algorithms

MDPI

Article

Asymmetric Sending-or-Not-Sending Twin-Field Quantum Key Distribution

Liliana Zisu [1,*], Ciprian Răcuciu [1,2], Nicu Bizon [3], Andrei Laurențiu Savu [1], Carmen Oprina [1] and Nicolae Nebancea [1]

[1] Doctoral School of Defence and Security Systems Engineering, "Ferdinand I" Military Technical Academy, 39–49 George Coșbuc Blvd., 050141 Bucharest, Romania; ciprian.racuciu@mta.ro (C.R.); andrei.savu@mta.ro (A.L.S.); carmen.oprina@mta.ro (C.O.); nicolae.nebancea@mta.ro (N.N.)
[2] Faculty of Informatics, "Titu Maiorescu" University, 22 Dâmbovnicului, 040441 Bucharest, Romania; ciprian.racuciu@prof.utm.ro
[3] Faculty of Electronics, Communications and Computers, Pitești University Centre, National University of Science and Technology POLITEHNICA Bucharest, 1 Targul din Vale Street, 110040 Pitești, Romania; nicu.bizon1402@upb.ro
* Correspondence: liliana.zisu@mta.ro

Abstract

We propose an improved protocol that combines the code-bit option $[z]$ of the Universal SNS framework with asymmetric sending probabilities across odd-indexed and even-indexed time windows. This approach increases the fraction of single-sided events that contribute to the raw key, while the $[z]$ option ensures that all heralded events involving the signal and vacuum intensities are retained as code bits. Numerical simulations demonstrate that the proposed protocol significantly outperforms both the SNS protocol with actively odd-parity pairing (SNS-AOPP) and the Universal SNS protocol with the $[x, y, z]$ option. At a secret key rate of 1 kbps, the proposed protocol extends the maximum secure distance by 103.7 km compared to SNS-AOPP. The key rate improvement reaches more than a factor of 11 over the entire distance range, and this result shows that the combination of the $[z]$ option with asymmetric sending probabilities provides a simple yet effective means of enhancing the performance of SNS-TF-QKD without requiring changes to the quantum hardware.

Keywords: quantum key distribution; phase-matching; sending-or-not-sending; secret key rate; decoy-state; AOPP

Check for updates

Academic Editors: Dunhui Xiao and Frank Werner

Received: 24 May 2026
Revised: 22 September 2026
Accepted: 5 October 2026
Published: 9 October 2026

Copyright: © 2026 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.

1. Introduction

The greatest challenge for Quantum Key Distribution (QKD) remains distance. Current state-of-the-art research is focused on developing quantum repeaters capable of restoring the quantum state without measuring it by using entanglement swapping, thereby enabling QKD communication on a continental or even intercontinental level. Although the main theoretical advantage lies in the fact that communication distance is, in principle, unlimited, the major drawback is the high level of technical complexity involved, which requires operation at temperatures close to absolute zero.

Another solution would be to divide the transmission distance into short segments of approximately 100 km, installing a trusted node at each segment, namely a secured point equipped with QKD infrastructure. Since each segment is short, optical losses remain low, making it possible to achieve key rates of hundreds of kbps or even Mbps per segment, with excellent performance over large total distances. The major trade-off is that security is no longer purely quantum over the entire transmission path, since the intermediate nodes must

be fully trusted, and the compromise of any one of them may affect the security of the entire network. Therefore, for national infrastructures, long-distance protocols remain the most viable solution over pure fiber-optic links, providing end-to-end security without trusted nodes. Their optimization, in terms of key rate, distance, and security, will contribute to the rapid development of resilient and scalable quantum infrastructures.

2. Methodology

2.1. Advances in QKD Transmission Distance

The evolution of QKD protocols has represented a continuous race against the exponential attenuation of optical fiber.

Initially, distance was severely limited by channel losses (η). The protocol BB84(1984) [1] was first demonstrated over 32 cm in a laboratory free-space environment [2], subsequently reaching operational limits of approximately 50–100 km through successive optimizations. Decoy-state QKD (2005) [3] further extended the achievable transmission distance to approximately 150–200 km by employing multiple pulse intensity levels, thereby enabling the detection and mitigation of photon-number-splitting (PNS) attacks. A major advance in both security and distance was achieved by Measurement-Device-Independent Quantum Key Distribution protocols (MDI-QKD), proposed in 2012 [4–9], through the elimination of detector-side vulnerabilities. MDI-QKD transfers the measurement process complexity to a potentially untrusted central node, commonly referred to as Charlie, thereby enabling transmission distances of approximately 300–400 km. Unlike previous protocols, whose key rates decrease linearly with transmittance ($R \sim \eta$), TF-QKD protocols (2018) [10–12], which rely on single-photon interference, allow the key rate to scale with the square root of transmittance ($R \sim \sqrt{\eta}$). This has led to a significant extension of the maximum secure distribution distance, with Liu et al. [13] reporting a distance record of 1002 km in ultra-low-loss optical fiber.

The improvements introduced, therefore, consist of the transition from InGaAs detectors, characterized by relatively high dark-count noise, typically in the range of 1–10 kHz, to SNSPDs, whose noise is extremely low, below 10 Hz; the adoption of the Twin-Field architecture and usage of fiber optics with ultra-low losses (pure silica core, G.654, LWPF, HCF, etc.) have reduced standard attenuation from 0.20 dB/km to 0.14–0.16 dB/km.

2.2. The SNS-TF-QKD Protocol: Background and Preliminaries

Twin-Field Quantum Key Distribution (TF-QKD) was proposed by Lucamarini et al. in 2018 [10] and it has been shown theoretically and subsequently experimentally that it achieves secretkey rates beyond the PLOB bound [14], which was previously considered a fundamental limit for quantum communication without repeaters. Since then, several TF-QKD variants have been introduced [11,12,15–20], and numerous experimental demonstrations have been reported [21–30]. Within this family of protocols, the sending-or-not-sending (SNS) protocol provides Measurement-Device-Independent (MDI) security against coherent attacks and has a large tolerance to phase misalignment. Therefore, the SNS protocol has been extensively studied both theoretically [31–37] and experimentally [21,22,25–28]. The actively odd parity pairing (AOPP) method can further enhance the key rate and extend the maximum secure transmission distance. The long-distance performance of the SNS protocol has been demonstrated, with a finite-key analysis achieving a secret key rate of 8.75×10^{-12} bits per pulse at 952 km [13].

Structurally, the SNS-TF-QKD protocol involves the following steps:

1. At any time window i, Alice (Bob) independently determines whether it is a decoy window or a signal window. If it is a decoy window, Alice (Bob) sends out to Charlie a decoy pulse in the coherent state $\left|\sqrt{\mu_d}e^{i\delta_A+i\gamma_A}\right\rangle$ ($\left|\sqrt{\mu_d}e^{i\delta_B+i\gamma_B}\right\rangle$). In each decoy window,

μ_d can vary randomly among several values. If it is a signal window, Alice (Bob) prepares a coherent state $\left|\sqrt{\mu_s}e^{i\delta_A+i\gamma_A}\right\rangle$ ($\left|\sqrt{\mu_s}e^{i\delta_B+i\gamma_B}\right\rangle$) with probability ϵ and sends it to Charlie or chooses not to send anything with a probability of $1-\epsilon$, where μ_d and μ_s represent the photon intensities of the decoy state and the signal state, respectively; δ_A and δ_B are the private random phase and γ_A and γ_B are the channel phase offsets.

2. After receiving the states sent by Alice and Bob, Charlie publicly announces the outcomes of all effective detection events. An event is regarded as effective in either of the following two situations: (1) Both parties have chosen a signal window and one of them has sent a signal pulse, while the other has decided not to send one, and Charlie records a single click in detector D_+ (respectively D_-) (2) Both parties have chosen a decoy window and prepared coherent states of the same intensity, and in this window their randomly selected phases δ_A and δ_B satisfy:

$$1 - |cos(\delta_A - \delta_B| \leq |\lambda| \tag{1}$$

corresponding to Charlie announcing a single click in detector D_+ (D_-). The value λ is determined by the size of phase slice chosen by Alice and Bob [38].

3. Alice and Bob publicly disclose their window choices (signal or decoy). They also announce the intensities of the pulses prepared in the decoy windows together with the random phase values δ_A and δ_B that each of them has used. These announcements allow them to classify the data and to estimate the parameters required by the secret key rate formula.

A Z-window is defined as a time window in which both Alice and Bob have selected the signal window. States prepared in Z-windows are referred to as Z-basis states, or simply Z-pairs, and effective events on this basis are denoted as Z-bits. Z_1-windows are Z-windows where exactly one party sends a single-photon state, resulting in either $|(01\rangle)$ or $|(10\rangle)$. These generate Z_1-pairs and form the Z_1-bits.

An X-window is defined by three conditions: (i) both parties select a decoy window, (ii) they choose the same coherent-state intensity, and (iii) their random phases δ_A and δ_B satisfy Equation (1). States from X-windows are called X-pairs, and the resulting bits are X-bits. X_1-windows are X-windows containing a two-mode single-photon state described by $|(\psi_1\rangle)\langle(\psi_1|)$ and $|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(e^{i(\delta_B+\gamma_B)}|01\rangle + e^{i(\delta_A+\gamma_A)}|10\rangle\right)$. These correspond to X_1-pairs and produce X_1-bits.

4. Alice and Bob randomly select a subset of Z-bits to perform error testing, which allows them to estimate the bit error rate in the Z-basis, E_Z. The test bits are subsequently discarded, and the remaining Z-bits are processed to distill the final key.
5. The secret key rate of the SNS protocol [11,31,39] is expressed as:

$$R = 2\epsilon(1-\epsilon)\mu_s e^{\mu_s} s_1^L\left[1 - H\left(e_1^U\right)\right] - fS_Z H(E_Z) \tag{2}$$

where ϵ represents the probability that Alice (Bob) transmits a signal state in a signal window, s_1^L and e_1^U are the lower bound of the count rate and the upper bound of the phase error rate of single-photon events in the Z-windows, S_Z is the count rate of Z-windows, E_Z represents the bit error rate of the signal, $H(x) = -xlog_2x - (1-x)log_2(1-x)$ is the binary Shannon entropy function, and f is the error correction efficiency.

In the asymptotic regime, s_1^L and e_1^U for the three-intensity decoy-state method (with intensities $\mu_0 = 0 < \mu_1 < \mu_2$) are given by [39]:

$$s_1 \geq s_1^L = \frac{p_2^L(\mu_2)\left[S_{\mu_1} - p_0^U(\mu_1)S_{\mu_0}\right] - p_2^U(\mu_1)\left[S_{\mu_2} - p_0^L(\mu_2)S_{\mu_0}\right]}{p_2^U(\mu_2)p_1^U(\mu_1) - p_2^L(\mu_1)p_1^L(\mu_2)} \tag{3}$$

$$e_1 \leq e_1^U = \frac{S_{\mu_1}E_{\mu_1} - p_0^L(\mu_1)S_{\mu_0}E_{\mu_0}}{p_1^L(\mu_1)s_1^L} \tag{4}$$

The probabilities $p_0^{L(U)}(\mu_i), p_1^{L(U)}(\mu_i), and p_2^{L(U)}(\mu_i)$ for $i = 0, 1, 2$ can be directly calculated [39] as follows:

$$p_0^{L(U)}(\mu_i) = P_{0,A}^{L(U)}(\mu_i)P_{0,B}^{L(U)}(\mu_i) \tag{5}$$

$$p_1^{L(U)}(\mu_i) = P_{0,A}^{L(U)}(\mu_i)P_{1,B}^{L(U)}(\mu_i) + P_{1,A}^{L(U)}(\mu_i)P_{0,B}^{L(U)}(\mu_i) \tag{6}$$

$$p_2^{L(U)}(\mu_i) = P_{0,A}^{L(U)}(\mu_i)P_{2,B}^{L(U)}(\mu_i) + P_{2,A}^{L(U)}(\mu_i)P_{0,B}^{L(U)}(\mu_i) + P_{1,A}^{L(U)}(\mu_i)P_{1,B}^{L(U)}(\mu_i) \tag{7}$$

3. Asymmetric SNS-TF-QKD Protocol

In the standard SNS protocol, Alice and Bob transmit signal pulses with an equal probability p. Under this symmetric setting, the probability of a single-sided event (where exactly one party transmits) is $2p(1-p)$, while the probabilities of send–send and vacuum–vacuum events are p^2 and $(1-p)^2$, respectively. In order to reduce send–send structural errors, the optimal sending probability in the original SNS is about 5% [40], which means that both parties transmit vacuum in 90% of all rounds, send–send events occur in only 0.25% of all time windows and only roughly 9.5% of rounds correspond to single-sided events that contribute to the raw key.

In contrast, employing asymmetric sending probabilities across different time windows increases the single-sided event probability. For instance, if in a given window Alice transmits with probability $p = 0.85$ and Bob with probability $1 - p = 0.15$, the single-sided event probability increases to 0.745, while the send–send probability remains as low as 0.1275. Asymmetric sending probabilities thus offer a simple yet effective way to increase the single-sided event fraction and enhance the raw key rate.

Under the $[z]$ option of the Universal SNS-TF-QKD protocol [41], all heralded events involving intensity μ_z or vacuum μ_v are used as code bits. Unlike the standard SNS protocol, which limits code bits to single-sided events (zv, vz), this approach also includes double-sided events, send–send (zz) and vacuum–vacuum (vv), while their inherent errors are corrected during post-processing.

Although the Universal SNS-TF-QKD protocol provides three code-bit options, the $[z]$ option is selected to simplify post-processing, with the reduction in the raw key rate being compensated by employing asymmetric sending probabilities. Consequently, the scheme we propose relies on two core strategies: asymmetric sending probabilities across odd-indexed and even-indexed time widows and the inclusion of double-sided events in the raw key generation under the [z] option of the Universal SNS-TF-QKD protocol.

The notation adopted in this work aligns with the Universal SNS-TF-QKD protocol framework and is defined as follows:

Heralded time window: A time window in which one, and only one, detector clicks at Charlie's measurement station, as announced by Charlie.

Heralded event: The event produced in a heralded time window.

Null time window: The time window when neither of Charlie's detectors click or both of them click.

The intensities used by Alice and Bob: Vacuum $\mu_v = 0$, μ_x, μ_y, and μ_z. They are chosen with probabilities p_v, p_x, p_y, and p_z, respectively.

lr-event or *lr*-window: An event or a time window when Alice sends out a pulse of intensity μ_l while Bob sends out μ_r, with $l,r \in \{x,y,z\}$.

N_{lr}: The number of *lr*-windows.

n_{lr}: The number of heralded *lr*-windows.

N_t: The total number of time windows in the protocol.

$\langle M \rangle$: The expected value of the quantity M.

Encoding: Alice (Bob) regards all heralded windows when she (he) uses intensity μ_v as a bit a value 0 (1) and those when she (he) uses intensity μ_z as a bit value 1 (0). A code bit from a heralded time window is a *wrong bit* when both of them have decided to send out non-vacuum pulses or both of them have decided to send out vacuums. A code bit from a heralded time window is a *right bit* when exactly one of Alice and Bob has decided to send out a non-vacuum pulse. An *untagged window* is a heralded time window *lv* or *vr* with $l, r \in \{z\}$, in which a single photon is actually sent by Alice or Bob. The bits from these untagged windows are defined as *untagged bits*. All untagged bits are right bits.

3.1. Description of the Proposed Protocol

We refer to the proposed protocol as the Asymmetric [z]-SNS-AOPP protocol. Its operational steps are detailed below.

1. Preparation and quantum transmission
   - Window selection: For each round i, Alice (Bob) selects between a signal window and a decoy window with probability p_s and 1- p_s.
     - If the signal window is selected, the time window is determined by the index i:
       - ➢ If i is odd, in the odd-indexed window, Alice sends a coherent state $\left|\sqrt{\mu_A} e^{i(\pi K_A + \frac{2\pi}{M} d_A)}\right\rangle$ with probability $p_{high} > 0.5$ while Bob sends a coherent state $\left|\sqrt{\mu_B} e^{i(\pi K_B + \frac{2\pi}{M} d_B)}\right\rangle$ with probability $p_{low} = 1 - p_{high}$.
       - ➢ Conversely, if i is even, in the even-indexed window, Bob sends a coherent state $\left|\sqrt{\mu_B} e^{i(\pi K_B + \frac{2\pi}{M} d_B)}\right\rangle$ with probability p_{high}, while Alice sends a coherent state with probability $p_{low} = 1 - p_{high}$.
       The intensity is $\mu_A(\mu_B) = \mu_Z$, where μ_Z is the signal state, the random key bit $K_A(K_B)\ \epsilon\ \{0, 1\}$, the discrete phase randomization number $d_A(d_B)$ is randomly chosen from $\{0, 1, 2, \cdots, M - 1\}$, and M is the number of maximum discrete phase that is modulated by Alice (Bob).
       The odd-indexed and even-indexed windows are separated by a fixed interval of 200–500 ps.
       Following the time window assignment, Alice and Bob independently make a send/not-send decision according to their respective probabilities.
     - If the decoy window is selected, Alice (Bob) prepares a coherent state $\left|\sqrt{\nu_A} e^{i(\pi K_A + \frac{2\pi}{M} d_A)}\right\rangle \left(\sqrt{\nu_B} e^{i(\pi K_B + \frac{2\pi}{M} d_B)}\right\rangle$, $\nu_A(\nu_B)\ \epsilon\ \{\mu_x, \mu_y, \mu_v\}$, and sends it to Charlie, where μ_x, μ_y are the decoy states and μ_v is the vacuum state.
       The intensities μ_x, μ_y, μ_v are selected with probabilities p_x,p_y and $p_z = 1 - p_x - p_y$, respectively.

2. Classical communication and data post-processing

All post-processing steps described below are performed separately for the two subsets of time windows defined by index parity, denoted $s \in \{O, E\}$, corresponding to odd-indexed and even-indexed windows, respectively.

(a) Announcement and code-bit selection
   - Charlie publicly announces which time windows are heralded and which are null.
   - Alice and Bob each publicly announce every time window in which they used intensity μ_x or μ_y, as well as the intensities used for null windows.
   - They retain as code bits only those heralded lr-windows with $l, r \in \{z, v\}$.

This yields ${n_t}^{(s)}$ code bits for subset s:

$$n_t^{(s)} = \sum_{l,r\in\{z,v\}} n_{lr}^{(s)} = n_{zz}^{(s)} + n_{zv}^{(s)} + n_{vz}^{(s)} + n_{vv}^{(s)} \tag{8}$$

The corresponding QBER of subset s is:

$$E_t^{(s)} = \frac{{n_{vv}}^{(s)} + {n_{zz}}^{(s)}}{{n_t}^{(s)}} \tag{9}$$

(b) Post-selection with AOPP

For each subset $s \in \{O, E\}$, Alice creates $n_{\text{odd}}^{(s)} = \min\left(n_1^{A,\,(s)},\, n_0^{A,\,(s)}\right)$ odd-parity pairs of that subset, where $n_1^{A,\,(s)}$ $\left(n_0^{A,\,(s)}\right)$ denotes the number of code bits for which Alice's bit value is 1 (0). If $n_1^{A,\,(s)} \geq n_0^{A,\,(s)}$, she randomly chooses $n_{\text{odd}}^{(s)} = n_0^{A,\,(s)}$ bits from those $n_1^{A,\,(s)}$ bits (with bit value 1) and then makes $n_{\text{odd}}^{(s)}$ random odd-parity pairs. If $n_1^{A,\,(s)} < n_0^{A,\,(s)}$, she randomly chooses $n_{\text{odd}}^{(s)} = n_1^{A,\,(s)}$ bits from those $n_0^{A,\,(s)}$ bits (with bit value 0) and then makes $n_{\text{odd}}^{(s)}$ random odd-parity pairs. She announces the positions of each pair, and Bob performs the parity check. Among these $n_{\text{odd}}^{(s)}$ pairs, $n_t^{\prime(s)}$ of them have odd parity at Bob's side and these $n_t^{\prime(s)}$ pairs will pass the parity check by Bob. Only two kinds of pairs can pass the parity check: a pair containing two bit-flip errors or a pair containing no bit-flip error. A pair with no bit-flip error is called a right pair. Also, a right pair will produce a right bit.

(c) Error correction

- They run error correction on the $n_t^{\prime(s)}$ code bits that survived AOPP.
- In doing the error test for the bit-flip error correction, they randomly take a small fraction δ of time windows of subset s to test the QBER. They have to discard the events of these time windows. Since they can verify faithfully the fact of zero error after error correction, $\delta = 0$ is used in the calculations.
- Alice announces the positions of all $n_E^{\prime(s)}$ bit-flip errors and the intensities used in those positions. The numbers of wrong bits and right bits are $n_E^{\prime(s)}$ and $n_R^{\prime(s)} = n_t^{\prime(s)} - n_E^{\prime(s)}$, respectively.
- For the decoy analysis, they announce the intensities used in the heralded time windows of subset s, except the $2n_R^{\prime(s)}$ bit positions belonging to the $n_R^{\prime(s)}$ right pairs.

(d) Lower bounds on $\langle n_{10}\rangle^{(s)}$ and $\langle n_{01}\rangle^{(s)}$

For each subset $s \in \{O, E\}$, knowing all time windows of vv, xv, and yv (and vv, vx, and vy), Alice (Bob) can verify the lower bound of $\langle n_{10}\rangle^{(s)}$ $\left(\langle n_{01}\rangle^{(s)}\right)$, which is the expected value of the number of untagged windows when she (he) sends out single-photon pulses. They publicly announce these bounds:

$$\langle n_{10}\rangle^{(s)} = {N_{zv}}^{(s)} e^{-\mu_z} \mu_z \langle s_{10}\rangle^{(s)} \tag{10}$$

$$\langle n_{01}\rangle^{(s)} = {N_{vz}}^{(s)} e^{-\mu_z} \mu_z \langle s_{01}\rangle^{(s)} \tag{11}$$

(e) Phase-error estimation from xx windows

For each subset $s \in \{O, E\}$, Alice and Bob publicly announce the phases of all heralded xx windows. Those xx windows with the phase slice $(\theta_A - \theta_B)$ of states $\left|\sqrt{\mu_A} e^{i\theta_A}\right\rangle \left|\sqrt{\mu_B} e^{i\theta_B}\right\rangle$ (with $\theta_A = \pi K_A + \frac{2\pi}{M} d_A$ and $\theta_B = \pi K_B + \frac{2\pi}{M} d_B$) satisfying the phase-slice condition

$$1 - |cos(\theta_A - \theta_B)| \leq \lambda, \tag{12}$$

will be used to verify the lower bound of $e_1^{ph,(s)}$; the phase-flip error rate of untagged bits in the decoy-state analysis; and also $e_1^{\prime ph,(s)}$, the phase-flip error rate after AOPP, using the iterative formulas in reference [36]. Here, $\lambda > 0$ is a small parameter, close to zero, fixed from channel tests and calibration.

(f) Key length calculation

They lower-bound the value of n_1', i.e., the number of untagged bits that survive AOPP, by the method in reference [36] using the total number of code bits and untagged code bits before AOPP. In addition, they know all heralded xx-window events satisfying the phase-slice condition in Equation (12). With these, they upper-bound the non-asymptotic value of e_1^{ph} by decoy-state analysis, as well as $e_1'^{ph}$, the phase-flip error rate of the survived code bits after AOPP, using the iterative formulas in reference [36]. The public announcement of $\langle n_{10}\rangle^{(O)}$ and $\langle n_{01}\rangle^{(O)}$ ($\langle n_{10}\rangle^{(E)}$ and $\langle n_{01}\rangle^{(E)}$) introduces an information leakage $\Delta^{(O)}$ ($\Delta^{(E)}$).

For each $s \in \{O, E\}$, the final secret key length is therefore:

$$\tilde{n}'^{(s)} = n'^{(s)} - \Delta^{(s)} \tag{13}$$

with

$$n'^{(s)} = n_1'^{(s)}\left[1 - H\left(e_1'^{ph,(s)}\right)\right] - f n_t'^{(s)} H\left(E_t'^{(s)}\right) - 2\left(log_2\frac{2}{\varepsilon_{cor}} - 2log_2\frac{1}{\sqrt{2}\varepsilon_{PA}\hat{\varepsilon}}\right) \tag{14}$$

where

$n_1'^{(s)}$ is the number of untagged bits after AOPP, $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy function, $e_1'^{ph,(s)}$ is the phase-flip error rate of the untagged code bits after AOPP, f is the error correction inefficiency, $n_t'^{(s)}$ is the number of survived code bits after AOPP, $E_t'^{(s)}$ is the quantum bit-flip error rate (QBER) after AOPP, ε_{cor} is the failure probability of error correction, ε_{PA} is the failure probability of privacy amplification, $\hat{\varepsilon}$ is the coefficient while using the chain rules of max- and min-entropy [32], and $\Delta^{(s)}$ is the additional information leakage of the final key due to classical communication in step (c) above.

3.2. Decoy-State Analysis

The decoy-state analysis follows the same procedure as in the Universal SNS-TF-QKD protocol [41], applied separately to each subset $s \in \{O, E\}$.

The single-photon yields $\langle s_{10}\rangle^{(s)}$ and $\langle s_{01}\rangle^{(s)}$ and the phase-flip error rate $\left\langle e_1^{ph}\right\rangle^{(s)}$ are estimated as follows:

$$\langle s_{10}\rangle^{(s)} \geq \langle s_{10}\rangle^{L,(s)} = \frac{e^{\mu_x}\mu_y^2\langle S_{xv}\rangle^{(s)} - e^{\mu_y}\mu_x^2\langle S_{yv}\rangle^{(s)} - \left(\mu_y^2 - \mu_x^2\right)\langle S_{vv}\rangle^{(s)}}{\mu_x\mu_y\left(\mu_y - \mu_x\right)}, \tag{15}$$

$$\langle s_{01}\rangle^{(s)} \geq \langle s_{01}\rangle^{L,(s)} = \frac{e^{\mu_x}\mu_y^2\langle S_{vx}\rangle^{(s)} - e^{\mu_y}\mu_x^2\langle S_{vy}\rangle^{(s)} - \left(\mu_y^2 - \mu_x^2\right)\langle S_{vv}\rangle^{(s)}}{\mu_x\mu_y\left(\mu_y - \mu_x\right)}, \tag{16}$$

$$\left\langle e_1^{ph}\right\rangle^{(s)} \leq \left\langle e_1^{ph}\right\rangle^{U,(s)} = \frac{\langle T_X\rangle^{(s)} - e^{-2\mu_x}\langle S_{vv}\rangle^{(s)}/2}{2\mu_x e^{-2\mu_x}\langle s_1\rangle^{(s)}} \tag{17}$$

where $\langle s_{10}\rangle^{(s)}\left(\langle s_{01}\rangle^{(s)}\right)$ represents the expected value of the counting rate of the time window when Alice (Bob) sends out a single-photon pulse and Bob (Alice) sends out vacuum, $\langle S_{lr}\rangle^{(s)}$ is the expected value of the counting rate of lr-windows, $\langle s_1\rangle^{(s)} = \left(\langle s_{10}\rangle^{(s)} + \langle s_{01}\rangle^{(s)}\right)/2$ is the expected value of the counting rate of all single-photon events for each subset s, and $\langle T_X\rangle^{(s)}$ is the expected value of the error counting rate of xx windows which satisfy the phase-slice condition in Equation (12). The observed values of $n_{vv}^{(s)}$ and $n_{zv}^{(s)}\left(n_{vz}^{(s)}\right)$ are available to Alice (Bob) from classical communications. They can therefore use these directly as input values in Equations (15)–(17), e.g., $S_{vv}^{(s)} = {}^{n_{vv}^{(s)}}/_{N_{vv}^{(s)}}$ and $S_{zv}^{(s)} = {}^{n_{zv}^{(s)}}/_{N_{zv}^{(s)}}$ $\left(S_{vz}^{(s)} = {}^{n_{vz}^{(s)}}/_{N_{vz}^{(s)}}\right)$. Consequently, when performing the decoy-state analysis after error correction, they do not need to reserve any time windows of type vv, zv, or vz as random samples to estimate

the observed values of $S_{vv}^{(s)}, S_{zv}^{(s)}$, and $S_{vz}^{(s)}$. The bound of $\langle S_{lr} \rangle$ can be calculated from the observed value S_{lr} by the Chernoff bound [38] for each subset s. Using the lower bound on $\langle s_{10} \rangle^{(s)}$ and $\langle s_{01} \rangle^{(s)}$ obtained above, Alice and Bob can compute the bound on $\langle n_{10} \rangle^{(s)}$ and $\langle n_{01} \rangle^{(s)}$ as given in Equations (10) and (11). After announcing these bounds, they can calculate $\langle n_1 \rangle^{(s)} = \langle n_{10} \rangle^{(s)} + \langle n_{01} \rangle^{(s)}$ and then obtain $n_1^{(s)}$ by applying the Chernoff bound again. The global bounds are then obtained by aggregating the contributions from both subsets: $\langle n_1 \rangle = \langle n_1 \rangle^{(O)} + \langle n_1 \rangle^{(E)}$.

The announcement of $\langle n_{10} \rangle^{(s)}$ and $\langle n_{01} \rangle^{(s)}$ may leak information about the confidential quantities related to the number of bits with value 1. Nevertheless, a secure key can still be obtained by deducting an amount δ from the final key length [42], with

$$\Delta^{(s)} \leq 2log_2\left(n_t{}^{(s)} - n_{vv}^{(s)} - \sum_{l',r' \in z} n_{lrr'}^{(s)}\right) \tag{18}$$

4. Security Analysis

4.1. Asymmetric Sending Probabilities

We consider a virtual entanglement-based protocol that is equivalent to the real protocol from Eve's perspective. In this virtual protocol, each user's decision to send or not send is represented by a virtual qubit:

$$\left|\Psi_{\mathbf{A}}\right\rangle = \sqrt{p_{\mathbf{A}}}|1\rangle_{\mathbf{A}}\,|\boldsymbol{\alpha}\rangle_{\mathbf{A}} + \sqrt{1-p_{\mathbf{A}}}|0\rangle_{\mathbf{A}}|0\rangle_{\mathbf{A}} \tag{19}$$

$$\left|\Psi_{\mathbf{B}}\right\rangle = \sqrt{p_{\mathbf{B}}}|1\rangle_{\mathbf{B}}\,|\boldsymbol{\alpha}\rangle_{\mathbf{B}} + \sqrt{1-p_{\mathbf{A}}}|0\rangle_{\mathbf{B}}|0\rangle_{\mathbf{B}} \tag{20}$$

where $|(0\rangle)$ and $|(1\rangle)$ denote the send and not-send decisions, respectively, and $|(\alpha\rangle)$ is the coherent state.

The single-photon states for the odd-indexed and even-indexed windows are:

$$\left|\boldsymbol{\psi}_1^{\mathbf{odd}}\right\rangle = \frac{\sqrt{p_{\mathbf{A}}(1-p_{\mathbf{B}})}}{\sqrt{N}}|10\rangle + \frac{\sqrt{(1-p_{\mathbf{A}})p_{\mathbf{B}}}}{\sqrt{N}}|01\rangle \tag{21}$$

$$\left|\boldsymbol{\psi}_1^{\mathbf{even}}\right\rangle = \frac{\sqrt{(1-p_{\mathbf{A}})p_{\mathbf{B}}}}{\sqrt{N}}|10\rangle + \frac{\sqrt{p_{\mathbf{A}}(1-p_{\mathbf{B}})}}{\sqrt{N}}|01\rangle \tag{22}$$

where:

$$N = p_{\mathbf{high}}^2 + p_{\mathbf{low}}^2 = p_{\mathbf{high}}^2 + \left(1-p_{\mathbf{high}}\right)^2 \tag{23}$$

In the $\{|(+\rangle),|(-\rangle)\}$ basis, with

$$|+\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{24}$$

and

$$|-\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}} \tag{25}$$

Equations (21) and (22) become:

$$\left|\boldsymbol{\psi}_1^{\mathbf{odd}}\right\rangle = \frac{p_{\mathbf{high}}}{\sqrt{N}}\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \frac{\left(1-p_{\mathbf{high}}\right)}{\sqrt{N}}\left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right) \tag{26}$$

$$\left|\boldsymbol{\psi}_1^{\mathbf{odd}}\right\rangle = \frac{1}{\sqrt{2N}}\left[|+\rangle + \left(2p_{\mathbf{high}}-1\right)|-\rangle\right] \tag{27}$$

$$\left|\boldsymbol{\psi}_1^{\mathbf{even}}\right\rangle = \frac{\left(1-p_{\mathbf{high}}\right)}{\sqrt{N}}\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \frac{p_{\mathbf{high}}}{\sqrt{N}}\left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right) \tag{28}$$

$$\left|\psi_1^{\text{even}}\right\rangle = \frac{1}{\sqrt{2N}}\left[|+\rangle - \left(2p_{\text{high}} - 1\right)|-\rangle\right] \tag{29}$$

Let $\mathcal{R}$ be the operator that exchanges the roles of Alice and Bob:

$$\mathcal{R}(|(a\rangle)_{\text{A}}|(b\rangle)_{\text{B}}) = |(b\rangle)_{\text{A}}|(a\rangle)_{\text{B}} \tag{30}$$

Applying $\boldsymbol{\mathcal{R}}$:

$$\boldsymbol{\mathcal{R}}\left|\psi_1^{\text{even}}\right\rangle = \frac{1}{\sqrt{2N}}\left(|+\rangle + \left(2p_{\text{high}} - 1\right)|-\rangle\right) = \left|\psi_1^{\text{odd}}\right\rangle \tag{31}$$

Since $\mathcal{R}$ is a classical relabeling operation that does not affect Eve's information, the security of the even window is identical to that of the odd window.

4.2. Subset-Based Security Analysis

The security analysis is performed separately for the odd-indexed and even-indexed time windows. For each subset $s \in \{O, E\}$, the QBER after AOPP $E_{\text{t}}^{\prime(s)}$ is determined as described in step (b), and the phase-flip error rate after AOPP $e_1^{\prime ph,(s)}$ is estimated from decoy-state analysis applied independently.

The global key length is then obtained by aggregating the contributions from both subsets:

$$\tilde{n}' = \sum_{s\in\{O,\,E\}} n'^{(s)} - \Delta^{(s)} \tag{32}$$

where $\Delta^{(s)}$ accounts for the information leakage from public announcements in subset s.

5. Simulation Results

The analysis was performed by comparison with the standard SNS protocol with AOPP. The parameters used in the numerical simulation (Table 1) reflect both the typical conditions of low-loss optical fiber and the effective performance of SNSPD detectors and post-quantum algorithms.

Table 1. Reference configuration for protocol simulation.

Category	Parameter	Value/Range
Quantum/optical channel	Fiber length (L)	100–800 km
	Fiber attenuation (α)	0.20 dB/km
	Transmittance (η)	$\eta_{det}\cdot 10^{-\alpha L/10}$
	Detection efficiency	$\eta_{det} = 0.50$
	Dark Count Rate	10^{-9}
	Misalignment error (e_d)	0.015
	Pulse repetition rate (f_clock)	1 GHz
Protocol	Signal intensity (μ_z)	0.4
	Decoy intensity (μ_x)	0.2
	Decoy intensity (μ_y)	0.05
	Vacuum intensity (μ_v)	0.0
	Number of phase slices (M)	16
Post-selection	Reconciliation efficiency factor (f)	1.1
	Block length (N)	10^{10} bits
Security	$\varepsilon_{\text{cor}} = \varepsilon_{\text{PA}} = \hat{\varepsilon}$	10^{-10}
Simulation	Platform	Python 3.11, numpy

The numerical simulation was carried out in the finite-key regime using four-intensity decoy-state analysis. The intensities used in the simulation are also summarized in Table 1.

The results obtained and presented in Table 2 demonstrate that the proposed protocol is superior to the SNS protocol with AOPP over the entire distance range, achieving a secret key rate more than 11 times higher, as illustrated in Figure 1.

Table 2. Secret key rates (in bits per pulse) of the simulated protocols.

Distance (km)	Secret Key Rate		Asymmetric [z]-SNS-AOPP vs. SNS-AOPP	
	Asymmetric [z]-SNS-AOPP	SNS-AOPP	Superior Protocol	Ratio
100	2.83×10^{-3}	2.56×10^{-4}	Asymmetric [z]-SNS-AOPP	11.1
200	2.83×10^{-4}	2.56×10^{-5}	Asymmetric [z]-SNS-AOPP	11.1
300	2.82×10^{-5}	2.52×10^{-6}	Asymmetric [z]-SNS-AOPP	11.2
400	2.78×10^{-6}	2.19×10^{-7}	Asymmetric [z]-SNS-AOPP	12.7
485	3.53×10^{-7}	0.0	Asymmetric [z]-SNS-AOPP	-

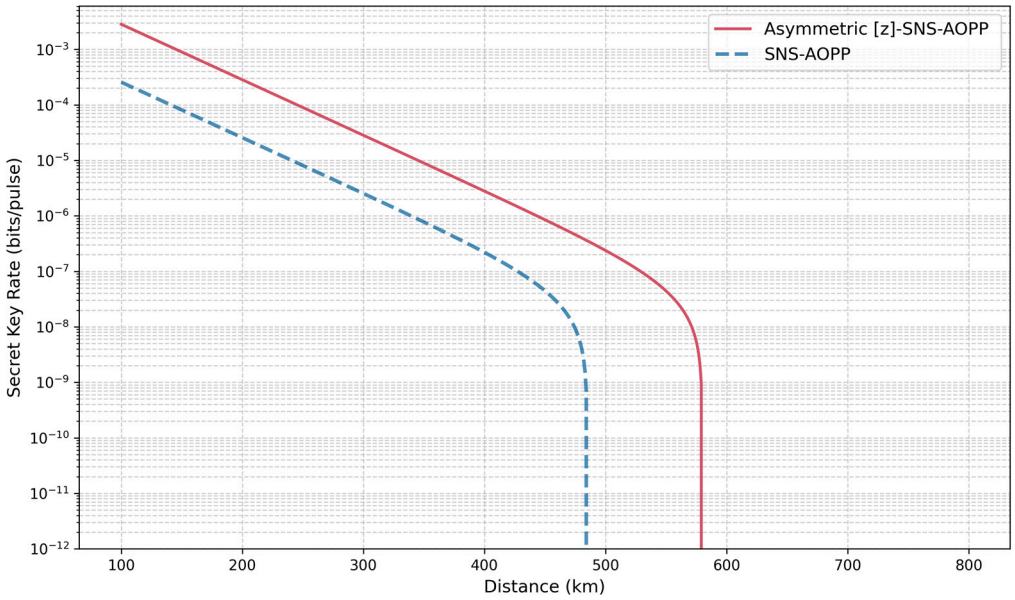


Figure 1. Secret key rate vs. transmission distance (km).

The results presented in Table 3 indicate that the Asymmetric [z] SNS-AOPP protocol is more robust and offers superior efficiency compared to SNS-AOPP.

At a secret key rate of 100 bps (Table 3), the Asymmetric [z] SNS-AOPP protocol reaches 528.8 km, extending the distance by 101.6 km relative to SNS-AOPP.

The largest distance gain is obtained at a secret key rate of 1 kbps: 103.7 km over SNS-AOPP.

The key rates of the proposed protocol reported in Table 4 are obtained without distance-dependent optimization of p_{high} and p_{low}. Even under this non-optimized configuration, the

proposed protocol achieves higher key rates than the Universal SNS universal with option $[x, y, z]$ at all tested distances (200–380 km), and the advantage grows with distance.

Table 3. Distance (km) at which a given secret key rate can be achieved.

Secret Key Rate	Asymmetric [z]-SNS-PM	SNS-AOPP	Superior Protocol	Gain
1 kbps	443.1	339.4	Asymmetric [z]-SNS-PM	103.7 km
100 bps	528.8	427.2	Asymmetric [z]-SNS-PM	101.6 km
1 bps	579.1	483.5	Asymmetric [z]-SNS-PM	95.6 km
0.1 bps	579.8	484.5	Asymmetric [z]-SNS-PM	95.3 km

Table 4. Key rate comparison between the proposed protocol and the Universal SNS with option $[x, y, z]$ ($N = 10^{10}$) at various transmission distances.

Protocol	200 km	300 km	350 km	380 km
Asymmetric $[z]$ SNS-AOPP	2.83×10^{-4}	2.82×10^{-5}	8.90×10^{-6}	4.44×10^{-6}
Universal SNS with option $[x, y, z]$	4.76×10^{-5}	2.95×10^{-6}	4.83×10^{-7}	8.12×10^{-8}

6. Conclusions

The proposed protocol extends the Universal SNS framework (option $[z]$) by introducing asymmetric probabilities, which increases the fraction of single-sided events contributing to the raw key. Our work demonstrates that a simple modification, asymmetric sending probabilities, can significantly enhance the performance of SNS-TF-QKD.

The security of the proposed protocol has been demonstrated in the finite-key regime within the composable security framework. The analysis covers all possible bias configurations, with the phase-flip error rate bounded by the worst case over the two subsets.

The proposed protocol can be implemented on existing SNS-TF-QKD setups by simply adjusting the sending probabilities, without requiring changes to the quantum hardware. This makes it a practical and cost-effective enhancement for real-world Quantum Key Distribution systems.

In the present work, the optical intensities are intentionally kept fixed for all considered protocols to ensure a fair and consistent comparison. Although a joint optimization of the sending probabilities and optical intensities may further improve the secret key rate, such an optimization is beyond the scope of this work and will be investigated in future research.

Author Contributions: Conceptualization, L.Z.; methodology, L.Z., C.R., and N.B.; software, L.Z., A.L.S., C.O., and N.N.; validation, A.L.S. and N.N.; formal analysis, L.Z.; investigation, L.Z.; resources, L.Z.; data curation, A.L.S. and L.Z.; writing—original draft preparation, L.Z.; writing—review and editing, L.Z., N.N., and A.L.S.; visualization, L.Z., N.N., A.L.S. and C.O.; supervision, C.R. and N.B.; project administration, C.R.; funding acquisition, N.B. All authors have read and agreed to the published version of the manuscript.

Funding: The article processing charge was covered by the National University of Science and Technology POLITEHNICA Bucharest, through the PubArt program.

Data Availability Statement: The data presented in this study are available within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

AOPP	Actively Odd-Parity Pairing
HCF	Hollow Core Fiber
LDPC	Low-Density Parity Check
LWPF	Low Water Peak Fiber
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
PLOB	Pirandola–Laurenza–Ottaviani–Banchi
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
SNSPD	Superconducting Nanowire Single-Photon Detector
SNS-TF-QKD	Sending-or-Not-Sending Twin-Field Quantum Key Distribution
TF-QKD	Twin-Field Quantum Key Distribution

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
3. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
4. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
5. Liu, Y.; Chen, T.Y.; Wang, L.J.; Liang, H.; Shentu, G.L.; Wang, J.; Cui, K.; Yin, H.L.; Liu, N.L.; Li, L. Experimental Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2013**, *111*, 130502. [CrossRef] [PubMed]
6. Da Silva, T.F.; Vitoreti, D.; Xavier, G.B.; Do Amaral, G.C.; Temporão, G.P.; Von Der Weid, J.P. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **2013**, *88*, 052303. [CrossRef]
7. Tang, Z.; Liao, Z.; Xu, F.; Qi, B.; Qian, L.; Lo, H.K. Experimental demonstration of polarization-encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2014**, *112*, 190503. [CrossRef] [PubMed]
8. Curty, M.; Xu, F.; Cui, W.; Lim, C.C.W.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 3732. [CrossRef] [PubMed]
9. Xu, F.; Xu, H.; Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052333. [CrossRef]
10. 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] [PubMed]
11. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
12. Ma, X.; Zeng, P.; Zhou, H. Phase-Matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
13. Liu, Y.; Zhang, W.J.; Jiang, C.; Chen, J.P.; Zhang, C.; Pan, W.X.; Ma, D.; Dong, H.; Xiong, J.M.; Zhang, C.J.; et al. Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber. *Phys. Rev. Lett.* **2023**, *130*, 210801. [CrossRef] [PubMed]
14. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef] [PubMed]
15. Tamaki, K.; Lo, H.-K.; Wang, W.; Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv* **2018**, arXiv:1805.05511.
16. 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]
17. Curty, M.; Azuma, K.; Lo, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Inf.* **2019**, *5*, 64. [CrossRef]
18. Lu, F.Y.; Yin, Z.Q.; Cui, C.H.; Fan-Yuan, G.J.; Wang, R.; Wang, S.; Chen, W.; He, D.Y.; Huang, W.; Xu, B.J.; et al. Improving the performance of Twin-Field Quantum Key Distribution. *Phys. Rev. A* **2019**, *100*, 022306. [CrossRef]
19. Currás-Lorenzo, G.; Navarrete, Á.; Azuma, K.; Kato, G.; Curty, M.; Razavi, M. Tight finite-key security for twin-field quantum key distribution. *npj Quantum Inf.* **2021**, *7*, 22. [CrossRef]

20. Maeda, K.; Sasaki, T.; Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat. Commun.* **2019**, *10*, 3140. [CrossRef] [PubMed]
21. Minder, M.; Pittaluga, M.; Roberts, G.L.; Lucamarini, M.; Dynes, J.F.; Yuan, Z.L.; Shields, A.J. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photon.* **2019**, *13*, 334–338. [CrossRef]
22. Liu, Y.; Yu, Z.W.; Zhang, W.; Guan, J.Y.; Chen, J.P.; Zhang, C.; Hu, X.L.; Li, H.; Jiang, C.; Lin, J.; et al. Experimental Twin-Field Quantum Key Distribution through Sending or. Not. Sending. *Phys. Rev. Lett.* **2019**, *123*, 100505. [CrossRef] [PubMed]
23. 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]
24. Zhong, X.; Hu, J.; Curty, M.; Qian, L.; Lo, H.-K. Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution. *Phys. Rev. Lett.* **2019**, *123*, 100506. [CrossRef] [PubMed]
25. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.Y.; Yu, Z.W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [CrossRef] [PubMed]
26. Liu, H.; Jiang, C.; Zhu, H.T.; Zou, M.; Yu, Z.W.; Hu, X.L.; Xu, H.; Ma, S.; Han, Z.; Chen, J.P.; et al. Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km. *Phys. Rev. Lett.* **2021**, *126*, 250502. [CrossRef] [PubMed]
27. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.J.; Han, Z.Y.; Ma, S.Z.; Hu, X.L.; Li, Y.H.; Liu, H.; et al. Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans. *Nat. Photon.* **2021**, *15*, 570. [CrossRef]
28. Pittaluga, M.; Minder, M.; Lucamarini, M.; Sanzaro, M.; Woodward, R.I.; Li, M.-J.; Yuan, Z.; Shields, A.J. 600 km repeater-like quantum communications with dual-band stabilization. *Nat. Photon.* **2021**, *15*, 530–535. [CrossRef]
29. Wang, Z.H.; Wang, R.; Yin, Z.Q.; Wang, S.; Lu, F.Y.; Chen, W.; He, D.Y.; Guo, G.C.; Han, Z.F. Tight finite-key analysis for mode-pairing quantum key distribution. *Nat. Photon.* **2022**, *16*, 154–161.
30. 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]
31. 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] [PubMed]
32. Jiang, C.; Yu, Z.-W.; Hu, X.-L.; Wang, X.-B. Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses. *Phys. Rev. Appl.* **2019**, *12*, 024061. [CrossRef]
33. Hu, X.-L.; Jiang, C.; Yu, Z.-W.; Wang, X.-B. Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters. *Phys. Rev. A* **2019**, *100*, 062337. [CrossRef]
34. Xu, H.; Yu, Z.-W.; Jiang, C.; Hu, X.-L.; Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate. *Phys. Rev. A* **2020**, *101*, 042330. [CrossRef]
35. Jiang, C.; Hu, X.L.; Xu, H.; Yu, Z.W.; Wang, X.B. Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects. *New J. Phys.* **2020**, *22*, 053048. [CrossRef]
36. Jiang, C.; Hu, X.-L.; Yu, Z.-W.; Wang, X.-B. Composable security for practical quantum key distribution with two way classical communication. *New J. Phys.* **2021**, *23*, 063038. [CrossRef]
37. Teng, J.; Yin, Z.Q.; Fan-Yuan, G.J.; Lu, F.Y.; Wang, R.; Wang, S.; Chen, W.; Huang, W.; Xu, B.J.; Guo, G.C.; et al. Sending-or-not-sending twin-field quantum key distribution with multiphoton states. *Phys. Rev. A* **2021**, *104*, 062441. [CrossRef]
38. Chernoff, H. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *Ann. Math. Stat.* **1952**, *23*, 493. [CrossRef]
39. Huang, J.; Li, W.; Qiao, Y. An Effective Parameter Analysis for Sending-or-Not-Sending Quantum Key Distribution with Untrusted Light. *Entropy* **2025**, *27*, 547. [CrossRef] [PubMed]
40. Shan, Y.G.; Zhou, Y.; Yin, Z.Q.; Wang, S.; Chen, W.; He, D.Y.; Guo, G.C.; Han, Z.F. Sending-or-not-sending quantum key distribution with phase postselection. *Phys. Rev. Appl.* **2024**, *22*, 024056. [CrossRef]
41. Hu, X.L.; Jiang, C.; Yu, Z.W.; Wang, X.B. Universal approach to sending-or-not-sending twin field quantum key distribution. *Quantum Sci. Technol.* **2022**, *7*, 045031. [CrossRef]
42. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight Finite-Key Analysis for Quantum Cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef] [PubMed]

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.