

A quantum blind signature scheme based on dense coding for non-entangled states

Ke Xing(邢柯), Ai-Han Yin(殷爱菡),and Yong-Qi Xue(薛勇奇)

Citation: Chin. Phys. B, 2024, 33 (**6**): 060309. DOI: 10.1088/1674-1056/ad2bed
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Dense coding capacity in correlated noisy channels with weak measurement

Jin-Kai Li(李进开), Kai Xu(徐凯), and Guo-Feng Zhang(张国锋)
Chin. Phys. B, 2021, 30 (**11**): 110302. DOI: 10.1088/1674-1056/abf34f

Effects of intrinsic decoherence on various correlations and quantum dense coding in a two superconducting charge qubit system

Wang Fei (王飞), Maimaitiyiming-Tusun (麦麦提依明·吐孙), Parouke-Paerhati (帕肉克·帕尔哈提), Ahmad-Abliz (艾合买提·阿不力孜)
Chin. Phys. B, 2015, 24 (**9**): 090307. DOI: 10.1088/1674-1056/24/9/090307

Efficient scheme for realizing quantum dense coding with GHZ state in separated low-Q cavities

Sun Qian (孙倩), He Juan (何娟), Ye Liu (叶柳)
Chin. Phys. B, 2014, 23 (**6**): 060305. DOI: 10.1088/1674-1056/23/6/060305

Quantum steganography with large payload based on dense coding and entanglement swapping of Greenberger-Horne-Zeilinger states

Ye Tian-Yu (叶天语), Jiang Li-Zhen (蒋丽珍)
Chin. Phys. B, 2013, 22 (**5**): 050309. DOI: 10.1088/1674-1056/22/5/050309

Cryptanalysis of fair quantum blind signatures

He Li-Bao(何立宝), Huang Liu-Sheng(黄刘生), Yang Wei(杨威), and Xu Rui(许瑞)
Chin. Phys. B, 2012, 21 (**3**): 030306. DOI: 10.1088/1674-1056/21/3/030306

A quantum blind signature scheme based on dense coding for non-entangled states

Ke Xing(邢柯)[†], Ai-Han Yin(殷爱菡)[‡], and Yong-Qi Xue(薛勇奇)

Department of Information Engineering, East China Jiaotong University, Nanchang 330013, *China*

(Received 20 October 2023; revised manuscript received 31 January 2024; accepted manuscript online 22 February 2024)

In some schemes, quantum blind signatures require the use of difficult-to-prepare multiparticle entangled states. By considering the communication overhead, quantum operation complexity, verification efficiency and other relevant factors in practical situations, this article proposes a non-entangled quantum blind signature scheme based on dense encoding. The information owner utilizes dense encoding and hash functions to blind the information while reducing the use of quantum resources. After receiving particles, the signer encrypts the message using a one-way function and performs a Hadamard gate operation on the selected single photon to generate the signature. Then the verifier performs a Hadamard gate inverse operation on the signature and combines it with the encoding rules to restore the message and complete the verification. Compared with some typical quantum blind signature protocols, this protocol has strong blindness in privacy protection, and higher flexibility in scalability and application. The signer can adjust the signature operation according to the actual situation, which greatly simplifies the complexity of the signature. By simultaneously utilizing the secondary distribution and rearrangement of non-entangled quantum states, a non-entangled quantum state representation of three bits of classical information is achieved, reducing the use of a large amount of quantum resources and lowering implementation costs. This improves both signature verification efficiency and communication efficiency while, at the same time, this scheme meets the requirements of unforgeability, non-repudiation, and prevention of information leakage.

Keywords: quantum blind signature, dense coding, non-entanglement, Hadamard gate

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.65.Ud **DOI:** 10.1088/1674-1056/ad2bed

1. Introduction

It is well known that quantum computing poses a serious challenge to the security of modern cryptography. The security of classical information technology relies on the complexity of mathematical problems, and solving such problems requires far more time than effective time. But quantum computers are extremely adept at tackling such problems. Fortunately, quantum cryptography, which is based on quantum mechanics and physical principles, can withstand attacks from quantum algorithms.[1] Thus quantum cryptography is gradually becoming an important option among the next-generation cryptographic techniques that can counter attacks from quantum computers. In classic digital signatures, there are already a variety of functions of mature algorithms and protocol systems. Scholars draw on their ideas, through the introduction of quantum technology, to comprehensively improve the security of various types of cryptographic protocols, gradually forming a new type of signature scheme — the quantum signature scheme.[2] Quantum signatures play a very important role in security aspects, such as identity authentication, data integrity, non-repudiation, and anonymity, and are widely used in fields such as electronic anonymous voting, contract signing, and electronic payments. With the continuous advancement of research on quantum signatures, increasing numbers of quantum signature schemes have been proposed for different scenarios. Branches of quantum signature protocols have gradually formed, such as quantum blind signatures, quantum homomorphic signatures, and quantum group signatures.[3–5]

A quantum blind signature (QBS) is a special type of quantum digital signature[6] in which the signer signs the sender's message without knowing the exact content of the signed message, thus protecting the privacy of the information owner. A vivid metaphor for blind signatures refers to placing a document in an envelope containing carbon paper. Then the signer signs the envelope without knowing the exact content of the document, thus completing the blind signature. Over the years, scholars have proposed increasingly practical quantum blind signature schemes based on real-life situations.[7,8]

In 2009, Wen *et al.*[9] first proposed a quantum weak blind signature scheme by utilizing the correlation between EPR entangled pairs. The scheme adopts quantum key distribution, and one-time one secret can not only guarantee the unconditional security of the message owner, but can also guarantee the anonymity of the message owner. Following this, quantum blind signatures quickly became a hot topic in the study of quantum signatures. In the research of signatures without entangled states, in 2011, Xu *et al.*[10] designed a non-entangled quantum group blind signature scheme for an e-voting system by combining the properties of group and blind signatures to ensure the anonymity of voters in the voting;

[†]Corresponding author. E-mail: 1400373041@qq.com
[‡]Corresponding author. E-mail: yinaihan@126.com

© 2024 Chinese Physical Society and IOP Publishing Ltd

this is signed under the supervision of arbitration and effectively protects against forgery attacks. In 2015, Xu *et al.*[11] proposed a more practical signature scheme based on the Xu scheme. This scheme allows the signer to complete the signature without the help of an arbiter, which avoids the problem of the huge storage capacity of the arbiter as a group manager in previous schemes. In addition, the signature can be verified again when the signer denies the signature. To make the signature scheme more suitable for real-world application scenarios. In 2018, Zhang *et al.*[12] proposed a third-party electronic payment protocol based on the design principle of an entanglement-free quantum blind signature. The scheme utilizes coding rules and quantum key distribution (QKD)[13–15] to secure the protocol. In addition, should disputes arise between participants, they can be resolved through a trusted third party. Gou *et al.*[16] proposed an improved payment protocol that is based on the scheme of Zhang. All the participants in this scheme only need to use single-particle quantum Z-gate operations during the payment process, which reduces the difficulty of quantum signature implementation and takes a big step forward in practicalization. Under the existing quantum technology conditions, to make the scheme more efficient and reduce the complexity of the signature process. In 2022, Xiong *et al.*[17] designed a quantum signature scheme based on single photon and unidirectional functions. System users can use one-way functions to encrypt information and perform controlled Hadamard gate operations with single photons to generate quantum signatures. The verifier can perform Hadamard gate inverse operations on the signature to restore the information and complete the verification. In recent years, scholars have proposed many quantum blind signature schemes in the signature research of entangled states.[18,19] In 2014, Tian *et al.*[20] proposed a broadcast multiple blind signature scheme by utilizing quantum invisible transmissions. In contrast to previous work, their scheme guarantees the properties of broadcast multiplicity and blind signatures through quantum key preparation, quantum encryption algorithms, and quantum invisible transmission states. Zhang *et al.*[21] improved Tian *et al*'s scheme by solving the problem that Alice, the sender of the message, can simulate any signer to sign messages at will. In 2019, Liang *et al.*[22] and Liu *et al.*[23] respectively proposed a signature protocol based on four-particle and five-particle entangled states as quantum channels. The difference between Liang *et al.*'s scheme and other signature schemes based on entangled four-qubit states is that this scheme not only uses entangled states to transmit messages but also employs the Vernam algorithm to achieve blindness. In Liu *et al.*'s scheme, five particles are used to entangle participants. In the case where the signer is unaware of the signed information content, if there is a disagreement, the signer can be traced. In 2020, Zheng *et al.*[24] designed a quantum signature scheme based on multi-particle GHZ states, which secures the signature via a quantum key string and introduces two random numbers and recovers the original message with only Bell-state measurements and projection measurements. The above signature schemes are all based on quantum invisible transmission state implementation, which utilizes the entanglement exchange properties of particles to sign the message. And as the number of entangled particles increases, it makes the signature process complicated and consumes a lot of quantum resources.

To improve the efficiency of entangled-state signatures and reduce implementation difficulty, in 2020, Li *et al.*[25] proposed a quantum blind signature protocol based on quantum walk (QW), which achieved quantum teleportation in single-particle states. In the proposed protocol, the sender does not need to prepare entangled particles in the initialization phase, but uses the QW system to generate the entangled states necessary for quantum stealth transmission. The same year, Niu *et al.*[26] proposed a blind signature protocol for quantum agents based on the principle of quantum dense coding using the execution of a unitary operator on a single quantum bit. The scheme employs dense coding instead of quantum invisible transmission of states, allowing a single quantum bit to mask 2 bits of classical information. The verifier has access to the original information through Bell-state measurements and encoding rules, reducing the use of quantum resources; however, the use of multi-particle entangled states and the complex signature process make the scheme difficult to realize. In 2021, Zhu *et al.*[27] used quantum Fourier transform to encrypt and transmit the measurement results, and designed an efficient quantum blind signature scheme based on quantum Fourier transform. The scheme uses quantum logic gates to operate on quantum states, realizing that a quantum state represents two bits of classical information.

Previously, we analyzed several typical signature schemes that use non-entangled states as quantum channels and entangled states as quantum channels. It can be seen from this that based on non-entangled signature schemes, the preparation and measurement of single photons are relatively easy to achieve under existing conditions. And with the continuous research of scholars, it continues to develop and improve in practical applications. But the efficiency of signatures is not high, and a large amount of quantum resources need to be prepared. In entangled-state-based signature schemes, utilizing the entanglement properties between particles can effectively ensure the security of the signature. However, it is difficult to prepare multi-particle entanglement resources, and the operations on entangled particles in the signature and verification stages are relatively complex.

Most blind signature schemes require the preparation of entangled states that are not easily realized to complete the

signature protocol, which is difficult for quantum hardware devices in practice and greatly reduces the efficiency and practicality of signatures.[28,29] To improve signature efficiency and reduce the use of quantum resources, we propose an efficient quantum blind signature scheme based on dense encoding for non-entangled states. In this scheme, the message owner blinds the message using a key and a hash function, after which quantum bits are prepared for the binary sequence of the blinded message according to dense coding rules.[30–32] The message owner utilizes dense encoding and hash functions to blind information, and no one, except the message owner and verifier, knows the content of the original message, effectively protecting the privacy of the message owner. This makes the signature scheme extremely blind. In the signature stage, the signer only needs to perform Hadamard gate operation on the selected single photon to generate the signature, and the verifier can recover the information and complete the verification by performing Hadamard gate inverse operation on the signature and combining it with the coding rules; this reduces the realization difficulty and improves the efficiency of the signature operation. To ensure the security of the signature scheme, we have designed a method of secondary distribution of particles to the signer, which also ensures that information is not leaked. Moreover, by combining dense encoding with single photons, a non-entangled quantum state is achieved to represent three bits of classical information, improving signature efficiency and practicality.

The paper is structured as follows: Section 2 briefly introduces the non-entangled state dense encoding principle of this scheme. Section 3 describes our proposed blind signature scheme. Section 4 analyzes the security of the scheme. Section 5 conducts efficiency analysis of the proposed scheme and compares it with other quantum blind signature schemes. Finally, we present our conclusions in Section 6.

2. Preliminary

For a better introduction to non-entangled state dense coding, let us assume that Alice and Charlie communicate with each other: Alice is the sender and Charlie is the receiver.

(1) Alice prepares a string of single-photon sequences S. The single-photon sequence S is a combination of S_1 and S_2 according to a coding rule to represent the secret message M to be sent. S_1 represents the single photon sequence sent to Charlie for the first time, and S_2 represents the single photon sequence sent to Charlie for the second time: $(S_1 \in (|0_1\rangle, |1_1\rangle, |+_1\rangle, |-_1\rangle), S_2 \in (|0_2\rangle, |1_2\rangle, |+_2\rangle, |-_2\rangle))$. The secret information M is encoded on the single photon sequence S according to the coding rules in Table 1. Alice records the coded sequence of single photons S and clearly knows whether the single photon belongs to S_1 or S_2. The specific coding rules are presented in Table 1.

(2) Alice rearranges the S_1 sequence and adds detection particles to form a new sequence S_{1-O-C}, which is sent to Charlie. Repeat the above for S_2 again. Charlie receives it and performs eavesdropping detection. After determining that the channel is secure, Charlie proceeds with the subsequent steps.

(3) After the above process is passed, Charlie takes out the detection particle from the sequence S_{1-O-C} to get the S_{1-O} sequence. Similarly, repeating the above steps will also give S_{2-O}. After Charlie takes out the detection particles, the particles in his hand are rearranged in the order of the original particles. S_1 and S_2 are generated by Alice using the rules in Table 1, and Charlie wants to recover the original information S_1 and S_2. Alice must disclose to Charlie the correct order of sequence of S_1 and S_2 within sequence S, as well as the measurement basis used for each particle. Subsequently, based on the coding rules and the information published by Alice, Charlie gets the original sequence S based on the first received as S_1 and the second received as S_2. Charlie then selects the correct measurement base for measurement, and decodes the measurement result based on the coding rules to get the secret message M.

Table 1. The single-photon dense coding rule.

Information sequence	Quantum state	Information sequence	Quantum state
000	$\|0_1\rangle$	001	$\|0_2\rangle$
111	$\|1_1\rangle$	110	$\|1_2\rangle$
011	$\|+_1\rangle$	010	$\|+_2\rangle$
100	$\|-_1\rangle$	101	$\|-_2\rangle$

Examples: Alice wants to send the message sequence 011001100010 to Charlie. Based on the dense coding rules and the sequence of messages to be sent, Alice prepares the single photon sequence $S(|+_1\rangle, |0_2\rangle, |-_1\rangle, |+_2\rangle)$, dividing the sequence S into S_1 and S_2. $S_1(|+_1\rangle, |-_1\rangle)$, $S_2(|0_2\rangle, |+_2\rangle)$.

First time sending: Alice rearranges S_1 and adds detection particles to form a new sequence $S_{1-O-C}(|-_1\rangle, |0\rangle, |+_1\rangle)$ and sends it to Charlie. Charlie informs Alice upon receipt of the S_{1-O-C} photon sequence, and Alice announces the position of the detected particle and the corresponding measurement base in the sent sequence. Same process as (2). After determining the channel security, Charlie takes out the detection particle from the sequence S_{1-O-C} to get the S_{1-O} sequence $(|-_1\rangle, |+_1\rangle)$.

Second sending: Alice rearranges the S_2 sequence and adds the detection particles to form a new sequence $S_{2-O-C}(|+_2\rangle, |-\rangle, |0_2\rangle)$, and sends the new sequence to Charlie. Charlie informs Alice after receiving the S_{2-O-C} photon sequence, and then Alice announces the position of the detected particles in the second transmission sequence and the corresponding measurement base. After determining the channel security, Charlie takes out the detection particle from the sequence S_{2-O-C} to get the S_{2-O} sequence $(|+_2\rangle, |0_2\rangle)$.

Alice announces to Bob the ordering of the sequence S and the correct measurement base. Bob restores the sequence $S(|+_1\rangle, |0_2\rangle, |-_1\rangle, |+_2\rangle)$ based on S_1 received for the first time and S_2 received for the second time, and selects the correct measurement base for measurement. The measurement results are decoded according to encoding rules to obtain secret information, 011001100010.

3. Quantum blind signature scheme

Combined with the current situation of e-banking payments, three participants are set up in this scheme. Alice is the consumer, Charlie is the merchant, and Bob is the bank. The assumptions for each party's role are as follows:

(1) Alice makes payments to the merchant (Charlie) through the electronic banking system, and the bank (Bob) needs to sign the payment statement. Due to the fact that consumers are unwilling to disclose the specific information of the bill, consumers need to blind the bill information.

(2) Bob (the signatory) signs the consumer's blind payment bill based on the information provided by Alice.

(3) Charlie is the signature verifier. Receive the billing information sent by the consumer (Alice) and the signature of the bank (Bob) regarding the billing, and verify the validity of the signature.

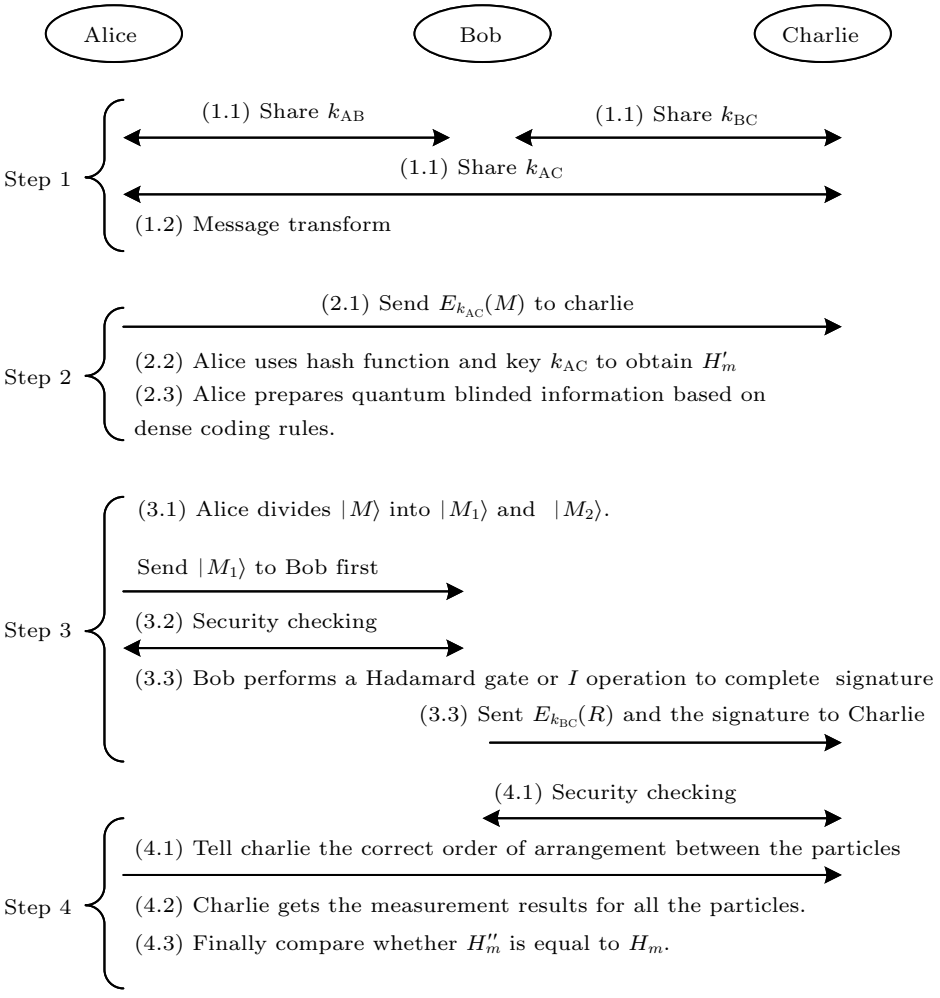


Fig. 1. The execution process of the quantum blind signature protocol.

Figure 1 depicts the basic flow of the quantum blind signature of this scheme. This signature system consists of four phases: an initialization phase, a message blinding phase, a signature phase and a verification phase. In the initialization phase, the participant obtains the key using quantum key distribution and Alice converts the signed message into binary. In the information blinding phase, Alice prepares the blinded sequence into quantum bits according to the dense coding rules. In the signature phase, the signer, Bob, encrypts the specified particles to produce a signature. The verification stage is where Charlie, the verifier, confirms the validity of the signature by comparing the information obtained based on the coding rules and measurements with the original information.

3.1. Initialization phase

Two types of measurement bases are used for both eavesdropping detection and signature verification in the signature process, namely, Z-base and X-base. And the X-base and Z-

base can be converted through the H-gate as follows. Here the H-gate is denoted as

$$H = \frac{1}{\sqrt{2}}(U_x + U_z) = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (1)$$

The operation results and process are

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \quad (2)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \quad (3)$$

(1) Key sharing: the consumer Alice secretly shares K_{AB} with bank Bob; consumer Alice secretly shares K_{AC} with merchant Charlie; bank Bob secretly shares K_{BC} with merchant Charlie. The above key distribution can be realized by an unconditionally secure quantum key distribution (QKD) protocol. Quantum key distribution is used to ensure the security of communication without transmitting any vital information.

(2) Message transform: Alice transforms the message to be signed into a binary $M = (m_1, m_2, \ldots, m_n) \in \{0,1\}^n$.

3.2. Blind the message phase

(1) For convenience in description, assume that the length of the billing information is n. Alice obtains $E_{K_{\mathrm{AC}}}(M)$ from M using the key K_{AC} and the one-time encryption algorithm, and sends it to Charlie.

(2) Alice computes the hash value of M using the hash function shared with Charlie to get H_M,

$$H_M = (h_M(1), h_M(2), \ldots, h_M(n)), \quad h_M(n) \in \{0,1\}^n. \quad (4)$$

Encrypting H_M with key K_{AC} to obtain $E_{K_{\mathrm{AC}}}(H_M)$, represented by H'_M, is called blind billing message:

$$K'_{\mathrm{AC}} = (k'_{\mathrm{AC}}(1), k'_{\mathrm{AC}}(2), \ldots, k'_{\mathrm{AC}}(n)), \quad (5)$$

$$H'_M = (h'_M(1), h'_M(2), \ldots, h'_M(n)),$$
$$h'_M(n) = h_M(n) \oplus k'_{\mathrm{AC}}(n). \quad (6)$$

(3) Alice and Charlie agreed in advance on dense coding rules. As in Table 1. Alice prepares quantum bits based on dense encoding rules for the n-bit blind message H'_M binary sequence (n if not a multiple of 3, blinded message H'_M complement 0 to reach a multiple of 3) length $n/3$, $|M\rangle = \{|m_1\rangle, |m_2\rangle, \ldots, |m_{n/3}\rangle\}$. This is called quantum blind billing information:

$$|m_{n/3}\rangle \in \{|0_1\rangle, |1_1\rangle, |+_1\rangle, |-_1\rangle, |0_2\rangle, |1_2\rangle, |+_2\rangle, |-_2\rangle\}^{\frac{n}{3}}. \quad (7)$$

The n-bit classical bit information in the bill is blinded by the hash function and key K_{AC}. Subsequently, the blinded information sequence of n bits is encoded into $n/3$-bit quantum bits according to dense encoding rules.

3.3. Signature phase

(1) Alice divides $|M\rangle$ into $|M_1\rangle$ and $|M_2\rangle$ and records the sequence information and sends the quantum message in two parts. The subscripts 1 and 2 indicate the sending order. Here, $|M_1\rangle \in (|0_1\rangle, |1_1\rangle, |+_1\rangle, |-_1\rangle)$ is sent to the signer Bob for the first time and $|M_2\rangle \in (|0_2\rangle, |1_2\rangle, |+_2\rangle, |-_2\rangle)$ is sent to Bob for the second time. Taking the sending of $|M_1\rangle$ as an example, Alice first sends $|M_1\rangle$ to Bob by rearranging the order and adding the detection particle.

Bob informs Alice after receiving the signature information, and Alice tells Bob the position and corresponding measurement basis of the detected particles through a classical channel. Bob takes measurements based on the information sent by Alice, and sends the measurement results to Alice. Alice compares Bob's measurements with the initial state in which the detection particles were added, and if the error rate is higher than the safety threshold set by both parties, the protocol is stopped and restarted. If below threshold, continue with the subsequent steps of the protocol.

(2) After Bob sheds the detected particle, Alice announces to Bob the position of $|0_1\rangle, |1_1\rangle$ in the single-photon sequence $|M_1\rangle$. Bob completes the signature by performing a Hadamard gate or I operation only on the $|0_1\rangle, |1_1\rangle$ in $|M_1\rangle$. Let the unoperated particle $|0_1\rangle, |1_1\rangle$ in $|M_1\rangle$ be denoted by $|N_1\rangle$ and have a total of i bits: $|N_1\rangle = (|n_1\rangle, |n_2\rangle, \ldots, |n_i\rangle) \in (|0_1\rangle, |1_1\rangle)$.

First, Bob selects the one-way function $F^1_{k_{\mathrm{BC}}}$ from the set of functions $\{F^1_\alpha\}_\alpha$ based on the first i bits of the key K_{BC}, where $F^1_{k_{\mathrm{BC}}} : \{0,1\}^* \to \{0,1\}^i$. Similarly, select $F^2_{k_{\mathrm{BC}}}$ from another function set $\{F^2_\beta\}_\beta$. Here, $F^1_{k_{\mathrm{BC}}}$ and $F^2_{k_{\mathrm{BC}}}$ are two completely different and independent one-way functions. Then, the i-bit classical bits R are randomly generated: $R = (r_1, r_2, \ldots, r_i) \in \{0,1\}^i$. Calculate $F_{k_{\mathrm{BC}}} = F^1_{k_{\mathrm{BC}}}(R) \oplus F^2_{k_{\mathrm{BC}}}(R)$, among which $F_{k_{\mathrm{BC}}} = (F_1, F_2, \ldots, F_i)$ based on the two one-way functions. The obtained value is XORed with the information R to obtain $W_{\mathrm{BC}} = F_{k_{\mathrm{BC}}} \oplus R$, $W_{\mathrm{BC}} = (w_1, w_2, \ldots, w_i)$.

(3) Bob generates a signature $S = \{|S_1,\rangle |S_2\rangle, \ldots, |S_i\rangle$ by performing a controlled Hadamard gate operation on the signature message $|N_1\rangle$ based on the value of W_{BC}, where $|S_i\rangle = H^{w_i}|n_i\rangle$. The definition $H^0 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unit operator and $H = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard gate. It follows from this

$$|S_i\rangle = \begin{cases} |0\rangle & (w_i = 0,\ n_i = 0), \\ |1\rangle & (w_i = 0,\ n_i = 1), \\ |+\rangle & (w_i = 1,\ n_i = 0), \\ |-\rangle & (w_i = 1,\ n_i = 1). \end{cases}$$

Figure 2 depicts its quantum signature circuit. Among them, a single photon $|n_i\rangle$ performs Hadamard gate or unit operator I operation under the control of the w_i value. When $w_i = 0$, the single photon $|n_i\rangle$ performs the unit operator I operation. When $w_i = 1$, $|n_i\rangle$ transitions from $|0\rangle$ to $|+\rangle$ or from $|1\rangle$ to $|-\rangle$ through Hadamard gate operation $|0\rangle \rightarrow |+\rangle, |1\rangle \rightarrow |-\rangle$.

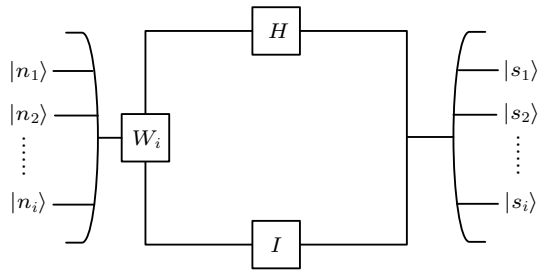


Fig. 2. Generation of the signature quantum circuit.

Bob encrypts R with key k_{BC} to obtain $E_{K_{\mathrm{BC}}}(R)$. Then send $E_{K_{\mathrm{BC}}}(R)$ and the particle sequence in hand to Charlie, the verifier. Bob tells the verifier, through a classical channel, to manipulate the particle position during the signature process. When sending $|M_2\rangle$ for the second time, perform the same signature operation as before.

3.4. Verification phase

(1) After receiving the signature information, the verifier Charlie informs the consumer Alice, who then informs Charlie through the classic channel of the correct order of $|M_1\rangle$ and $|M_2\rangle$ in $|M\rangle$.

In the same operation as Bob, Charlie selects functions $F^1_{k_{\mathrm{B}}}$ and $F^2_{k_{\mathrm{B}}}$ from the set of functions $\{F^1_\alpha\}_\alpha$ and $\{F^2_\beta\}_\beta$ based on the shared key K_{BC}. Charlie decrypts $E_{K_{\mathrm{BC}}}(R)$ and obtains R. Based on the value of R and the one-way function, Charlie performs the same operation as Bob, $F_{k_{\mathrm{BC}}} = F^1_{k_{\mathrm{BC}}}(R) \oplus F^2_{k_{\mathrm{BC}}}(R)$ and $W_{\mathrm{BC}} = F_{k_{\mathrm{BC}}} \oplus R$, to obtain W_{BC}. Charlie then performs the reverse of Bob's operation; when $w_i = 0$, Charlie chooses $M_z = \{|0\rangle, |1\rangle\}$ to measure the state of $|S_i\rangle$, and when $w_i = 1$, Charlie chooses $M_x = \{|+\rangle, |-\rangle\}$ to measure the state of $|S_i\rangle$. Thus, if the measurement is $|S_i\rangle = |0,\rangle |+\rangle$, then $n_i = 0$, and if $|S_i\rangle = |1\rangle, |-\rangle$, then $n_i = 1$. For particles that Bob does not manipulate, Charlie makes $M_x = \{|+,\rangle |-\rangle\}$ measurements of them.

(2) Charlie after obtaining measurements of all particles. After sorting according to the correct order between particles as told by Alice. Then, the blinded message H'_M is obtained according to the dense coding rule. Simultaneously decrypt H'_M using key K_{AC} to obtain H''_M. Finally, the $E_{K_{\mathrm{AC}}}(M)$ sent by Alice is decrypted by the key K_{AC} to get the bill classic bit message M. Charlie utilizes the hash function shared with Alice to calculate the hash value of the bill message M to get the H_M.

(3) Then, compare whether H''_M is equal to H_M. If equal, accept the signature: otherwise, reject the signature.

4. Security analysis

In our scheme, we use a quantum key distribution protocol that has proven unconditional security with shared keys. The security of the signing process is ensured by the use of quantum keys, secondary distribution and rearrangement. In this section, we show that our scheme satisfies the properties of blindness, non-deniability, non-forgery, and prevention of information leakage.

4.1. Message's blindness

In our quantum signature scheme, the original message is blind to Bob. In the information blinding phase, Alice uses the hash function shared with Charlie to compute the hash value of the bill message, and then encrypts the H_M using the key K_{AC} to obtain $E_{K_{\mathrm{AC}}}(H_M)$, which is used to represent H'_M and is called a blinded bill message. Subsequently, Alice prepares quantum bits for the n-bit blind message H'_M based on dense encoding rules. If Bob wants to know the billing information, he must know that Alice and Charlie share the hash function, key K_{AC}, and dense encoding rules. The encoding rules were agreed upon by Alice and Charlie in advance, and only Alice and Charlie know what classical bits every single particle represents. Even if Bob knows the hash function and the dense encoding rules, since the hash function is unidirectional, the original message cannot be recovered, even if the hash is intercepted. The key distribution is realized by unconditionally secure quantum key distribution, and it is impossible for him to know the key K_{AC}. Therefore, Bob did not know the contents of the message when he signed it.

4.2. Non-deniability

In our signature scheme, once Charlie has successfully verified and accepted the signature, neither Alice nor Bob can deny it. In the initial stage, Alice encrypts the billing information with the key K_{AC} to get $E_{K_{\mathrm{AC}}}(M)$, and sends it to Charlie. In the signature phase, according to the secret shared with Charlie, Bob chooses the one-way functions $F^1_{k_{\mathrm{BC}}}$ and $F^2_{k_{\mathrm{BC}}}$ from the function sets $\{F^1_\alpha\}_\alpha$ and $\{F^2_\beta\}_\beta$ to sign.

First, the signature is verified by Charlie using the key K_{AC}, K_{BC} and a one-way function to obtain the initial message. Then, compare whether H''_M is equal to H_M to complete the verification. Thus, Charlie can confirm a blind message generated by Alice, and Alice cannot deny this valid signature. Charlie decrypts $E_{K_{\mathrm{BC}}}(R)$ and obtains R to perform a Hadamard gate reversal operation on the signature to determine its validity. Therefore, Bob cannot deny his signature under the premise that Charlie declared it valid. In addition, the signing and verification phases use key acquisition one-way functions for signing and verification, and the shared key has the unconditional security of the QKD protocol. Therefore, neither party can deny it.

4.3. Non-forgery

This scheme mainly analyzes the unforgeability from two aspects: internal forgery and external forgery.

(1) Firstly, we prove that the participants Alice and Charlie cannot forge Bob's signature. Since the signature process, the signature is based on a one-way function with a random number R to obtain W_{BC} to manipulate particles to complete the signature. If Alice wants to forge a signature, she must know the key K_{BC} that generated the one-way function and the random number R that Bob generated. If Charlie wants to forge a signature, he must know the location of the particle in the signature that Alice told Bob to manipulate. Charlie's random operation on particles to forge signatures without knowing the exact location of the operation can only produce an invalid signature. Therefore, internal attackers cannot forge signatures.

(2) Suppose that Eve, an external attacker, wants to forge a signature; she must get a signature based on the same message M, key and encoding rules. Just like the operation of the signer Bob, the W_{BC} calculated by $F_{k_{\mathrm{BC}}} = F^1_{k_{\mathrm{BC}}}(R) \oplus F^2_{k_{\mathrm{BC}}}(R)$ and $W_{\mathrm{BC}} = F_{k_{\mathrm{BC}}} \oplus R$ is used to manipulate the particles to complete the signature $|S_i\rangle = H^{w_i}|n_i\rangle$. Finally, Charlie obtains W_{BC} based on the information sent by Bob, and compares H''_M with H_M for verification, making it easy to see if the signature was forged. And Eve cannot know the key; she only has $1/2^n$ probability to guess the value of K_{BC}, K_{AC}. Therefore, external attackers cannot forge signatures.

4.4. Capability to prevent information leakage

From the above description, we can see that an attacker who wants to forge a signature can only do so by cracking the key and the encoding rules. The key in the signature is shared through QKD, and the QKD protocol has been proven to be unconditionally secure. Obviously, attackers cannot obtain the key shared by the participants. In this section, we will discuss whether an attacker is able to push out the original message and the key from the message in the classical channel.

Assuming that the attacker Eve has the ability to obtain all the information of the classical channel, she can obtain R, $E_{K_{\mathrm{AC}}}(M)$, and W_{BC}. With this information, Eve can get the value of $F_{k_{\mathrm{BC}}}$ by $W_{\mathrm{BC}} \oplus R$. The one-way functions $F^1_{k_{\mathrm{BC}}}$ and $F^2_{k_{\mathrm{BC}}}$ cannot perform the reverse operation, so Eve cannot deduce the key from the information in the classic channel. Even if the attacker accidentally knows the dense encoding rules and the position of the particles to be manipulated, and accurately measures the particles, she still cannot obtain the original information. This is because, during the signature process, Alice redistributes the quantum sequence twice after it is rearranged, and the particles sent twice need to be measured and integrated to restore the original message. Add detection particles to the particles sent for the first time, and terminate the second time if eavesdropping is detected. Therefore, the messages measured by the attacker are scattered and useless, and she does not know the number of times the measured particles were sent.

5. Efficiency analysis

In this section, we compare our protocol with existing major quantum signature protocols. Compared to previous work, our advantages can be reflected in the coding capacity, length of signed messages, and efficiency. Here, we analyze the performance of quantum signature protocols from two aspects. One considers the number of quantum bits and classical bits to be transmitted when signing n-bit messages, as well as the complexity of the protocol's signature and verification processes, including the preparation of quantum resources, comparison of quantum states, and measurement of quantum states. We define signature efficiency as

$$\eta = \frac{B_{\mathrm{m}}}{Q_{\mathrm{t}} + B_{\mathrm{t}}}, \tag{8}$$

where B_{m} is the number of bits of the signature message, Q_{t} is the number of quantum bits transmitted, and B_{t} denotes the number of classical bits transmitted in the scheme. In this scheme, it is assumed to sign n-bit messages. For Q_{t}, in the blinding phase, Alice encodes the message to be signed into $n/3$ bit quantum bits according to the dense coding rule. Subsequently, Alice transmits $n/3$ bits of quantum bits to Bob for a signature. Therefore, the value of Q_{t} is calculated as $n/3$ bits. For B_{t}, during the blinding phase, Alice sends a total of n bits of messages M to Charlie; in the signature stage, Alice sends $n/6$ bits of information to Bob, telling him the position of the particle operation. During the verification phase, Bob sends $n/6$ bits of information to Charlie, telling him the location of the signature operation. Therefore, the value of B_{t} has been calculated to be $4n/3$ bits. According to Eq. (8), the calculation shows that the efficiency of this program is 60%. In Refs. [17,26,27], the same method was used to calculate efficiencies of 50%, 33.3%, and 33.3%, respectively. The results obtained are shown in Table 2. Based on the data in the table, it is easy to see that our signature efficiency is higher than the previous protocols.

In terms of signature length, in our scheme, the signer only performs Hadamard gates or I operations on $|0\rangle$ and $|1\rangle$ in the quantum state based on the signature position instructed by Alice, and the signature length is $n/6$. This reduces the length and complexity of the signature. In the protocol in Ref. [17], the signer uses the one-way function value generated by the key to operate on each non-entangled particle to complete the signature, with a signature length of n. In the protocol in Ref. [27], the signer measures the Bell state of $n/2$ two-particle entangled states in their hands, and then

sends the measurement results to the verifier via block encoding and quantum Fourier transform technology to complete the signature, with a signature length of $n/2$. In the protocol in Ref. [26], $n/2$ GHZ three-particle entangled states are prepared and distributed to participants. The signer completes the signature by performing a unitary operator on each particle based on the information to be signed, with a signature length of $n/2$.

Table 2. Comparison between different signature protocols.

	Our protocol	Ref. [17]	Ref. [27]	Ref. [26]
Signature efficiency	60%	50%	33.3%	33.3%
Quantum resources	single-photon state	single-photon state	Bell states	GHZ states
Measurement basis	X-based or Z-based	X-based or Z-based	Bell basis	Bell basis
Signature length	$n/6$	n	$n/2$	$n/2$
Coding capacity	3	1	1/3	2/3

In terms of coding capacity, in our scheme, quantum bits are prepared for signature messages according to the single-photon dense coding rules in Table 1. By utilizing the secondary distribution and rearrangement of non-entangled quantum states, a non-entangled quantum state represents three bits of classical information. The encoding capacity represents how much classical bit information a qubit represents; therefore, the encoding capacity is 3. In the second section, we explained in detail how to improve the encoding capacity. In the protocol in Ref. [17], single photon states are prepared as signature resources based on 0 corresponding to $|0\rangle$ and 1 corresponding to $|1\rangle$. Then, the length of both the signed quantum bit message and the signature message is n; therefore, the coding capacity is 1. In the protocol in Ref. [27], for n-bit signature information, each of the three participants prepares $n/2$ two-particle entangled states and performs a unitary operator on the quantum state based on the signature information, so that the quantum state shields the classical information of 2 bits. According to calculations, three particles transmit a classical bit in the protocol. The encoding capacity is $1/3$. In the protocol in Ref. [26], $n/2$ GHZ entangled states need to be prepared if there are n bits of information. However, the GHZ state is a quantum state entangled by three particles and requires joint measurement via the Bell basis. Therefore, in the protocol, three particles transmit two classical bits with an encoding capacity of $2/3$.

Therefore, the above comparison indicates that our protocol demonstrates significant signature efficiency and encoding capacity compared to other protocols, resulting in smaller quantum resource consumption. Moreover, the signer only operates on some of the quanta during the signature process, instead of operating on each quantum bit to complete the signature in protocols.[17,26,27] This reduces the length of the signature, and the efficiency of the quantum signature is greatly improved.

6. Conclusions

Inspired by the idea of dense coding, this paper proposes an entanglement-free state quantum blind signature scheme based on dense coding. The protocol uses non-entangled states as quantum resources to complete the signature protocol, which uses the secondary distribution and rearrangement of non-entangled quantum states to allow a single particle to carry three bits of classical information. It saves quantum resources, improves signature efficiency, and effectively solves the problem of inefficient quantum utilization that existed in the past signature process. At the same time, the security of the communication channel and the coding sequence is ensured by utilizing distribution twice and sequential rearrangement. Under existing technical conditions, the protocol proposed in this article is easier to implement.

Acknowledgement

Project supported by the National Natural Science Foundation of China (Grant No. 61762039).

References

[1] Amjad M and Raju 2018 *Journal of Trend in Scientific Research and Development* **2** 482
[2] Xin X J, Ding L, Li C Y, Sang Y X, Yang Q L and Li F G 2021 *Quantum Information Processing* **21** 1
[3] Chen F L, Wang Z H and Hu Y M 2019 *Entropy* **21** 336
[4] Shang T, Pei Z, Chen R and Liu J 2019 *Computers, Materials & Continua* **59** 149
[5] hen F L and Han Z F 2016 *International Journal of Quantum Information* **14** 1650041
[6] Fan L and Cao C 2019 *International Journal of Quantum Information* **17** 1950007
[7] Tiliwalidi K, Zhang J Z and Xie S C 2019 *International Journal of Theoretical Physics.* **58** 3510
[8] Feng X N, Wu H Y, Zhou X L and Yao Y 2022 *Quantum Information Processing* **22** 5
[9] Wen X J, Niu X M, Ji L P and Tian Y 2009 *Opt. Commun.* **282** 666
[10] Xu R, Huang L S, Yang W and He L B 2011 *Opt. Commun.* **284** 3654
[11] Xu G B and Zhang K J 2015 *Quantum Information Processing* **14** 2577
[12] Guo X, Zhang J Z and Xie S C 2018 *International Journal of Theoretical Physics* **57** 2657
[13] He Y F and Ma W P 2021 *Modern Physics Letters B* **35** 2150195
[14] Lei L and Zhi L 2022 *Information Sciences* **585** 232
[15] Zhou Y H, Qin S F, Shi W M and Yang Y G 2022 *Quantum Information Processing* **21** 303
[16] Gou X L, Shi R H, Shi Z and Li K C 2021 *Modern Physics Letters A* **36** 2150040
[17] Xiong Z H and Yin A H 2022 *Quantum Information Processing* **21** 140
[18] Chen B C and Yan L L 2021 *International Journal of Theoretical Physics* **60** 4006
[19] Xia C Y, Li H F and Hu J 2021 *Euro. Phys. J. Plus* **136** 633

[20] Tian Y, Chen H, Ji S F, Han Z P, Lian H G and Wen X J 2014 *Optical and Quantum Electronics* **46** 769
[21] Zhang W, Qiu D W, Zou X F and Mateus P 2017 *Quantum Information Processing* **16** 150
[22] Liang X Q, Wu Y L, Zhang Y H, Wang S S and Xu G B 2019 *International Journal of Theoretical Physics* **58** 31
[23] Liu G, Ma W P, Cao H and Lyu L D 2019 *International Journal of Theoretical Physics* **58** 1999
[24] Zheng T, Chang Y and Zhang S B 2020 *Quantum Information Processing* **19** 163
[25] Li X Y, Chang Y, Zhang S B, Dai J Q and Zheng T 2020 *International Journal of Theoretical Physics* **59** 2059
[26] Niu X F, Ma W P, Chen B Q, Liu G and Wang Q Z 2020 *International Journal of Theoretical Physics* **59** 1121
[27] Zhu H F, Zhang Y L and Li Z X 2021 *International Journal of Theoretical Physics.* **60** 2311
[28] Xin X J, He Q Q, Wang Z, Yang Q L and Li F G 2019 *Modern Physics Letters A* **34** 1950166
[29] Wang M Q, Wang X and Zhan T 2018 *Quantum Information Processing* **17** 275
[30] Aili M and Abulizi A 2019 *International Journal of Theoretical Physics* **58** 364
[31] He W T, Wang J, Zhang T T, Alzahrani F, Hobiny A, Alsaedi A, Hayat T and Deng F G 2019 *International Journal of Theoretical Physics* **58** 2834
[32] Meher N 2020 *J. Phys. B: Atom. Mol. Opt. Phys.* **53** 065502