

Quantum circuit-based proxy blind signatures: A novel approach and experimental evaluation on the IBM quantum cloud platform

Xiaoping Lou(娄小平), Huiru Zan(昝慧茹), and Xuejiao Xu(徐雪娇)

Citation: Chin. Phys. B, 2024, 33 (**5**): 050307. DOI: 10.1088/1674-1056/ad22d5
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Analysis of learnability of a novel hybrid quantum—classical convolutional neural network in image classification

Tao Cheng(程涛), Run-Sheng Zhao(赵润盛), Shuang Wang(王爽), Rui Wang(王睿), and Hong-Yang Ma(马鸿洋)
Chin. Phys. B, 2024, 33 (**4**): 040303. DOI: 10.1088/1674-1056/ad1926

Gray code based gradient-free optimization algorithm for parameterized quantum circuit

Anqi Zhang(张安琪), Chunhui Wu(武春辉), and Shengmei Zhao(赵生妹)
Chin. Phys. B, 2024, 33 (**2**): 020311. DOI: 10.1088/1674-1056/ad09cd

Deep learning framework for time series classification based on multiple imaging and hybrid quantum neural networks

Jianshe Xie(谢建设) and Yumin Dong(董玉民)
Chin. Phys. B, 2023, 32 (**12**): 120302. DOI: 10.1088/1674-1056/accb45

High-fidelity universal quantum gates for hybrid systems via the practical photon scattering

Jun-Wen Luo(罗竣文) and Guan-Yu Wang(王冠玉)
Chin. Phys. B, 2023, 32 (**3**): 030303. DOI: 10.1088/1674-1056/ac8734

Variational quantum simulation of thermal statistical states on a superconducting quantum processer

Xue-Yi Guo(郭学仪), Shang-Shu Li(李尚书), Xiao Xiao(效骁), Zhong-Cheng Xiang(相忠诚), Zi-Yong Ge(葛自勇), He-Kang Li(李贺康), Peng-Tao Song(宋鹏涛), Yi Peng(彭益), Zhan Wang(王战), Kai Xu(许凯), Pan Zhang(张潘), Lei Wang(王磊), Dong-Ning Zheng(郑东宁), and Heng Fan(范桁)
Chin. Phys. B, 2023, 32 (**1**): 010307. DOI: 10.1088/1674-1056/aca7f3

Quantum circuit-based proxy blind signatures: A novel approach and experimental evaluation on the IBM quantum cloud platform

Xiaoping Lou(娄小平), Huiru Zan(咎慧茹), and Xuejiao Xu(徐雪娇)†

College of Information Science and Engineering, Hunan Normal University, Changsha 410081, *China*

(Received 8 October 2023; revised manuscript received 16 January 2024; accepted manuscript online 26 January 2024)

This paper presents a novel approach to proxy blind signatures in the realm of quantum circuits, aiming to enhance security while safeguarding sensitive information. The main objective of this research is to introduce a quantum proxy blind signature (QPBS) protocol that utilizes quantum logical gates and quantum measurement techniques. The QPBS protocol is constructed by the initial phase, proximal blinding message phase, remote authorization and signature phase, remote validation, and de-blinding phase. This innovative design ensures a secure mechanism for signing documents without revealing the content to the proxy signer, providing practical security authentication in a quantum environment under the assumption that the CNOT gates are securely implemented. Unlike existing approaches, our proposed QPBS protocol eliminates the need for quantum entanglement preparation, thus simplifying the implementation process. To assess the effectiveness and robustness of the QPBS protocol, we conduct comprehensive simulation studies in both ideal and noisy quantum environments on the IBM quantum cloud platform. The results demonstrate the superior performance of the QPBS algorithm, highlighting its resilience against repudiation and forgeability, which are key security concerns in the realm of proxy blind signatures. Furthermore, we have established authentic security thresholds (82.102%) in the presence of real noise, thereby emphasizing the practicality of our proposed solution.

Keywords: proxy blind signature, quantum circuits, quantum computation, IBM quantum cloud platform

PACS: 03.67.Dd, 03.67.–a **DOI:** 10.1088/1674-1056/ad22d5

1. Introduction

In the realm of network environments, digital signature mechanisms serve as one of the means to safeguard the security of network information, effectively addressing issues related to forgery, repudiation, impersonation, and tampering. Electronic signatures based on mathematical ciphers typically employ public key encryption techniques, replacing traditional manual signatures and seals.[1] A typical set of digital signatures defines two complementary operations: one for signing and the other for verification. With the advance of quantum algorithms,[2,3] traditional digital signature schemes are no longer deemed secure. The development of quantum cryptography led to the creation of encryption algorithms rooted in the principles of quantum mechanics, such as quantum key distribution (QKD),[4,5] quantum secret sharing (QSS),[6,7] and quantum secure direct communication (QSDC).[8,9] The general principles of quantum-based signature schemes were initially proposed in 2002, based on GHZ tripartite states,[10] which are implemented through quantum encryption with the assistance of an arbiter. One advantage of the arbiter is that the authentication process is not solely carried out by the recipient, thereby mitigating the risk of recipient forgery under specific circumstances.

Various application scenarios have given rise to diverse forms of digital signatures, including proxy signatures, blind signatures, threshold signatures, and more. Among these, proxy signatures[11] involve the initial signer designating a proxy signer who is granted the authority to sign a message on their behalf. On the other hand, blind signatures, originally proposed by Chaum,[12] demanded that the signer remain unaware of the message being signed, effectively preserving the confidentiality of the message content. In practical terms, a combination of these two methods can be explored. For instance, the original signer might be traveling or engaged in other official duties and they wish to delegate someone to sign on their behalf. However, the content of the document should remain unknown to the proxy. In such a scenario, a proxy blind protocol is required, enabling the signer to specify the proxy to perform the signing task.

Recently, Chen *et al.*,[13] utilizing Bell states and tripartite entangled states, introduced a quantum proxy blind signature (QPBS) scheme applicable to electronic cash payments. In 2016, Wang *et al.*[14] proposed a QPBS scheme based on W-states, employing robust tripartite W-states to enable the participation of four parties without the need for any quantum unitary operations on the part of the participants. In 2017, Zeng *et al.*[15] presented an efficient and straightforward QPBS scheme that utilizes XOR operations for message blinding encoding. In 2018, Zhang *et al.*[16] introduced a QPBS scheme employing a six-particle entangled state as a quantum channel, introducing a trusted third party to mitigate potential dishonest behavior by verifiers. In the same year, Niu *et al.*[17] proposed a quantum multi-proxy blind signature scheme based on a four-particle cluster state, which not only

†Corresponding author. E-mail: xuxuejiao@hunnu.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

conserves resources compared to previous QPBS schemes but also offers enhanced security. However, in 2020, Zhou *et al.*[18] identified previously overlooked security vulnerabilities in the scheme proposed by Niu *et al.*, particularly in defending against verifier forgery attacks, and introduced corresponding improvement measures to address this deficiency. In 2022, Luo *et al.*[19] introduced two QPBS schemes based on controlled quantum teleportation, utilizing six-particle entangled states and five-particle cluster states, respectively, as the quantum channels for message transmission in the scheme.

To date, quantum proxy blind signatures based on multi-photon entanglement have achieved significant advancements. However, the complexity of multi-photon quantum cryptography is high and its practicality is limited. Furthermore, the efficiency of generating and distributing multi-particle entanglement is relatively low, which constrains both security and transmission distances. In recent years, companies such as IBM have offered quantum cloud services, allowing users to deploy quantum circuits and utilize quantum computing resources, bridging the gap between quantum computing theory and practice. We propose a quantum circuit-based quantum proxy blind signature (QPBS) scheme. Specifically, several participants prepare initial quantum states, blind message in close proximity in quantum circuit, authorize and sign the message, and validate the message at a distance. Additionally, a trusted entity serves as an arbiter for verification, engaging in communication with participants using conventional cryptography to assist the recipient in verifying the signature's validity. The method proposed in our study exhibits several advantages. First, existing quantum proxy blind signature protocols are predominantly theoretical because they necessitate the preparation of multipartite entangled states and particle distribution, thereby requiring further practical validation. Our innovation lies in presenting a highly practical approach, implementable using quantum programming techniques on the IBM Qiskit platform. Second, while current quantum proxy blind signature schemes are largely based on theoretical calculations, assuming an ideal environment, our protocol has undergone experimentation in both simulation simulators and real noisy environments. We have established authentic security thresholds (82.102%) in the presence of real noise, thereby emphasizing the practicality of our proposed solution. It is important to note that the protocol requires execution under the security assumption of the CNOT gate.

This paper is arranged as follows. In Section 2, we illustrate the fundamental definitions and principles of quantum computing including quantum logic gates and quantum measurement that will be used in Section 3. In Section 3, a QPBS scheme is developed step by step with proximal and remote phases. Section 4 provides an instance example of theoretical computation and the experiment results in Qiskit. Section 5 discusses the security and the characteristics of the proposed QPBS scheme. Section 6 contains some conclusions.

2. Preliminaries

To make our scheme easier to understand, we illustrate the fundamental definitions and principles in quantum computing including quantum logic gates and quantum measurement. Linear algebra is the language of quantum computing, which is widely used to describe qubit states, quantum operations, and to predict what a quantum computer does in response to a sequence of instructions.[20] The fundamental descriptions pertain to a Hilbert space denoted as H. It is assumed, without sacrificing generality, that the dimension of the Hilbert space is 2. A spanning set for the Hilbert space H_2 is the set

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \ |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}. \tag{1}$$

There is also another special form, i.e., the vectors

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2}$$

are a couple of bases in H_2, named as X basis, where

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}, \ |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}. \tag{3}$$

They are in a quantum superposition of $|0\rangle$ and $|1\rangle$.

2.1. Quantum logic gates

In quantum circuits, a fundamental computation unit is the quantum logic gate, which could be applied as an operator performed on quantum bits. The following quantum logic gates are involved in our scheme.

The H gate could transform the vectors $|0\rangle, |1\rangle$ to $|+\rangle, |-\rangle$,

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}, \tag{4}$$

i.e., $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$.

The NOT gate, also known as the Pauli X gate, flips the $|0\rangle$ state to $|1\rangle$, and vice versa. The NOT gate is equivalent to RX for the angle T, i.e., $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$.

The CNOT gate consists of a control bit and a target bit, which is used to create entangled qubits and is one of the significant gates in quantum computing. Here, C means the controlled and NOT is the quantum X gate, which is also known as the CX gate, i.e.,

$$\begin{aligned}&\text{CNOT}|00\rangle = |00\rangle, \ \ \text{CNOT}|01\rangle = |01\rangle,\\ &\text{CNOT}|10\rangle = |11\rangle, \ \ \text{CNOT}|11\rangle = |10\rangle.\end{aligned} \tag{5}$$

2.2. Quantum measurement

Quantum measurements can be performed to observe the output of each quantum circuit. When a system in a quantum state is measured, the observer performing the measurement will not see a quantum state vector but rather some classical state. In other words, measurements act as the interface between quantum and classical information, through which classical information is extracted from quantum states. These types of measurements are known as a standard basis measurement.

ZBM (measurement on Z-basis $\{|0\rangle,|1\rangle\}$): Involves measurements with respect to the $\{|0\rangle,|1\rangle\}$ basis.

XBM (measurement on X-basis $\{|+\rangle,|-\rangle\}$): Entails measurements based on the $\{|+\rangle,|-\rangle\}$ basis.

3. Proposed proxy blind signature on quantum circuits

The scheme involves a total of five participants, with Alice as the message owner, Bob as the original signer, Charlie as the proxy signer, David as the signature verifier, and TC as the trusted third party. The scheme is divided into four distinct stages: the initial phase, the blind phase, the authorization signing phase, and the verification phase.

Assumption 1 It is assumed that the quantum CNOT gates can be operated securely. In other words, the inputs of the message owner, Alice, are strictly private to the CNOT gates operator, encompassing Bob, Charlie, and David.

3.1. Initial phase

Step 1 To protect the information transmitted in the classical channel, the protocol of QKD[4,5] is employed by Alice to share keys K_{AC} and K_{AT} with Charlie and TC, while Bob shares key K_{BT} with TC, Charlie shares key K_{CT} with TC, and David shares key K_{DT} with TC. The length of these shared keys in the scheme is denoted as n.

Step 2 Alice prepares a classical message that requires signing, which is encoded into the corresponding quantum sequences $|A\rangle=\{|a_1\rangle,|a_2\rangle,\ldots,|a_n\rangle\}$ on the quantum circuit, i.e., classical bit $a_i=1/0$ then $|a_i\rangle=|1\rangle/|0\rangle$, where $i\in\{1,2,\ldots,n\}$.

Step 3 Bob, Charlie, and David each prepare quantum sequences $|B\rangle=\{|b_1\rangle,|b_2\rangle,\ldots,|b_n\rangle\}$, $|C\rangle=\{|c_1\rangle,|c_2\rangle,\ldots,|c_n\rangle\}$, and $|D\rangle=\{|d_1\rangle,|d_2\rangle,\ldots,|d_n\rangle\}$ with an initial state of $|0\rangle$ on the quantum circuits.

3.2. Proximal blinding message phase

Step 1 Bob, Charlie, and David each apply a Hardamard gate to the initial state $|0\rangle$ on the quantum circuits. The quantum entanglement system is collectively constructed by CNOT gate to control Alice's quantum circuit's qubit A. Here, B, C and D work as control qubits, A works as target qubit. The four parties can be represented as

$$|\psi\rangle=A\otimes B\otimes C\otimes D. \tag{6}$$

The system's state can be represented as

$$|\psi\rangle=\begin{cases}\dfrac{1}{2\sqrt{2}}(|0000\rangle+|0110\rangle+|1010\rangle+|1100\rangle+|1001\rangle+|1111\rangle+|0011\rangle+|0101\rangle)_{ABCD}, & a_i=0,\\ \dfrac{1}{2\sqrt{2}}(|0001\rangle+|0100\rangle+|1000\rangle+|1110\rangle+|1011\rangle+|1101\rangle+|0010\rangle+|0111\rangle)_{ABCD}, & a_i=1.\end{cases} \tag{7}$$

Alice measures qubits A in the Z-basis, leading to the collapse of the four-particle entangled state in the quantum entangled system. The measurement results are randomly $|0\rangle$ and $|1\rangle$, and the Eq. (7) can also be described as

$$|\psi\rangle=\begin{cases}\dfrac{1}{2\sqrt{2}}[|0\rangle\otimes(|000\rangle+|011\rangle+|101\rangle+|110\rangle)+|1\rangle\otimes(|001\rangle+|010\rangle+|100\rangle+|111\rangle)_{ABCD}], & a_i=0,\\ \dfrac{1}{2\sqrt{2}}[|0\rangle\otimes(|001\rangle+|010\rangle+|100\rangle+|111\rangle)+|1\rangle\otimes(|000\rangle+|011\rangle+|101\rangle+|110\rangle)_{ABCD}], & a_i=1.\end{cases} \tag{8}$$

Table 1. The state's evolution of the four-party quantum system after message blinding.

$a_i=0$				$a_i=1$			
M_A	M_B	M_C	M_D	M_A	M_B	M_C	M_D
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

The ZBM results of Alice M_A serve as the blinded classical message. The state's evolution of the system after blinding is illustrated in Table 1.

Step 2 Alice encrypts the original classical message with K_{AT}, obtaining $A'=E_{\mathrm{AT}}(A)$, and sends it to TC.

3.3. Remote authorization and signature phase

Step 1 Alice encrypts the blinded classical message M_A using the key K_{AC}, resulting in

$$M'_A=E_{\mathrm{AC}}(M_A). \tag{9}$$

Subsequently, Alice transmits classical state M'_A to Charlie.

Step 2 Charlie requests authorization from Bob, the protocol terminates if Bob declines. If Bob consents, he performs ZBM on $|B\rangle$. Bob encrypts the measurement results M_B using the key K_{BT} and sends an authorization credential as denoted below to TC:

$$M'_B = E_{\mathrm{BT}}(M_B). \tag{10}$$

Step 3 TC instructs Charlie to commence the signing process. Charlie decrypts the message $M'_A = E_{\mathrm{AC}}(M_A)$ sent by Alice using the key K_{AC}, resulting in the retrieval of M_A. Charlie performs ZBM on quantum states $|C\rangle$ and obtains the result M_C. Thereafter, Charlie encrypts the measurement results M_A and M_C using the key K_{CT} to obtain

$$\mathcal{S}ig = E_{\mathrm{CT}}(M_A, M_C). \tag{11}$$

He sends them to TC, which serves as the signature for the message.

3.4. Remote validation and de-blinding phase

Step 1 $A' = E_{\mathrm{AT}}(A)$, $M'_B = E_{\mathrm{BT}}(M_B)$, and $\mathcal{S}ig = E_{\mathrm{CT}}(M_A, M_C)$ are decrypted by TC, resulting in the retrieval of messages A and M_B, M_A, M_C. TC encrypts M_A and M_B using key K_{DT}, producing the result

$$\mathcal{V}al = E_{\mathrm{DT}}(M_A, M_B), \tag{12}$$

which is then sent to David.

Step 2 David decrypts $\mathcal{V}al$ using the key K_{DT}, obtaining M_A, and M_B. David conducts ZBM on the $|D\rangle$, yielding the result M_D. Based on M_D and the blind evolution process as illustrated in Table 1, David deduces Charlie's measurement result $\mathcal{M}_C \oplus \mathcal{A}$.

Step 3 David encrypts $\mathcal{M}_C \oplus A$ with K_{DT} and sends it to TC for verification. If $\mathcal{M}_C \oplus \mathcal{A} \neq M_C \oplus A$, David rejects the signature. Otherwise, TC encrypts M_A and sends it to David. David performs the de-blinding calculation

$$A = M_A \oplus M_B \oplus M_C \oplus M_D. \tag{13}$$

David acknowledges that M_C is a valid quantum proxy blind signature for blind messages.

4. Protocol instance and experiments

4.1. Protocol instance

In this section, an instance example of the protocol is provided to prove its correctness and feasibility. Suppose that four parties share several pairs of four-bit pre-key $K_{\mathrm{AT}} = \{1010\}$, $K_{\mathrm{BT}} = \{0011\}$, $K_{\mathrm{CT}} = \{1100\}$, $K_{\mathrm{DT}} = \{1001\}$ and $K_{\mathrm{AC}} = \{0101\}$. Table 2 shows the details of this example.

Table 2. Protocol instance.

Phase	2.1	2.2	2.3	2.4
Alice	$K_{\mathrm{AT}} = \{1010\}$ $K_{\mathrm{AC}} = \{0101\}$ $\|A\rangle = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$	$M_A = \{\|1\rangle, \|1\rangle, \|0\rangle, \|0\rangle\}$ $E_{\mathrm{AT}}(A) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$	$E_{\mathrm{AC}}(M_A) = \{\|1\rangle, \|0\rangle, \|0\rangle, \|1\rangle\}$	
Bob	$K_{\mathrm{BT}} = \{0011\}$		$M_B = \{\|1\rangle, \|1\rangle, \|0\rangle, \|0\rangle\}$ $E_{\mathrm{BT}}(M_B) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$	
Charlie	$K_{\mathrm{CT}} = \{1100\}$ $K_{\mathrm{AC}} = \{0101\}$		$E_{\mathrm{AC}}(M_A) = \{\|1\rangle, \|0\rangle, \|0\rangle, \|1\rangle\}$ $M_A = \{\|1\rangle, \|1\rangle, \|0\rangle, \|0\rangle\}$ $M_C = \{\|0\rangle, \|0\rangle, \|1\rangle, \|0\rangle\}$ $E_{\mathrm{CT}}(M_A) = \{\|0\rangle, \|0\rangle, \|0\rangle, \|0\rangle\}$ $E_{\mathrm{CT}}(M_C) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|0\rangle\}$	
David	$K_{\mathrm{DT}} = \{1001\}$			$E_{\mathrm{DT}}(M_A) = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$ $E_{\mathrm{DT}}(M_B) = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$ $M_D = \{\|0\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$ $\mathcal{M}_C \oplus \mathcal{A} = \{\|0\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$ $E_{\mathrm{DT}}(\mathcal{M}_C \oplus A) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|0\rangle\}$ $A = M_A \oplus M_B \oplus M_C \oplus M_D$ $= \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$
TP		$E_{\mathrm{AT}}(A) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$	$E_{\mathrm{BT}}(M_B) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$ $E_{\mathrm{CT}}(M_A) = \{\|0\rangle, \|0\rangle, \|0\rangle, \|0\rangle\}$ $E_{\mathrm{CT}}(M_C) = \{\|1\rangle, \|1\rangle, \|1\rangle, \|0\rangle\}$ $E_{\mathrm{DT}}(M_C) = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$	$E_{\mathrm{DT}}(M_A) = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$ $E_{\mathrm{DT}}(M_B) = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$ $M_C \oplus A = \{\|0\rangle, \|1\rangle, \|1\rangle, \|1\rangle\}$ $E_{\mathrm{DT}}(M_C) = \{\|0\rangle, \|1\rangle, \|0\rangle, \|1\rangle\}$

4.2. Experiment results

In the context of our research, we designed quantum circuits to execute the quantum proxy blind signature protocol proposed in this paper on the IBM quantum cloud platform. The quantum circuits are depicted in Figs. 1 and 2, wherein $q[3]$ is controlled by Alice for the preparation of blind messages $|0\rangle$ and $|1\rangle$ as $|A\rangle$ in Eq. (7). The quantum circuit $q[0]$ is utilized as $|B\rangle$ in Eq. (7) by Bob for generating the authorization credentials, while $q[1]$ and $q[2]$ are employed as $|C\rangle$ and $|D\rangle$ in Eq. (7) by Charlie and David in the signature generation and validation phases. Figure 3 shows the programming source codes of protocol in Qiskit, the total number of runs (shots) was set to 8192. Table 3 presents the probability distribution of 8192 outcomes in both an idealized environment (ibmq qasm simulator), and a noisy environment (ibmq quito processor). The results reveal that the probabilities associated with the eight superposition states outlined in Eq. (7) are approximately equal. Note that it has been determined that the valid range for signature verification in a noisy environment is 8.531% to 11.465%. These eight valid results collectively account for an accuracy rate of 82.102% among all the outcomes, which can also serve as a security threshold for the protocol.

It is worth noting that both Figs. 1 and 2 have a dividing line. On the left side of the line, the main focus is on implementing Phases 3.1 and 3.2, which need to be completed in close proximity. On the right side of the line, the primary objective is to accomplish Phases 3.3 and 3.4, which can be effectively executed remotely in practical scenarios.

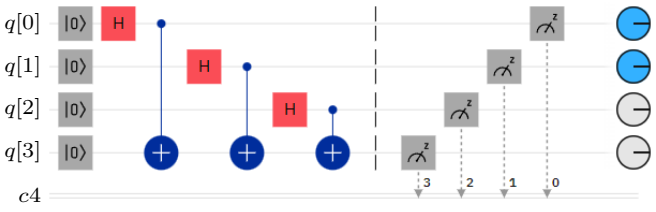


Fig. 1. Quantum circuits and real-time results of the proxy blind signature protocol when $a_i = 0$.

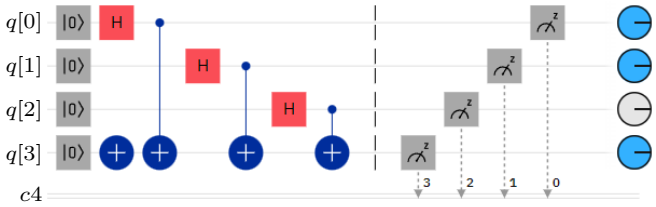


Fig. 2. Quantum circuits and real-time results of the proxy blind signature protocol when $a_i = 1$.

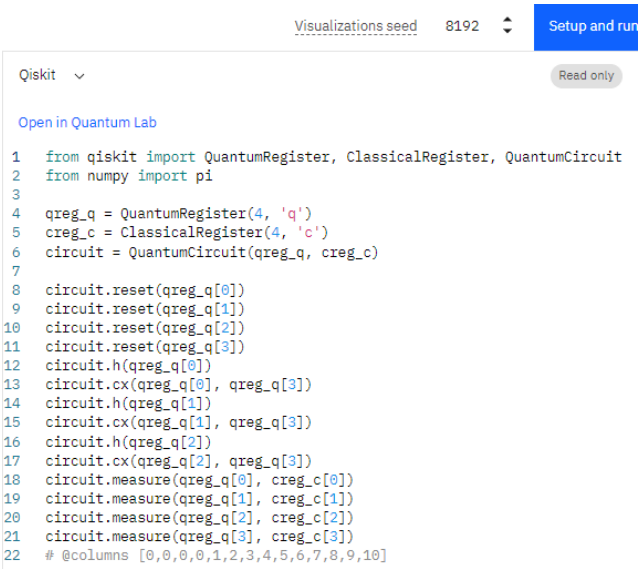


Fig. 3. The source code programming in the Qiskit programming of the IBM quantum cloud platform.

Table 3. Results from 8192 runs of the proxy blind signature protocol in ideal and noisy environment.

Ibmq_qasm_simulator			Ibmq_quito		
Results of $q[0],q[1],q[2],q[3]$	Probability	Verification	Results of $q[0],q[1],q[2],q[3]$	Probability	Verification
$\|0\rangle,\|0\rangle,\|0\rangle,\|0\rangle$	12.424%	valid	$\|0\rangle,\|0\rangle,\|0\rangle,\|0\rangle$	10.911%	valid
$\|0\rangle,\|0\rangle,\|0\rangle,\|1\rangle$	0.000%	invalid	$\|0\rangle,\|0\rangle,\|0\rangle,\|1\rangle$	3.318%	invalid
$\|0\rangle,\|0\rangle,\|1\rangle,\|0\rangle$	0.000%	invalid	$\|0\rangle,\|0\rangle,\|1\rangle,\|0\rangle$	1.719%	invalid
$\|0\rangle,\|0\rangle,\|1\rangle,\|1\rangle$	13.223%	valid	$\|0\rangle,\|0\rangle,\|1\rangle,\|1\rangle$	9.812%	valid
$\|0\rangle,\|1\rangle,\|0\rangle,\|0\rangle$	0.000%	invalid	$\|0\rangle,\|1\rangle,\|0\rangle,\|0\rangle$	1.831%	invalid
$\|0\rangle,\|1\rangle,\|0\rangle,\|1\rangle$	12.400%	valid	$\|0\rangle,\|1\rangle,\|0\rangle,\|1\rangle$	11.440%	valid
$\|0\rangle,\|1\rangle,\|1\rangle,\|0\rangle$	12.827%	valid	$\|0\rangle,\|1\rangle,\|1\rangle,\|0\rangle$	9.360%	valid
$\|0\rangle,\|1\rangle,\|1\rangle,\|1\rangle$	0.000%	invalid	$\|0\rangle,\|1\rangle,\|1\rangle,\|1\rangle$	2.090%	invalid
$\|1\rangle,\|0\rangle,\|0\rangle,\|0\rangle$	0.000%	invalid	$\|1\rangle,\|0\rangle,\|0\rangle,\|0\rangle$	2.810%	invalid
$\|1\rangle,\|0\rangle,\|0\rangle,\|1\rangle$	12.124%	valid	$\|1\rangle,\|0\rangle,\|0\rangle,\|1\rangle$	11.465%	valid
$\|1\rangle,\|0\rangle,\|1\rangle,\|0\rangle$	12.761%	valid	$\|1\rangle,\|0\rangle,\|1\rangle,\|0\rangle$	9.219%	valid
$\|1\rangle,\|0\rangle,\|1\rangle,\|1\rangle$	0.000%	invalid	$\|1\rangle,\|0\rangle,\|1\rangle,\|1\rangle$	2.370%	invalid
$\|1\rangle,\|1\rangle,\|0\rangle,\|0\rangle$	12.209%	valid	$\|1\rangle,\|1\rangle,\|0\rangle,\|0\rangle$	10.520%	valid
$\|1\rangle,\|1\rangle,\|0\rangle,\|1\rangle$	0.000%	invalid	$\|1\rangle,\|1\rangle,\|0\rangle,\|1\rangle$	2.415%	invalid
$\|1\rangle,\|1\rangle,\|1\rangle,\|0\rangle$	0.000%	invalid	$\|1\rangle,\|1\rangle,\|1\rangle,\|0\rangle$	1.345%	invalid
$\|1\rangle,\|1\rangle,\|1\rangle,\|1\rangle$	12.032%	valid	$\|1\rangle,\|1\rangle,\|1\rangle,\|1\rangle$	9.375%	valid

5. Security and analysis

5.1. Blindness

In the proposed scheme, the proxy signer, Charlie, is responsible for signing the blinded message rather than the original message. On one hand, Charlie is unaware of the original message $|A\rangle$. This is because Charlie does not possess knowledge of the measurement results of quantum sequences from other participants, making it impossible for him to recover the original message from the blinded one. On the other hand, the ciphertext containing the original message is encrypted by Alice using the key $|K_{\mathrm{AT}}\rangle$, which is known only to Alice and TC. As a result, other participants do not have access to the complete information of the original message. In summary, Charlie remains oblivious to the actual content of the original message being signed, thus satisfying the blindness requirement for proxy blind signatures in this scheme.

5.2. Non-repudiation

After being verified as valid, Charlie cannot repudiate the signature he submitted, and Alice and Bob cannot deny their authorization actions. During the authorization signing phase, participants Alice, Bob, and Charlie each perform measurements on their respective quantum circuits and encrypt the corresponding measurement results before sending them to TC. Subsequently, TC forwards the received encrypted measurement results to David for signature verification.

The measurement results of quantum states are protected by shared keys when transmitted over channels. In this scheme, the keys are based on the protocol of QKD, which is a proven secure method. The quantum circuits of Alice, Bob, and Charlie constitute a quantum system with entanglement between them. The quantum state only collapses to a definite state after the participants complete measurements of the quantum states they hold. Therefore, until the particles are measured, no one can accurately deduce the quantum state information held by others. The quantum states of circuits cannot be accurately replicated, making it impossible for attackers to forge particles, obtain correct measurement results, or deceive the verification process. Indeed, a potential security concern arises with the CNOT gates because there exists the possibility of information leakage after the CNOT gate. This potential vulnerability stems from the fact that the output of $q[3]$ may be altered by the controlling bits manipulated by Bob, Charlie, and David. Fortunately, the protocol operates under a stringent assumption, as indicated earlier in Subsection 3.1, asserting that the quantum CNOT gates can be securely operated. Consequently, David can use these measurement results to determine whether participants Alice, Bob, and Charlie engaged in repudiation of the signature, thus demonstrating the non-repudiation property of the proposed proxy blind signature scheme.

5.3. Unforgeability

The character of unforgeability refers to the impossibility for both internal participants and external attackers, such as Eve, to successfully counterfeit the signature of the agent signer, Charlie. In this scheme, a trusted center (TC) exists, to which participants must submit the original message $|A\rangle$, the blinded message M_A, the authorization credential M_B, and the signature M_C, rather than M_D. Consequently, TC possesses the capability of assisting verification. However, he could not forge a valid signature without M_C, which perfectly matches M_D in Table 1. Similarly, Charlie and David are not able to forge signatures since they have no idea about M_B and M_C, respectively.

Counterfeiting attacks by internal participants are infeasible. Charlie's signature is composed of a combination of keys and their measurement results. Assuming that the message owner, Alice, is a malicious participant planning to forge Charlie's signature for illicit gain, Alice would first need to acquire the keys K_{CT}, which are shared between Charlie and TC via the protocol of QKD. Therefore, Alice cannot forge the signature with the key. Furthermore, the measurement results are Charlie's private information, and the quantum system is in a superposition state, making it impossible for Alice to obtain accurate measurement results. Consequently, the forged signature would be detected by David in step 3 of the verification stage. Even if Alice and Charlie conspired in an attack, they would still be unable to forge signatures. This is because, without the cooperation of the original signer, Bob, they cannot know Bob's measurement results M_B, thus lacking the authorization credentials for Charlie to sign on behalf of Bob. Any forged signature would inevitably fail David's verification. Therefore, internal participants cannot successfully execute a counterfeiting attack.

Counterfeiting attacks by external attacker Eve are also impossible. This is because Eve lacks access to any portion of the quantum entanglement state system or the shared keys among scheme participants in the four-party quantum system. Consequently, compared to internal participants, Eve has even less useful information for forging signatures, making it impossible to successfully counterfeit Charlie's signature.

6. Conclusion

In this paper, a quantum blind signature scheme is proposed. Unlike existing QPBS schemes based on theoretical computations, this scheme constructs quantum circuits on the IBM quantum cloud platform, Qiskit. Participants employ quantum Hadamard gates and CNOT gates on the quantum

circuit to control the original message state, utilizing the measurement outcomes as blinded messages, authorized agent credentials, and signatures. A theoretical example is calculated to demonstrate the correctness of the scheme. Furthermore, experiments are conducted in both ideal and noisy environments on the IBM quantum cloud platform, yielding compelling data that substantiates the practical feasibility of the proposed scheme. The aforementioned security analysis indicates that this scheme possesses blindness, non-repudiation, and unforgeability, meeting the security requirements of quantum blind signature schemes. It holds promise for applications in fields such as e-commerce and e-government. However, the protocol is limited by the security assumption of the CNOT gate. In other words, while the protocol gains an advantage by eliminating the need for the advance preparation of entangled states, it introduces a security drawback related to the security of CNOT gates.

Acknowledgments

Project supported by the General Project of Natural Science Foundation of Hunan Province (Grant Nos. 2024JJ5273 and 2023JJ50328) and the Scientific Research Project of Education Department of Hunan Province (Grant Nos. 22A0049 and 22B0699).

References

[1] Rivest R L, Shamir A and Adleman L 1983 *Communications of the ACM* **26** 96
[2] Grover L K 1996 *Proc. 28th Annu. ACM Symp. on Theory of Computing*, May 22–24, 1996, New York, US, p. 212
[3] Shor P W 1999 *SIAM Review* **41** 303
[4] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[5] Gong L H, Song H C, He C S, Liu Y and Zhou N R 2014 *Physica Scripta* **89** 035101
[6] Wang J, Li L, Peng H and Yang Y 2017 *Phys. Rev. A* **95** 022320
[7] Ouyang Y, Tan S H, Zhao L and Fitzsimons J F 2017 *Phys. Rev. A* **96** 052333
[8] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[9] Cao Z W, Feng X Y, Peng, J Y, Zeng G H and Qi X F 2015 *Int. J. Theor. Phys.* **54** 1871
[10] Zeng G and Keitel C H 2002 *Phys. Rev. A* **65** 042312
[11] Mambo M, Usuda K and Okamoto E 1996 *IEICE Trans. Fund. Electr.* **79** 1338
[12] Chaum D, Rivest R L and Sherman A T 1983 *Advances in Cryptology: Proceedings of CRYPTO* '82 August 23–25, 1982, Boston, US, p. 199
[13] Chen Y Z, Liu Y and Wen X J 2011 *Chin. J. Quant. Elect.* **28** 341
[14] Wang H, Shi R H, Zhong H, Cui J, Zhang S and Wang K T 2016 *Chin. J. Quant. Elect.* **33** 35
[15] Zeng C, Zhang J Z and Xie S C 2017 *Chin. J. Compu. Syste.* **38** 1485
[16] Zhang J L, Zhang J Z and Xie S C 2018 *Int. J. Theor. Phys.* **57** 1612
[17] Niu X F, Zhang J Z and Xie S C 2018 *Commun. Theor. Phys.* **70** 043
[18] Zhou B M, Lin L D, Wang W and Liu Y 2020 *Int. J. Theor. Phys.* **59** 465
[19] Luo Q, Zhang T, Huang X and Jing N 2022 *Entropy* **24** 1421
[20] Nielsen M A and Chuang I L 2010 *Quantum computation and quantum information* (New York: Cambridge university press) pp. 15–45