1. Cryptography toolbox
Here, we introduce threats faced by information processing (as shown in Fig. S1), the corresponding information security objectives and classical cryptographic techniques to tackle such threats [1]. First, eavesdropping, which threatens the confidentiality of information, can be prevented using symmetric cryptography and asymmetric cryptography (i.e., public-key cryptography). Second, tampering, which destroys the integrity of data, can be approached with a one-way hash function, message authentication code and digital signatures. Third, disguise, in which the attacker pretends to be the real information sender, can deal with message authentication codes and digital signatures. Finally, one may repudiate his or her certain behavior, and the digital signatures provide the efficacy of non-repudiation.

2. One-time pad
Define that encryption algorithm $E$ maps plaintexts $m \in M$ to ciphertexts $c \in C$. According to Shannon’s information theory, an algorithm $E$ is perfectly secret if $C$ and $M$ are independent, i.e., $Pr(m, c) = Pr(m) \times Pr(c)$. The one-time pad [2] encryption satisfies the above definition, where a plaintext is paired using the XOR operation with a random secret key of the same length. Learning the ciphertext does not increase any plaintext information. In addition, each encryption requires a new and independent random key; hence, knowing details about the previous key does not help the attacker.

In our one-time universal$_2$ hashing quantum digital signatures (OTUH-QDS) scheme, we utilize the one-time pad to encrypt the hash value and the irreducible polynomial to acquire the signature so that we can completely conceal the information of (almost) universal$_2$ hash functions.

3. LFSR-based Toeplitz hashing and message authentication
The LFSR-based Toeplitz matrix [3] is the almost universal$_2$ hash function, where the hash function is determined by an irreducible polynomial $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ of degree $n$ over the Galois field GF(2) and $n$-bit random initial vector, just requiring a total of $2n$ bits. The randomness of the initial vector and irreducible polynomial...
together guarantees the security of LFSR-based Toeplitz hashing. The collision probability of LFSR-based Toeplitz hashing is bounded by $\epsilon = m/2^n-1$, which quantifies the upper bound on the probability of finding any two different documents with the same hash value. The LFSR-based Toeplitz hashing operation can be written as $h_{p,s}(M) = H_{nm} \cdot M = \text{Hash}$, where $p = (a_{n-1}, a_{n-2}, ..., a_1, a_0)$ represents an irreducible polynomial and $s = (b_n, b_{n-1}, ..., b_2, b_1)^T$ is the initial vector. $p$ and $s$ are random and determine the Toeplitz matrix $H_{nm}$ with $n$ rows and $m$ columns. $M = (M_1, M_2, ..., M_m)^T$ is the message in the form of an $m$-bit vector. The Toeplitz matrix can be written as $H_{nm} = (s, s_1, ..., s_{m-1})$, where the initial vector $s = (b_n, b_{n-1}, ..., b_2, b_1)^T$ is the first column. The LFSR, determined by $p$, will be performed $m-1$ times to generate $s_1, s_2, ..., s_{m-2}$ and $s_{m-1}$. To be specific, LFSR will shift down every element in the previous column, and add a new element to the top of the column. For example, LFSR will first transform $s$ into $s_1 = (b_{n+1}, b_n, ..., b_3, b_2)^T$, where $b_{n+1} = p \cdot s$, and likewise, transform $s_1$ to $s_2$. Then the $m$ vectors $s, s_1, ..., s_{m-1}$ will together construct the Toeplitz matrix $H_{nm} = (s, s_1, ..., s_{m-1})$, and the hash value of the message is $H_{nm} \cdot M = \text{Hash}$.

Supplementary Figure S2. **Comparing message authentication and digital signatures.** (a) Information-theoretically secure message authentication. Aida and Basel are the message sender and recipient, respectively, while Eve is the attacker. Eve tries to make Basel accept the tampered tag and message $\{\text{Tag}', M'\}$. The black dotted line represents Eve’s attack process. (b) OTUH-QDS. For Bob’s forgery attack, he tries to make Charlie accept the forged signature and document $\{\text{Sig}', \text{Doc}'\}$. The red solid line represents the authentication classical channel, which has information-theoretical security by performing message authentication.

**Failure probability of authentication.**—Here, we first provide the information-theoretical security proof of message authentication [3]. We remark that the security proof in the original literature is omitted [3], we provide a detailed proof here, and the conclusions are consistent. Suppose the message authentication scenario that an attacker Eve captures a tag and message $\{\text{Tag}, M\}$ from the sender Aida, as shown in Fig. S2a. Note that the tag is acquired by using random secret key $\text{Key}$ to encrypt hash value $\text{Hash}$ with a one-time pad, i.e., $\text{Tag} = h_{p,s}(M) \oplus \text{Key}$. Eve cannot obtain any information of the Toeplitz hash function and the hash value due to the one-time pad. Eve can only randomly guess the initial vector $s$ and irreducible polynomial $p$. Eve can tamper with the message successfully if and only if he guesses a combination $\{t, m\}$ with a very small probability that meets the relationship $h_{p,s}(m) = t$. Eve sends a new (tampered) tag and message $\{\text{Tag}' = \text{Tag} \oplus t, M' = M \oplus m\}$ to the recipient Basel. In this case, the recipient will accept the message because of the one-time pad. Eve can tamper with the message successfully if and only if he guesses a combination $\{t, m\}$ with a very small probability that meets the relationship $h_{p,s}(M \oplus m) = h_{p,s}(M) \oplus h_{p,s}(m) = \text{Tag} \oplus t \oplus \text{Key}$. It must be mentioned that $m \neq 0$ due to the requirement of a valid forge. Thus, the failure probability $\epsilon_{\text{aut}}$ of authentication by using LFSR-based Toeplitz hashing can be defined by the probability of one successfully choosing a combination $\{t, m\}$ with the relationship $h(m) = t$ and $m \neq 0$,

$$
\epsilon_{\text{aut}} = \Pr[h_{p,s}(m) = t, m \neq 0].
$$

(1)

We remark that the attacker Eve does not have any prior information about $p$ and $s$ and can only guess randomly. Moreover, before Eve sends the tag and message to the recipient, Eve also cannot be sure if he guessed correctly even if he exhausts all the possibilities, which is with the information-theoretical security [3]. To quantify the failure probability $\epsilon_{\text{aut}}$, we need to consider two cases, $t = 0$ and $t \neq 0$. Note that $h_{p,s}(M)$ can be rewritten as

$$
h_{p,s}(M) = h_{p,M}(s) = \sum_{i=0}^{m-1} M_{i+1} W^i \cdot s,
$$

(2)

where $W$ is the $n \times n$ circulant matrix with the first row being $p$. Denote the characteristic value of $W$ as $\lambda_i$ $(i = 1, 2, 3, ..., n)$. One can diagonalize the matrix $\sum_{i=0}^{m-1} M_{i+1} W^i$, and the diagonal elements are $\lambda_i$. After
calculation, it can be verified that \( p(x) \) is just the characteristic polynomial of \( W \), which means that there is the relationship \( p(\lambda_i) = 0 \). For the first case \( h_{p,M}(s) = t = 0 \), since \( s \neq 0 \), \( h_{p,M}(s) = 0 \) only if there exists a zero diagonal element in the diagonalized matrix, i.e., it has a zero characteristic value. Thus, there exists a \( \lambda_i \) satisfying \( m(\lambda_i) = 0 \). This is equivalent to \( p(x)|m(x) \) since \( p(\lambda_i) = 0 \). The probability of such an event is at most the number of possible irreducible factors of \( M(x) \) divided by the total number of irreducible polynomials of degree \( n \). The former is at most \( m/n \), and the latter is at least \( 2^{n-1}/n \) [4]. Thus, the probability of \( h_{p,s}(m) = t = 0 \) is at most \( (m/n)/(2^{n-1}/n) = m/2^{n-1} \). We include all the cases in which there exists a \( \lambda_i \) satisfying \( m(\lambda_i) = 0 \) in the first case, which is equivalent to the fact that the rank of \( \sum_{i=0}^{m-1} M_{i+1}W^i \) is less than \( n \). Thus, for the second case \( h_{p,M}(s) = t \neq 0 \), the rank of \( \sum_{i=0}^{m-1} M_{i+1}W^i \) is equal to \( n \). This means that \( h_{p,M}(s) = \sum_{i=0}^{m-1} M_{i+1}W^i \cdot s \) is a bijection, i.e., one-to-one mapping. There are \( 2^n - 1 \) possible values of \( s \neq 0 \) corresponding to the \( 2^n - 1 \) different tag values, so the probability of \( h_{p,s}(m) = t \neq 0 \) is \( 1/(2^n - 1) \). Therefore, the upper bound on the failure probability of message authentication using LFSR-based Toeplitz hashing is [3]

\[
\epsilon_{\text{aut}} = \max \left\{ \frac{1}{2n-1}, \frac{m}{2^n-1} \right\} = \frac{m}{2^n-1}.
\]

We remark that message authentication is the premise and foundation for realizing the information-theoretical security of quantum key distribution [5], where the basis sift, error verification, and privacy amplification steps all require message authentication to ensure the information-theoretical security.

4. Secure OTUH-QDS against Bob’s forgery attack

Now, we will show that Bob’s forgery attack in our OTUH-QDS protocol will be related to Eve’s attack in secure message authentication, as shown in Fig. S2b. These two types of attacks are different but have many correlations. In message authentication, the message sender Adia and recipient Basel are honest and trust each other all the time. They will get together to against Eve’s attack. A successful attack in message authentication is when Eve changes the tag and message and the recipient will accept it. In our OTUH-QDS, there are two types of Bob’s forgery attacks since the signer Alice cannot be regarded as always honest. The first type is that Bob can generate a new signature and document if Alice has not signed a document at all. The second type is that Bob can change the signature and document if Alice has signed a document. Note that Bob does not have any information about the initial vector and the irreducible polynomial before he forwards the signed signature and document to charlie, which is the same as Eve in message authentication. We assume that the information-theoretically secure message authentication and OTUH-QDS will be performed many rounds to transfer multiple messages and sign multiple documents, respectively. Obviously, for the first round, the initial vector and irreducible polynomial are new and random. The failure probability is the same between Eve’s attack in message authentication and Bob’s forgery attack with the second type in OTUH-QDS since the attacker’s purpose and the conditions for success are exactly the same, i.e., the failure probability are both \( m/2^{n-1} \).

However, there is an important difference between message authentication and OTUH-QDS in the second round and beyond. In message authentication (Adia and Basel are always honest), the input initial vector and the irreducible polynomial can be fixed [5, 6] in later rounds since the attacker Eve cannot know the initial vector and the irreducible polynomial after message authentication has been performed. Bob also does not have any information about the initial vector and the irreducible polynomial before forwarding the signed document and signature to charlie. However, Charlie will forward his key bit strings to Bob after Charlie receives the document and signature forwarded by Bob. Thus, Bob can obtain all the information of the initial vector and the irreducible polynomial after the implementation of each round of digital signatures. To forbid Bob to exploit the information from the previous round to implement the attack. An important observation in our OTUH-QDS protocol is that the initial vector and the irreducible polynomial cannot be fixed and must be randomly updated in every round. In other words, the universal2 hash function will only be used once and then be updated. Thus, we denote it as one-time universal2 hashing, which is similar to the one-time pad.

5. Algorithms for testing irreducibility of polynomials over GF(2)

Irreducible polynomial.—A crucial point is that in every round, the signer must randomly choose an irreducible polynomial in our OTUH-QDS scheme. In our protocol, Alice finishes this task with an \( n \)-bit quantum random number. Denote the format of the irreducible polynomial as \( p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \), where \( a_i = 0 \) or 1. Then \( p(x) \) can be characterized by an \( n \)-bit string \( p = (a_{n-1}, a_{n-2}, \cdots, a_1, a_0) \), i.e., every bit of the string determines a corresponding coefficient of \( p(x) \). To generate the irreducible polynomial, Alice first uses the \( n \)-bit random number to generate a polynomial \( p_1(x) \), and checks out whether \( p_1(x) \) is irreducible. If \( p_1(x) \) is irreducible,
where $\nu$ is any prime factor of $n$ and $\gcd(f(x), g(x))$ represents the greatest common divisor (GCD) of $f(x)$ and $g(x)$. In our scheme, $n = 128 = 2^7$, i.e., $n$ only has one prime factor “2”. Thus, to verify condition (2), we just need to examine $\gcd\left(x^{2^7} - x, p(x)\right) = 1$. To speed up our calculation, we utilize fast modular composition (FMC) algorithms and an extended Euclidean algorithm [8]. The FMC algorithms can calculate $x^{2^{128}}$ and $x^{2^{64}} \mod p(x)$ with high speed by calculating $x^{2^{27}}$ and $x^{2^{34}}$, while the extended Euclidean algorithm can quickly finish the GCD calculation. Thus, conditions (A) and (B) can be verified efficiently. In our simulation, we search 1000 irreducible polynomials, and on average, it takes 73.6 tests to find an irreducible polynomial, consistent with the conclusion [3] that the total number of irreducible polynomials of order $n$ in GF(2) is at least $2^{n-1}/n$ and at most $2^n/n$ [4]. We implement our simulation in a desktop with an Intel i5-10400 CPU (with RAM of 8 GB), and on average, it takes approximately 0.36 seconds to generate an irreducible polynomial of order 128 from a 128-bit random input.

6. Numerical simulation of our QDS via quantum key distribution element

Considering the case that we have two quantum key distribution links between Alice-Bob and Alice-Charlie, the two links have the same loss. Alice and Bob share one set of secret keys $S_1$, while Alice and Charlie share the other set of secret keys $S_2$ by implementing quantum key distribution (QKD) with the key rate $R_{QKD}$. For the requirement of secret sharing, Alice, Bob and Charlie utilize $K_a$, $K_b$ and $K_c$ as their correlation keys, respectively, where $K_a = S_1 \oplus S_2$, $K_b = S_1$ and $K_c = S_2$. Therefore, the signature rate can be defined as $R_{QDS} = R_{QKD}/3n$, since one needs a 3n-bit key to implement OTUH and OTP in our OTUH-QDS protocol.

(6.1) Sending-or-not-sending twin-field quantum key distribution [9].

The secure key rate is given by

$$R_{QKD} = 2t(1-t)\mu e^{-\mu}Y_1 \left[1 - H\left(e_{1i}^{ph}\right)\right] - QZfH(E^Z),$$

where $t$ is the probability of sending the signal pulse at a signal window, $\mu$ is the intensity of the signal pulse, $Y_1$ is the counting rate of $Z_1$-windows, $QZ$ is the observed counting rate of $Z$-windows, $e_{1i}^{ph} = e_{1i}^{X1}$ is the phase-flip error rate for $Z_1$-windows, $E^Z$ is the bit error rate for $Z$-windows, and $f$ is the error correction efficiency. The yield $Y_1$ and error rate $e_{1i}^{X1}$ can be estimated by exploiting the decoy-state method,

$$Y_1 \geq \frac{\mu^2/2}{\mu^2 - \nu^2} \left[ e^{\nu}(Q_{00} + Q_{0\nu}) - \frac{\nu^2}{\mu^2} e^{\mu}(Q_{\mu0} + Q_{0\mu}) - 2 \frac{\mu^2 - \nu^2}{\mu^2} Q_{00} \right],$$

$$e_{1i}^{X1} \leq \frac{1}{2\nu Y_1} \left( e^{2\nu} E_{1i}^{pm} Q_{1i}^{pm} - \frac{1}{2} Y_0 \right),$$

where $\nu$ is the intensity of the decoy pulse, $Q_{k\nu,k\nu}$ is the gain when Alice chooses intensity $k_a$ and Bob chooses intensity $k_b$ ($k_a, k_b \in \{\mu, \nu, 0\}$), $E_{1i}^{pm}$ is the bit error rate, $Q_{1i}^{pm}$ is the gain of intensity $\nu$ for both Alice and Bob after successful postselected phase-matching and $Y_0 = Q_{00}$ is the counting rate of the vacuum state.
The gain $Q_{k_a,k_b}$ can be given as

$$Q_{k_a,k_b} = 2(1 - p_d)e^{-\frac{k_a + k_b}{2\eta}} \left[ I_0 \left( \sqrt{k_a k_b \eta} \right) - (1 - p_d) e^{-\frac{k_a + k_b}{2\eta}} \right],$$

(8)

where $\eta = \eta_d^2 \times 10^{-\alpha L/10}$ is the total efficiency and $\eta_d$, $\alpha$ and $L$ are the detector efficiency, attenuation coefficient and distance, respectively. $p_d$ is the dark count rate, and $I_0(x)$ is the modified Bessel function of the first kind. The gain $Q^\text{pm}_\nu$ and bit error rate $E^\text{pm}_\nu$ can be given by

$$Q^\text{pm}_\nu = Q^\text{pm}_{c,\nu} + Q^\text{pm}_{e,\nu},$$

(9)

$$E^\text{pm}_\nu = \left[ e_\nu^2 Q^\text{pm}_{c,\nu} + (1 - e_\nu^2) Q^\text{pm}_{c,\nu} \right] / Q^\text{pm}_\nu,$$

(10)

where $e_\nu^2$ is the misalignment rate of the X basis. Therein, the correct gain $Q^\text{pm}_{c,\nu}$ and incorrect gain $Q^\text{pm}_{e,\nu}$ are

$$Q^\text{pm}_{c,\nu} \approx \frac{1 - p_d}{\delta} \sqrt{\frac{\pi}{2\nu \sqrt{\eta}}} \text{erf} \left( \sqrt{\frac{\nu \sqrt{\eta}}{2\delta}} \right) - (1 - p_d)^2 e^{-2\nu \sqrt{\eta}},$$

(11)

$$Q^\text{pm}_{e,\nu} \approx \frac{1 - p_d}{\delta} e^{-2\nu \sqrt{\eta}} \sqrt{\frac{\pi}{2\nu \sqrt{\eta}}} \text{erfi} \left( \sqrt{\frac{\nu \sqrt{\eta}}{2\delta}} \right) - (1 - p_d)^2 e^{-2\nu \sqrt{\eta}},$$

(12)

where $\text{erf}(x)$ and $\text{erfi}(x)$ are the error function and imaginary error function, respectively. The gain $Q_Z$ and bit error rate $E^Z$ can be given by

$$Q_Z = (1 - t)^2 Q_0 + 2t(1 - t)Q \mu + t^2 Q \mu \mu,$$

(13)

and

$$E^Z = \frac{(1 - t)^2 Q_0 + t^2 Q \mu \mu}{(1 - t)^2 Q_0 + t(1 - t)(Q \mu \mu + Q \mu) + t^2 Q \mu \mu}.$$

(14)

In the simulation, we set $p_d = 10^{-8}$, $f = 1.1$, $\eta_d = 85\%$, $e_d = 2\%$ and $\alpha = 0.167$ dB/km. The light intensities and probability $t$ are globally optimized.

(6.2) Phase-matching quantum key distribution [10].

Here we present the simulation details of the phase-matching quantum key distribution. The overall secure key rate is given by

$$R_{\text{QKD}} = \frac{2}{D} Q \mu [1 - h(E^\text{ph}) - f h(E^b)],$$

(15)

where $Q \mu$ is the total gain of the signal pulses, $2/D$ is the phase-sifting factor with $D = 16$, $f$ is the error correction efficiency, $h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary entropy function, $E^\text{ph}$ is the phase error rate and $E^b$ is the bit error rate. The overall phase-error rate [11] is bounded by $E^\text{ph} \leq 1 - q_1$, where $q_1 = \mu e^{-\mu \nu} Y_1 / Q \mu$. By using the decoy state method with three intensities, the yield of the single-photon component can be given as

$$Y_1 \geq \frac{\mu}{\mu \nu - \nu^2} \left( Q \nu e^{\nu} - Q \mu e^{\nu} \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Q_0 \right).$$

(16)

For simulation, the gain of intensity $k$ ($k \in \{\mu, \nu, 0\}$) is $Q_k = 1 - (1 - 2p_d) e^{-k\eta}$. The bit error rate is $E^b = [p_d + \eta \mu (e_\Delta + e_d)] e^{-\eta_d \mu} / Q \mu$, where $p_d$ is the dark count rate, $\eta = \eta_d \times 10^{-\alpha L/20}$ is the channel transmittance, $e_\Delta$ is the extra misalignment error and the intrinsic error $e_\Delta = \sin^2 (\frac{\Delta}{2})$. In the simulation, we set $p_d = 10^{-8}$, $f = 1.1$, $\eta_d = 85\%$, $\alpha = 0.167$ dB/km and $e_d = 2\%$. The intensities $\mu, \nu$ are globally optimized.

(6.3) Discrete-modulated continuous-variable quantum key distribution [12].

In the case of reverse reconciliation, the secret key rate under collective attacks in the asymptotic limit is given by $R_{\text{QKD}} = p_{\text{pass}} [I(X; Z) - \max_{p \in S} \chi(Z; E)]$, where $I(X; Z)$ is the classical mutual information between Alice’s string
and the secret key rate is with experimental observations. According to [12], this key rate can be reformulated as a convex optimization problem, homodyne detection conditioned that Alice generates bit 0 or 1. The set $S$ contains all density operators compatible with experimental observations. According to [12], this key rate can be reformulated as a convex optimization problem, and the secret key rate is $R = \min_{\rho \in S} D(\rho || Z[\mathcal{G}(\rho)]) - p_{pass} \delta_{EC}$, where $D(\rho || \sigma) = Tr(\rho \log_2 \rho) - Tr(\rho \log_2 \sigma)$ is the quantum relative entropy. $\mathcal{G}$ is a map describing classical postprocessing. For the reverse reconciliation, we have $\mathcal{G}(\sigma) = K \sigma K^\dagger$, where $K = \sum_{\omega=0}^{1} |\omega\rangle_R \otimes (|0\rangle \langle 0| + |1\rangle \langle 1|)_A \otimes (|\mathcal{T}_2\rangle_R$ with $I_0 = \int_{-\infty}^{0} dq |q\rangle \langle q|$ and $I_1 = \int_{-\infty}^{\infty} dq |q\rangle \langle q|$. We set $\Delta_c = 0$ in our simulation. $Z$ is a pinching quantum channel, and we have $\mathcal{Z}(\rho) = \sum_j Z_j \rho Z_j$, where $Z_0 = |0\rangle \langle 0|_R \otimes I_{AB}$ and $Z_1 = |1\rangle \langle 1|_R \otimes I_{AB}$. $\delta_{EC} = (1 - \beta) H(Z) + \beta h(e)$ is the amount of information leakage per signal, where $e = \frac{1}{p_{pass}} \left( \frac{1}{2} \int_{-\Delta_c}^{0} p(q|0) dq + \frac{1}{2} \int_{0}^{\infty} p(q|1) dq \right)$. The convex optimization problem can be described as follows:

$$\begin{align*}
\text{minimize} \quad & D(\rho || Z[\mathcal{G}(\rho)]) \\
\text{subject to} \quad & Tr[\rho(\langle i \mid 1 \rangle \otimes \hat{q})] = p_x \langle \hat{q} \rangle_i, \\
& Tr[\rho(\langle i \mid \hat{p} + \hat{n} \rangle) = p_x \langle \hat{p} \rangle_i, \\
& Tr[\rho(\langle i \mid \hat{p} + \hat{n} \rangle) = p_x \langle \hat{n} \rangle_i, \\
& Tr[\rho(\langle i \mid \hat{d} \rangle) = p_x \langle \hat{d} \rangle_i, \\
& Tr[\rho] = 1, \\
& \rho \geq 0, \\
& Tr_B[\rho] = \sum_{i,j=0}^{3} \sqrt{F_{ij}} \langle \phi_j | i \rangle \langle i | A, \\
\end{align*}$$

(17)

where $\hat{n} = \frac{1}{2} (\hat{q}^2 + \hat{p}^2 - 1) = \hat{\alpha}^\dagger \hat{\alpha}$ and $\hat{d} = \hat{q}^2 - \hat{p}^2 = \hat{\alpha}^2 + (\hat{\alpha}^\dagger)^2$. We consider a quantum channel with transmittance $\eta = 10^{-0.167 L/10}$ where $L$ is the distance and excess noise $\xi = 0.01$. In such a model, we have $P(q|0) = \frac{1}{\sqrt{\pi(1+\eta \xi)}} e^{-\frac{[\alpha - \sqrt{\eta \xi}]^2}{1+\eta \xi}}$ and $P(q|1) = \frac{1}{\sqrt{\pi(1+\eta \xi)}} e^{-\frac{[\alpha + \sqrt{\eta \xi}]^2}{1+\eta \xi}}$. The expectation values can be given by

$$\begin{align*}
\langle \hat{q} \rangle = \sqrt{2 \eta} Re(\alpha), \\
\langle \hat{p} \rangle = \sqrt{2 \eta} Im(\alpha), \\
\langle \hat{n} \rangle = \eta |\alpha|^2 + \frac{\eta \xi}{2}, \\
\langle \hat{d} \rangle = \eta |\alpha|^2 + (\alpha^*)^2. \\
\end{align*}$$

(18)

$\alpha$ is the amplitude of the signal, and we optimize $\alpha$ in the interval of $[0.35, 0.6]$ with a step of 0.01.

(6.4) Gaussian-modulated continuous-variable quantum key distribution [13].

From an information-theoretic point of view, in the case of reverse reconciliation, Alice and Bob can distill perfectly correlated secret key bits provided that the amount of information they share $I_{AB}$ is higher than the information acquired by Eve $\chi_{BE}$ under collective attacks. Therefore, the secret key rate is defined as $R = I_{AB} - \chi_{AB}$. Considering the inefficiency of error correction, a factor $\beta$ is introduced as the reconciliation efficiency, and the secret key rate formula is $R_{QKD} = \beta I_{AB} - \chi_{AB}$. In our numerical simulation, we use $\beta = 0.95$. We calculate the mutual information using

$$I_{AB} = \frac{1}{2} \log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}},$$

(19)

where $V$ is the variance of the thermal state observed at Alice’s lab, and $\chi_{tot}$ is the total excess noise added between Alice and Bob. Here, we detail the formula of $\chi_{tot}$ as follows:

$$\chi_{tot} = \frac{1}{\eta T(1 + v_{el}) + \xi - 1},$$

(20)

where $T$ is the transmission of the quantum channel, $\xi$ is the excess noise, $v_{el}$ is the electronic noise and $\eta$ is the detection losses. To draw the line, we set $\eta = 0.85$, $v_{el} = 0$, $\xi = 0.01$, $T = 10^{-0.167 L/10}$ and $V$ is optimized. $L$ is
the distance. Under collective attacks, Eve’s accessible information is upper bounded by the Holevo quantity $\chi_{BE}$ satisfying

$$\chi_{BE} = G \left( \frac{\lambda_1 - 1}{2} \right) + G \left( \frac{\lambda_2 - 1}{2} \right) - G \left( \frac{\lambda_3 - 1}{2} \right) - G \left( \frac{\lambda_4 - 1}{2} \right), \tag{21}$$

where $G(x) = (x+1)\log_2(x+1) - x \log_2 x$, and $\{\lambda_i\}$ are the symplectic eigenvalues of the covariance matrix characterizing the quantum state. Calculation shows that $\lambda^2_{1,2} = \frac{1}{2} [A \pm \sqrt{A^2 - 4B}]$, where $A = V^2(1-2T) + 2T + T^2(V+\xi-1+\frac{1}{2})$ and $B = T^2(V/T - V + V\xi + 1)^2$ and $\lambda^2_{3,2} = \frac{1}{2} [C \pm \sqrt{C^2 - 4D}]$, where $C = \frac{V\sqrt{B+T(V+1/T-1+\xi)+A/\eta(1+\eta)/A}}{T(V+\xi/\eta)}$ and $D = \frac{\sqrt{B+V/\eta(1+\eta)-1}}{T(V+\xi/\eta)}$.

(6.5) Measurement-device-independent quantum key distribution [14].

For the measurement-device-independent quantum key distribution, we consider Alice and Bob sending a coherent state and the ideal case where only the channel loss and detector efficiency are taken into consideration. The secret key rate is given by

$$R_{QKD} = \frac{1}{2\epsilon^2 \eta^2}, \tag{22}$$

where $\epsilon$ is the natural constant, $\eta = \eta_d \times 10^{-\alpha L/20}$ is the total channel transmittance and $L$ is the distance between Alice and Bob. We set $\eta_d = 85\%$, $\alpha = 0.167$ dB/km.

**7. Numerical simulation of our QDS via quantum secret sharing element**

Different from quantum key distribution, quantum secret sharing can directly offer secret sharing correlation with unconditional security via quantum laws. In quantum secret sharing of three users, Alice is the dealer, while both Bob and Charlie are players. Even though one of Bob and Charlie is dishonest, they can also generate the secure correlation key $K_a = K_b \oplus K_c$. We assume that the distances of Alice-Bob and Alice-Charlie are the same. The signature rate can be defined as $R_{QDS} = R_{QSS}/3n$, since one needs a 3n-bit key for OTUH and OTP.

(7.1) Prepare-and-measure quantum secret sharing [15].

Using the Greenberger-Horne-Zeilinger (GHZ) state can realize quantum secret sharing directly. Here, we consider an equivalent prepare-and-measure protocol. In our simulation, we only consider the photon loss in the quantum channel and detector. Therefore, the secret key rate is given by

$$R_{QSS} = \eta^2, \tag{23}$$

where $\eta = \eta_d \times 10^{-\alpha L/10}$, $\eta_d = 85\%$ and $\alpha = 0.167$ dB/km. $L$ is the distance between Alice and Bob (Charlie).

(7.2) Measurement-device-independent quantum secret sharing [16].

By exploiting the postselected GHZ state, one can also realize quantum secret sharing. We only consider the photon loss from quantum channels and detectors here. The secret key rate of using a single-photon source can be given by

$$R_{QSS} = \frac{1}{4} \eta_d \eta^2. \tag{24}$$

Here, we have $\eta = \eta_d \times 10^{-\alpha L/10}$, $\eta_d = 85\%$, $\alpha = 0.167$ dB/km and assume that there is no loss of Alice’s photon. The factor 1/4 comes from only two of eight GHZ states that can be identified. $L$ is the distance between Alice and Bob (Charlie).

(7.3) Round-robin quantum secret sharing [17].

The secret key rate per pulse of the round-robin quantum secret sharing with a twin-field for sending $d$ coherent pulses each train in the case of the inside adversary can be written as

$$R_{QSS} = \frac{1}{d} \{ \hat{Q}[1 - h(\hat{e}_p)] - Qfh(\hat{e}_b) \}, \tag{25}$$
Supplementary Table S1. List of the experimental data used for one-time secure key generation.

|     | Alice-Bob (101 km) | Alice-Charlie (126 km) |
|-----|--------------------|------------------------|
| $n_z^\mu$ | 4616266           | 5225387                |
| $n_z^\nu$ | 258671            | 296285                 |
| $n_z^\omega$ | 258671          | 296285                 |
| $n_0^\mu$  | 11189             | 14080                  |
| $n_0^\nu$ | 1035046           | 1311484                |
| $n_0^\omega$ | 1035046         | 1311484                |
| $m_0^\omega$ | 3446             | 9401                  |

where we have $\hat{Q} = \min\{Q_A, Q_B\}$. $Q_A$ and $Q_B$ are the gains of Charlie’s successful detection from Alice and Bob, respectively. The phase error rate is

$$\hat{e}_p = \frac{e_{src}}{Q} + \left(1 - \frac{e_{src}}{Q}\right) \frac{n_{th}}{d-1}. \quad (26)$$

The average gain $Q$ and bit error rate $e_b$ of each train can be written as

$$Q = \frac{1}{2} [1 - (1 - dp_d)e^{-2\mu\eta}], \quad (27)$$

and

$$e_b = \frac{ed(1 - e^{-2\mu\eta}) + dp_de^{-2\mu\eta}/2}{1 - (1 - dp_d)e^{-2\mu\eta}}, \quad (28)$$

where $\eta = \eta_d \times 10^{-\alpha L/10}$ is the efficiency between Alice and Bob (Charlie). In addition, we have the gains $Q_A = Q_B = Q/2$ due to the symmetry. Let $n$ be the total photon number in a train of optical pulses with total intensity $\mu$. Then, the probability of finding more than $n_{th}$ photons in a train of optical pulses can be written as

$$\Pr(n > n_{th}) = e_{src} := 1 - \sum_{n=0}^{n_{th}} \frac{e^{-\mu\mu^n}}{n!}. \quad (29)$$

where $n_{th}$ is an integer constant chosen in this protocol. For the simulation, we set $p_d = 10^{-8}$, $f = 1.1$, $\eta_d = 85\%$, $\alpha = 0.167$ dB/km and $e_d = 2\%$. The intensity $\mu$, the selected integer $n_{th}$ and the number of optical pulses $d$ are globally optimized.

(7.4) Single-qubit quantum secret sharing [18].

For the single-qubit quantum secret sharing protocol with a single photon source, the final key rate can be easily derived based on phase-error correction

$$R_{QSS} = Q_1[1 - h(e_p) - fh(e_b)], \quad (30)$$

where $e_p = e_b = p_d(1 - 2e_d)/Q_1 + e_d$ and $Q_1 = \mu e^{-\mu}(2p_d + \eta - 2p_d\eta)$. $\eta = \eta_d \times 10^{-\alpha L/10}$ is the total transmittance; $2L$ is the total distance. The intensity $\mu$ is globally optimized. We set $p_d = 10^{-8}$, $f = 1.1$, $\eta_d = 85\%$, $\alpha = 0.167$ dB/km and $e_d = 2\%$.

(7.5) Differential-phase-shift quantum secret sharing [19].

The final key rate for differential-phase-shift quantum secret sharing using a twin-field is bounded by

$$R_{QSS} = Q_\mu[-(1 - 2\mu) \log_2(P_{co}) - fh(E_\mu)], \quad (31)$$

where $Q_\mu$ is the gain of the whole system. $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ is the Shannon entropy, and $f$ is the error correction efficiency. $P_{co}$ is the upper bound of collision probability when considering individual attacks,
which can be concluded as $P_{cc} = 1 - E_\mu^2 - (1 - 6E_\mu)^2/2$. The total gain and the total error rate with an intensity of $\mu$ are given by

$$Q_\mu = 1 - (1 - 2p_d)e^{-\mu\eta},$$

$$E_\mu Q_\mu = e_d Q_\mu + \left(\frac{1}{2} - e_d\right) 2p_d e^{-\mu\eta},$$

where $e_d$ is the misalignment error rate of detectors. $\eta = \eta_d \times 10^{-\alpha L/10}$ is the efficiency between Alice and Bob (Charlie), where $\eta_d$ is the detection efficiency of Charlie’s detectors. The intensity is globally optimized. We set $p_d = 10^{-8}$, $f = 1.16$, $\eta_d = 85\%$, $\alpha = 0.167$ dB/km and $e_d = 2\%$.

8. Experimental details

In the transmitting end, a master laser generates a repetition rate of 200 MHz and phase-randomized laser pulses 1.6 ns-wide at 1550.12 nm. To avoid using a phase modulator, we utilize two slave lasers to generate relative phases 0 and $\pi$ by using the quantum properties of the beam splitter. An asymmetric interferometer with a 2 ns time delay divides each master pulse into two pairs of optical pulses with relative phases 0 and $\pi$. Then, the two pairs of optical pulses are injected into two slave lasers through the optical circulator. With the help of controlling the trigger electrical signal of two slave lasers, one generates a quantum signal only in the first time-bin or the second time-bin to constitute the Z basis, and one prepares a quantum signal both in two time-bins with a 0 or $\pi$ phase difference to constitute the X basis. A 50 GHz bandwidth fiber Bragg grating is exploited to precompensate for pulse broadening and to remove extra spurious emission. The 2 ns-wide synchronization pulses with repetition rates of 100 kHz are transmitted via the quantum channel by using wavelength division multiplexed. The slave pulse width is 400 ps, which is much larger than the 10 ps timing resolution of the programmable delay chip, which means that the time consistency can be accurately calibrated. The spectral consistency is naturally satisfied through the laser seeding technique [20].

In the receiving end, a 30:70 biased beam splitter is used to perform passive basis detection after a wavelength division demultiplexer. A probability of 30% is measured in phase interference and the probability of 70% is used to receive in the time basis. A Faraday-Michelson interferometer realizes the phase measurement, where phase drift is compensated in real time by using the phase shifter. Two single photon detectors are used to measure the first time bin and the second time bin in the Z basis. Another two single photon detectors are used to measure the 0 and $\pi$ phase difference in the X basis. The total insertion losses of the time and phase bases are 4.25 and 8 dB, respectively. The efficiency of single-photon detectors is 20% at a 160 dark count per second. To decrease the after-pulse probability, we set the dead times to 10 and 25 $\mu$s for the Bob-Alice and Charlie-Alice links, respectively.

A four-intensity decoy-state protocol [21–23] is adopted, where the intensities of the Z basis are set as $\mu = 0.35$ and $\nu = 0.15$, and the intensity of the X basis is $\omega = 0.3$. The intensity of the vacuum state is 0, which does not contain any basis information. The corresponding probabilities are $p_\mu = 0.78$, $p_\nu = 0.1$, $p_\omega = 0.08$ and $p_0 = 0.04$. Thereinto, the amplitude modulator generates two different intensities, and the intensity of $\omega$ is double that of $\nu$ since it has two pulses in the X basis.

The error correction and privacy amplification are carried out using a field-programmable gate array. Each time, privacy amplification will be performed after accumulating data approximately to the size of 4 Mb via approximately ten times of error correction, where the data size excludes the amount of information leaked in error correction. For the link of Alice-Bob with 101 km (Alice-Charlie with 126 km), one needs to accumulate approximately 153 (560) seconds of data for privacy amplification to extract a secure key. Here, we only list the experimental data of one set and calculation results related to privacy amplification, as shown in Tables S1 and S2.

To compare with the experimental results, we use the relevant experimental parameters to simulate the secure key rate, as shown in Table III. The length of the final key, which is $\varepsilon$-correct and $\varepsilon$-sec-secure, can be given by [24, 25]

$$\ell = \sum_{i}^{\pi} \left[1 - h\left(\frac{\mu^{i}}{\nu^{i}}\right)\right] - \lambda_{EC} - \log_{2}\frac{2}{\varepsilon_{cor}} - 6\log_{2}\frac{22}{\varepsilon_{sec}},$$

where $h(x) := -x \log_{2} x - (1 - x) \log_{2} (1 - x)$, and $\pi (x)$ denotes the upper (lower) bound of the observed value $x$. Using the decoy-state method for finite sample sizes, the expected numbers of vacuum events $\sum_{0}^{\pi}$ and single-photon events $\sum_{1}^{\pi}$ can be written as

$$\sum_{0}^{\pi} = (e^{-\mu p_\mu} + e^{-\nu p_\nu}) \frac{\mu}{p_\mu},$$

and

$$\sum_{1}^{\pi} \geq \frac{\mu^{\nu} e^{-\mu p_\mu} + \mu^{\nu} e^{-\nu p_\nu}}{\mu^{\nu} - \nu^{\nu}} \times \left(e^{-\mu p_\mu} \frac{\mu}{p_\mu} - \nu^{\nu} e^{-\nu p_\nu} \frac{\nu}{p_\nu} - \mu^{\nu} e^{-\nu p_\nu} \frac{\nu}{p_\nu} - \mu^{\nu} e^{-\mu p_\mu} \frac{\mu}{p_\mu}\right),$$
where \( n_k^{x(z)} \) is the count of \( k \) \((k \in \{\mu, \nu, \omega\})\) intensity pulse measured in the \( Z(X) \) basis, and \( x^* \) is the corresponding expected value of observed value \( x \). The upper and lower bounds can be acquired \([26]\) by using the variant of the Chernoff bound, \( \overline{x} = x + \beta + \sqrt{2\beta x + \beta^2} \) and \( \underline{x} = x - \frac{\beta}{2} - \sqrt{2\beta x + \frac{\beta^2}{4}} \), where \( \beta = \ln \frac{2}{x_{\text{sec}}} \). The expected number of single-photon events \( x_{1}^{x(z)} \) in \( X_0 \) can be given by \([23]\)

\[
\overline{x}_{1}^{x(z)} = \frac{\mu \omega e^{-\omega} p_\omega}{\mu \nu - \nu^2} \left( e^{\nu} \frac{p_\nu}{p_\omega} - \frac{\nu^2}{\mu^2} e^{\mu \frac{p_\mu}{p_\omega}} - \frac{\mu^2 - \nu^2 \frac{m_0}{m_0}}{\mu^2} \right).
\]

(36)

In addition, the expected number of bit errors \( t_{1}^{xx} \) associated with the single-photon event in \( X_0 \) is \( t_{1}^{xx} \leq m_0^x - \frac{\epsilon x}{15} \), with \( t_{1}^{xx} = \frac{\epsilon x^x}{2p_\omega p_0} \frac{m_0^{x^x}}{p_0} \). For a given expected value, the upper and lower bounds of the observed value can be given as \( \overline{x} = x^* + \frac{\beta}{2} + \sqrt{2\beta x^* + \beta^2} \) and \( \underline{x} = x^* - \sqrt{2\beta x^*} \), respectively. By using random sampling without replacement, the phase error rate in the \( Z \) basis is

\[
\overline{e}_{1}^{zz} = \frac{t_{1}^{xx}}{\overline{x}_{1}^{xx}} + \gamma^U \left( \frac{t_{1}^{xx}}{\overline{x}_{1}^{xx}}, \frac{\overline{x}_{1}^{xx}}{\overline{x}_{1}^{xx}}, \frac{\overline{x}_{1}^{xx}}{\overline{x}_{1}^{xx}} \right)_{15},
\]

(37)

where we have \( \gamma^U(n, k, \lambda, \epsilon) = \frac{(1-2\lambda)^A G}{n+1} + \frac{\lambda A G}{(n+1)^e} + 4\lambda(1-\lambda)G}{2+\frac{\lambda G}{(n+1)^e}} \), with \( A = \max\{n, k\} \) and \( G = \frac{n+k}{nk} \). 

Experimental demonstration the single-bit-type QDS of Ref. \([27]\).

All the shared keys do not require error correction, and privacy amplification, i.e., \( n_\mu \), can be used for signature. For a one-bit message, suppose that \( 2L \) bits of keys are used. Then the security level of the signature can be bounded by \([28]\)

\[
\epsilon = \max(P(\text{honest abort}), P(\text{repudiation}), P(\text{forge})),
\]

(38)

\[
P(\text{honest abort}) = 2e^{-(s_a - \overline{E})^2 L},
\]

(39)

\[
P(\text{repudiation}) = 2e^{-(s_a - s_a)^2 L},
\]

(40)

\[
P(\text{forge}) = 2e^{-(s_a - s_a)^2 L}.
\]

(41)
where we choose \( s_a = \frac{p_c - E}{3}, s_v = \frac{2(p_c - E)}{3} \), and \( E \) is the upper bound bit error rate of the signal state. \( p_c \) can be determined by

\[
\frac{E}{2} + \frac{1}{2} (1 - h(p_c)) = h(p_c)
\]

(42)

where \( \frac{E}{2} = \frac{E}{n} \).

Note that it is different between the Bob-Alice link and Charlie-Alice link. The parameters \( E \) and \( p_c \) should choose the maximal and minimum values, respectively. By using the experimental data, we can estimate \( p_c = 7.06\% \), \( s_a = 5.79\% \), \( s_v = 4.52\% \) and \( E = 3.24\% \). Thus, to sign one bit, we need raw keys with \( 2L = 1.09 \times 10^6 \times 4.66 \times 10^5 \) bits, and the probability of honest abort, repudiation and forge are \( P(\text{honest abort}) = P(\text{repudiation}) = P(\text{forge}) = 10^{-38} \times 10^{-16} \), respectively. When the length of the document is one megabit, the signature security bound \( \hat{\epsilon} = 10^{-16} \) is \( \epsilon = 1 - (1 - e^{10^{-6}}) \approx 10^6 \). 

\[ \epsilon = 10^{-32} \times 10^{-10} \]

---

* hlyin@nju.edu.cn
† yfu@iphy.ac.cn
‡ zbchen@nju.edu.cn

[1] B. Schneier, Secrets and lies: digital security in a networked world (John Wiley & Sons, 2015).
[2] C. E. Shannon, Communication theory of secrecy systems, The Bell System Technical Journal 28, 656 (1949).
[3] M. O. Rabin, Probabilistic algorithms in finite fields, SIAM Journal on computing 9, 273 (1980).
[4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography (CRC press, 1997).
[5] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature 589, 214 (2021).
[6] M. O. Rabin, Probabilistic algorithms in finite fields, SIAM Journal on computing 9, 273 (1980).
[7] J. Von Zur Gathen and J. Gerhard, Modern computer algebra (Cambridge university press, 1999).
[8] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. A 89, 012318 (2010).
[9] Y. Fu, H.-L. Yin, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature 589, 214 (2021).
[10] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A 98, 062323 (2018).
[11] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X 8, 031043 (2018).
[12] P. Zeng, W. Wu, and X. Ma, Symmetry-protected privacy: beating the rate-distance linear bound over a noisy channel, Phys. Rev. Appl. 13, 064013 (2020).
[13] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymmetric security analysis of discrete-modulated continuous-variable quantum key distribution, Phys. Rev. X 9, 041064 (2019).
[14] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A 76, 042305 (2007).
[15] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. 108, 130503 (2012).
[16] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A 59, 1829 (1999).
[17] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent multipartite quantum communication, Phys. Rev. Lett. 114, 005001 (2015).
[18] J. Gu, Y.-M. Xie, W.-B. Liu, Y. Fu, H.-L. Yin, and Z.-B. Chen, Secure quantum secret sharing without signal disturbance monitoring, Opt. Express 29, 32244 (2021).
[19] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Experimental single qubit quantum secret sharing, Phys. Rev. Lett. 95, 230505 (2005).
[20] J. Gu, X.-Y. Cao, H.-L. Yin, and Z.-B. Chen, Differential phase shift quantum secret sharing using a twin field, Opt. Express 29, 9165 (2021).
[21] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tan, Z. Yuan, R. Penty, and A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics 10, 312 (2016).
[22] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. 94, 230505 (2005).
[23] J. Gu, X.-Y. Cao, H.-L. Yin, and Z.-B. Chen, Differential phase shift quantum secret sharing using a twin field, Opt. Express 29, 9165 (2021).
[24] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A 59, 1829 (1999).
[25] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent multipartite quantum communication, Phys. Rev. Lett. 114, 005001 (2015).
[26] J. Gu, Y.-M. Xie, W.-B. Liu, Y. Fu, H.-L. Yin, and Z.-B. Chen, Secure quantum secret sharing without signal disturbance monitoring, Opt. Express 29, 32244 (2021).
[27] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Experimental single qubit quantum secret sharing, Phys. Rev. Lett. 95, 230505 (2005).
[28] J. Gu, X.-Y. Cao, H.-L. Yin, and Z.-B. Chen, Differential phase shift quantum secret sharing using a twin field, Opt. Express 29, 9165 (2021).
[29] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tan, Z. Yuan, R. Penty, and A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics 10, 312 (2016).
[30] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. 94, 230505 (2005).
[27] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Phys. Rev. A 93, 032325 (2016).

[28] X.-B. An, H. Zhang, C.-M. Zhang, W. Chen, S. Wang, Z.-Q. Yin, Q. Wang, D.-Y. He, P.-L. Hao, S.-F. Liu, et al., Practical quantum digital signature with a gigahertz bb84 quantum key distribution system, Opt. Lett. 44, 139 (2019).