's M pulses contain random intensities and phases, chosen from the sets $\{\beta_0, \beta_1, \ldots\}$ and $[0, 2\pi)$, respectively. $j, k \in \{0, 1, \ldots, M-1\}$ are the bases' indices and $b, b' \in \{0, 1\}$ are the information bits. Charlie conducts one-photon interferences and publishes the untrustworthy measurement results, which are utilized by Alice and Bob to estimate the channel parameters and extract the original secret message.

Step 1: Encoding. Alice encodes the message to be transmitted into ciphertext using local random numbers shared with Bob. Note that the shared key can be obtained by running the rest of the procedures in this protocol, in which case random numbers are sent instead of the ciphertext. The encoding process includes forward error correction (FEC) coding, secure coding [37], and INCUM (increase capacity using masking) [50]. These processes eliminate the protocol's reliance on quantum memory, and their details are provided in Appendix A.

Step 2: State preparation. Alice and Bob independently select a mode to operate in: coding mode, with a probability of $1 - p$, or multi-intensity mode, with a probability of p, where $p \ll 1$. The specifics of the coding mode and multi-intensity mode are detailed below.

Coding mode: Alice sends M weak coherent states (WCSs) with the same base $|\alpha e^{i\pi(b_A/M)}\rangle = |\alpha e^{i\pi[(bM+A)/M]}\rangle$, where $b = 0$ or 1, which is the information bit value and is encoded in the phases as $b_A = bM + A \in \{0, 1, \ldots, 2M-1\}$, with $A \in \{0, 1, \ldots, M-1\}$ being the base index and M the total number of bases. Bob sends M WCSs with different bases $|\alpha e^{i\pi(b_B/M)}\rangle \in \left\{|\alpha e^{i\pi(b_0/M)}\rangle, |\alpha e^{i\pi(b_1/M)}\rangle, \ldots, |\alpha e^{i\pi(b_{M-1}/M)}\rangle\right\}$, where $b_B = b'M + B \in \{0, 1, \ldots, 2M-1\}$ and b' is a random bit in 0 or 1. The order of Bob's WCSs is random.

Multi-intensity mode: Alice and Bob send M WCSs with random intensities and random phases $|\beta_a e^{i\phi_a}\rangle, |\beta_b e^{i\phi_b}\rangle$. β_a and β_b are randomly selected light intensities in $\{\beta_0, \beta_1, \ldots\}$, and $\phi_a, \phi_b \in [0, 2\pi)$ are random phases.

Step 3: Charlie's measurement. One-photon interferences between pulses from Alice and Bob are conducted by Charlie, and the measurement results are announced on the public channel. Let D_0 and D_1 denote the measurement outcomes of the detectors D_0 and D_1, respectively; and their values can be set to "0", indicating a no-click event, or "1", indicating a click event. Alice and Bob discard the events where no detector clicks or both of them click, retaining only the one-click events, namely $D_0 \oplus D_1 = 1$.

Step 4: Mode matching. After all measurements are completed, Alice and Bob publish their selection of modes and retain events where they chose the same mode. In coding mode, Alice and Bob publish the basis information A and B and retain the events where they choose the same basis. In multi-intensity mode, Alice and Bob publish the intensities β_a and β_b and the phase information ϕ_a and ϕ_b, and then retain the events where $\beta_a = \beta_b$ and $|\phi_a - \phi_b| = 0$ or π.

Step 5: Parameter estimation. Alice and Bob randomly publish some bit values in coding modes to estimate the quantum bit error rate (QBER), and use multi-intensity modes to estimate the amount of information leakage.

Step 6: Decoding. Bob decodes the message from the ciphertext. The details of the decoding process are described in Appendix A.

It is important to note that mode mismatches occur with a probability of $2p(1-p)$, resulting in the possible loss of information transmitted by Alice. This necessitates the use of error-correcting codes during the pre-encoding process.

3. Security Analysis

According to quantum wiretap channel theory, when the capacity of the main channel is higher than that of the wiretap channel, a feasible coding scheme can be found that achieves secure and reliable information transmission. We introduce an equivalent entanglement-based protocol, the details of which are given in Appendix B, and analyze its security so as to determine the achievable secrecy capacity R of our HDOPI-QSDC protocol. Generally, we know that [51]

$$R = \max\{I(A:B) - I(A:E), 0\}, \tag{1}$$

where $I(A:B)$ is the mutual information of Alice and Bob and $I(A:E)$ is the mutual information of Alice and Eve.

Firstly, we consider the achievable secrecy capacity R^{D_0} when only detector D_0 clicks. We assume that Alice and Bob use the Z basis to transmit information and the X basis to estimate the amount of information leakage. The channels are treated as cascaded channels of a binary erasure channel (BEC) and binary symmetric channel (BSC). The QBER E_μ^{Z,D_0} and E_μ^{X,D_0}, the gain $Q_\mu^{D_0}$, and the inefficiency function for FEC f can be determined through

experiments, where $\mu = |\alpha|^2$ represents the light intensity of Alice and Bob. Thus, the mutual information $I(A:B)$ satisfies

$$I(A:B) \leq Q_\mu^{D_0} \cdot \left[1 - fH_2\left(E_\mu^{Z,D_0}\right)\right], \tag{2}$$

where $H_2(x)$ is the binary entropy function $H_2(x) = -x\log(x) - (1-x)\log(1-x)$. The upper bound of $I(A:E)$ is given by

$$\begin{aligned} I(A:E) &\leq Q_\mu^{D_0} \cdot H_{2M}\left(E_\mu^{X,D_0}\right) \\ &= -Q_\mu^{D_0} \sum_{n=0}^{2M-1} \lambda_{0n}\log(\lambda_{0n}), \end{aligned} \tag{3}$$

where λ_{0n} is defined as

$$\begin{aligned} \lambda_{0n} &= \frac{1}{Q_\mu^{D_0}}\left(\sum_{l=0}^{\infty} C_{2Ml+n}\sqrt{Y_{2Ml+n}^{D_0}}\right)^2 \\ &= \frac{1}{Q_\mu^{D_0}}\left(\sum_{l=0}^{\infty} \mathrm{e}^{-|\alpha|^2}\frac{(\sqrt{2}\alpha)^{2Ml+n}}{\sqrt{(2Ml+n)!}}\sqrt{Y_{2Ml+n}^{D_0}}\right)^2, \end{aligned} \tag{4}$$

and C_{2Ml+n} is the probability amplitude when the number of photons in the channel is $2Ml+n$ in the event that only detector D_0 clicks. $Y_{2Ml+n}^{D_0}$ represents the yield of the $|2Ml+n\rangle$ photon state when only detector D_0 clicks, and the details are explained in Appendix B. Therefore, we know that

$$R^{D_0} = \frac{q}{M} \cdot Q_\mu^{D_0} \cdot \left[1 - fH_2\left(E_\mu^{Z,D_0}\right) - H_{2M}\left(E_\mu^{X,D_0}\right)\right], \tag{5}$$

where $q = 1 - 2p(1-p)$ is the successful rate of mode matching.

The result is similar for the achievable secrecy capacity R^{D_1} when only detector D_1 responds; that is,

$$R^{D_1} = \frac{q}{M} \cdot Q_\mu^{D_1} \cdot \left[1 - fH_2\left(E_\mu^{Z,D_1}\right) - H_{2M}\left(E_\mu^{X,D_1}\right)\right]. \tag{6}$$

Finally, the total achievable secrecy capacity R of the HDOPI-QSDC protocol is given by

$$R = \max\left\{R^{D_0}, 0\right\} + \max\left\{R^{D_1}, 0\right\}. \tag{7}$$

Although the above information-theoretic framework guarantees the feasibility of secure information transmission within our protocol, its resistance to certain well-known attacks should be discussed further. One such attack is the intercept-resend attack, where an adversary Eve attempts to extract information by intercepting, measuring, and then resending quantum states to the intended recipient. However, our protocol is inherently resistant to this attack for the following reasons: First, single-photon interference eliminates the vulnerabilities in direct transmission. Unlike traditional QSDC, Alice and Bob do not exchange qubits directly. Instead, they send phase-encoded weak coherent pulses to a central untrusted relay Charlie, where information is distilled from phase correlations through single-photon interference. If Eve intercepts the photons, she inevitably collapses their quantum states, disrupting the interference and introducing detectable errors in the QBER. Furthermore, intercepting a single path is ineffective since complete information is only reconstructed through interference at the relay. Second, our frame-by-frame encoding scheme (detailed in Appendix A) prevents meaningful data extraction, as each frame carries

not only its own ciphertext but also secure keys for subsequent frames. Even in the worst case scenario, where Eve controls both channels and conducts the interference by herself, our encoding strategy not only ensures that this behavior will be immediately perceived by Alice and Bob but also prevents her from obtaining the original secret information, leaving her with only pieces of codewords. Moreover, since this pre-encoding occurs before the secret information is modulated onto quantum states, the scheme effectively leverages the one-time-pad property, significantly reducing the risk of information leakage. Third, INCUM technology further strengthens the protocol's security by adding another protective layer of masking with locally generated random numbers. This technique restricts Eve's effective reception rate to Bob's level, making it even more difficult for her to reconstruct the original information. Together, these mechanisms grant our protocol resistance to intercept-resend attacks.

Another related threat is the PNS attack, where Eve exploits the multi-photon pulses in a practical weak coherent source by splitting off a photon while allowing the remaining photons to reach the legitimate recipient, gaining information without being detected. Our protocol resists this attack through a multi-intensity mode, which functions similarly to the decoy-state method [7–9]. Since Eve cannot tell whether a pulse is in encoding mode or multi-intensity mode before her measurement, she cannot selectively attack multi-photon pulses without introducing detectable anomalies. By comparing channel parameters of different light intensities that have different mean photon numbers, Alice and Bob can identify the inconsistencies caused by eavesdropping attempts. As a result, the additional pulses with randomized light intensities and phases protect the multi-photon components of WCS-based encoding schemes, noticeably enhancing their secrecy capacity and ensuring security in the face of PNS attacks.

While quantum communication protocols are theoretically secure under ideal conditions, the measurement devices used in practical systems retain certain loopholes. Imperfections in detectors can be utilized to bypass security guarantees, such as the bright illumination attack [52] and the dead time attack [53]. Our protocol inherits the MDI nature of MDI-QSDC by shifting measurements to an untrusted third party Charlie and relying solely on his results. Because Alice and Bob do not directly receive photons or perform measurements, any inherent imperfections in their detectors do not expose them to vulnerabilities such as side-channel attacks. The security of this protocol relies on quantum interference rather than Charlie's honesty. Even if his detectors are fully controlled by Eve and are maliciously manipulated, Eve has no chance learning any useful information as it is only derived from post-processed correlations between Alice and Bob, as long as they strictly follow the correct procedures. In addition, as mentioned earlier, parameters such as error rates are carefully monitored, and any unexpected deviations are identified instantly. Although our protocol is not fully DI and may suffer from certain side-channel attacks, such as Trojan-horse attacks on light sources [54], its architecture, which includes placing the measurement in an untrusted location, decouples the security from the trustworthiness of the detectors, making it immune to many common attacks targeting measurement devices.

A final security concern is the assumption of an infinite block length in our analysis. In practical communication systems, Alice and Bob can only send finite numbers of WCS pluses rather than an idealized infinite number. This finite block length introduces statistical fluctuations in the estimation of channel parameters, which further tightens the upper bound of the secrecy channel capacity. Notably, unlike investigations in QKD systems [55–57], where random keys are negotiated, QSDC involves the direct transmission of deterministic information, and its performance under these conditions requires specific handling and analysis. While a comprehensive study of finite block length effects and their impact on practical QSDC systems is beyond the scope of this paper, valuable insights

on this topic can be found in Refs. [58,59]. In the following discussion, we adhere to the asymptotic limit, assuming an infinite block length.

4. Performance

In this section, we analyze the performance of the HDOPI-QSDC protocol. We denote the channel transmittance from Alice and Bob to Charlie as $\eta = \eta_d\sqrt{\eta_c}$, where η_d is the detection efficiency and η_c is the channel loss function. The gain is expressed as

$$Q_\mu^{D_0} = Q_\mu^{D_1} = 1 - \mathrm{e}^{-2\eta\mu} + 2p_d\mathrm{e}^{-2\eta\mu}, \tag{8}$$

where p_d is the rate of dark counts. The QBER is given by

$$E_\mu^{X,D_0} = E_\mu^{X,D_1} = \frac{\mathrm{e}^{-2\eta\mu}}{Q_\mu^{D_0}}(p_d + 2\eta\mu\delta), \tag{9}$$

where δ is the misalignment error. We assume that Alice and Bob use light pulses with infinite numbers of intensities in the multi-intensity mode, thus the yield of the $|2Ml + n\rangle$ photon state is

$$Y_{2Ml+n}^{D_0} = Y_{2Ml+n}^{D_1} = 1 - (1 - 2p_d)(1 - \eta)^{2Ml+n}. \tag{10}$$

The simulation parameters are as described in Table 1. Following Equation (7), we illustrate the performance of the HDOPI-QSDC protocol and compare it to the PLOB bound [42], the performance of OPI-QSDC (with an optimized intensity $u = 0.046$ as stated in [49]), DL04 ([14], INCUM-enhanced and with ideal sources), and MDI-QSDC ([19], INCUM-enhanced and with ideal sources) in Figure 2. OPI-QSDC can be regarded as an HDOPI-QSDC protocol with $M = 1$, since it uses 0 and π phases in its coding mode. In the case where $M = 2$, our high-dimensional protocol has a higher secrecy capacity and a roughly 50 km longer transmission distance than the original. As M increases, its secrecy capacity starts to reduce but its maximum transmission distance grows slightly. When $M \geq 5$, its secrecy capacity lags behind that of the original, though within a relatively short range, while its maximum distance outperforms the original by nearly 60 km. The benefit of further increasing M diminishes, since the maximum transmission distance hardly lengthens any further and the secrecy channel capacity continues to drop. The determination of a proper M should be guided by the specific needs of the system in practical applications. That is to say, $M = 1$, i.e., the original OPI-QSDC, provides a balance between practicality, secrecy capacity, and transmission distance, while a more complicated experimental setup leads to a considerable extension in communication distance and secrecy channel capacity when $M = 2$, 3, or 4.

Table 1. Key parameter settings of the simulation.

Parameter	Value	Description
ζ	0.2 dB/km	attenuation coefficient
η_d	14.5%	detector efficiency
p_d	8×10^{-8}	dark count rate
δ	1.5%	misalignment error
f	1.2	FEC efficiency
u	0.15	light intensity

Table 2 provides a concise comparison between our work and previous studies. It highlights key differences in terms of quantum resources, encoding methodologies, security guarantees, reliance on quantum memory, and performance metrics, thereby clarifying the advantages of our approach.

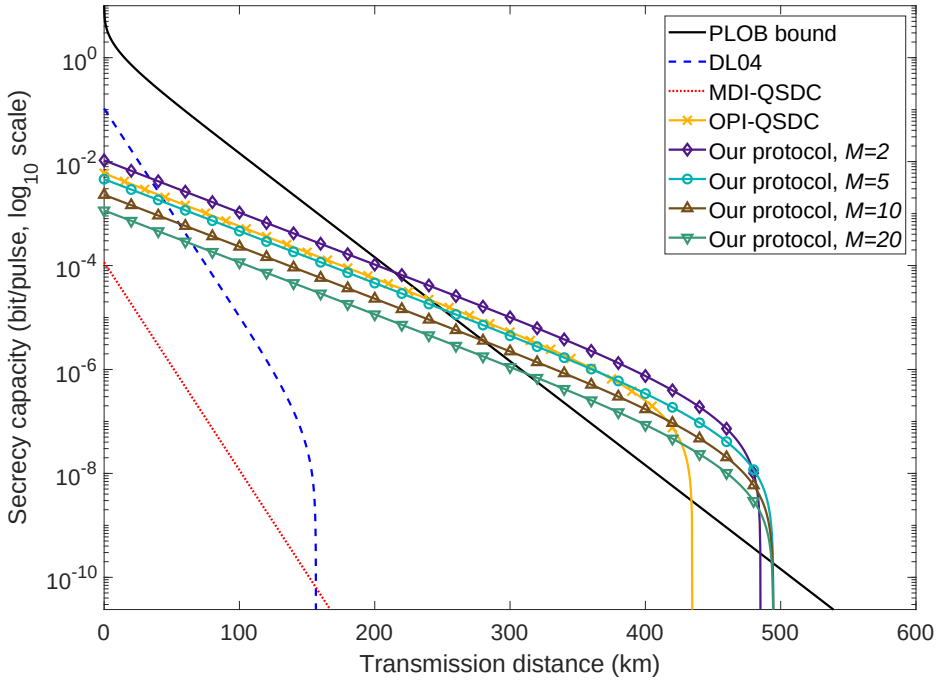


Figure 2. Achievable secrecy channel capacity R in $\log_{10}$ scale in terms of transmission distance. The black solid line is the PLOB bound, the red dotted line represents the MDI-QSDC protocol [19] (with INCUM), and the blue dashed line represents the DL04 protocol [14] (with INCUM). The orange line with "x" markers displays the performance of the OPI-QSDC protocol [49], and the purple, cyan, brown, and green lines with hollow markers are our HDOPI-QSDC protocol with $M = 2$, $M = 5$, $M = 10$, and $M = 20$ bases, respectively. The secrecy capacity of our protocol breaks the PLOB bound at 214.17 km (when $M = 2$), and its maximum distance is about 494.58 km (when $M = 20$).

Table 2. Comparison with other typical QSDC protocols.

	DL04 [14]	**MDI-QSDC [19]**	**OPI-QSDC [49]**	**Our Protocols**
Quantum resources	single photons (ideal) WCSs (practical)	single photons and entanglement pairs	single photons (ideal) WCSs (practical)	single photons (ideal) WCSs (practical)
Encode messages in	polarizations	Bell states	$0/\pi$ phases	multislice phases
Resistance to measurement-device attacks?	No	Yes	Yes	Yes
Resistance to PNS attacks?	No	No	Yes	Yes
Quantum memory free?	No	No	Yes	Yes
Break PLOB bound?	No	No	Yes	Yes
Approx. secrecy capacity at 100 km (bit/pulse)	1.03×10^{-5}	1.16×10^{-8}	5.72×10^{-4}	1.05×10^{-3} ($M = 2$) 1.15×10^{-4} ($M = 20$)
Approx. distance at 1×10^{-10} bit/pulse secrecy capacity	156.48 km	151.61 km	434.76 km	485.07 km ($M = 2$) 493.94 km ($M = 20$)

5. Conclusions

In this work, we present a high-dimensional one-photon-interference quantum secure direct communication protocol (HDOPI-QSDC), that generalizes the original one-photon-interference quantum secure direct communication framework to high-dimensional encoding. This advancement results in an enhanced secrecy channel capacity and an extended transmission distance, while maintaining a measurement-device-independent characteristic even though it involves the imperfect measurement devices of legitimate users. The security of the protocol is analyzed utilizing the quantum wiretap channel theory, and the secrecy channel capacity is derived. Furthermore, its resistance to common quantum threats is examined. Numerical simulations demonstrate that the HDOPI-QSDC protocol not only achieves a higher secrecy capacity but also improves the transmission distance by up to approximately 60 km compared to its predecessors, reaching a maximum range of 494 km, which effectively doubles the communication length of traditional protocols. These promising results suggest that our protocol holds potential for future applications, such as intercity quantum communications in government, finance, and healthcare sectors, where its extended range and high capacity could reduce reliance on quantum repeaters. Leveraging the merit of its deterministic information transmission, QSDC integrated with classic or post-quantum cryptography could boost the bandwidth of secure communication and provide an extra layer of protection by transferring only the secret keys via quantum channels, ensuring the hybrid system remains resistant to both quantum and classical adversaries.

However, the proposed protocol is subject to several key constraints that require further investigation. First, our security analysis assumes an infinite block length, which simplifies the derivation of the secrecy capacity by neglecting the statistical fluctuations introduced by finite block lengths in the estimation of channel parameters. In practice, the finite size of the information block leads to tighter bounds and potentially a lower performance. Second, the protocol also presumes an unlimited number of light intensities in the multi-intensity mode. Although three or four intensities should suffice in real-world systems, a detailed capacity analysis of these limited intensity values is needed. Third, the experimental implementation of our protocol faces significant difficulties, due to its heavy reliance on high-precision phase operations. Achieving adequate one-photon interference visibility requires maintaining phase coherence over long distances, between the independent lasers at Alice's and Bob's stations. Consequently, the precise synchronization of remote lasers is critical, and active, continuous phase compensation and stabilization is essential to counter environmental disturbances. Moreover, developing high-efficiency and low-noise single-photon detectors remains a substantial challenge. While recent advancements in optical systems [60,61], detector performance [62,63], and protocol optimization [64,65] have shed light on these experimental hurdles with proof-of-principle demonstrations [66–68], further innovations will be necessary for the practical deployment of this protocol.

Author Contributions: Conceptualization, X.-J.L.; formal analysis, X.-J.L. and Y.-T.L.; software, X.-J.L.; validation, Y.-T.L.; writing—original draft preparation, Y.-T.L. and X.-J.L.; writing—review and editing, X.-B.P. and Y.-R.Z.; supervision, G.-L.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under Grants No. 62471046 and No. 62401324; the Beijing Advanced Innovation Center for Future Chip (ICFC); and the Tsinghua University Initiative Scientific Research Program.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author Xiang-Jie Li was employed by the company Future Research Lab, China Mobile Research Institute. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Appendix A. Details of Encoding and Decoding Processes

In coding modes, the messages to be transmitted are encoded into frames, and each frame contains the information bits and the raw keys that will be distilled later and used to encode future frames. This removes the need for quantum memory by immediately preparing and sending quantum states without storing them, and it is possible within QSDC because it can examine whether there is eavesdropping in the transmission. Here, we denote $\mathcal{M} \in \{0,1\}^m$ as plaintext to be transferred from Alice to Bob, $\mathcal{K} \in \{0,1\}^m$ as keys extracted from a key pool to pre-encrypt the message $\mathcal{M}$, and $\mathcal{Y} = \mathcal{M} \oplus \mathcal{K}$ as the ciphertext. Then, a LDPC encoder of length k and rate $\mathcal{R}_p$, satisfying $k\mathcal{R}_p = m$, is applied for pre-coding, and it outputs $\mathcal{X} \in \{0,1\}^k$ to a cache. From the cache a sequence $\mathcal{X}_i \in \{0,1\}^{k_i}$ is retrieved, and it forms the input of the secure coding module in the i-th frame. However, in the special case that the cache becomes exhausted, $\mathcal{X}_i$ comes from a random number generator (RNG). Let $\mathcal{R}_i$ be the secure coding rate of the i-th frame and $\mathcal{C}_i \in \{0,1\}^{n_{\mathcal{C}_i}}$ be the codeword of $\mathcal{X}_i$, with length $n_{\mathcal{C}_i}$. An XOR operation is performed on $\mathcal{C}_i$ with a random bit sequence $\mathcal{L}_i \in \{0,1\}^{n_{\mathcal{C}_i}}$. This implements the INCUM method [50], namely by masking the ciphertext $\mathcal{C}_i$ using local random numbers $\mathcal{L}_i$, producing $\mathcal{C}_i' = \mathcal{C}_i \oplus \mathcal{L}_i$, which is then modulated onto quantum states. The encoded quantum state pluses are transmitted to Charlie for measurement. The main channel capacity of the i-th frame is denoted as $C_{m_i} \equiv \max I_i(A:B)$, and the wiretap channel capacity is $C_{w_i} \equiv \max I_i(A:E)$. The achievable secrecy channel capacity $R_i \equiv C_{m_i} - C_{w_i}$ can then be calculated. These parameters must satisfy [37]

$$\frac{k_i}{n_{\mathcal{C}_i}} \leq \mathcal{R}_i - C_{w_{i-1}}, \quad \mathcal{R}_i < C_{m_{i-1}}, \tag{A1}$$

to ensure the security of the communication. A diagram of the detailed encoding and decoding process is illustrated in Figure A1, and its steps are as written below.

To initialize a new round of communication, in which case $i = 1$, $\mathcal{X}_1$ should be picked from an RNG. k_1 and $\mathcal{R}_1$ should be properly selected to meet the criteria in Equation (A1). A usable shared key $\mathcal{S}_1$ with length $n_{\mathcal{C}_1} \cdot R_1$ can be distilled if C_{m_1} and C_{w_1} both fulfill Equation (A1) as well.

When $i > 1$ and $\mathcal{K}$ is sufficient to use, Alice's encoding processes and Bob's decoding processes include the following steps:

(1) Alice uses $\mathcal{K} \in \{0,1\}^m$ to pre-encrypt $\mathcal{M} \in \{0,1\}^m$ into the ciphertext $\mathcal{Y} = \mathcal{M} \oplus \mathcal{K}$.
(2) Alice pre-encodes $\mathcal{Y}$ into $\mathcal{X}$, which is stored in a cache.
(3) Alice fetches the k_i-bit length of $\mathcal{X}_i \in \{0,1\}^{k_i}$ from the cache to accomplish secure coding, where the parameters should satisfy Equation (A1) and the output is $\mathcal{C}_i \in \{0,1\}^{n_{\mathcal{C}_i}}$.
(4) Alice applies INCUM using a locally generated random bit string $\mathcal{L}_i$, and obtains $\mathcal{C}_i' = \mathcal{C}_i \oplus \mathcal{L}_i$.
(5) Alice modulates $\mathcal{C}_i'$ into qubits if she selects the coding mode in **Step 2** of our protocol, otherwise she prepares the multi-intensity mode.
(6) Charlie conducts **Step 3**.
(7) Steps (5) to (6) are repeated until $\mathcal{C}_i'$ is entirely transmitted.

(8) Alice and Bob conduct **Step 4** and **Step 5** and use these parameters to calculate C_{m_i}, C_{w_i}, and R_i. If Equation (A1) is satisfied, a shared key $\mathcal{S}_i$ could be distilled for future frames.

(9) Steps (3) to (8) are repeated until $\mathcal{X}$ is entirely transmitted.

(10) Alice announces random bit values of $\mathcal{L}$ in positions where Bob has received information. Bob first applies de-INCUM to obtain $\mathcal{C}_i = \mathcal{C}'_i \oplus \mathcal{L}_i$ and then decodes $\mathcal{C}_i$ to $\mathcal{X}_i$ with a secure coding decoder. After that he obtains $\mathcal{Y}$ from a $(k, k\mathcal{R}_p)$-LDPC decoder and finally retrieves the original message $\mathcal{M} = \mathcal{Y} \oplus \mathcal{K}$ utilizing the shared key $\mathcal{K}$.

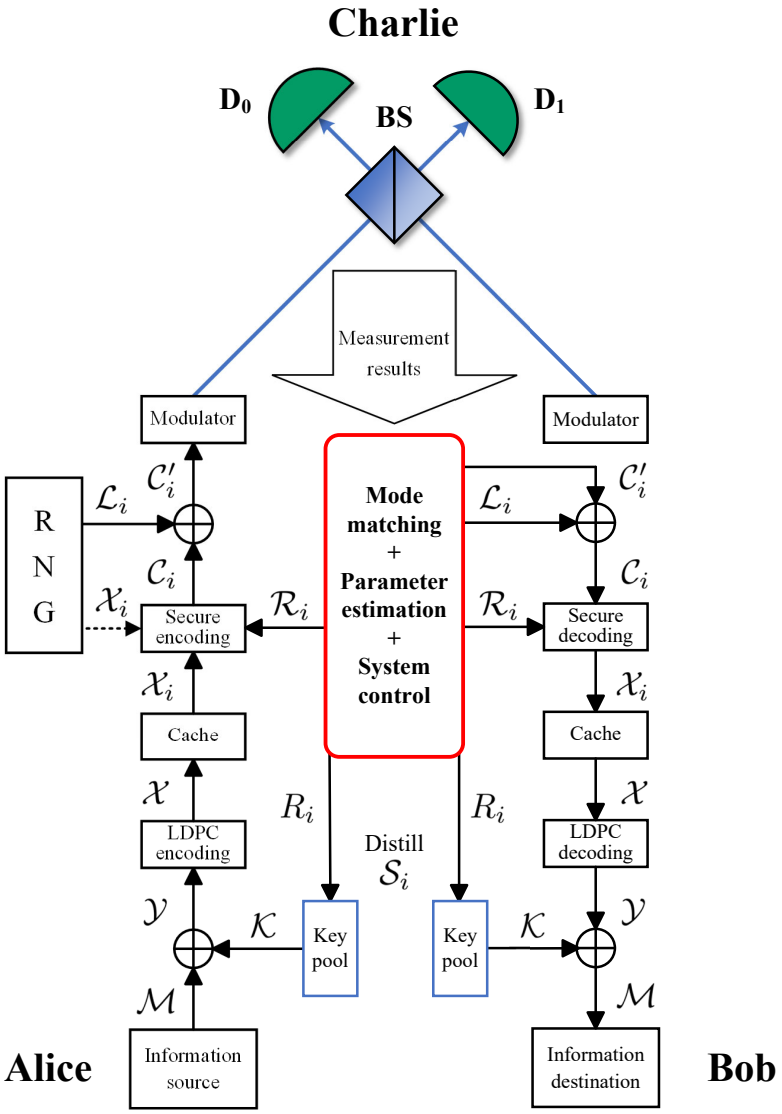


Figure A1. Encoding and decoding processes of the HDOPI-QSDC protocol. BS, 50:50 beam splitter; D_0 and D_1, single-photon detectors; RNG, random number generator. The blue arrows indicate the transmission direction of qubits, and the black arrows classical bits. The black dotted arrow is only used in situations where there is an empty cache or key pool and at the beginning of a new round of communication.

Appendix B. Details of Security Analysis

First, we define two entangled pairs

$$|\Phi(\alpha)\rangle_{Aa} = \frac{1}{\sqrt{2M}} \sum_{b_A=0}^{2M-1} |b_A\rangle_A |\alpha e^{\pi i \frac{b_A}{M}}\rangle_a, \tag{A2}$$

$$|\Phi(\alpha)\rangle_{Bb} = \frac{1}{\sqrt{2M}} \sum_{b_B=0}^{2M-1} |b_B\rangle_B |\alpha e^{\pi i \frac{b_B}{M}}\rangle_b, \tag{A3}$$

where the subscripts A and B of the quantum states indicate that they are retained by Alice and Bob, and a and b indicate that they are sent to Charlie by Alice and Bob, respectively. The A and B states are in a codeword space of dimension $2M$, thus b_A and b_B can take values from $\{0, 1, \ldots, 2M-1\}$. Then, we introduce an entanglement-based protocol, taking advantage of these two entangled pairs, which is equivalent in security to our HDOPI-QSDC protocol. For convenience, we refer to this protocol as protocol II and the HDOPI-QSDC protocol as protocol I. Protocol II contains the following steps:

Step 1: Encoding. Same as protocol I.

Step 2′: State preparation. Alice and Bob select a coding mode with the probability of $1-p$ or select a multi-intensity mode with p, where $p \ll 1$.

Coding mode: Alice prepares M entangled pairs all in the state $|\Phi(\alpha)\rangle_{Aa}$. She sends the photon a to Charlie and retains the photon A locally. Similarly, Bob prepares M entangled pairs $|\Phi(\alpha)\rangle_{Bb}$, sends b to Charlie and retains B.

Multi-intensity mode: Same as protocol I.

Step 3: Charlie's measurement. Same as protocol I.

Step 3′: Alice and Bob's measurement. After Charlie's measurement, if Alice sent the coding mode photon, she measures the local states A in the computational bases. To ensure the equivalence of protocols II and I, we assume that Alice can perform deterministic measurements based on the encoding results. This means that if she wants to send a logical bit 0, and the base index she chooses is also 0, the measurement results of M local states will be all $|0\rangle_A$. If Bob sent the coding mode photon, he measures the local states B using M different bases.

Note that this step is commutative to **Step 3**. If we exchange these two steps, then protocol II will reduce to protocol I. Thus, the two protocols are equivalent in security.

Step 4: Mode matching. Same as protocol I.

Step 5: Parameter estimation. Same as protocol I.

Step 6: Decoding. Same as protocol I.

Next, we derive the secrecy channel capacity of protocol II. In **Step 2′**, we defined the joint state $|\phi\rangle_{AaBb}$ of Alice and Bob, which is

$$\begin{aligned} |\phi\rangle_{AaBb} &= |\Phi(\alpha)\rangle_{Aa} \otimes |\Phi(\alpha)\rangle_{Bb} \\ &= \frac{1}{\sqrt{2M}} \sum_{b_A=0}^{2M-1} |b_A\rangle_A |\alpha e^{\pi i \frac{b_A}{M}}\rangle_a \otimes \frac{1}{\sqrt{2M}} \sum_{b_B=0}^{2M-1} |b_B\rangle_B |\alpha e^{\pi i \frac{b_B}{M}}\rangle_b \\ &= \frac{1}{2M} \sum_{b_A, b_B} |b_A\rangle_A |b_B\rangle_B |\alpha e^{\pi i \frac{b_A}{M}}\rangle_a |\alpha e^{\pi i \frac{b_B}{M}}\rangle_b. \end{aligned} \tag{A4}$$

Then, Alice and Bob send their photons a and b to Charlie, respectively.

In **Step 3**, Charlie uses a 50:50 beam splitter to perform single-photon interferences, which result in

$$\begin{aligned} |\phi\rangle_{AaBb} &\to |\phi\rangle_{ABD_0D_1} \\ &= \frac{1}{2M} \sum_{b_A, b_B} |b_A\rangle_A |b_B\rangle_B |\frac{\alpha}{\sqrt{2}}(e^{\pi i \frac{b_A}{M}} + e^{\pi i \frac{b_B}{M}})\rangle_{D_0} |\frac{\alpha}{\sqrt{2}}(e^{\pi i \frac{b_A}{M}} - e^{\pi i \frac{b_B}{M}})\rangle_{D_1}. \end{aligned} \tag{A5}$$

We first consider the case where only detector D_0 clicks, i.e., $|(\alpha/\sqrt{2})(e^{\pi i(b_A/M)} - e^{\pi i(b_B/M)})\rangle_{D_1} = |0\rangle_{D_1}$, which implies $b_B = b_A$. Thus, we obtain

$$\begin{aligned}
|\phi\rangle_{ABD_0D_1} =& \frac{1}{2M}\sum_{b_A}|b_A\rangle_A|b_A\rangle_B|\sqrt{2}\alpha e^{\pi i\frac{b_A}{M}}\rangle_{D_0}|0\rangle_{D_1} \\
=& \frac{1}{2M}\sum_{b_A}|b_A\rangle_A|b_A\rangle_B\left[e^{-|\alpha|^2}\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha e^{\pi i\frac{b_A}{M}})^l}{\sqrt{l!}}|l\rangle_{D_0}\right]|0\rangle_{D_1} \\
=& \frac{e^{-|\alpha|^2}}{2M}\left\{\sum_{b_A}e^{\pi i\frac{b_A\cdot 0}{M}}|b_A\rangle_A|b_A\rangle_B\left[\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha)^{2Ml}}{\sqrt{(2Ml)!}}|2Ml\rangle_{D_0}\right]|0\rangle_{D_1}\right. \\
&+\sum_{b_A}e^{\pi i\frac{b_A\cdot 1}{M}}|b_A\rangle_A|b_A\rangle_B\left[\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha)^{2Ml+1}}{\sqrt{(2Ml+1)!}}|2Ml+1\rangle_{D_0}\right]|0\rangle_{D_1}+\cdots \\
&\left.+\sum_{b_A}e^{\pi i\frac{b_A\cdot(2M-1)}{M}}|b_A\rangle_A|b_A\rangle_B\left[\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha)^{2Ml+2M-1}}{\sqrt{(2Ml+2M-1)!}}|2Ml+2M-1\rangle_{D_0}\right]|0\rangle_{D_1}\right\} \\
=& \frac{e^{-|\alpha|^2}}{\sqrt{2M}}\left[|\Phi_{00}\rangle_{AB}\left(\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha)^{2Ml}}{\sqrt{(2Ml)!}}|2Ml\rangle_{D_0}\right)|0\rangle_{D_1}\right. \\
&+|\Phi_{01}\rangle_{AB}\left(\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha)^{2Ml+1}}{\sqrt{(2Ml+1)!}}|2Ml+1\rangle_{D_0}\right)|0\rangle_{D_1}+\cdots \\
&\left.+|\Phi_{0(2M-1)}\rangle_{AB}\left(\sum_{l=0}^{\infty}\frac{(\sqrt{2}\alpha)^{2Ml+2M-1}}{\sqrt{(2Ml+2M-1)!}}|2Ml+2M-1\rangle_{D_0}\right)|0\rangle_{D_1}\right],
\end{aligned} \tag{A6}$$

where $|\Phi_{mn}\rangle$ is the $2M$-dimensional Bell state

$$|\Phi_{mn}\rangle = \frac{1}{\sqrt{2M}}\sum_{j=0}^{2M-1}e^{\pi i\frac{jn}{M}}|j\rangle|j\oplus m \pmod{2M}\rangle. \tag{A7}$$

After Charlie's measurement, we can trace out systems D_0 and D_1 from $|\phi\rangle_{ABD_0D_1}$, and then obtain the joint state of Alice and Bob, which is

$$\begin{aligned}
\rho_{AB} =& \sum_{n=0}^{2M-1}\rho_{AB}^n \\
=& \frac{1}{Q}\sum_{n=0}^{2M-1}\left(\sum_{l=0}^{\infty}e^{-|\alpha|^2}\frac{\left(\sqrt{2}\alpha\right)^{2Ml+n}}{\sqrt{(2Ml+n)!}}\right)^2|\Phi_{0n}\rangle\langle\Phi_{0n}| \\
\equiv& \frac{1}{Q}\sum_{n=0}^{2M-1}\left(\sum_{l=0}^{\infty}C_{2Ml+n}\right)^2|\Phi_{0n}\rangle\langle\Phi_{0n}|,
\end{aligned} \tag{A8}$$

where Q is a normalization coefficient.

We assume that Eve performs a coherent attack using an auxiliary system $|E\rangle$ and further consider it as a collective attack, applying the quantum de Finetti theorem [69]. Therefore, the state that Alice, Bob, and Eve jointly form is

$$|\phi\rangle_{ABE} = \sum_{m,n}\sqrt{\lambda_{mn}}|\Phi_{mn}\rangle|E_{mn}\rangle, \tag{A9}$$

where $|E_{mn}\rangle$ is the orthogonal basis of the auxiliary system $|E\rangle$. From Equation (A8), it is clear that

$$\lambda_{0n} = \frac{1}{Q}\left(\sum_l C_{2Ml+n}\right)^2, \tag{A10}$$

$$\lambda_{mn} = 0 \quad (m \neq 0). \tag{A11}$$

The joint system of Alice and Eve after tracing out Bob's system can be expressed as

$$\begin{aligned}
\rho_{AE} &= \mathrm{Tr}_B(|\phi\rangle_{ABE}\langle\phi|) \\
&= \sum_i \langle i_B|\phi\rangle_{ABE}\langle\phi|i_B\rangle \\
&= \sum_{i,n,n'} \sqrt{\lambda_{0n}}\langle i_B|\Phi_{0n}\rangle|E_{0n}\rangle\langle E_{0n'}|\langle\Phi_{0n'}|i_B\rangle\sqrt{\lambda_{0n'}} \\
&= \sum_{i,n,n'} \sqrt{\lambda_{0n}}\langle i_B|\frac{1}{\sqrt{2M}}\sum_{b_A=1}^{2M-1} \mathrm{e}^{\pi \mathrm{i}\frac{b_A\cdot n}{M}}|b_A\rangle_A|b_A\rangle_B|E_{0n}\rangle \\
&\quad \langle E_{0n'}|\frac{1}{\sqrt{2M}}\sum_{b'_A=1}^{2M-1} \mathrm{e}^{-\pi \mathrm{i}\frac{b'_A\cdot n'}{M}}\langle b'_A|_A\langle b'_A|_B|i_B\rangle\sqrt{\lambda_{0n'}} \\
&= \sum_{b_A,n,n'} \frac{\sqrt{\lambda_{0n}\lambda_{0n'}}}{2M}\mathrm{e}^{\pi \mathrm{i}\frac{b_A(n-n')}{M}}|b_A\rangle_A\langle b_A| \otimes |E_{0n}\rangle\langle E_{0n'}|.
\end{aligned} \tag{A12}$$

In **Step 3'**, Alice measures the local state A and obtains the value b_A. Then, the state of Eve becomes

$$\begin{aligned}
\rho_E^{b_A} &= \mathrm{Tr}_A(|b_A\rangle_A\langle b_A|\rho_{AE}|b_A\rangle_A\langle b_A|) \\
&= \sum_{n,n'}^{2M-1} \sqrt{\lambda_{0n}\lambda_{0n'}}\mathrm{e}^{\pi \mathrm{i}\frac{b_A(n-n')}{M}}|E_{0n}\rangle\langle E_{0n'}|.
\end{aligned} \tag{A13}$$

According to the Holevo bound, the maximum mutual information between Alice and Eve can be written as follows [70]:

$$\begin{aligned}
\max I(A:E) &= S\left(\sum_{b_A} p(b_A)\rho_E^{b_A}\right) - \sum_{b_A} p(b_A) S\left(\rho_E^{b_A}\right) \\
&= S\left(\frac{1}{2M}\sum_{b_A,n,n'} \sqrt{\lambda_{0n}\lambda_{0n'}}\mathrm{e}^{\pi \mathrm{i}\frac{b_A(n-n')}{M}}|E_{0n}\rangle\langle E_{0n'}|\right) \\
&= S\left(\sum_{n=0}^{2M-1} \lambda_{0n}|E_{0n}\rangle\langle E_{0n}|\right) \\
&= -\sum_{n=0}^{2M-1} \lambda_{0n}\log(\lambda_{0n}) \\
&\equiv H_{2M}\left(E_\mu^{Z,D_0}\right).
\end{aligned} \tag{A14}$$

Here, $S(\cdot)$ is the von Neumann entropy, and $p(b_A)$ is the distribution of $\rho_E^{b_A}$. In the assumption of an infinite block length, Alice sends bits $b_A \in \{0, 1, \ldots, 2M-1\}$ with equal probability $p(b_A) = 1/(2M)$.

In **Step 5**, Alice and Bob can use the multi-intensity mode to estimate the yield $Y_{2Ml+n}^{D_0}$ of the quantum state $|2Ml+n\rangle$ and then deduce the amount of information leakage, which is given by

$$\lambda_{0n} = \frac{1}{Q_\mu^{D_0}}\left(\sum_{l=0}^{\infty} C_{2Ml+n}\sqrt{Y_{2Ml+n}^{D_0}}\right)^2, \tag{A15}$$

and

$$I(A:E) = -Q_{\mu}^{D_0} \sum_{n=0}^{2M-1} \lambda_{0n} \log(\lambda_{0n}). \tag{A16}$$

Finally, Alice and Bob use the QBER E_{μ}^{Z,D_0}, the gain $Q_{\mu}^{D_0}$, and the inefficiency function for FEC f to estimate the achievable secrecy channel capacity in the case where only detector D_0 clicks:

$$R^{D_0} = \frac{q}{M} \cdot Q_{\mu}^{D_0} \cdot \left[1 - fH_2\left(E_{\mu}^{Z,D_0}\right) - H_{2M}\left(E_{\mu}^{X,D_0}\right)\right], \tag{A17}$$

where the coefficient q/M is the result of the mode matching in **Step 4**. The result is similar for the achievable secrecy channel capacity R^{D_1} when only detector D_1 responds, which is

$$R^{D_1} = \frac{q}{M} \cdot Q_{\mu}^{D_1} \cdot \left[1 - fH_2\left(E_{\mu}^{Z,D_1}\right) - H_{2M}\left(E_{\mu}^{X,D_1}\right)\right]. \tag{A18}$$

Therefore, the total achievable secrecy channel capacity R of protocol II, as well as that of protocol I, is given by

$$R = \max\left\{R^{D_0}, 0\right\} + \max\left\{R^{D_1}, 0\right\}. \tag{A19}$$

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, 10–12 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]
3. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum Cryptography without Bell's Theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef] [PubMed]
4. Lo, H.K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
5. Tomamichel, M.; Leverrier, A. A Largely Self-Contained and Complete Security Proof for Quantum Key Distribution. *Quantum* **2017**, *1*, 14. [CrossRef]
6. Curty, M.; Azuma, K.; Lo, H.K. Simple Security Proof of Twin-Field Type Quantum Key Distribution Protocol. *npj Quantum Inf.* **2019**, *5*, 11. [CrossRef]
7. Lo, H.K.; Ma, X.F.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
8. Ma, X.F.; Qi, B.; Zhao, Y.; Lo, H.K. Practical Decoy State for Quantum Key Distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
9. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
10. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
11. Wang, W.; Tamaki, K.; Curty, M. Measurement-Device-Independent Quantum Key Distribution with Leaky Sources. *Sci. Rep.* **2021**, *11*, 1678. [CrossRef]
12. Wang, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Measurement-Device-Independent Quantum Key Distribution Robust against Environmental Disturbances. *Optica* **2017**, *4*, 1016–1023. [CrossRef]
13. Long, G.L.; Liu, X.S. Theoretically Efficient High-Capacity Quantum-Key-Distribution Scheme. *Phys. Rev. A* **2002**, *65*, 032302. [CrossRef]
14. Deng, F.G.; Long, G.L. Secure Direct Communication with a Quantum One-Time Pad. *Phys. Rev. A* **2004**, *69*, 052319. [CrossRef]
15. Mi, S.; Wang, T.j.; Jin, G.s.; Wang, C. High-Capacity Quantum Secure Direct Communication with Orbital Angular Momentum of Photons. *IEEE Photonics J.* **2015**, *7*, 1–8. [CrossRef]
16. Wu, F.; Yang, G.; Wang, H.; Xiong, J.; Alzahrani, F.; Hobiny, A.; Deng, F. High-Capacity Quantum Secure Direct Communication with Two-Photon Six-Qubit Hyperentangled States. *Sci. China Phys. Mech. Astron.* **2017**, *60*, 120313. [CrossRef]
17. Ahn, B.; Park, J.; Lee, J.; Lee, S. High-Dimensional Single Photon Based Quantum Secure Direct Communication Using Time and Phase Mode Degrees. *Sci. Rep.* **2024**, *14*, 888. [CrossRef]
18. Cao, Z.; Wang, L.; Liang, K.; Chai, G.; Peng, J. Continuous-Variable Quantum Secure Direct Communication Based on Gaussian Mapping. *Phys. Rev. Appl.* **2021**, *16*, 024012. [CrossRef]
19. Niu, P.H.; Zhou, Z.R.; Lin, Z.S.; Sheng, Y.B.; Yin, L.G.; Long, G.L. Measurement-Device-Independent Quantum Communication without Encryption. *Sci. Bull.* **2018**, *63*, 1345–1350. [CrossRef]

20. Liu, L.; Niu, J.L.; Fan, C.R.; Feng, X.T.; Wang, C. High-Dimensional Measurement-Device-Independent Quantum Secure Direct Communication. *Quantum Inf. Process.* **2020**, *19*, 404. [CrossRef]
21. Ying, J.W.; Zhou, L.; Zhong, W.; Sheng, Y.B. Measurement-Device-Independent One-Step Quantum Secure Direct Communication. *Chin. Phys. B* **2022**, *31*, 120303. [CrossRef]
22. Zhou, L.; Sheng, Y.B. One-Step Device-Independent Quantum Secure Direct Communication. *Sci. China Phys. Mech. Astron.* **2022**, *65*, 250311. [CrossRef]
23. Zhou, L.; Xu, B.W.; Zhong, W.; Sheng, Y.B. Device-Independent Quantum Secure Direct Communication with Single-Photon Sources. *Phys. Rev. Appl.* **2023**, *19*, 014036. [CrossRef]
24. Das, N.; Basu, S.; Paul, G.; Rao, V.S. User-Authenticated Device-Independent Quantum Secure Direct Communication Protocol. In Proceedings of the 2024 IEEE 37th International System-on-Chip Conference (SOCC), Dresden, Germany, 16–19 September 2024; pp. 1–6.
25. Pan, D.; Long, G.L.; Yin, L.; Sheng, Y.B.; Ruan, D.; Ng, S.X.; Lu, J.; Hanzo, L. The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1898–1949. [CrossRef]
26. 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]
27. Kwek, L.C.; Cao, L.; Luo, W.; Wang, Y.; Sun, S.; Wang, X.; Liu, A.Q. Chip-Based Quantum Key Distribution. *AAPPS Bull.* **2021**, *31*, 15. [CrossRef]
28. Xie, Y.M.; Lu, Y.S.; Weng, C.X.; Cao, X.Y.; Jia, Z.Y.; Bao, Y.; Wang, Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference. *PRX Quantum* **2022**, *3*, 020315. [CrossRef]
29. Yang, K.X.; Mao, Y.L.; Chen, H.; Dong, X.; Zhu, J.; Wu, J.; Li, Z.D. Experimental Measurement-Device-Independent Quantum Conference Key Agreement. *Phys. Rev. Lett.* **2024**, *133*, 210803. [CrossRef]
30. Wang, S.; He, D.Y.; Yin, Z.Q.; Lu, F.Y.; Cui, C.H.; Chen, W.; Zhou, Z.; Guo, G.C.; Han, Z.F. Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System. *Phys. Rev. X* **2019**, *9*, 021046. [CrossRef]
31. Zhang, W.; Ding, D.S.; Sheng, Y.B.; Zhou, L.; Shi, B.S.; Guo, G.C. Quantum Secure Direct Communication with Quantum Memory. *Phys. Rev. Lett.* **2017**, *118*, 220501. [CrossRef]
32. Zhu, F.; Zhang, W.; Sheng, Y.; Huang, Y. Experimental Long-Distance Quantum Secure Direct Communication. *Sci. Bull.* **2017**, *62*, 1519–1524. [CrossRef]
33. Qi, Z.; Li, Y.; Huang, Y.; Feng, J.; Zheng, Y.; Chen, X. A 15-User Quantum Secure Direct Communication Network. *Light Sci. Appl.* **2021**, *10*, 183. [CrossRef] [PubMed]
34. Cao, Z.; Lu, Y.; Chai, G.; Yu, H.; Liang, K.; Wang, L. Realization of Quantum Secure Direct Communication with Continuous Variable. *Research* **2023**, *6*, 0193. [CrossRef]
35. Pan, D.; Liu, Y.C.; Niu, P.; Zhang, H.; Zhang, F.; Wang, M.; Song, X.T.; Chen, X.; Zheng, C.; Long, G.L. Simultaneous Transmission of Information and Key Exchange Using the Same Photonic Quantum States. *Sci. Adv.* **2025**, *11*, eadt4627. [CrossRef] [PubMed]
36. Wu, J.; Lin, Z.; Yin, L.; Long, G.L. Security of Quantum Secure Direct Communication Based on Wyner's Wiretap Channel Theory. *Quantum Eng.* **2019**, *1*, e26. [CrossRef]
37. Sun, Z.; Song, L.; Huang, Q.; Yin, L.; Long, G.L.; Lu, J.; Hanzo, L. Toward Practical Quantum Secure Direct Communication: A Quantum-Memory-Free Protocol and Code Design. *IEEE Trans. Commun.* **2020**, *68*, 5778–5792. [CrossRef]
38. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
39. Bellare, M.; Tessaro, S.; Vardy, A. Semantic Security for the Wiretap Channel. In *Advances in Cryptology—CRYPTO 2012*; Safavi-Naini, R., Canetti, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 294–311. [CrossRef]
40. Shah, S.M.; Sharma, V. Enhancing Secrecy Rates in a Wiretap Channel. *Digit. Commun. Netw.* **2020**, *6*, 129–135. [CrossRef]
41. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the Rate-Distance Limit of Quantum Key Distribution without Quantum Repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
42. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental Limits of Repeaterless Quantum Communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
43. Ma, X.F.; Zeng, P.; Zhou, H. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
44. Wang, X.B.; Yu, Z.W.; Hu, X.L. Sending or Not Sending: Twin-Field Quantum Key Distribution with Large Misalignment Error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
45. Yu, Z.W.; Hu, X.L.; Jiang, C.; Xu, H.; Wang, X.B. Sending-or-Not-Sending Twin-Field Quantum Key Distribution in Practice. *Sci. Rep.* **2019**, *9*, 3080. [CrossRef]
46. Cui, C.; Yin, Z.Q.; Wang, R.; Chen, W.; Wang, S.; Guo, G.C.; Han, Z.F. Twin-Field Quantum Key Distribution without Phase Postselection. *Phys. Rev. Appl.* **2019**, *11*, 034053. [CrossRef]
47. Wang, R.; Yin, Z.Q.; Lu, F.Y.; Wang, S.; Chen, W.; Zhang, C.M.; Huang, W.; Xu, B.J.; Guo, G.C.; Han, Z.F. Optimized Protocol for Twin-Field Quantum Key Distribution. *Commun. Phys.* **2020**, *3*, 1–7. [CrossRef]
48. Zeng, P.; Zhou, H.; Wu, W.; Ma, X. Mode-Pairing Quantum Key Distribution. *Nat. Commun.* **2022**, *13*, 3903. [CrossRef]

49. Li, X.J.; Wang, M.; Pan, X.B.; Zhang, Y.R.; Long, G.L. One-Photon-Interference Quantum Secure Direct Communication. *Entropy* **2024**, *26*, 811. [CrossRef]
50. Long, G.L.; Zhang, H. Drastic Increase of Channel Capacity in Quantum Secure Direct Communication Using Masking. *Sci. Bull.* **2021**, *66*, 1267–1269. [CrossRef]
51. Csiszar, I.; Korner, J. Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
52. 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]
53. Weier, H.; Krauss, H.; Rau, M.; Fürst, M.; Nauerth, S.; Weinfurter, H. Quantum Eavesdropping without Interception: An Attack Exploiting the Dead Time of Single-Photon Detectors. *New J. Phys.* **2011**, *13*, 073024. [CrossRef]
54. 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]
55. Scarani, V.; Renner, R. Security Bounds for Quantum Cryptography with Finite Resources. In *Theory of Quantum Computation, Communication, and Cryptography*; Kawano, Y., Mosca, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 83–95.
56. Li, H.W.; Zhao, Y.B.; Yin, Z.Q.; Wang, S.; Han, Z.F.; Bao, W.S.; Guo, G.C. Security of Decoy States QKD with Finite Resources against Collective Attacks. *Opt. Commun.* **2009**, *282*, 4162–4166. [CrossRef]
57. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight Finite-Key Analysis for Quantum Cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef]
58. Wu, J.; Long, G.L.; Hayashi, M. Quantum Secure Direct Communication with Private Dense Coding Using a General Preshared Quantum State. *Phys. Rev. Appl.* **2022**, *17*, 064011. [CrossRef]
59. Sun, Z.Z.; Pan, D.; Cheng, Y.B.; Liu, Y.C.; Ruan, D.; Long, G.L. Multi-Intensity Quantum Secure Direct Communication Relying on Finite Block-Length. *IEEE Trans. Commun.* **2024**, *72*, 4633–4647. [CrossRef]
60. Du, H.; Paraiso, T.K.; Pittaluga, M.; Lo, Y.S.; Dolphin, J.A.; Shields, A.J. Twin-Field Quantum Key Distribution with Optical Injection Locking and Phase Encoding on-Chip. *Optica* **2024**, *11*, 1385–1390. [CrossRef]
61. Peng, Q.; Chen, J.P.; Xing, T.; Wang, D.; Wang, Y.; Liu, Y.; Huang, A. Practical Security of Twin-Field Quantum Key Distribution with Optical Phase-Locked Loop under Wavelength-Switching Attack. *npj Quantum Inf.* **2025**, *11*, 7. [CrossRef]
62. Hao, H.; Zhao, Q.Y.; Huang, Y.H.; Deng, J.; Yang, F.; Ru, S.Y.; Liu, Z.; Wan, C.; Liu, H.; Li, Z.J.; et al. A Compact Multi-Pixel Superconducting Nanowire Single-Photon Detector Array Supporting Gigabit Space-to-Ground Communications. *Light Sci. Appl.* **2024**, *13*, 25. [CrossRef]
63. Zou, K.; Hu, X. Fabrication Development of High-Performance Fractal Superconducting Nanowire Single-Photon Detectors. *IEEE J. Sel. Top. Quantum Electron.* **2024**, *31*, 3801410. [CrossRef]
64. Zhou, Y.; Yin, Z.Q.; Wang, R.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Twin-Field Quantum Key Distribution with Partial Phase Postselection. *Phys. Rev. Appl.* **2022**, *18*, 054026. [CrossRef]
65. Zhou, L.; Lin, J.; Jing, Y.; Yuan, Z. Twin-Field Quantum Key Distribution without Optical Frequency Dissemination. *Nat. Commun.* **2023**, *14*, 928. [CrossRef]
66. Zhong, X.; Wang, W.; Qian, L.; Lo, H.K. Proof-of-Principle Experimental Demonstration of Twin-Field Quantum Key Distribution over Optical Channels with Asymmetric Losses. *npj Quantum Inf.* **2021**, *7*, 8. [CrossRef]
67. Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Wang, R.Q.; Ye, P.; Zhou, Y.; Fan-Yuan, G.J.; Wang, F.X.; Chen, W.; et al. Twin-Field Quantum Key Distribution over 830-Km Fibre. *Nat. Photonics* **2022**, *16*, 154–161. [CrossRef]
68. Clivati, C.; Meda, A.; Donadello, S.; Virzì, S.; Genovese, M.; Levi, F.; Mura, A.; Pittaluga, M.; Yuan, Z.; Shields, A.J.; et al. Coherent Phase Transfer for Real-World Twin-Field Quantum Key Distribution. *Nat. Commun.* **2022**, *13*, 157. [CrossRef] [PubMed]
69. Renner, R. Symmetry of Large Physical Systems Implies Independence of Subsystems. *Nat. Phys.* **2007**, *3*, 645–649. [CrossRef]
70. Holevo, A.S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **1973**, *9*, 3–11.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.