entropy

MDPI

*Article*

# Twin-Field Quantum Digital Signature with Fully Discrete Phase Randomization

**Jiayao Wu, Chen He, Jiahui Xie, Xiaopeng Liu and Minghui Zhang ***

School of Information Science and Technology, Northwest University, Xi'an 710127, China;
wujiayao@stumail.nwu.edu.cn (J.W.); chenhe@nwu.edu.cn (C.H.); 202032849@stumail.nwu.edu.cn (J.X.);
liuxiaopeng@stumail.nwu.edu.cn (X.L.)
* Correspondence: zhangmh@nwu.edu.cn

**Abstract:** Quantum digital signatures (QDS) are able to verify the authenticity and integrity of a message in modern communication. However, the current QDS protocols are restricted by the fundamental rate-loss bound and the secure signature distance cannot be further improved. We propose a twin-field quantum digital signature (TF-QDS) protocol with fully discrete phase randomization and investigate its performance under the two-intensity decoy-state setting. For better performance, we optimize intensities of the signal state and the decoy state for each given distance. Numerical simulation results show that our TF-QDS with as few as six discrete random phases can give a higher signature rate and a longer secure transmission distance compared with current quantum digital signatures (QDSs), such as BB84-QDS and measurement-device-independent QDS (MDI-QDS). Moreover, we provide a clear comparison among some possible TF-QDSs constructed by different twin-field key generation protocols (TF-KGPs) and find that the proposed TF-QDS exhibits the best performance. Conclusively, the advantages of the proposed TF-QDS protocol in signature rate and secure transmission distance are mainly due to the single-photon interference applied in the measurement module and precise matching of discrete phases. Besides, our TF-QDS shows the feasibility of experimental implementation with current devices in practical QDS system.

**Keywords:** quantum digital signature; twin-field key generation protocol; discrete-phase-randomized source

check for updates

**Citation:** Wu, J.; He, C.; Xie, J.; Liu, X.; Zhang, M. Twin-Field Quantum Digital Signature with Fully Discrete Phase Randomization. *Entropy* **2022**, *24*, 839. https://doi.org/10.3390/e24060839

Academic Editor: Giuseppe Vallone

Received: 16 May 2022
Accepted: 16 June 2022
Published: 18 June 2022

## 1. Introduction

Digital signature is one of the kernel sciences behind classical cryptography [1]. It is particularly significant in modern communication as it can be used in a variety of applications, such as electronic mail, software distribution and financial transactions. The security of classical digital signature is guaranteed by computational difficulty assumption, which, however, will no longer be secure with the rapid development of quantum algorithms [2–4]. A full-fledged treatment for this issue towards quantum digital signature (QDS) [5] that paves a way to realize signature with information theory security is presented.

The first quantum signature protocol was introduced in 2001 [6], which can be considered as the original form of QDS. In general, earlier signature protocols [7–12] may impose several restrictions on QDS, such as non-destructive state comparison, long-time quantum memory and secure quantum channel, for obtaining a secure quantum signature. However, in practice, these requirements cannot be fully satisfied, resulting in security loopholes of real-life implementation. Subsequently, some practical QDS protocols [13–18] that do not attach these restrictions had been proposed and experimentally demonstrated.

For QDS protocols, a general scenario is that QDS can be divided into two assignments: distribution stage and messaging stage. The former uses the quantum part of quantum key distribution (QKD), i.e., key generation protocol (KGP), to distribute keys for users without further classical post-processing. The latter allows two receivers to verify the authenticity of a signature declaration. During the distribution stage, a KGP, such as

BB84-KGP [19,20] or measurement-device-independent KGP (MDI-KGP) [21–24], will be adopted to generate correlated keys between users. However, the performance of both KGPs is restricted by the fundamental rate-loss limit (referred to as PLOB bound) [25,26], which is equal to $-\log_2(1-\eta)$, where $\eta$ is the channel transmittance; this implies that the key generation rate can only vary with the channel transmittance linearly, asymptotically as $1.44\eta$ bits per channel use. Some newly proposed QKD protocols with better performance have accordingly improved the performance of KGPs, since KGP is regarded as a part of QKD. Recently, twin-field QKD (TF-QKD) protocol [27] has been proven to be capable of overcoming the PLOB bound. The reason is that the single-photon interference utilized in TF-QKD enables the key rate scale with the square root of the channel transmittance. Subsequently, various variants of original TF-QKD were designed and implemented for overcoming the PLOB bound [28–39].

In general, TF-QKD systems with decoy-state method [38–42] require users to emit coherent states with a continuous-phase-randomized source (CPRS); however, this is difficult to achieve in practice and may open a security loop. Remarkably, this issue can be solved by discrete-phase-randomized source (DPRS) instead and a rigorous security proof was already presented by Cao et al. [43]. The recently proposed TF-QKDs with discrete-phase-randomized source [44,45] closed the gap between theory and practice, and can be implemented with current optical devices. In particular, Zhang et al. [44] proposed a TF-QKD variant with $M$ phase slices both in the code mode and the test mode. Currás-Lorenzo et al. [45] put forward a discrete-phase-randomized TF-QKD protocol with only two phases in the code mode, which provides a higher key rate than that in [44] since its key rate is not restricted by the sifting factor. Inspired by this work, we propose a practical discrete-phase-randomized TF-QDS protocol. In fact, TF-QDS is a kind of MDI-QDS performed at the single-photon level. We use a numerical approach to derive the bounds on parameters in the asymptotic case. For each given distance, we optimize the key rate over the signal intensity and decoy intensity of coherent pulses, and fix the vacuum intensity. For comparison, we plot the simulation results of various QDSs under the same experimental parameters and find that our TF-QDS can achieve higher signature rate and longer transmission distance compared with BB84-QDS [13] and MDI-QDS [16], when the number of discrete phase slices $M \geq 6$. The TF-QDS improves on current QDSs by overcoming the PLOB bound.

In addition, we compare the performance of our TF-QDS with two possible TF-QDSs constructed by two different KGPs: KGP with CPRS [38] and KGP with DPRS [44]. These two newly constructed protocols are called TF-QDS with CPRS and TF-QDS with DPRS, respectively. The simulation results demonstrate that our TF-QDS with $M = 6$ can exceed the performance of TF-QDS with CPRS due to the exact matching of phases. Its signature rate is 5–15 times that of TF-QDS with CPRS when the transmission distance ranges from 100 km to 300 km, and the maximum signature distance obtainable can be increased by 5%. Furthermore, we compare the performance between our TF-QDS and TF-QDS with DPRS for four different $M$. The results show that, for the same $M$, our method can achieve better performance in terms of both signature rate and secure distance. The reason for this is that in our protocol, only two phases are encoded in the code mode and the key generation rate is not restricted by $M$. On the other hand, the increase of $M$ tightens the upper bound of Eve's side information estimated in the test mode. Therefore, for our protocol, the signature rate increases with $M$. However, in TF-QDS with DPRS, $M$ phases are encoded in the code mode, so its signature rate tends to zero with the increase of $M$, which is caused by the filtering factor.

In this work, we devote Section 2 to the description of our TF-QDS. We review the TF-KGP [45] in Section 3. In Section 4, the security analysis is carried out. We give numerical simulation results in Section 5, and summarize our work in Section 6.

## 2. TF-QDS Protocol with Fully Discrete Phase Randomization

We consider a simple structure for our TF-QDS protocol to sign a one-bit message: a signer, Alice, generates a signature declaration with TF-KGPs performed by Alice–Bob and Alice–Charlie in the key distribution stage, and then transmits it to one of two receivers (Bob and Charlie), say Bob. Bob first verifies the signature and then forwards it to Charlie who then further verifies its authenticity in the messaging stage. The detailed process for our TF-QDS is illustrated in Figure 1. It is therefore clear that at most one party is dishonest in such a tripartite setting. If there is more than one dishonest party, then the real protocol will actually fail. We describe our TF-QDS protocol as follows.

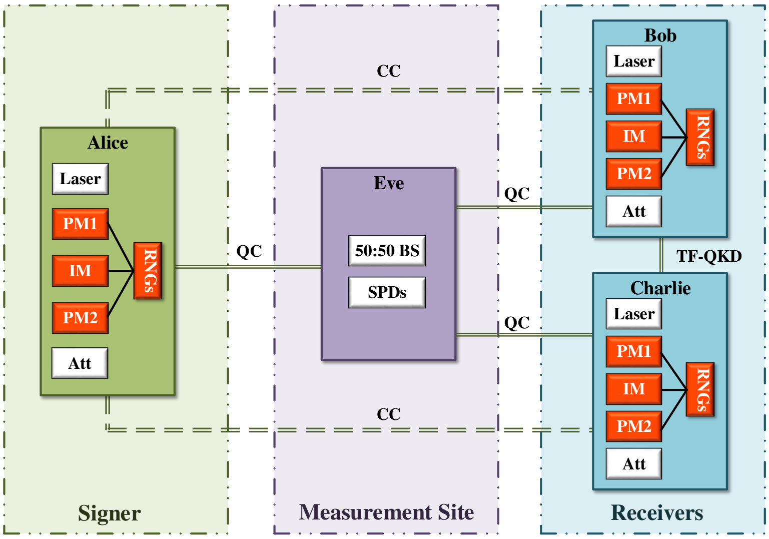

**Figure 1.** Schematic diagram of our TF-QDS. Alice and Bob (Alice and Charlie) prepare discrete-phase-randomized weak coherent-state pulses with a phase modulator (PM1). Intensity modulator (IM) is used to generate decoy states and PM2 is used to encode key bits. All the modulations are combined with random number generators (RNGs). The encoded pulses are attenuated by an attenuator (Att) and then sent out to the measurement site Eve. Alice's and Bob's (Alice's and Charlie's) pulses interfere at a 50:50 beam splitter (BS). The interference result is recorded with two single-photon detectors (SPDs). The solid lines represent the quantum channels (QCs) through which Alice and Bob (Alice and Charlie) use KGP to distribute keys. The dotted lines represent the authenticated classical channels (CCs) through which parties exchange and transmit some classical message. A TF-QKD link is shared between Bob and Charlie for performing the symmetrization of keys in full secrecy.

### 2.1. Distribution Stage

1. For each message $m = 0$ or 1, Alice and Bob use the discrete-phase-randomized TF-KGP [45] to generate keys of length $n_k$, Alice holds the key $K_m^{AB}$ and Bob holds the key $K_m^B$. Similarly, Alice and Charlie perform the discrete-phase-randomized TF-KGP [45] to generate keys $K_m^{AC}$ and $K_m^C$, respectively. The detailed steps for key distribution can be found in Section 3. Alice's signature for $m$ is $Sig_m = (K_m^{AB}, K_m^{AC})$.
2. For each $m$, Bob and Charlie perform the symmetrization of keys. That is, Bob (Charlie) randomly chooses half of the bits in his key $K_m^B$ ($K_m^C$), called $K_{m,forward}^B$ ($K_{m,forward}^C$), and then sends these bits to Charlie (Bob) using an authenticated classical channel. The remaining bits in $K_m^B$ ($K_m^C$) are named $K_{m,keep}^B$ ($K_{m,keep}^C$). After the symmetrization of keys, Bob's and Charlie's keys are denoted as $S_m^B = (K_{m,keep}^B, K_{m,forward}^C)$ and $S_m^C = (K_{m,keep}^C, K_{m,forward}^B)$ respectively; therefore, Alice cannot distinguish whether a key is Bob's or Charlie's, which guarantees the security against repudiation. In addition, Bob (Charlie) can only obtain half of $K_m^C$ ($K_m^B$), which guarantees the security against forging.

### 2.2. Messaging Stage

1. For signing a one-bit message $m$, Alice sends the signature declaration $(m, Sig_m)$ to Bob.
2. Bob checks and records the number of mismatches between the declaration $Sig_m$ and his key $S^B_m$. Particularly, Bob separately calculates the number of mismatches for the key $K^B_{m,keep}$ that received directly from Alice and the key $K^C_{m,forward}$ that forwarded by Charlie. If the number of mismatches for both parts is fewer than $S_a(n_k/2)$, he accepts the signature, where $S_a < 1/2$ is a small threshold determined by experimental parameters and a desired security level.
3. Bob then forwards $(m, Sig_m)$ to Charlie.
4. Charlie checks the number of mismatches between $Sig_m$ and $S^C_m$. The verification method is similar to that performed by Bob, except with a different threshold $S_v$, where $0 < S_a < S_v < 1/2$. If the number of mismatches for $K^C_{m,keep}$ and $K^B_{m,forward}$ is fewer than $S_v(n_k/2)$, Charlie accepts $Sig_m$ as the original signature generated by Alice. It is worth noting that two different thresholds $S_a$ and $S_v$ are required to ensure the non-repudiation of QDS protocol.

## 3. TF-KGP

TF-KGP, as a part of QDS, is performed in pairs separately by Alice–Bob and Alice–Charlie to distribute keys without further error correction and privacy amplification. This section takes Alice and Bob as an example to review the TF-KGP with fully discrete phase randomization [45]. The distributed keys among Alice and Bob correspond to the keys $K^{AB}_m$ and $K^B_m$ described in Section 2.

### 3.1. Preparation

See the tasks below for the states of Alice's and Bob's delivering to Eve depending on their chosen mode for transmission. Alice and Bob choose the code mode and test mode randomly. The code mode is used for key generation and the test mode is used for parameter estimation. For the code mode, Alice (Bob) prepares a bit $k_a$ $(k_b)$ randomly and generates a coherent state $|(-1)^{k_a}\sqrt{\mu}\rangle$ $(|(-1)^{k_b}\sqrt{\mu}\rangle)$, where $\mu$ is the signal intensity. For the test mode, Alice (Bob) prepares a discrete-phase-randomized coherent state $|\sqrt{\beta_a}e^{i\theta_a}\rangle$ $(|\sqrt{\beta_b}e^{i\theta_b}\rangle)$, which is modeled by a random intensity $\beta_a$ $(\beta_b) \in \{\beta_0, \beta_1, \mu\}$ ($\beta_0 = 0$ is a vacuum intensity and $\beta_1$ is a decoy intensity) and a random phase $\theta_a$ $(\theta_b) = 2\pi m/M$ ($m \in \{0, 1, 2, \ldots, M-1\}$ and $M$ is number of dividing the phase interval $[0, 2\pi)$ into slices [32]).

### 3.2. Measurement

An untrusted intermediate node, Eve, performs the single-photon interference on the incoming pulses through a 50:50 BS followed by two detectors SPD0 and SPD1. A successful round corresponds to only one detector being clicked, and is unsuccessful otherwise. Eve then announces the successful rounds publicly.

### 3.3. Sifting

Alice and Bob exchange their intensity and mode through an authenticated classical channel and retain data from those in which they have used the same mode. For rounds of code mode, Alice and Bob generate sifted keys $k_A$ and $k_B$. By disclosing $L$ bits of sifted keys, they can calculate the quantum bit error rate (QBER), $E_k = (1/L)\sum k^r_A \oplus k^r_B$, where $k^r_A$ and $k^r_B$ denote Alice's and Bob's exposed bits respectively, after which they are discarded. The remaining $n_k$ bits in $k_A$ and $k_B$ are Alice's and Bob's final keys $K^{AB}_m$ and $K^B_m$, respectively. It is necessary for Bob to flip his bits corresponding to rounds with SPD1 clicked. For rounds of test mode, Alice and Bob calculate the gains $\{Q_\beta\}$ in which they both select the same intensity and the same phase $\theta_a = \theta_b$, and the gains $\{Q^-_\beta\}$ in which they select the same intensity and the opposite phase $\theta_a = \theta_b \pm \pi$.

### *3.4. Parameter Estimation*

Alice and Bob use the gains $\{Q_\beta\}$ and $\{Q_\beta^-\}$ to separately estimate the phase error rates $e_{ph,same}$ and $e_{ph,diff}$ according to the numerical method (see Appendix A), where $e_{ph,same}$ ($e_{ph,diff}$) indicates the phase error rate of successful code mode rounds in which Alice and Bob use the same (opposite) phase.

## 4. Security Analysis

We followed the method in Ref. [46] to estimate Eve's smooth min-entropy [47] on Bob's reserved key $K^B_{m,keep}$, and then use it to bound the probability that Eve makes errors less than a certain value.

Eve can obtain some information from parameter estimation and mode declaration. Here, we define $\kappa$ and $\zeta$ as the classical information disclosed during parameter estimation and mode declaration, respectively. $K^B_{m,forward}$ is the extra information leaked to Eve under the case that Charlie is Eve. All these information is defined on one quantum system living in the Hilbert space, which is a combination of the following elements: $\kappa$, $\zeta$ and $K^B_{m,forward}$, as well as Eve's ancilla quantum system following her general attack. The information that Eve obtains about $K^B_{m,keep}$ is summarized as $E$. Then, Eve's smooth min-entropy with access to $E$ is given by

$$H^{\epsilon_k}_{min}(K^B_{m,keep}|E) \geq \frac{n_k}{2}(1 - I_{AE}), \tag{1}$$

where the inequality holds up to $\log_2(1/\epsilon_k)$. Here, $I_{AE}$ denotes the information leaked to Eve, which can be bounded by the phase error rates $e_{ph,same}$ and $e_{ph,diff}$ as

$$I_{AE} \leq \frac{1}{2}h(e_{ph,same}) + \frac{1}{2}h(e_{ph,diff}), \tag{2}$$

where $h(x)$ is a Shannon binary entropy function $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. The phase error rates cannot be directly observed from experiments, their estimation can be found in Appendix A. With the upper bound on $I_{AE}$, we can further evaluate Eve's smooth min-entropy.

Secondly, according to the proposition in Ref. [16], the upper bound on the average probability that Eve's eavesdropping makes at most $r$ errors with the given smooth min-entropy is

$$\langle p \rangle \leq \sum_{t=0}^{r} \binom{\frac{n_k}{2}}{t} 2^{-H^{\epsilon_k}_{min}(K^B_{m,keep}|E)} + \epsilon_k. \tag{3}$$

Furthermore, for large $n_k$, the probability for Eve to make fewer than $r$ errors for any $g > 0$ is given by

$$\mathcal{P}(\text{Eve makes fewer than } r \text{ errors}) := p \leq g, \tag{4}$$

except with probability at most

$$\epsilon_F := \frac{1}{g}(2^{-\frac{n_k}{2}[(1-I_{AE})-h(2r/n_k)]} + \epsilon_k). \tag{5}$$

Thus, we can determine the condition that Eve can make fewer than $r$ errors with a non-negligible probability as

$$(1 - I_{AE}) - h(2r/n_k) > 0. \tag{6}$$

If this condition is met, the probability of Eve making fewer than $r$ errors will be arbitrarily small by increasing the length of signature. We define $p_E$ as:

$$(1 - I_{AE}) - h(p_E) = 0. \tag{7}$$

A physical interpretation behind Equation (7) is that $p_E$ is the minimum error rate that Eve makes when guessing Bob's key except with negligible probability $\epsilon_F$. The upper bound on QBER between Alice's and Bob's keys is $\overline{E_k}$. Therefore, as long as the condition of $p_E > \overline{E_k}$ is satisfied, we can obtain a secure signature by increasing $n_k$, which means that

$$(1 - I_{AE}) - h(\overline{E_k}) > 0. \tag{8}$$

For demonstrating the security of TF-QDS protocol, we aim to show that the following three inherent properties for signature systems can be guaranteed [48].

### *4.1. Robustness*

In the messaging phase, Bob would reject Alice's signature declaration when the mismatch rate between $n_k/2$ bits received from either Alice or Charlie and Alice's declaration is higher than $S_a$. The QBER (mismatch rate) $E_k$ between Alice's and Bob's keys can be estimated by utilizing $L$ bits. According to the Serfling inequality [49], we can obtain the upper bound on QBER as follows:

$$\overline{E_k} \geq E_k + \tau(\frac{n_k}{2}, L, \epsilon_P), \tag{9}$$

where

$$\tau(\frac{n_k}{2}, L, \epsilon_P) = \sqrt{\frac{(\frac{n_k}{2} - L + 1)\ln(\frac{1}{\epsilon_P})}{Ln_k}}. \tag{10}$$

This suggests that the upper bound on QBER is true except with a small probability $\epsilon_P$. The failure probability decays exponentially in the parameter $L$ for any fixed value of the function $\tau$. We set $\overline{E_k} := \max\{\overline{E_{k,B}}, \overline{E_{k,C}}\}$, where $\overline{E_{k,B}}$ and $\overline{E_{k,C}}$ correspond to the upper bounds on QBERs for Alice–Bob and Alice–Charlie, respectively. Here, we should make $S_a$ greater than $\overline{E_k}$, except with probability of at most $\epsilon_P$, so the probability of an honest abort is restricted to

$$\mathbf{P}(\text{honest abort}) \leq 2\epsilon_p. \tag{11}$$

### *4.2. Non-Repudiation*

Non-repudiation means that the signature declaration generated by an original signatory is accepted by one receiver but rejected by the other.

For repudiation, the number of mismatches between Alice's declaration $Sig_m$ and Bob's key $S_m^B$ must be less than $S_a(n_k/2)$, and that between $Sig_m$ and Charlie's key $S_m^C$ must be greater than $S_v(n_k/2)$. This suggests that Alice should make Bob accept her signature and make Charlie reject her signature. That is, a necessary condition for successful repudiation is that the mismatch rate between $Sig_m$ and $S_m^B$ is not equal to that between $Sig_m$ and $S_m^C$. In this protocol, the symmetrization of keys performed between Bob and Charlie makes their respective keys contain an equal error rate, resulting in security against repudiation. According to the results in Ref. [13], the probability of Alice's successful repudiation can be bounded as

$$\mathbf{P}(\text{repudiation}) \leq 2\text{exp}[-\frac{1}{4}(S_a - S_v)^2 n_k], \tag{12}$$

where

$$S_a = \overline{E_k} + \frac{P_E - \overline{E_k}}{3}, \quad S_v = \overline{E_k} + \frac{2(P_E - \overline{E_k})}{3}. \tag{13}$$

### *4.3. Unforgeability*

Forgery attack performed by a dishonest internal user is considered in our analysis since it is more convenient for insiders to perform a forgery attack than external attackers. Suppose that Bob wants to forge Alice's signature: he needs to transmit Charlie a forged signature and make the number of mismatches contained in the forged signature fewer than $S_v(n_k/2)$. As mentioned above, $\overline{E_k}$ is the upper bound on QBER between Alice's and

Charlie's keys, and $p_E$ indicates the minimum error rate that Bob makes errors associated with Charlie's key. When Equation (8) holds, we choose $S_v$ such that $\overline{E_k} < S_v < p_E$. This suggests that there is a higher probability for Charlie to accept Alice's original signature. On the contrary, Charlie will likely reject Bob's forged signature, since the probability of Bob creating a forged signature with an error rate fewer than $S_v$ is restricted by Equation (4) as

$$\mathcal{P}(\text{Bob makes fewer than } S_v(n_k/2) \text{ errors}) := p \leq g, \tag{14}$$

except with probability at most $\epsilon_F$. If the estimation of parameters $E_k$ and $e_{ph}$ (containing $e_{ph,same}$ and $e_{ph,diff}$) fails, which separately occur with probabilities $\epsilon_P$ and $\epsilon_{ph}$, then we think for simplicity that Bob can successfully forge Alice's signature. Thus, the probability of Bob's successful forging can be bounded as

$$\mathbf{P}(\text{forge}) \leq g + \epsilon_F + \epsilon_P + 2\epsilon_{ph}. \tag{15}$$

This equation is valid for any choice of parameters greater than zero. The probability for Bob to forge a signature can be arbitrarily small by increasing $n_k$.

In summary, the security level is bounded as

$$\xi = \max\{\mathbf{P}(\text{honest abort}), \mathbf{P}(\text{repudiation}), \mathbf{P}(\text{forge})\}. \tag{16}$$

## 5. Numerical Simulation

In this section, we give simulation results for TF-QDS with two-intensity decoy-state method in the asymptotic scenario. The channel model given in Ref. [45] is employed to obtain observable gains and QBERs for TF-KGP. For simplicity, we assume that the channel is symmetrical for each pair of parties. For each given distance, we optimize the key rate over the signal intensity $\mu$ and the decoy intensity $\beta_1$ of coherent pulses, and fix the vacuum intensity $\beta_0 = 0$.

We plot the signature rate $R$ as a function of the transmission distance with optimal values of intensities $\mu$ and $\beta_1$ for a given security level $10^{-8}$, as shown by dashed lines in Figure 2. The signature rate is defined as $R = 1/N$, where $N$ indicates the total number of pulses required to sign a 1-bit message given a certain security level. If we set a fixed security level, then the signature rate can be bounded by Equation (12) with parameters $e_{ph,same}(e_{ph,diff})$, $\overline{E_k}$ and $P_E$. The optimal values of intensity $\mu$ with different numbers of phase slices $M$ against the transmission distance can be found in Figure 3. These optimal values are obtained by maximizing the key rate of KGP. The experimental parameters used for numerical simulation refer to a recent experiment [50], which are listed in Table 1. We also give the simulation results of signature rate without performing any optimization for comparison. In this case, we plot the signature rate curves with fixed values of all intensities ($\mu = 0.06$, $\beta_1 = 10^{-4}$ and $\beta_0 = 0$), represented by solid lines in Figure 2. As depicted in Figure 2, numerical optimization yields a significant improvement in transmission distance compared to nonoptimization, especially when $M$ is relatively small. In particular, the maximum signature distance reached with intensity optimization increased by more than two times when $M = 4$.

**Table 1.** Parameter setting in simulation. $\alpha$—loss coefficient of fiber at telecommunication wavelength; $p_d$—dark count rate of detectors; $\eta_d$—detection efficiency of detectors; $e_d$—optical misalignment error; $f$—error correction inefficiency.

| $\alpha$ | $p_d$ | $\eta_d$ | $e_d$ | $f$ |
|---|---|---|---|---|
| 0.16 | $10^{-8}$ | 35% | 2% | 1.15 |

Furthermore, Figure 2 shows the performance of TF-QDS for different $M$. The maximum signature distances when $M = 8$ and $M = 12$ have only slight differences under the same experimental parameters, corresponding to 317 km and 325 km, respectively. This suggests that it is not necessary to increase the number of phase slices to achieve significant improvements. On the other hand, for $M = 4$, $M = 6$ and $M = 8$, there is a distinct improvement in terms of signature distance for larger $M$.

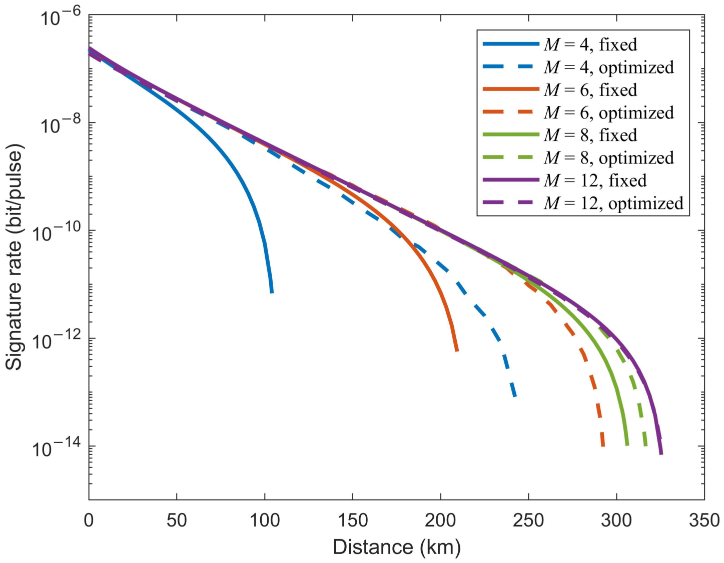

**Figure 2.** Signature rate vs. the transmission distance with optimal intensities (dashed lines) and fixed intensities (solid lines) for four different numbers of phase slices $M$. ($M = 4$ blue, $M = 6$ red, $M = 8$ green, $M = 12$ purple).

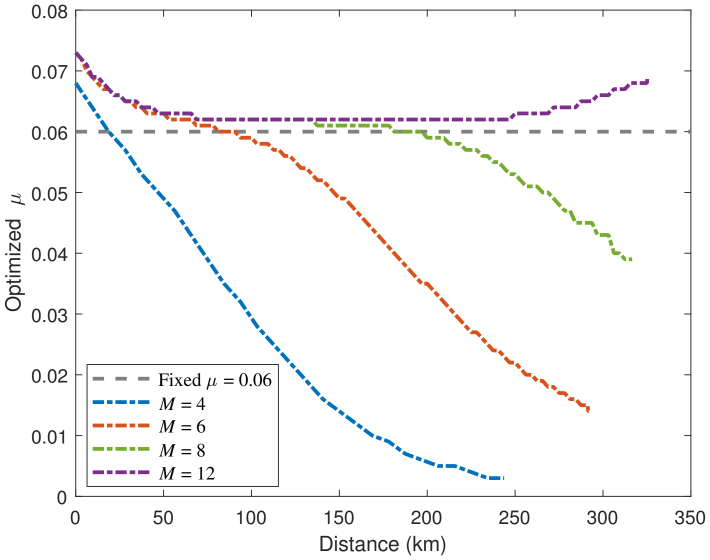

**Figure 3.** Optimal values of the signal intensity $\mu$ vs. the transmission distance for four different $M$.

We perform a numerical simulation of $M = 8$ to evaluate the potential impact of using more decoy states in terms of performance. Figure 4 shows the comparison of simulation results for TF-QDS with different numbers of decoy intensities. The results show that the signature rate and transmission distance of TF-QDS with two decoy states is close to that of three [51] (and four) decoy states. Therefore, for our TF-QDS protocol, the two-intensity decoy state is sufficient for practical usage, and there is no need to introduce more decoy states for longer transmission distances.

We compare the performance of our TF-QDS with BB84-QDS and MDI-QDS in Figure 5. For a fair comparison, we plot the signature rate curves of three QDSs by using the same experimental parameters without intensity optimization. The channel models given in Ref. [32] are utilized to calculate gains and QBERs for BB84-QDS and MDI-QDS. As shown in Figure 5, BB84-QDS shows the highest signature rate when the transmission distance is less than 45 km. Once the distance is more than 45 km, the signature rate of TF-QDS exceeds that of BB84-QDS. Compared with MDI-QDS, the signature rate of TF-QDS is always better than that of MDI-QDS when $M \geq 6$. In addition, TF-QDS can obtain a secure signature at longer transmission distance than BB84-QDS and MDI-QDS when $M \geq 6$. Among these QDS protocols, the maximum signature distance for TF-QDS is 520 km when $M = 12$, whereas the maximum signature distances for BB84-QDS and MDI-QDS are 182 km and 334 km, respectively. This is because the measurement module of TF-QDS is realized with single-photon interference which requires only one photon to survive the loss of over half of the transmission distance. Twin-field approach overcomes the PLOB bound and significantly extends the secure signature distance.

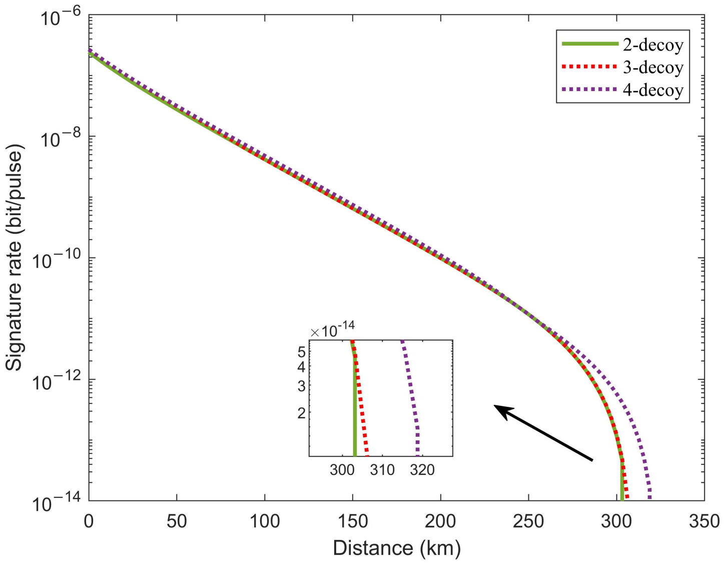

**Figure 4.** Signature rate versus the transmittance distance by using two-intensity (green solid line), three-intensity (red dotted line) and four-intensity (purple dotted line) decoy-state methods for $M = 8$.

Our TF-QDS protocol is built upon the TF-KGP in Ref. [45] where users emit coherent-states with a discrete-phase-randomized source in the test mode. We can further propose two possible TF-QDS protocols: TF-QDS with CPRS and TF-QDS with DPRS, which are separately constructed by KGP in Ref. [38] and KGP in Ref. [44], respectively. We compare the performance of our TF-QDS with two newly constructed TF-QDSs with the same experimental parameters given in Ref. [38].

Firstly, we compare the simulation results of our TF-QDS and TF-QDS with CPRS in Figure 6. Remarkably, the results show that our TF-QDS with only six discrete phase slices can exceed the performance of TF-QDS with CPRS. In detail, our protocol can achieve a secure signature at the maximum transmission distance of 408 km with $M = 6$, while the maximum transmission distance for TF-QDS with CPRS is 388 km. Besides, its signature rate increases by more than one order of magnitude since 69 km. The reason for this improvement is that a tighter bound on the phase error rate can be obtained, since the phase post-selection in discrete version makes the users' phases exactly matched.

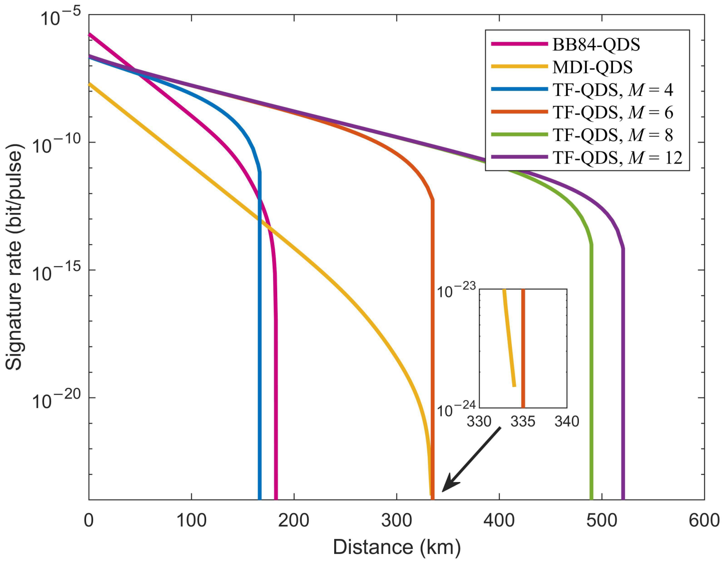

**Figure 5.** Results of our TF-QDS, BB84-QDS and MDI-QDS.

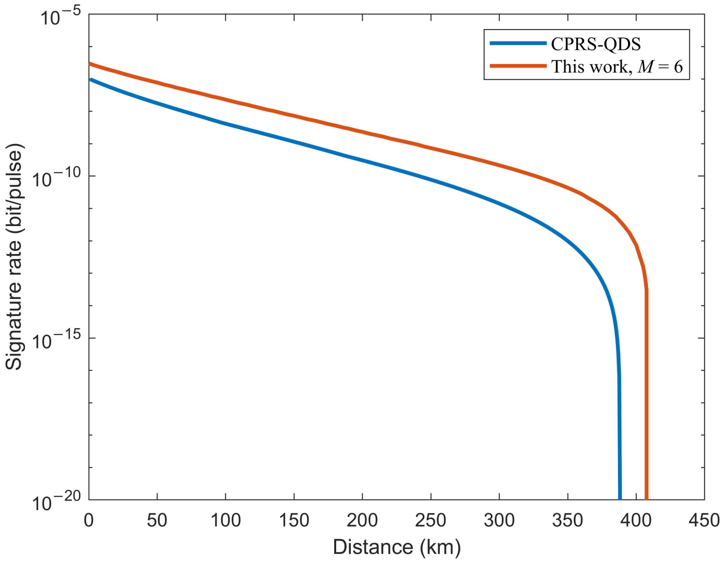

**Figure 6.** Results of our TF-QDS and TF-QDS with CPRS.

Furthermore, we compare the performance between our TF-QDS and TF-QDS with DPRS for different $M$. Both TF-QDS protocols utilize a discrete-phase-randomized source, with the main difference being that, for the proposed TF-QDS, only two phases rather than $M$ phases are encoded in the code mode. The simulation results are shown in Figure 7, where solid lines correspond to the results of our TF-QDS, and dashed lines correspond to the results of TF-QDS with DPRS. Figure 7 illustrates that our TF-QDS can deliver a higher signature rate than that of TF-QDS with DPRS for the same phase slice. The fact is that the signature rate of our protocol increases with $M$, while the signature rate of TF-QDS with DPRS approaches 0 as $M$ increases, due to the sifting factor. Furthermore, our TF-QDS can transmit a longer signature distance when the same signature rate is obtained. The reason for this is that we can obtain a tighter bound on the phase error rate compared with TF-QDS with DPRS, as illustrated in Figure 8. Detailed data on signature rate $R$ and transmission distance for both TF-QDSs are listed in Table 2.

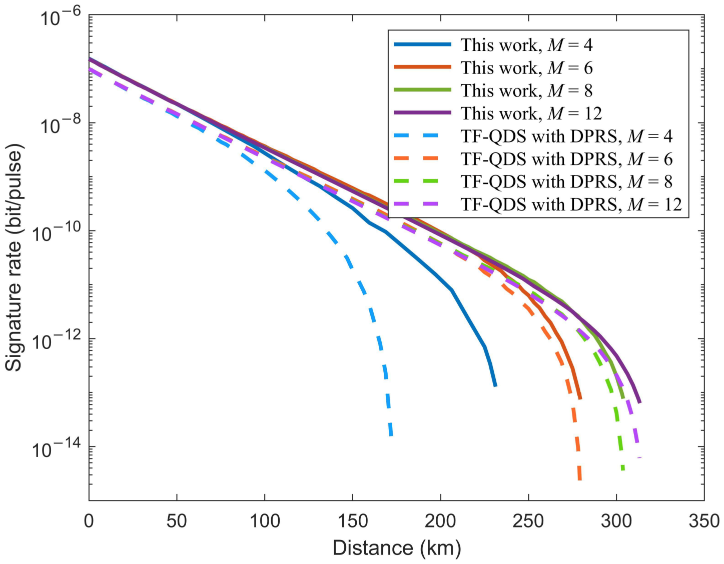

**Figure 7.** Results of our TF-QDS and TF-QDS with DPRS for four different $M$.

**Table 2.** Comparison of signature rate $R$ and transmission distance for our work and TF-QDS with DPRS for different $M$. More general comparison results are shown in Figure 6. The second and third rows indicate the signature rates of two protocols at 100 km and 200 km, respectively. The fourth row shows the secure transmission distances when the signature rate is $10^{-12}$ and the bottom row gives the comparison of maximum transmission distances obtainable.

| | **Protocols** | $M = 4$ | $M = 6$ | $M = 8$ | $M = 12$ |
|---|---|---|---|---|---|
| $R$ at 100 km | This work | $3.37 \times 10^{-9}$ | $3.66 \times 10^{-9}$ | $3.50 \times 10^{-9}$ | $3.42 \times 10^{-9}$ |
| (bits/pulse) | TF-QDS with DPRS | $1.30 \times 10^{-9}$ | $2.36 \times 10^{-9}$ | $2.27 \times 10^{-9}$ | $2.23 \times 10^{-9}$ |
| $R$ at 200 km | This work | $2.08 \times 10^{-11}$ | $9.31 \times 10^{-11}$ | $8.77 \times 10^{-11}$ | $8.30 \times 10^{-11}$ |
| (bits/pulse) | TF-QDS with DPRS | - | $5.75 \times 10^{-11}$ | $5.64 \times 10^{-11}$ | $5.38 \times 10^{-11}$ |
| Distance | This work | 222.2 | 267.7 | 288.8 | 291.8 |
| (km) | TF-QDS with DPRS | 164.8 | 262.2 | 281.7 | 283.9 |
| Maximum | This work | 231.3 | 279.4 | 303.8 | 313.3 |
| distance (km) | TF-QDS with DPRS | 171.9 | 279.3 | 303.7 | 313.1 |

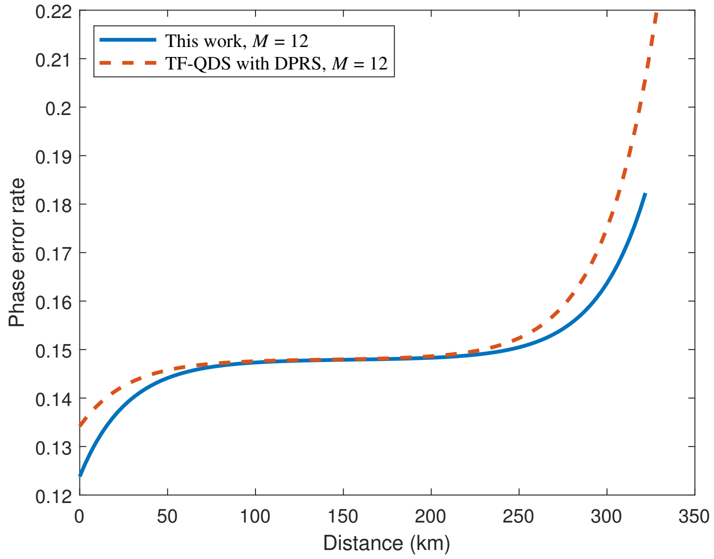

**Figure 8.** Comparison the upper bound of phase error rate between our TF-QDS and TF-QDS with DPRS for $M = 12$.

## 6. Conclusions

We present a TF-QDS protocol with fully discrete phase randomization. Unlike most previous variants of QDS that emit weak coherent-state pulses with a continuous-phase-randomized source, our TF-QDS uses a discrete-phase-randomized source instead, which can be realized with common optical components and further applied in practical QDS systems. As well as this, the protocol had been proved to be secure against forging and repudiation.

For better performance, we optimize intensities of signal state and decoy state to improve the signature rate. We compare the performance of our TF-QDS with BB84-QDS and MDI-QDS by numerical simulation. The results demonstrate that our TF-QDS can achieve the best performance in terms of signature rate and secure transmission distance when the phase slices $M \geq 6$. Moreover, we provide a clear comparison between several possible TF-QDSs constructed by different TF-KGPs and find that our TF-QDS with $M = 6$ already exceeds TF-QDS with CPRS due to the exact matching of phases. The signature rate is 5–15 times that of TF-QDS with CPRS when the transmission distance ranges from 100 km to 300 km, and its maximum signature distance obtainable increases by 5%. Furthermore, we compare the performance of our TF-QDS with TF-QDS with DPRS for four different $M$. The simulation results show that our TF-QDS achieves a higher signature rate and a longer secure distance than that of the TF-QDS with DPRS for the same $M$.

In summary, the proposed TF-QDS with fully discrete phase randomization is more feasible in experimental implementation; meanwhile, it is an effective solution for a higher signature rate over a longer transmission distance.

**Author Contributions:** Conceptualization, J.W. and M.Z.; methodology, J.W. and M.Z.; software, J.W. and J.X.; validation, J.W., J.X. and X.L.; formal analysis, J.W., C.H., J.X. and M.Z.; investigation, J.W.; resources, C.H. and M.Z.; data curation, J.W. and J.X.; writing—original draft preparation, J.W.; writing—review and editing, J.W. and M.Z.; visualization, J.W.; supervision, C.H.; project administration, C.H. and M.Z.; funding acquisition, M.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the National Natural Science Foundation of China (Grant No. 61801385), China Postdoctoral Science Foundation (Grant No. 221628), Natural Science Basic Research Plan in Shaanxi Province of China (Grant No. 2020JQ-602) and Foundation of Shaanxi Province Education Department.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Data are contained within the article

**Acknowledgments:** The authors would like to thank the anonymous reviewers for their invaluable and constructive comments.

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

## Appendix A. Parameter Estimation

Eve's side information $I_{AE}$ can be bounded by phase error rates $e_{ph,same}$ and $e_{ph,diff}$; however, these cannot be observed through experiments directly. Thus, we need to estimate the upper bounds on $e_{ph,same}$ and $e_{ph,diff}$ by using the observable data in the test mode. Here, we just describe the estimation approach for $e_{ph,same}$ since the process is similar for both terms. According to Ref. [45], $e_{ph,same}$ can be written as

$$e_{ph,same} = \frac{1}{2p_{succ,same}} \left\langle \lambda_{\text{even}} \middle| \hat{M}_{ab}^{\dagger} \hat{M}_{ab} \middle| \lambda_{\text{even}} \right\rangle, \tag{A1}$$

where $p_{succ,same}$ is the probability that Alice and Bob use the same phases in a code mode round and Eve reports a successful detection. More precisely, we describe Eve's collective attack as a two-outcome general measurement $\{\hat{M}_{ab}, \hat{M}^{f}_{ab}\}$ on the photonic systems $ab$, where $\hat{M}_{ab}$ $(\hat{M}^{f}_{ab})$ is the Kraus operator corresponding to the announcement of the round as successful (unsuccessful) and $a$ and $b$ are the photon numbers sent to Eve by Alice and Bob respectively. $|\lambda_{\mathrm{even}}\rangle$ and $|\lambda_{\mathrm{odd}}\rangle$ are unnormalized states and can be defined as

$$|\lambda_{\mathrm{even}}\rangle_{ab} = \sum_{n=0, n\in N_0}^{M-1} \sqrt{P^{\beta}_{n\,\mathrm{mod}\,M}}|\lambda^{\beta}_{n\,\mathrm{mod}\,M}\rangle_{ab}, \tag{A2}$$

$$|\lambda_{\mathrm{odd}}\rangle_{ab} = \sum_{n=0, n\in N_1}^{M-1} \sqrt{P^{\beta}_{n\,\mathrm{mod}\,M}}|\lambda^{\beta}_{n\,\mathrm{mod}\,M}\rangle_{ab}, \tag{A3}$$

where $N_0$ $(N_1)$ is the set of non-negative even (odd) numbers, and

$$|\lambda^{\beta}_{n\,\mathrm{mod}\,M}\rangle_{ab} = \sum_{l=0}^{\infty} \sqrt{\frac{P_{Ml+n|\beta}}{P^{\beta}_{n\,\mathrm{mod}\,M}}}|\lambda_{Ml+n}\rangle_{ab}, \tag{A4}$$

$$P^{\beta}_{n\,\mathrm{mod}\,M} = \sum_{l=0}^{\infty} P_{Ml+n|\beta}, \tag{A5}$$

with $P_{n|\beta}$ is a Poisson distribution. The states $|\lambda^{\beta}_{n\,\mathrm{mod}\,M}\rangle_{ab}$ have a slight dependence on the intensity $\beta$, and their yields can be written as

$$Y^{\beta}_{n\,\mathrm{mod}\,M} = ||\hat{M}_{ab}|\lambda^{\beta}_{n\,\mathrm{mod}\,M}\rangle||^2. \tag{A6}$$

The estimation of upper bound on $e_{ph,same}$ can be considered an optimization problem and solved by a linear programming [45] shown in Equation (A7).

$$\begin{aligned}
&\max \frac{1}{2p_{succ,same}}\left\langle \lambda_{\mathrm{even}}\middle|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}\middle|\lambda_{\mathrm{even}}\right\rangle s.t.\\
&p_{succ,same} = \frac{1}{2}\left\langle \lambda_{\mathrm{even}}\middle|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}\middle|\lambda_{\mathrm{even}}\right\rangle + \frac{1}{2}\left\langle \lambda_{\mathrm{odd}}\middle|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}\middle|\lambda_{\mathrm{odd}}\right\rangle,\\
&Q_{\beta} = \sum_{n=0}^{M-1} P^{\beta}_{n\,\mathrm{mod}\,M} Y^{\beta}_{n\,\mathrm{mod}\,M},\ \forall\beta\in\Psi,\\
&Y^{\mu}_{n\,\mathrm{mod}\,M} \le 1, \forall n\in\{0,\ldots,M-1\},\\
&Y^{\beta_1}_{n\,\mathrm{mod}\,M} - Y^{\beta_2}_{n\,\mathrm{mod}\,M} \le \sqrt{1-F^{\beta_1,\beta_2}_{n}}, \forall\beta_1,\beta_2\in\Psi, n\in\{0,\ldots,M-1\},\\
&Y^{\beta}_{0\,\mathrm{mod}\,M} \le 1 - Q_{\beta_0} + 2\sqrt{F^{\beta,\beta_0}_{0}\left(1-F^{\beta,\beta_0}_{0}\right)\left(1-Q_{\beta_0}\right)Q_{\beta_0}} + F^{\beta,\beta_0}_{0}\left(2Q_{\beta_0}-1\right), \forall\beta\in\Psi,
\end{aligned} \tag{A7}$$

where $\Psi = \{\beta_1, \mu\}$ is the collection of all test-mode intensities, but not including vacuum, and $F^{\beta_1,\beta_2}_{n}$ is given by

$$F^{\beta_1,\beta_2}_{n} = \left|\left\langle \lambda^{\beta_1}_{n\,\mathrm{mod}\,M}|\lambda^{\beta_2}_{n\,\mathrm{mod}\,M}\right\rangle_{ab}\right|^2 = \left[\sum_{l=0}^{\infty}\sqrt{\frac{P_{Ml+n|\beta_1}}{P^{\beta_1}_{n\,\mathrm{mod}\,M}}}\sqrt{\frac{P_{Ml+n|\beta_2}}{P^{\beta_2}_{n\,\mathrm{mod}\,M}}}\right]^2. \tag{A8}$$

## References

1. Diffie, W.; Hellman, M.E. New directions in cryptography. In *Secure Communications and Asymmetric Cryptosystems*; Simmons, G.J., Ed.; Routledge: London, UK; New York, NY, USA, 2019; pp. 143–180.
2. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
3. Nielsen, M.A.; Chuang, I.L. Quantum computation and quantum information. *Am. J. Phys.* **2002**, *70*, 558–559. [CrossRef]
4. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
5. Amiri, R.; Andersson, E. Unconditionally secure quantum signatures. *Entropy* **2015**, *17*, 5635–5659. [CrossRef]

6. Gottesman, D.; Chuang, I. Quantum digital signatures. *arXiv* **2001**, arXiv:quant-ph/0105032.
7. Andersson, E.; Curty, M.; Jex, I. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev. A* **2006**, *74*, 022304. [CrossRef]
8. Dunjko, V.; Wallden, P.; Andersson, E. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.* **2014**, *112*, 040502. [CrossRef]
9. Collins, R.J.; Donaldson, R.J.; Dunjko, V.; Wallden, P.; Clarke, P.J.; Andersson, E.; Jeffers, J.; Buller, G.S. Realization of Quantum Digital Signatures without the Requirement of Quantum Memory. *Phys. Rev. Lett.* **2014**, *113*, 040502. [CrossRef]
10. Clarke, P.J.; Collins, R.J.; Dunjko, V.; Andersson, E.; Jeffers, J.; Buller, G.S. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.* **2012**, *3*, 1174. [CrossRef]
11. Wallden, P.; Dunjko, V.; Kent, A.; Andersson, E. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A* **2015**, *91*, 042304. [CrossRef]
12. Donaldson, R.J.; Collins, R.J.; Kleczkowska, K.; Amiri, R.; Wallden, P.; Dunjko, V.; Jeffers, J.; Andersson, E.; Buller, G.S. Experimental demonstration of kilometer-range quantum digital signatures. *Phys. Rev. A* **2016**, *93*, 012329. [CrossRef]
13. Amiri, R.; Wallden, P.; Kent, A.; Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **2016**, *93*, 032325. [CrossRef]
14. Yin, H.L.; Fu, Y.; Chen, Z.B. Practical quantum digital signature. *Phys. Rev. A* **2016**, *93*, 032316. [CrossRef]
15. Zhang, C.M.; Zhu, Y.; Chen, J.J.; Wang, Q. Practical quantum digital signature with configurable decoy states. *Quantum Inf. Process.* **2020**, *19*, 151. [CrossRef]
16. Puthoor, I.V.; Amiri, R.; Wallden, P.; Curty, M.; Andersson, E. Measurement-device-independent quantum digital signatures. *Phys. Rev. A* **2016**, *94*, 022328. [CrossRef]
17. Yin, H.L.; Wang, W.L.; Tang, Y.L.; Zhao, Q.; Liu, H.; Sun, X.X.; Zhang, W.J.; Li, H.; Puthoor, T.V.; You, L.X.; et al. Experimental measurement-device-independent quantum digital signatures over a metropolitan network. *Phys. Rev. A* **2017**, *95*, 042338. [CrossRef]
18. Roberts, G.L.; Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Comandar, L.C.; Sharpe, A.W.; Shields, A.J.; Curty, M.; Puthoor, I.V.; Andersson, E. Experimental measurement-device-independent quantum digital signatures. *Nat. Commun.* **2017**, *8*, 1098. [CrossRef]
19. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
20. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A.* **2005**, *72*, 012326. [CrossRef]
21. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
22. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
23. Ma, X.; Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062319. [CrossRef]
24. Primaatmaja, I.W.; Lavie, E.; Goh, K.T.; Wang, C.; Lim, C.C.W. Versatile security analysis of measurement-device-independent quantum key distribution. *Phys. Rev. A* **2019**, *99*, 062332. [CrossRef]
25. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **2009**, *102*, 050503. [CrossRef] [PubMed]
26. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
27. 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]
28. Tamaki, K.; Lo, H.K.; Wang, W.Y.; Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv* **2018**, arXiv:1805.05511.
29. 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]
30. Liu, Y.; Yu, Z.W.; Zhang, W.J.; 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]
31. 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]
32. Ma, X.; Zeng, P.; Zhou, H.Y. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
33. Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [CrossRef]
34. 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*, 149. [CrossRef]
35. Cui, C.H.; 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]
36. Lu, F.Y.; Yin, Z.Q.; Wang, R.; Fan, G.J.; Wang, S.; He, D.Y.; Chen, W.; Huang, W.; Xu, B.J.; Guo, G.C. Practical issues of twin-field quantum key distribution. *New J. Phys.* **2019**, *21*, 123030. [CrossRef]

37. Lu, F.Y.; Yin, Z.Q.; Cui, C.H.; Fan, 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]
38. 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]
39. Grasselli, F.; Curty, M. Practical decoy-state method for twin-field quantum key distribution. *New J. Phys.* **2019**, *21*, 073001. [CrossRef]
40. 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]
41. Teng, J.; Lu, F.Y.; Yin, Z.Q.; Fan, G.J.; Wang, R.; Wang, S.; Chen, W.; Huang, W.; Xu, B.J.; Guo, G.C. Twin-field quantum key distribution with passive-decoy state. *New J. Phys.* **2020**, *22*, 103017. [CrossRef]
42. Yu, Y.; Wang, L.; Zhao, S.M.; Mao, Q.P. Decoy-state phase-matching quantum key distribution with source errors. *Opt. Express* **2021**, *29*, 2227–2243. [CrossRef]
43. Cao, Z.; Zhang, Z.; Lo, H.K.; Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.* **2015**, *17*, 053014. [CrossRef]
44. Zhang, C.M.; Xu, Y.W.; Wang, R.; Wang, Q. Twin-field quantum key distribution with discrete-phase-randomized sources. *Phys. Rev. Appl.* **2020**, *14*, 064070. [CrossRef]
45. Currás, L.G.; Wooltorton, L.; Razavi, M. Twin-field quantum key distribution with fully discrete phase randomization. *Phys. Rev. Appl.* **2021**, *15*, 014016. [CrossRef]
46. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.H.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307. [CrossRef]
47. Tomamichel, M.; Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **2011**, *106*, 110506. [CrossRef]
48. Pirandola, S.; Andersen, U.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
49. Hoeffding, W. *The Collected Works of Wassily Hoeffding*; Springer: Berlin, Germany, 1994; pp. 409–426.
50. Minder, M.; Pittaluga, M.; Roberts, G.L.; Lucamarini, M.; Dynes, J.F.; Yuan, Z.L.; Shields, A.L. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **2019**, *13*, 334–338. [CrossRef]
51. Wang, X.B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **2013**, *87*, 012320. [CrossRef]