

Quantum designated verifier signature scheme based on Lagrange interpolation

Xu-Feng Li(李旭峰), Dong-Huan Jiang(姜东焕), Yu-Guang Yang(杨宇光), and Guang-Bao Xu(徐光宝)
Citation: Chin. Phys. B, 2026, 35 (**4**): 040304. DOI: 10.1088/1674-1056/ae0679
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Mode-pairing quantum key distribution with multi-step advantage distillation

Shizhuo Li(李世卓), Xin Liu(刘馨), Zhenrong Zhang(张振荣), and Kejin Wei(韦克金)
Chin. Phys. B, 2025, 34 (**9**): 090307. DOI: 10.1088/1674-1056/adf4a9

Protection path and security-metric-based resource allocation algorithm in quantum key distribution optical networks

Li Liu(刘力), Shengtong Zhai(翟晟童), Yao Pu(蒲瑶), and Xu Zhang(张旭)
Chin. Phys. B, 2025, 34 (**9**): 090306. DOI: 10.1088/1674-1056/adefd6

Verifiable quantum secret sharing scheme based on orthogonal product states

Chen-Ming Bai(白晨明), Lu Liu(刘璐), and Sujuan Zhang(张素娟)
Chin. Phys. B, 2024, 33 (**7**): 070302. DOI: 10.1088/1674-1056/ad342a

Efficient quantum private comparison protocol based on one direction discrete quantum walks on the circle

Jv-Jie Wang(王莒杰), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Chin. Phys. B, 2022, 31 (**5**): 050308. DOI: 10.1088/1674-1056/ac5a3f

Semi-quantum private comparison protocol of size relation with *d*-dimensional GHZ states

Bing Wang(王冰), San-Qiu Liu(刘三秋), and Li-Hua Gong(龚黎华)
Chin. Phys. B, 2022, 31 (**1**): 010302. DOI: 10.1088/1674-1056/ac1413

Quantum designated verifier signature scheme based on Lagrange interpolation

Xu-Feng Li(李旭峰)[1], Dong-Huan Jiang(姜东焕)[2], Yu-Guang Yang(杨宇光)[3], and Guang-Bao Xu(徐光宝)[1,†]

[1] *College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao* 266590, *China*
[2] *College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao* 266590, *China*
[3] *Faculty of Information Technology, Beijing University of Technology, Beijing* 100124, *China*

(Received 23 June 2025; revised manuscript received 30 August 2025; accepted manuscript online 15 September 2025)

Quantum designated verifier signature (QDVS) schemes can be applied in many scenarios, such as e-voting and electronic bidding. In this paper, we propose a novel QDVS scheme based on Lagrange interpolation. By avoiding the preparation of entangled states and the operation of comparing quantum states, our scheme effectively reduces the complexity of the signature scheme. In the process of identity authentication our scheme assigns a unique identity identifier to the signer Alice and the verifier Bob to ensure non-repudiation of the signature. Security analysis shows that the scheme can effectively resist common threats such as forgery attacks and interception attacks. In addition, the qubit efficiency of our scheme reaches 100%. Compared with existing QDVS schemes, the proposed scheme shows significant advantages in terms of resource consumption, computational complexity and practical application feasibility.

Keywords: quantum designated verifier signature, Lagrange interpolation, qubit efficiency

PACS: 03.67.Dd, 03.65.Ud

DOI: 10.1088/1674-1056/ae0679 **CSTR:** 32038.14.CPB.ae0679

1. Introduction

Digital signatures were originally proposed by Diffie and Hellman in 1976.[1] As an application based on asymmetric cryptography, the core of a digital signature lies in encrypting message digests through a private key to generate digital signatures that are widely used in a variety of fields such as e-commerce, digital certificates, file transfers and network communications. In the traditional digital signature system, the signer first uses a one-way hash function to digest the original message, generating a fixed-length digest. Subsequently, the signer encrypts the digest using his private key to generate a digital signature. This signature is transmitted along with the original message to the receiver. The security of traditional digital signature schemes relies on computational complexity, such as decomposing large numbers and solving discrete logarithmic problems. However, with the advent of quantum computing, these schemes may face serious challenges. In contrast, quantum signatures based on the quantum no-cloning theorem and the quantum uncertainty principle are more resilient to attacks brought about by increased computing power.

The quantum signature concept was first proposed by Gottesman and Chuang based on quantum one-way functions.[2] Subsequently, Li *et al*. proposed an arbitrated quantum signature scheme.[3] In their scheme, a trusted third party, which acts as an arbitrator, determines the validity of the signature. In 2015, a new quantum blind signature scheme based on Bell states was proposed.[4] Then many quantum blind signatures were proposed.[5–9] In 2024, a secure quantum group signature scheme based on three-qubit entangled states was proposed.[10] This scheme has unforgeability and non-repudiation, and is mainly applied to scenarios where group members' signatures and privacy protection are required. In addition, scholars have also put forward many quantum secret sharing protocols. For example, Bai *et al*.[42] suggested a verifiable quantum secret sharing protocol that adopts d-dimensional product states and Lagrange interpolation technology. Their scheme demonstrates both effectiveness and superiority in achieving secure and verifiable quantum secret sharing.

Quantum signature schemes have a wide range of applications. For example, in electronic bidding, bidders may utilize quantum signatures to authenticate their proposals, guaranteeing that only designated tenderers can validate bid authenticity. This feature protects the bidder's privacy.[11–16] In e-voting, voters can use quantum signatures to encrypt their ballot information, ensuring that only designated vote-counting agencies can verify the validity of the ballots.[17–23]

QDVS allows signers to designate one or more verifiers, and the validity of the signature can only be verified by designated verifiers. The QDVS scheme should possess the following security properties.[24–26]

(1) Correctness: If the signer uses the signature algorithm correctly and the signature is verified by the signature algorithm, then all designated verifiers should accept the validity

†Corresponding author. E-mail: xu_guangbao@163.com

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

of the signature.

(2) Non-transferability: Even if the verifier is convinced of the signature's authenticity, he cannot prove to any third party that the signature comes from the signer Alice or himself.

(3) Hiding the source: A third party cannot determine whether the signature comes from Alice or Bob; this feature protects the signers' privacy.

(4) Unforgeability: It is impossible to create a valid signature without the private keys of the signer and the designated verifier.

Due to the wide applicability of QDVS, many QDVS schemes have been proposed in recent years. Based on quantum one-way functions and Greenberger–Horne–Zeilinger (GHZ) states, Shi *et al.*[25] proposed a QDVS scheme in which the verifier, Bob, can generate the same signature as the signer, Alice, and the validity of the signature can only be verified by Bob. After analyzing Shi's scheme, Xin *et al.*[27] proposed a QDVS scheme based on Bell states. This new scheme overcame the shortcomings of Shi's scheme. Notably, Shi's scheme does not require any quantum one-way functions or quantum state comparison algorithms, achieving higher quantum bit efficiency. In terms of security, this scheme can resist forgery attacks, retransmission attacks and impersonation attacks. Then, Zhang *et al.*[28] proposed a QDVS scheme without a third party based on Bell states. The security of this scheme relies on the fundamental principles of quantum mechanics. The scheme does not require any quantum key distribution protocol (QKDP), quantum one-way functions or state swapping test operations, improving the efficiency of quantum signatures. However, the preparation of Bell states and GHZ states requires a lot of resources.

In this paper, we construct a QDVS scheme based on Lagrangian interpolation. Our scheme does not use entangled states, thereby avoiding the complications associated with their preparation. Additionally, it does not require the operation of quantum state comparison. These features significantly simplify the operational process and enhance the feasibility and practicality of our scheme. In addition, our scheme does not need to use quantum one-way functions, which improves the efficiency of the signature. Compared with existing schemes, our scheme achieves 100% qubit efficiency. Therefore, our scheme has better security and efficiency.

The paper is organised as follows. In Section 2, we introduce the necessary preliminary knowledge about this scheme. In Section 3, our QDVS scheme based on Lagrange interpolation is described in detail. In Section 4, the security of the scheme is analysed. A brief conclusion is given in Section 5.

2. Preliminaries

To facilitate understanding of our scheme, in this section we will briefly summarize the relevant preliminary knowledge.

Assume we have two random number sequences $x = (x_1, x_2, x_3, \ldots, x_n)$ and $y = (y_1, y_2, y_3, \ldots, y_n)$, where $x_i \neq x_j$ when $i \neq j$ for $j = 1, 2, 3, \ldots, n$ and $i = 1, 2, 3, \ldots, n$. We will construct the polynomial $L(x)$ from the sequences x and y using the Lagrange interpolation. $L(x)$ is the unique $(n-1)$-degree polynomial formed by the sequences x and y

$$l_i(x) = \prod_{j=1, j\neq i}^{n} \frac{x - x_j}{x_i - x_j}. \tag{1}$$

The Lagrange interpolation polynomial can be expressed as

$$L(x) = \sum_{i=1}^{n} y_i l_i(x). \tag{2}$$

To better understand this, we take a simple example. Assume the random number sequences $x = (1, 2, 4)$ and $y = (1, 4, 16)$. Now we need to calculate the interpolation result at $x = 3$. The corresponding Lagrange basis polynomials $l_1(x), l_2(x), l_3(x)$ are

$$\begin{aligned} l_1(x) &= \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} = \frac{(x-2)(x-4)}{(1-2)(1-4)} \\ &= \frac{1}{3}(x-2)(x-4), \end{aligned} \tag{3}$$

$$\begin{aligned} l_2(x) &= \frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} = \frac{(x-1)(x-4)}{(2-1)(2-4)} \\ &= -\frac{1}{2}(x-1)(x-4), \end{aligned} \tag{4}$$

$$\begin{aligned} l_3(x) &= \frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)} = \frac{(x-1)(x-2)}{(4-1)(4-2)} \\ &= \frac{1}{6}(x-1)(x-2). \end{aligned} \tag{5}$$

So, we can obtain the Lagrange interpolation polynomial

$$\begin{aligned} L(x) &= y_1 l_1(x) + y_2 l_2(x) + y_3 l_3(x) \\ &= 1 \times \frac{1}{3}(x-2)(x-4) - 4 \times \frac{1}{2}(x-1)(x-4) \\ &\quad + 16 \times \frac{1}{6}(x-1)(x-2) \\ &= x^2. \end{aligned} \tag{6}$$

We calculate the interpolation result at $x = 3$ and obtain $L(3) = 9$.

3. Our QDVS scheme

Our QDVS scheme includes four phases: initialization phase, key generation phase, signature phase and verification phase. In our scheme, Alice represents the signer, Bob represents the verifier and Trent represents the trusted third party. The main steps of the QDVS scheme are shown in Fig. 1.

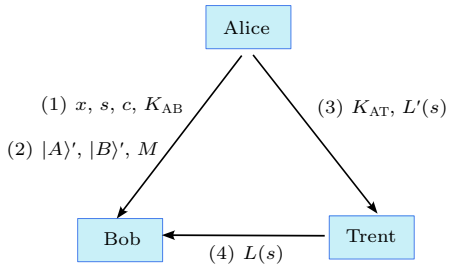


Fig. 1. Schematic of the QDVS scheme. (1) Alice shares random sequences numbers x, c, random number s and K_{AB} with Bob. (2) Alice calculates $|A\rangle, |B\rangle$, then adds decoy particles to $|A\rangle$ and $|B\rangle$ to obtain $|A\rangle'$ and $|B\rangle'$. She sends $|A\rangle', |B\rangle'$ and M to Bob. Bob receives $|A\rangle', |B\rangle'$ and calculates $L'(s)$. (3) Alice shares K_{AT} with Trent. Alice calculates $L'(s)$ and sends it to Trent. (4) Trent publishes the value of $L(s)$ on the public board. Bob compares $L'(s)$ with $L(s)$.

3.1. Initialization phase

Let $Y = |0\rangle\langle 1| - |1\rangle\langle 0|$, $Y^- = |1\rangle\langle 0| - |0\rangle\langle 1|$ and $YY^- = (Y^-)Y = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. $X = |1\rangle\langle 0| + |0\rangle\langle 1|$ and $XX = I$. F is a function that converts a binary number to a decimal number. The symbol "$\oplus$" is the XOR operation.

Alice and Bob each have their own identity identifiers, and these two identifiers are public between them. Assume that Alice's identity is $ID_A = (ID_{A_1}, ID_{A_2}, \ldots, ID_{A_i}, \ldots, ID_{A_n})$ and Bob's identity is $ID_B = (ID_{B_1}, ID_{B_2}, \ldots, ID_{B_i}, \ldots, ID_{B_n})$, where $ID_A \in \{0,1\}^n$ and $ID_B \in \{0,1\}^n$ for $i = 1,2,3,\ldots,n$. All the symbols and their descriptions are provided in Table 1.

Table 1. Notation table.

Symbol	Description
Y, Y^-, X	unitary operations
$\oplus$	XOR operation
F	binary conversion function
H	Hadamard operator
ID_A, ID_B	identification of identities
K_{AB}, K_{AT}	private keys
M	the message to be signed
h	decoy particle

3.2. Key generation phase

Alice shares the n-bit private key $K_{AB} = (K_{AB_1}, K_{AB_2}, \ldots, K_{AB_n}) \in \{0,1\}^n$, the n-bit random number $c = (c_1, c_2, c_3, \ldots, c_n) \in \{0,1\}^n$, $x = (x_1, x_2, x_3, \ldots, x_n)$ and the decimal random number s ($s \in n$) with Bob through QKDP,[29–31] where $x_i \neq x_j$ when $i \neq j$ for $j = 1,2,3,\ldots,n$ and $i = 1,2,3,\ldots,n$.

Trent shares the n-bit private key $K_{AT} = (K_{AT_1}, K_{AT_2}, \ldots, K_{AT_n}) \in \{0,1\}^n$ with Alice through QKDP.

3.3. Signature phase

Let $M = (m_1, m_2, m_3, \ldots, m_n)$ is a $2n$-bit message that needs to be signed, where $m_i \in \{00, 01, 10, 11\}$ for $i = 1,2,3,\ldots,n$.

Step 1: Alice forms an n-bit string $a = (a_1, a_2, a_3, \ldots, a_n) \in \{0,1\}^n$ and $b = (b_1, b_2, b_3, \ldots, b_n) \in \{0,1\}^n$ with M, where a_i is the first bit of m_i and b_i is the second bit of m_i for $i = 1,2,3,\ldots,n$.

Alice uses function F to convert the binary number m_i into the decimal number y_i, where $y = (y_1, y_2, y_3, \ldots, y_n)$ for $y_i \in \{0,1,2,3\}$ and $i = 1,2,3,\ldots,n$. The conversion process is shown in Table 2.

Table 2. Conversion table.

Signed message	Value after conversion
$m_i = 00$ ($a_i = 0, b_i = 0$)	$y_i = 0$
$m_i = 01$ ($a_i = 0, b_i = 1$)	$y_i = 1$
$m_i = 10$ ($a_i = 1, b_i = 0$)	$y_i = 2$
$m_i = 11$ ($a_i = 1, b_i = 1$)	$y_i = 3$

Step 2: Alice calculates the Lagrangian interpolation polynomial $L(x)$ according to the sequences x and y. The calculation method is shown in the preliminaries.

When Alice completes the calculation, she will obtain a polynomial $L(x)$ of degree $(n-1)$ in terms of x. Then Alice calculates the value of $L(x)$ at $x = s$ and obtains $L(s)$, where $L(s)$ is a decimal number. Then she encrypts $L(s)$ using the key K_{AT} and sends it to Trent.

Step 3: (1) Alice converts the classical sequences $a = (a_1, a_2, a_3, \ldots, a_n) \in \{0,1\}^n$ and $b = (b_1, b_2, b_3, \ldots, b_n) \in \{0,1\}^n$ into quantum sequences $|a\rangle$ and $|b\rangle$, respectively.

$$|a\rangle = \{|a_1\rangle, |a_2\rangle, \ldots, |a_n\rangle\}, |a_i\rangle \in \{|0\rangle, |1\rangle\}, \tag{7}$$

$$|b\rangle = \{|b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle\}, |b_i\rangle \in \{|0\rangle, |1\rangle\}. \tag{8}$$

(2) Alice performs the operation $Y^{c_i \oplus ID_{B_i}} H^{K_{AB_i} \oplus ID_{A_i}}$ on each $|a_i\rangle$ to obtain

$$|A_i\rangle = Y^{c_i \oplus ID_{B_i}} H^{K_{AB_i} \oplus ID_{A_i}} |a_i\rangle, \quad i = 1,2,3,\ldots,n. \tag{9}$$

Alice performs the operation $X^{c_i \oplus ID_{B_i}} H^{K_{AB_i} \oplus ID_{A_i}}$ on each $|b_i\rangle$ to obtain

$$|B_i\rangle = X^{c_i \oplus ID_{B_i}} H^{K_{AB_i} \oplus ID_{A_i}} |b_i\rangle, \quad i = 1,2,3,\ldots,n. \tag{10}$$

(3) Then Alice obtains the quantum sequences $|A\rangle = (|A_1\rangle, |A_2\rangle, \ldots, |A_n\rangle)$ and $|B\rangle = (|B_1\rangle, |B_2\rangle, \ldots, |B_n\rangle)$, where $|A_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and $|B_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ for $i = 1, 2, \ldots, n$.

Step 4: To detect eavesdropping, Alice generates $2h$ decoy particles, each of which is randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. She adds $2h$ decoy particles at random to the quantum sequences $|A\rangle = \{|A_1\rangle, |A_2\rangle, \ldots, |A_n\rangle\}$ and $|B\rangle = \{|B_1\rangle, |B_2\rangle, \ldots, |B_n\rangle\}$. Then she obtains the quantum sequences $|A\rangle'$ and $|B\rangle'$.

Then Alice sends the quantum sequences $|A\rangle'$, $|B\rangle'$ and message M to Bob.

3.4. Verification phase

Step 1: After Bob has received the quantum sequences $|A\rangle'$, $|B\rangle'$ and message M, Alice publishes the positions and the initial states of all the decoy particles mixed in the quantum sequences $|A\rangle'$ and $|B\rangle'$. Bob measures the decoy particles

with the corresponding measurement bases and compares the measurement results with the initial decoy particles published by Alice. If there is no error, Bob gets the quantum sequences $|A\rangle$ and $|B\rangle$; otherwise, he restarts the protocol.

Step 2: Bob performs $H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}(Y^-)^{c_i\oplus ID_{\mathrm{B}_i}}$ operation on $|A_i\rangle$ and $H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}X^{c_i\oplus ID_{\mathrm{B}_i}}$ on $|B_i\rangle$, where $i = 1,2,3,\ldots,n$,

$$\left|a_i'\right\rangle = H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}(Y^-)^{c_i\oplus ID_{\mathrm{B}_i}}\left|A_i\right\rangle, \tag{11}$$

$$\left|b_i'\right\rangle = H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}X^{c_i\oplus ID_{\mathrm{B}_i}}\left|B_i\right\rangle. \tag{12}$$

Then Bob can obtain the quantum sequences $|a'\rangle$ and $|b'\rangle$. Bob measures each $|a_i'\rangle$ with the basis of $\{|0\rangle,|1\rangle\}$. If the measurement result is 0, Bob sets $a_i' = 0$; otherwise, $a_i' = 1$. Similar to this, Bob measures each $|b_i'\rangle$ with the basis of $\{|0\rangle,|1\rangle\}$. If the measurement result is 0, Bob sets $b_i' = 0$; otherwise, $b_i' = 1$. Then he obtains the classical sequences $a' = (a_1', a_2', a_3', \ldots, a_n') \in \{0,1\}^n$ and $b' = (b_1', b_2', b_3', \ldots, b_n') \in \{0,1\}^n$. According to the values of sequences a' and b', Bob can obtain the sequence $y' = (y_1', y_2', y_3', \ldots, y_n')$ by using the function F, where $y_i' \in \{0,1,2,3\}$ for $i = 1,2,3,\ldots,n$.

Step 3: Bob calculates the polynomial $L'(x)$ according to x and y'. He obtains a polynomial $L'(x)$ of degree $(n-1)$ in terms of x. Then he lets $x = s$ to obtain the value of $L'(s)$.

After Bob completes the calculation, he sends a notice to Trent. After receiving the notice, Trent publishes the value of $L(s)$ on the public board. Then Bob compares $L(s)$ with $L'(s)$. If $L(s) = L'(s)$, he accepts the signature; otherwise, he rejects the signature.

4. Correctness

In this section, we verify the correctness of the signature scheme. According to Eqs. (9)–(12), we can obtain

$$\left|a_i\right\rangle = H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}(Y^-)^{c_i\oplus ID_{\mathrm{B}_i}}Y^{c_i\oplus ID_{\mathrm{B}_i}}H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}\left|a_i\right\rangle, \tag{13}$$

$$\left|b_i\right\rangle = H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}X^{c_i\oplus ID_{\mathrm{B}_i}}X^{c_i\oplus ID_{\mathrm{B}_i}}H^{K_{\mathrm{AB}_i}\oplus ID_{\mathrm{A}_i}}\left|b_i\right\rangle, \tag{14}$$

where $i = 1,2,3,\ldots,n$. So Bob can calculate the same classical sequences a and b as Alice. Then he can obtain the sequence y and calculate the value of $L'(s)$. Therefore, the whole process of the signature scheme is correct.

To verify the correctness of the protocol, we simulate the operations of Alice and Bob using the Origin Quantum Computing Platform.

In the experiment, we employed two qubits, both initialized in the state $|0\rangle$, and conducted the experiment 1000 times using the Monte Carlo method for simulation. The operations performed by Alice on the quantum states are illustrated in Fig. 2. From Fig. 2, we can see that Alice first applies the H operation to the first $|0\rangle$ state followed by the Y operation. For the second $|0\rangle$ state, she first applies the H operation followed by the X operation. The quantum states that may appear after Alice's operation, and the probability of each quantum state occurring, are shown in Fig. 3. From Figs. 2 and 3, it can be observed that the original quantum state undergoes collapse after Alice performs HY and HX operations on the initial quantum state $|0\rangle$.

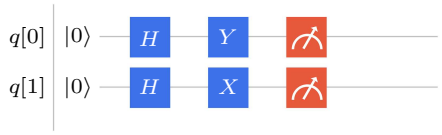


Fig. 2. The quantum circuit diagram of Alice.



Fig. 3. The experimental results of signer Alice.

Subsequently, Bob performs the operations on the quantum states as shown in Fig. 4, which can be regarded as a continuation of Alice's operations. Specifically, Bob first performs the HY operation on the first $|0\rangle$ state followed by the YH operation. For the second $|0\rangle$ state, he first performs the HX operation followed by the XH operation. The final quantum states after Bob's operations are depicted in Fig. 5. Therefore, through the experiment, we have verified the correctness of Eqs. (13) and (14).

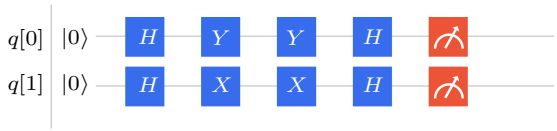


Fig. 4. The quantum circuit diagram of Bob.

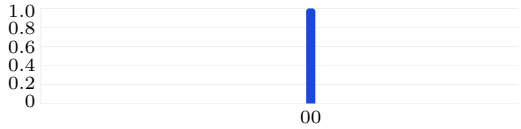


Fig. 5. The experimental results of verifier Bob.

The above arguments demonstrate the validity of our QDVS scheme.

5. Security analysis

5.1. Entanglement measurement attack

In this section, we analyze entanglement measurement attacks. In our QDVS scheme, Alice randomly selects decoy particles from the set $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ and adds them to the quantum sequences $|A\rangle$ and $|B\rangle$, resulting in quantum sequences $|A\rangle'$ and $|B\rangle'$, and then sends them to Bob.

Assume there is an attacker, Eve, who attempts to intercept these sequences during transmission and perform some

operations. Eve performs a collective operation U and an auxiliary system $|\eta\rangle$ on each particle of the quantum sequences $|A\rangle'$ and $|B\rangle'$. Eve's attack process is as follows:

$$\begin{aligned}
U(|0\rangle|\eta\rangle) &= \alpha|0\rangle|\eta_1\rangle+\beta|1\rangle|\eta_2\rangle,\\
U(|1\rangle|\eta\rangle) &= \alpha'|0\rangle|\eta_1'\rangle+\beta'|1\rangle|\eta_2'\rangle; \qquad (15)\\
U(|+\rangle|\eta\rangle) &= \frac{1}{\sqrt{2}}(\alpha|0\rangle|\eta_1\rangle+\beta|1\rangle|\eta_2\rangle\\
&\quad+\alpha'|0\rangle|\eta_1'\rangle+\beta'|1\rangle|\eta_2'\rangle)\\
&= \frac{1}{2}\{|+\rangle(\alpha|\eta_1\rangle+\beta|\eta_2\rangle+\alpha'|\eta_1'\rangle+\beta'|\eta_2'\rangle)\}\\
&\quad+\frac{1}{2}\{|-\rangle(\alpha|\eta_1\rangle-\beta|\eta_2\rangle\\
&\quad+\alpha'|\eta_1'\rangle-\beta'|\eta_2'\rangle)\}, \qquad (16)\\
U(|-\rangle|\eta\rangle) &= \frac{1}{\sqrt{2}}(\alpha|0\rangle|\eta_1\rangle+\beta|1\rangle|\eta_2\rangle\\
&\quad-\alpha'|0\rangle|\eta_1'\rangle-\beta'|1\rangle|\eta_2'\rangle)\\
&= \frac{1}{2}\{|+\rangle(\alpha|\eta_1\rangle+\beta|\eta_2\rangle-\alpha'|\eta_1'\rangle-\beta'|\eta_2'\rangle)\}\\
&\quad+\frac{1}{2}\{|-\rangle(\alpha|\eta_1\rangle-\beta|\eta_2\rangle\\
&\quad-\alpha'|\eta_1'\rangle+\beta'|\eta_2'\rangle)\}, \qquad (17)
\end{aligned}$$

where U holds $U^\dagger U=I$. So, we can get

$$\begin{aligned}
|\alpha|^2\langle\eta_1|\eta_1\rangle+|\beta|^2\langle\eta_2|\eta_2\rangle=1,\\
|\alpha'|^2\langle\eta_1'|\eta_1'\rangle+|\beta'|^2\langle\eta_2'|\eta_2'\rangle=1. \qquad (18)
\end{aligned}$$

To avoid being detected during the eavesdropping, Eve needs to ensure that the particles $\{|0\rangle,|1\rangle\}$ in the quantum sequences $|A\rangle'$ and $|B\rangle'$ remain in their original states after the entanglement measurement attack. If the particles $\{|0\rangle,|1\rangle\}$ are disturbed after the entanglement measurement attack, then Eve's attack behavior will be detected.[32–34] To ensure that the attacking behavior is not detected, Eve's operation U needs to satisfy the conditions $\alpha=\beta'=1$, $\alpha'=\beta=0$. Therefore, we obtain

$$\begin{aligned}
U(|0\rangle|\eta\rangle)=|0\rangle|\eta_1\rangle,\\
U(|1\rangle|\eta\rangle)=|1\rangle|\eta_2'\rangle. \qquad (19)
\end{aligned}$$

From to Eq. (19), we can get

$$\begin{aligned}
U(|+\rangle|\eta\rangle) &= \frac{1}{\sqrt{2}}U((|0\rangle+|1\rangle)|\eta\rangle)\\
&= \frac{1}{\sqrt{2}}[U(|0\rangle|\eta\rangle)+U(|1\rangle|\eta\rangle)]\\
&= \frac{1}{\sqrt{2}}[|0\rangle|\eta_1\rangle+|1\rangle|\eta_2'\rangle]\\
&= \frac{1}{2}[|+\rangle(|\eta_1\rangle+|\eta_2'\rangle)+|-\rangle(|\eta_1\rangle-|\eta_2'\rangle)], \qquad (20)\\
U(|-\rangle|\eta\rangle) &= \frac{1}{\sqrt{2}}U((|0\rangle-|1\rangle)|\eta\rangle)\\
&= \frac{1}{\sqrt{2}}[U(|0\rangle|\eta\rangle)-U(|1\rangle|\eta\rangle)]\\
&= \frac{1}{\sqrt{2}}[|0\rangle|\eta_1\rangle-|1\rangle|\eta_2'\rangle]\\
&= \frac{1}{2}[|+\rangle(|\eta_1\rangle-|\eta_2'\rangle)+|-\rangle(|\eta_1\rangle+|\eta_2'\rangle)]. \qquad (21)
\end{aligned}$$

Similarly, in order to eavesdrop on the quantum channel without being detected, after the entanglement measurement attack the original states $\{|+\rangle,|-\rangle\}$ in the quantum sequences $|A\rangle'$ and $|B\rangle'$ should also remain unaffected. Therefore, Eqs. (16) and (17) should satisfy

$$\begin{aligned}
U(|+\rangle|\eta\rangle)=\frac{1}{2}|+\rangle(|\eta_1\rangle+|\eta_2'\rangle),\\
U(|-\rangle|\eta\rangle)=\frac{1}{2}|-\rangle(|\eta_1\rangle+|\eta_2'\rangle). \qquad (22)
\end{aligned}$$

Therefore, in our scheme, although the attacker Eve may attempt to obtain information about the quantum sequence through entanglement measurement attacks, according to the conclusion of Eq. (22), the auxiliary particles remain in their initial state even after the entanglement measurement attack. This ensures that the attacker Eve cannot extract any information about the quantum sequence from the auxiliary system $|\eta\rangle$. Thus, our QDVS scheme can resist Eve's attacks.

5.2. Designated verifcation property

In this scheme, Alice and Bob share the key K_{AB} through the unconditionally secure BB84 protocol,[25,35,36] which ensures the security of the key. Thus, it eliminates the possibility of other parties using the key to obtain signature-related information. In the message transmission phase, all information is encrypted with the keys to ensure the security of the transmitted information.

In addition, the validity verification of the signature relies on comparing the values of $L(s)$ and $L'(s)$. The value of $L(s)$ is published by Trent, and remains confidential before Bob provides feedback to Trent. So third parties are unable to gain knowledge of the secret. Therefore, the validity of the signature can only be verified by Bob.

5.3. Non-transferability

Non-transferability is one of the properties of the QDVS. The designated verifiers cannot prove to any third party that the signature was generated by the signer or themselves.

In our QDVS scheme, the signer Alice and the verifier Bob share the key K_{AB} and a set of random number sequences. During the encryption phase, Alice constructs the Lagrange interpolation polynomial $L(x)$ using the random number sequence x shared with Bob and the sequence y derived from the signature information. She then computes the value of $L(s)$ using the shared random number s, and sends it to Trent. After Bob finishes the calculation and obtains the value of $L'(s)$, he notifies Trent, who then makes the value of $L(s)$ public. Bob then determines the validity of the signature by comparing the values of $L'(s)$ and $L(s)$. Thus, it can be seen that Bob can

generate the same signature as Alice but he cannot prove the true source of the signature to a third party. Even if the keys of Alice and Bob are made public, a third party cannot determine whether the signature was generated by the signer Alice or simulated by the verifier Bob.

Therefore, our scheme has non-transferability, which ensures that the true source of the signature will not be disclosed, thus protecting the privacy of the signer. In addition, Bob cannot prove to a third party whether the signature was forged by him, which also prevents the signature from being misused or abused.

5.4. Unforgeability

In our QDVS scheme, both Alice and Bob can generate the same signature, but Bob cannot prove the true source of the signature to a third party. Therefore, Bob cannot forge a valid signature.

Assume that Eve is an external attacker who wants to forge the signature information M. However, according to the BB84 protocol the private key K_{AB} is shared between Alice and Bob, which ensures unconditional security of K_{AB}. Therefore, Eve cannot forge the signature by stealing the key. Therefore she can only obtain information about M by eavesdropping on quantum sequences $|A\rangle$ and $|B\rangle$. During the transmission process, we randomly add decoy particles $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to quantum sequences $|A\rangle$ and $|B\rangle$. As described in Refs. [38–41], Eve's eavesdropping behavior during the sequence transmission process will inevitably be detected by the signer Alice or the verifier Bob.

Thus, Eve is unable to forge the signature, demonstrating that our scheme achieves unforgeability.

5.5. Hidden source

The proposed QDVS scheme has the property of information hiding, which can effectively protect the signer's privacy. In some special circumstances, when the signer wishes to conceal the signed information, source hiding can play a critical role. In our scheme, the signer Alice and the verifier Bob can generate the same signing information. No third party can prove who actually signed the information, even if the private keys of Alice and Bob are publicly disclosed.

6. Comparisons with other schemes

In this section, we mainly analyze the aspects of security and efficiency, and compare our scheme with similar QDVS schemes. The results of the comparison are shown in Table 3.

Table 3. Comparisons with other schemes.

schemes	Designated verifier	Quantum one-way function	Entangled state	Efficiency
Ref. [24]	single	No	No	100%
Ref. [25]	single	Yes	Yes	50%
Ref. [26]	single	Yes	No	33.3%
Ref. [27]	single	No	Yes	66.7%
Our scheme	single	No	No	100%

First, we analyze the efficiency of the protocol. The qubit efficiency η_q is defined as $\eta_q = \delta_1/\delta_2$, where δ_1 represents the number of classical bits transmitted during quantum transmission and δ_2 represents the total number of quantum bits transmitted by the quantum channel (the quantum bits used to detect eavesdropping attacks, as well as the keys and random numbers transmitted and shared during the quantum key distribution phase are ignored). In this scheme, Alice sends the quantum bit sequences $|A'\rangle$ and $|B'\rangle$ to Bob. So, the total number of transmitted qubits $\delta_2 = 2n$. During the verification stage, Bob decodes the quantum bit sequences $|A'\rangle$ and $|B'\rangle$ to obtain n-bit classical information a' and b', Thus, the total number of transmitted classical bits is $\delta_1 = 2n$. By calculation, the quantum bit efficiency is given by $\eta_q = \delta_1/\delta_2 = 2n/2n = 100\%$.

Second, many existing QDVS schemes rely on the preparation of entangled states such as Bell states and GHZ states.[27,29] However, the preparation process of these entangled states not only has high technical requirements but also consumes significant resources, which is an important limiting factor in practical applications. In contrast, our scheme avoids the preparation of entangled states, thereby significantly reducing resource consumption and improving the feasibility and practicality of the scheme.

In addition, our scheme employs the Lagrange interpolation. In this approach, the validity of the signature is determined by comparing the values of $L(s)$ and $L'(s)$. This process completely eliminates the operation of comparing quantum states, not only simplifying the verification process but also significantly improving the efficiency of the signature. In this way, our scheme greatly enhances execution efficiency while maintaining a high level of security.

7. Conclusion

Most existing QDVS schemes rely on the preparation of entangled states and a comparison of quantum states, which not only increase the complexity of the signing process but also limit their practical applicability. To address these issues, we propose a QDVS scheme based on Lagrange interpolation,

which significantly enhances the efficiency of signature verification.

Our scheme does not require the preparation of entangled states, quantum state comparison operations or quantum one-way functions, thereby reducing the complexity of the signature. Through rigorous theoretical analysis and simulation experiments, it has been demonstrated that this scheme possesses various security features, including resistance to eavesdropping attacks, non-repudiation and source hiding. Furthermore, the scheme is also capable of resisting forgery, interception and impersonation attacks. Additionally, the qubit efficiency of our scheme reaches 100%. Therefore, our scheme is practical, secure and efficient.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No. 62171264), the Natural Science Foundation of Shandong Province of China (Grant No. ZR2023MF080), and Beijing Natural Science Foundation (Grant No. 4252014).

References

[1] Diffie W and Hellman M 1976 *IEEE Trans. Inf. Theory* **22** 664
[2] Gottesman D and Chuang I L 2001 *Quantum Physics*
[3] Li Q, Li C Q, Chan W L, Wang C J and Long D Y 2013 *Quantum Inf. Process* **12** 2427
[4] Shi W M, Zhang J B, Zhou Y H and Yang Y G 2015 *Quantum Inf. Process* **14** 3019
[5] Lai H, Luo M X, Pieprzyk J, Qu Z G, Li S D and Orgun M A 2017 *China Inf. Sci.* **60** 082501
[6] Feng X N, Wu H Y, Zhou X L and Yao Y 2023 *Quantum Inf. Process* **22** 5
[7] Zhang M H and Xie J H 2022 *Mod. Phys. Lett. B* **36** 2250064
[8] Zhang J H, Xue, N, Wang H, Zhang T, Huang X, Li J X and Du L 2025 *Int. J. Theor. Phys.* **66** 14
[9] He L, Ma J F, Mo R and Wei D W 2019 *Security and Communication Networks* **2019** 1
[10] Lan L, Lu R and Zhong J 2024 *Int. J. Theor. Phys.* **63** 59
[11] Xue Y X, Lu X Y, Au M H and Zhang C R 2024 *Cryptology ePrint Archive* **2024** 553
[12] Qiu S J, Xin X J and Zhang J H 2024 *Quantum Inf. Process* **23** 287
[13] Zhang L, Zhang J H, Xin X J, Huang M and Li C Y 2023 *Int. J. Theor. Phys.* **62** 254
[14] Prajapat S, Kumar P, Kumar S, Das A K, Shetty S and Hossain M S 2024 *IEEE Access* **12** 14647
[15] Thanalakshmi P, Anitha R, Anbazhagan N, Park C, Joshi G P and Seo C 2022 *Mathematics* **10** 1642
[16] Song Y Q, Wu Y S, Wu S Y, Li D D, Wen Q Y, Qin S J and Gao F 2014 *Sci. China Phys. Mech. Astron.* **67** 250311
[17] Zheng M, Xue K, Li S and Yu N *Quantum Inf. Process* **20** 230
[18] Xin X J, Ding L, Li C, Sang Y X, Yang Q L and Li F G 2022 *Quantum Inf. Process* **21** 33
[19] Xin X J, Wang Z, Yang Q J and Li F G 2020 *Int. J. Theor. Phys.* **59** 918
[20] Zhang Y, Xin X J and Li F G 2020 *Modern Phys. Lett. A* **35** 2050148
[21] Zhang L, Zhang J H, Xin X J and Li C Y 2023 *Int. J. Theor. Phys.* **62** 166
[22] Bennett C H, Divincenzo D P, Fuchs C A, Mor T, Rains E, Shor P W and Smolin J A 2024 *Int.J. Theor. Phys.* **63** 11
[23] Prajapat S, Gautam U and Gautam D 2024 *Mathematics* **12** 2558
[24] Rong M X, Xin X J and Li F G 2020 *Acta Phys. Sin.* **69** 190302 (in Chinese)
[25] Shi W M, Zhou Y H and Yang Y G 2015 *Int. J. Theor. Phys.* **54** 3115
[26] Shi W M, Wang Y M, Zhou Y H and Yang Y G 2018 *Optik* **164** 753
[27] Xin X J, Wang Z, Yang Q and Li F G 2020 *Quantum Inf. Process* **19** 79
[28] Zhang L, Zhang J H, Xiang J X and Li C Y 2023 *Quantum Inf. Process* **22** 452
[29] Ma H Q, Han Y X, Dou T Q and Li P Y 2023 *Chin. Phys. B* **32** 020304
[30] He Q Q, Xin X J and Yang Q L 2021 *Quantum Inf. Process* **20** 26
[31] Yang X L, Li Y Q and Li H W 2025 *Chin. Phys. B* **34** 020301
[32] Zhou J P, Zhou Y Y, Zhou X J and Bao X 2023 *Chin. Phys. B* **32** 080306
[33] Chen X M, Chen L and Yan Y L 2022 *Chin. Phys. B* **31** 120304
[34] Li X K, Song X Q, Guo Q W, Zhou X Y and Wang Q 2021 *Chin. Phys. B* **30** 060305
[35] Yang C W, Luo Y P and Hwang T 2014 *Quantum Inf. Process* **13** 2007
[36] Yang L, Xiang C and Li B 2014 *China Communications* **10** 19
[37] Jiang D H, Hu Q Z, Liang X Q and Xu G B 2019 *Quantum Inf. Process* **18** 268
[38] Xu G B, Wen Q Y, Qin S J and Yang Y H 2016 *Phys. Rev. A* **93** 032341
[39] Bennett C H, Divincenzo D P, Fuchs C A, Mor T, Rains E, Shor P W and Smolin J A 1999 *Phys. Rev. A* **59** 1070
[40] Huang W, Wen Q Y, Liu B, Gao F and Sun Y 2014 *Quantum Inf. Process* **13** 649
[41] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[42] Bai C M, Liu L and Zhang S J 2024 *Chin. Phys. B* **33** 070302