Counterfactual Quantum Secret Sharing

Nomi Lae, Shehbaz Tariq, Saw Nang Paing, Jason William Setiawan, Sunghwan Kim, *Senior Member, IEEE*, Trung Q. Duong, *Fellow, IEEE*, and Hyundong Shin, *Fellow, IEEE*

***Abstract*—The emerging quantum technology has highlighted the necessity for secure and efficient secret sharing in quantum networks. In this paper, we introduce a verifiable multiparty counterfactual quantum secret sharing (QSS) protocol, enhancing security and efficiency. This QSS protocol utilizes a low-depth quantum circuit to encrypt and decrypt information, which comprises a unitary operator constructed using a preshared secret key. To ensure the robustness and verifiability of the shared secret key, the protocol imposes constraints on the participants with the Chinese remainder theorem. The most significant advantage of our proposed QSS protocol is incorporating counterfactual communication, which considerably enhances the scheme's security by enabling exchange-free information sharing among participants, thereby minimizing the risk of eavesdropping or intercept-and-resend attacks. Furthermore, we incorporate a weighted-threshold mechanism that provides flexibility, enabling diverse use cases to design security protocols for quantum networks. The security analysis of the counterfactual QSS protocol and its implementation on IBM Quantum computers reveals strong resilience to internal and external attacks, along with high efficiency and robustness, making it effective for quantum encryption in the noisy intermediate-scale quantum era.**

***Index Terms*—Chinese remainder (or Sunzi's) theorem, counterfactual quantum protocols, quantum secret sharing.**

I. Introduction

SECURITY in conventional cryptographic schemes primarily relies on computational complexity, assuming that adversaries have limited computational resources [1]. However, the emergence of quantum computing, a radically different paradigm that exploits the principles of quantum mechanics—such as superposition and entanglement—fundamentally challenges this assumption [2]–[4]. These quantum properties have enabled the creation of unconditionally secure, anonymous, and secret communication systems, significantly advancing the field of quantum cryptography [5]–[7]. Consequently, classical cryptographic concepts, including secret sharing, must be reevaluated for their feasibility and adaptability in the quantum computing era.

A. Related Works

Secret sharing was first introduced through two foundational schemes developed independently: one based on Lagrange interpolation and the other utilizing linear geometric projections [8]. In secret sharing, a secret is divided into multiple parts and distributed among authorized participants. The secret can only be reconstructed when these participants collaborate according to a specified protocol. This concept has led to the development of numerous protocols designed to address a wide range of scenarios and security requirements, including access structures, secret verification, and fraud detection [9]–[13]. While the primary goal of secret sharing is to protect sensitive information by distributing shares among multiple parties, its applications extend to areas such as hierarchical access control, electronic voting, group signatures, secure multiparty computing, and electronic auctions [14].

The transition from classical secret sharing to the quantum domain was achieved through the use of multipartite entangled Greenberger–Horne–Zeilinger (GHZ) states, marking a significant development in the field of quantum secret sharing (QSS) [15]. Subsequently, numerous QSS protocols have been proposed, utilizing techniques such as the quantum Fourier transform, Grover's algorithm, and error-correcting codes in conjunction with mathematical tools such as Lagrange interpolation and the Chinese remainder theorem (CRT) [16]–[24]. Furthermore, unitary operation-based encryption techniques, including quantum permutation padding [25], and experimental quantum homomorphic encryption [26], have demonstrated promising prospects for interaction-free delegated quantum computing. These advancements can be integrated with secret sharing protocols for various applications.

B. Motivations

Despite significant research interest in QSS protocols, many existing methods remain challenging to implement, as they rely on fault-tolerant quantum computers and noiseless quantum channels. This presents a considerable limitation in the noisy intermediate-scale quantum (NISQ) era, where quantum states and operations are susceptible to gate operation errors, decoherence, and channel noise [27]–[29]. The recently proposed CRT-based weighted-threshold QSS protocol and the

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) under RS-2025-00556064 and by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-2021-0-02046) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). The work of T. Q. Duong was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109 and in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant Program RGPIN-2025-04941. *(Corresponding author: Hyundong Shin; Sunghwan Kim.)*

N. Lae, S. Tariq, S. N. Paing, J. W. Setiawan, and H. Shin are with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104, Republic of Korea (e-mail: hshin@khu.ac.kr). N. Lae and S. Tariq contributed equally to this paper.

S. Kim is with the School of Electronic Engineering, Kyonggi University, Republic of Korea (e-mail: skim@kyonggi.ac.kr).

T. Q. Duong is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada, and also with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, UK. (e-mail: tduong@mun.ca).

two-qubit-based protocol address some practical shortcomings by exploiting the reversibility of single-qubit phase-shift unitary operations and employing entanglement, respectively [30], [31]. These schemes are more flexible, simple, and efficient than the traditional QSS protocols. However, they require verifications of the validity of the reconstructed secret's correctness, vulnerability to dishonest participants, and impracticability when the number of participants increases. Additionally, the two-qubit-based protocol increases noise due to entangling gates, making it more difficult to implement on quantum computers than single-qubit-based gates, further hindering efficiency and reliability.

Although the QSS protocol plays a crucial role in protecting sensitive information, particularly in military and government applications, the protocol remains vulnerable to counterfactual attacks, which pose a severe risk to the security of shared secret keys [32]. Counterfactual communication is a novel mode of communication that enables information transmission without requiring any information-carrying particles to travel through the channel [33]. Attackers can exploit the intrinsic properties of counterfactual communications to remain undetected within the channel, enabling them to execute counterfactual attacks [34].

C. Contributions

To address the aforementioned issues, we propose a verifiable $(\mathcal{W}, \omega, n)$-multiparty weighted-threshold counterfactual QSS scheme, where $\mathcal{W}$, ω, and n denote a set of weights, a threshold value, and a participant number, respectively. This protocol employs a quantum unitary operation to encrypt and decrypt quantum information using a secret key. The QSS scheme leverages the CRT to split and reconstruct the key, making it suitable for both quantum and classical information sharing in the NISQ era, offering enhanced security and practicality. A key feature of our protocol is the use of counterfactual communication techniques, which rely on photon interference in the quantum channel rather than the exchange of physical particles, ensuring a highly secure communication channel.

In our counterfactual QSS protocol, counterfactual quantum secure direct communication (QSDC) is employed to transfer classical information—such as co-prime integers and remainders—among participants in a counterfactual manner. Meanwhile, quantum information is transmitted through a counterfactual quantum channel using quantum state transfer (QST). The secret key is then reconstructed using the CRT, followed by a verification process to ensure its correctness and security. This verifiable mechanism confirms the integrity of the reconstructed secret key by detecting dishonest behavior during the verification stage and preventing malicious participants from accessing the secret unless they cooperate honestly. Moreover, the inherent properties of counterfactual communication provide strong resistance against eavesdropping and intercept-and-resend attacks, ensuring the privacy and confidentiality of shared secrets. To evaluate the efficiency of counterfactual QSDC and QST protocols, we analyze their transmission success probabilities. The results demonstrate that these counterfactual protocols are highly efficient when a large number of inner and outer cycles of the nested Mach-Zehnder interferomenter (MZI) are used. Finally, we conduct a security analysis of the counterfactual QSS protocol and assess its feasibility by implementing the devised unitary encryption scheme on the cloud IBM Quantum (IBMQ) computers.

The remainder of this paper is organized as follows. Section II introduces the fundamental concepts of counterfactual quantum communication (CQC), including counterfactual QSDC and QST protocols. Section III presents the proposed weighted-threshold counterfactual QSS scheme. Section IV provides the security analysis of the designed counterfactual QSS protocol. Section V presents the numerical analysis, evaluating the security of quantum encryption and analyzing its IBMQ implementation. Finally, Section VI summarizes our findings and discusses potential extensions and generalizations of our study.

II. Preliminaries

This section briefly introduces CQC, quantum encryption, and the CRT.

A. Counterfactual Communication

CQC combines interaction-free measurement (IFM) [35], [36] and the quantum Zeno effect (QZE) to enable information transmission without particles passing through the channel [33], [37], [38]. IFM detects the presence of an absorptive object (AO) in an interferometer without direct interaction [35], while the QZE preserves a quantum state through frequent measurements [39]. In this CQC framework, the absence of an AO in the interferometer encodes bit 0, while its presence encodes bit 1. We summarize CQC, counterfactual QSDC, and counterfactual QST protocols used in our proposed method.

1) Counterfactual Secure Direct Communication: Counterfactual QSDC enables the direct transmission of classical information from Alice to Bob without the need for a private key and without any information-carrying particle passing through the channel [40]. The protocol requires each party to initially prepare $2N$ maximally entangled Bell pairs. In this setup, Alice's qubits act as quantum AOs (QAOs), while Bob's qubits act as photons. The initial composite state of Alice and Bob can be expressed as follows:

$$|\Psi\rangle_j = |\phi_0\rangle_{\mathrm{A}_{1j}\mathrm{A}_{2j}} |\phi_1\rangle_{\mathrm{B}_{1j}\mathrm{B}_{2j}} \tag{1}$$

where $|\phi_0\rangle_{\mathrm{A}_{1j}\mathrm{A}_{2j}}$ and $|\phi_1\rangle_{\mathrm{B}_{1j}\mathrm{B}_{2j}}$ denote the maximally entangled Bell pairs of Alice and Bob, respectively, and $j = 1, 2, \ldots, 2N$. Fig. 1 demonstrates the counterfactual QSDC protocol, which involves the following steps.

- **Counterfactual entanglement swapping:** Alice and Bob send their respective qubits A_{2j} and B_{1j} to the counterfactual swap (C-Swap) gate. This gate swaps two entangled pairs as follows:

$$|\tilde{\Psi}\rangle_j = |\phi_0\rangle_{\mathrm{A}_{1j}\mathrm{B}_{1j}} |\phi_1\rangle_{\mathrm{A}_{2j}\mathrm{B}_{2j}} . \tag{2}$$

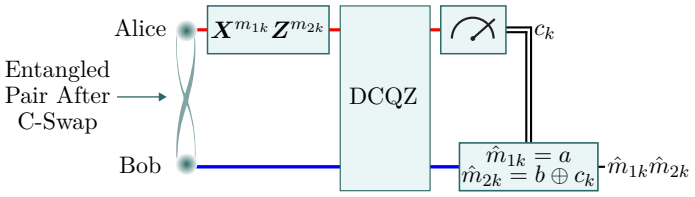


Fig. 1. A counterfactual QSDC protocol. After the C-Swap gate, Alice and Bob share entangled pairs, where half of these pairs are used for message encoding. Alice encodes two classical bits $m_1 m_2$ using the unitary operations before transmitting them through the DCQZ gate. Bob then decodes the transmitted information $\hat{m}_{1k}\hat{m}_{2k}$ based on the measurement outcome from Alice.

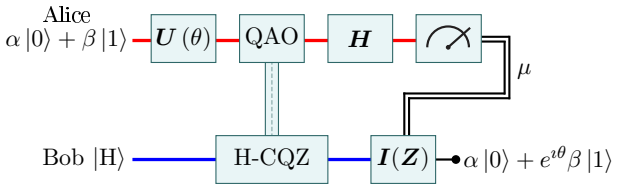


Fig. 2. A counterfactual QST protocol. Initially, Alice holds a QAO, and Bob inputs a horizontally polarized photon $|\mathrm{H}\rangle$ to the H-CQZ gate. If Alice wants to add a phase shift to a qubit to be transmitted, she applies $\boldsymbol{U}(\theta)$ on her QAO before the H-CQZ operation, where θ represents the phase information. Following the H-CQZ operation, Alice performs the Hadamard gate $\boldsymbol{H}$ on her qubit, conducts measurement in the computational basis, and discloses the result μ. If $\mu=0$ (1), Bob reconstructs the transmitted quantum state by applying the $\boldsymbol{I}$ ($\boldsymbol{Z}$) gate on his qubit.

- **Security checking:** Alice randomly selects N entangled pairs, announces their positions to Bob, and measures their corresponding qubits to verify the security of the swapped entangled pairs. If the pairs are secure, they proceed to the next step.
- **Encoding:** On the remaining N entangled pairs, Alice encodes her message by applying the $\boldsymbol{X}^{m_{1k}}\boldsymbol{Z}^{m_{2k}}$ operation on her qubit, where $\boldsymbol{X}=|0\rangle\langle 1|+|1\rangle\langle 0|$ and $\boldsymbol{Z}=|0\rangle\langle 0|-|1\rangle\langle 1|$ are Pauli operators and $m_{1k}m_{2k}\in\{00,01,10,11\}$, $k=1,2,\ldots,N$.
- **Counterfactual transmission:** Utilizing the dual form of chained quantum Zeno (CQZ) operations [37], Alice and Bob engage in the counterfactual transmission of Alice's encoded message.
- **Decoding:** Alice measures her qubit in the Hadamard basis and announces the result c_k through a classical channel. Based on the detector click D_{ab} after the dual CQZ (DCQZ) operation and Alice's announcement, Bob decodes Alice's message as $\hat{m}_{1k}=a$ and $\hat{m}_{2k}=b\oplus c_k$, where $\oplus$ denotes the binary addition.

2) Counterfactual State Transfer: Counterfactual QST allows the transfer of an arbitrary quantum state from Alice to a remote party, Bob, without transmitting information-carrying particles through a channel, as shown in Fig. 2 [41]. It is facilitated by the horizontally polarized CQZ (H-CQZ) gate, which changes the photon polarization in the presence of AO [33], [42]. In this setup, Alice holds a QAO, while Bob inputs a photon into the H-CQZ gate. The initial composite state of Alice and Bob can be written as

$$|\eta_0\rangle_{\mathrm{AB}}=(\alpha|0\rangle_{\mathrm{A}}+\beta|1\rangle_{\mathrm{A}})|\mathrm{H}\rangle_{\mathrm{B}} \tag{3}$$

where $|\alpha|^2+|\beta|^2=1$. To transfer a phase-shifted arbitrary quantum state, Alice applies a unitary operation $\boldsymbol{U}(\theta)=|0\rangle\langle 0|+e^{\imath\theta}|1\rangle\langle 1|$ on her QAO before the H-CQZ operation where $\imath=\sqrt{-1}$ and $\theta\in[0,2\pi]$ represents phase information. After the H-CQZ operation, the qubits of Alice and Bob become entangled as follows:

$$|\eta_1\rangle_{\mathrm{AB}}=\alpha|0\rangle_{\mathrm{A}}|\mathrm{H}\rangle_{\mathrm{B}}+\beta e^{\imath\theta}|1\rangle_{\mathrm{A}}|\mathrm{V}\rangle_{\mathrm{B}}. \tag{4}$$

To disentangle the qubits, Alice performs the Hadamard gate $\boldsymbol{H}=(\boldsymbol{X}+\boldsymbol{Z})/\sqrt{2}$ on her qubit and measures it on the computational basis. Then, she communicates the measurement outcome μ to Bob. If $\mu=0$ (1), then Bob applies the $\boldsymbol{I}$ ($\boldsymbol{Z}$) gate on his qubit to reconstruct the transmitted quantum state.

B. Quantum Encryption

Now, we discuss quantum encryption that utilizes unitary operators for encrypting data and their corresponding Hermitian conjugate operators for decryption [25].

1) Quantum Encryption Circuit: A quantum circuit for encryption can be generated according to Algorithm 1. The resulting circuit is denoted as $\boldsymbol{U}(\theta_{\mathrm{key}})$, where θ_{key} is a random seed derived from the provided `secret_key`. To ensure hardware compatibility, the circuit undergoes transpilation, mapping logical gates to native basis gates of the target quantum processor, optimizing execution fidelity, and minimizing depth [43], [44].

2) Encryption of Classical Information: To encrypt a k-bit classical sequence, it is divided into $\ell=k/n$ chunks, where n is the number of qubits used per chunk. If k is not divisible by n, the sequence is padded with zeros. Each qubit is initialized to $|0\rangle^{\otimes n}$ with the $\boldsymbol{X}$ gate applied to encode 1, leaving 0 unchanged. After encoding, the encryption circuit is applied, and the qubits are measured, retaining the most possible 2^n chunks. This process repeats for all ℓ chunks, which are combined to form the encrypted sequence. Padded bits are removed to finalize the encryption [25].

3) Encryption of Quantum Information: The encryption of quantum information involves three key steps. First, the quantum state is prepared as a linear combination of its eigenstates, $\boldsymbol{\rho}=\sum_k \lambda_k|\psi_k\rangle\langle\psi_k|$, and sent to the input of the quantum encryption circuit. This encryption circuit transforms each eigenstate $|\psi_k\rangle$ into an encrypted state $|\psi_k\rangle=\boldsymbol{U}(\theta_{\mathrm{key}})$. The density matrix of the encrypted quantum state then becomes $\boldsymbol{\rho}_{\mathrm{enc}}=\boldsymbol{U}(\theta_{\mathrm{key}})\,\boldsymbol{\rho}\boldsymbol{U}(\theta_{\mathrm{key}})^{\dagger}$ where the superscript $\dagger$ denotes the Hermitian conjugate. Then, quantum state tomography can be used to analyze the encrypted state by estimating it through measurements on multiple copies. Finally, the encrypted state $\boldsymbol{\rho}_{\mathrm{enc}}$ is transmitted through a quantum channel.

4) Decryption: The decryption process for both classical and quantum information includes the application of the Hermitian conjugate of the encryption circuit, denoted as

Algorithm 1 Quantum Encryption Circuit Generation

Input: `num_qubits`, `basis_gates`, `secret_key`, `required_depth`
Output: Encryption Quantum Circuit
Initialize `random_seed` with `secret_key`
Define `circuit` as QuantumCircuit(`num_qubits`)
while depth of `circuit` < `required_depth` **do**
  Select q_1, q_2 randomly from 0 to `num_qubits - 1`
  Generate random angles $\theta, \phi, \lambda, \gamma$
  if `num_qubits = 1` **then**
    Add U3 gate to `circuit` with θ, ϕ, λ on q_1
  else if $q_1 \neq q_2$ **then**
    Add CU3 gate to `circuit` with θ, ϕ, λ using q_1, q_2
  end if
  Transpile `circuit` to match `basis_gates`
end while
Trim `circuit` to `required_depth`
return `circuit`

$\boldsymbol{U}\left(\theta_{\text{key}}\right)^{\dagger}$. However, a successful decryption process can only be realized if the party attempting to decrypt possesses the correct θ_{key}, as $2^n!$ combinations of quantum permutation matrices are possible for generating encrypted circuits. The advantages of this encryption technique in the quantum domain are described in [25].

C. Weighted-Threshold Secret Sharing With CRT

The CRT-based weighted-threshold secret sharing scheme provides securely distributing secret keys among a hierarchical group of participants. Each participant is assigned a weight, and a threshold value ω is defined, requiring that a subset of participants whose combined weights meet or exceed ω to reconstruct the secret key θ_{key}. The CRT ensures the existence of a unique secret key θ_{key} that satisfies a system of congruences. By leveraging this property, the scheme enables participants to securely share their assigned parameters, modular values, and remainders to reconstruct the key collectively.

III. Counterfactual Secret Sharing

We present the proposed counterfactual QSS scheme using a weighted-threshold CRT methodology to enable secure and efficient distribution of secret keys among n participants. This QSS protocol is structured into three primary phases, including the key generation and distribution phase, the reconstruction phase, and the verification phase. The scheme utilizes counterfactual QSDC and QST, leveraging the enhanced security offered by counterfactuality.

A. Key Generation and Distribution Phase

In this phase, the dealer formulates the access structure for participants by adjusting the weight values attributed to each individual. In the traditional QSS protocol outlined in [30], the dealer plays a pivotal role in preparing and sharing private keys. The dealer is responsible for determining the allocation

Algorithm 2 Key Generation and Distribution

Input: $w_i \in \mathcal{W}$ weights, n participants, threshold ω
Output: Secret key θ_{key} for dealer, $\boldsymbol{s}_i = (a_i, m_i)$ for each participant P_i
for all $w_i \in \mathcal{W}$ **do**
  Generate co-prime integers m_i
  ▷ Adjust m_i according to weight w_i
end for
for $x \in \mathcal{X} = \left\{\prod_{i=1}^{n} m_i^k \;\middle|\; k = 0, 1\right\}$ **do**
  if $\sum_{i=1}^{n} w_i < \omega$ **then**
    Add x to set $\mathcal{A}$ ▷ For sums less than ω
  else if $\sum_{i=1}^{n} w_i \geq \omega$ **then**
    Add x to set $\mathcal{B}$ ▷ For sums satisfying ω
  end if
end for
Determine θ_{key} where $\max \mathcal{A} < \theta_{\text{key}} \leq \min \mathcal{B}$
  ▷ Choose θ_{key} between $\max \mathcal{A}$ and $\min \mathcal{B}$
for $i = 1$ to n **do**
  $a_i \leftarrow \theta_{\text{key}} \mod m_i$ ▷ Calculate remainder a_i
end for
Distribute $\boldsymbol{s}_i$ using counterfactual QSDC
return θ_{key} for dealer, $\boldsymbol{s}_i$ for each P_i

of these keys to participants and encrypting quantum particles using the assigned keys, ensuring secure communication. The weighted-threshold scheme introduces an additional layer of security. In this scheme, the dealer assigns a weight $w_i \in \mathcal{W}$ to the ith participant, reflecting their significance within the group. A threshold value ω is defined, requiring that a subset of participants satisfies $\sum_{i=1}^{k} w_i \geq \omega$ for successful secret reconstruction. This constraint guarantees that only authorized participants with a sufficient combined weight can access the secret key.

The CRT ensures the existence of a unique integer, the secret key θ_{key}, which satisfies a system of simultaneous congruences as follows:

$$\theta_{\text{key}} = \left(\sum_{i=1}^{n} a_i \prod_{j \neq i}^{n} \frac{M}{m_j} \right) \mod M \tag{5}$$

where a_i is the remainder of the Euclidean division of $x \in \mathcal{X} = \left\{\prod_{i=1}^{n} m_i^k \;\middle|\; k = 0, 1\right\}$ by m_i and $M = \prod_{i=1}^{n} m_i$ [45]. The moduli $m_1, m_2, \ldots, m_n$ are pairwise relatively prime positive integers, ensuring uniqueness and solvability. The remainders satisfy $0 \leq a_i \leq m_i$ for each i. The dealer then distributes shares to each participant in the form of pairs $\boldsymbol{s}_i = (a_i, m_i)$. Similar to this distribution phase, the dealer in the counterfactual QSS protocol disseminates shares of the modulus and the remainder to all participants. Initially, n participants are assigned weights $w_i \in \mathcal{W}$, and the dealer generates co-prime integers m_i for each participant. Based on these weights, the dealer generates a key and specific shares for each participant. For low w_i, the corresponding integer m_i consists of a product of smaller prime numbers, while a high value of weight w_i leads to m_i being composed of a product of larger prime numbers. To guarantee the secure distribution

of classical data, the counterfactual QSDC is utilized, as described in Algorithm 2.

B. Reconstruction Phase

This phase requires participants to collaborate in reconstructing the secret key. The involved members exchange their modulus and remainder values, then apply the CRT algorithm to reconstruct the key, denoted as $\hat{\theta}_{\text{key}}$. In this phase, each participant has already received their share $\boldsymbol{s}_i = (a_i, m_i)$ during the distribution phase. Secret key reconstruction is achieved when a sufficient subset of participants cooperatively shares their a_i and m_i values. By solving the system of congruences using the CRT algorithm, the secret key θ_{key} can be securely retrieved. This process ensures that only participants meeting the predefined threshold condition can reconstruct the secret. As outlined in Algorithm 3, the participants exchange their share values by using counterfactual QSDC. Counterfactuality enhances the robustness of counterfactual QSS, offering a reliable and secure solution for quantum communication in multiparty settings.

C. Verification Phase

In the final phase, the participants authenticate the reconstructed key $\hat{\theta}_{\text{key}}$ by applying it to the encryption algorithm (see Algorithm 3). Subsequently, these parties perform counterfactual QST to convey quantum states $\boldsymbol{\sigma}_j$ securely to the dealer. The dealer then verifies whether the reconstructed key $\hat{\theta}_{\text{key}}$ matches the original dealer key θ_{key}. Finally, the participants collaborate to reconstruct the secret key, as described in Algorithm 3. The involved members exchange their modulus and remainder values and subsequently apply the CRT algorithm to reconstruct the key. A schematic representation of the designed counterfactual QSS scheme and its various stages is shown in Fig. 3.

Algorithm 3 Key Reconstruction and Verification

Input: $\boldsymbol{s}_i = (a_i, m_i)$ for each participant
Output: Reconstructed key $\hat{\theta}_{\text{key}}$
function DECOYSTATES($\{\boldsymbol{\rho}_1, \boldsymbol{\rho}_2, \ldots, \boldsymbol{\rho}_m\}$)
    Prepare sequence of decoy states $\{|\phi\rangle\langle\phi|\}$
    Insert decoy states randomly into $\{\boldsymbol{\rho}_1, \boldsymbol{\rho}_2, \ldots, \boldsymbol{\rho}_m\}$
    Check for eavesdropper presence
end function
function CRT($\mathcal{S} = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_k\}$)
    return $\hat{\theta}_{\text{key}}$ from CRT algorithm
end function
Participants:
for all P_i, $i = 1, 2, \ldots, k$ **do**
    Exchange modulus m_i among participants using
    counterfactual QSDC
    for all m_j, $j \neq i$ **do**
        if $m_j \neq m_i$ and $\gcd(m_i, m_j) = 1$ **then**
            Continue the process
        else
            Abort the process
        end if
    end for
    if participant is the leader **then**
        Prepare and send quantum states $\boldsymbol{\sigma}_j$ using
        counterfactual QST
    end if
    Send a_i to all other participants
    Reconstruct key using CRT: $\hat{\theta}_{\text{key}} \leftarrow \text{CRT}(\mathcal{S})$
    Encrypt quantum states using $\hat{\theta}_{\text{key}}$
    Send encrypted states to the dealer
end for
Dealer:
for $i = 1, 2, \ldots, k$ **do**
    Decrypt received quantum states
end for
Announce results to all participants
if all results are valid **then**
    Key is verified
else
    Abort the process
end if

IV. SECURITY ANALYSIS

Since the shared secret key is a fundamental requirement of the designed protocol, it is crucial that its portion is not leaked to eavesdroppers. Additionally, as counterfactual QSDC and QST play essential roles in the key sharing and verification stages, ensuring the secure transmission of messages and quantum states is imperative. It has been proven that counterfactual QSDC is secure against various types of external attacks, such as man-in-the-middle and Trojan horse attacks [40]. To further ensure the security of the transmitted quantum states, we analyze the security of the counterfactual QST in Section IV-A. The potential attacks that Eve may launch in the counterfactual QSDC and QST are categorized as external attacks. In addition to these attacks, internal attacks may also arise, where one or more dishonest participants attempt to obtain the secret key without collaborating with others. To mitigate these threats, the devised protocol incorporates a crucial verification step, which is fundamental in all secure communication scenarios. Moreover, the counterfactual nature of the protocol eliminates the need for entangling gates, distinguishing it from conventional approaches. These aspects collectively enhance the security and reliability of the counterfactual QSS protocol, ensuring robust communication without relying on entangling gates.

A. Security of Counterfactual QST

To intercept quantum states transferred between the dealer and the participants, Eve can attempt various attacks, despite being constrained by the no-cloning theorem in quantum mechanics. The two most typical attacks she can employ are the man-in-the-middle and entangle-and-measure attacks.

1) Man-in-the-Middle Attacks: To verify security, d decoy particles in the computational and Hadamard basis states $|0\rangle$, $|1\rangle$, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are inserted into the quantum

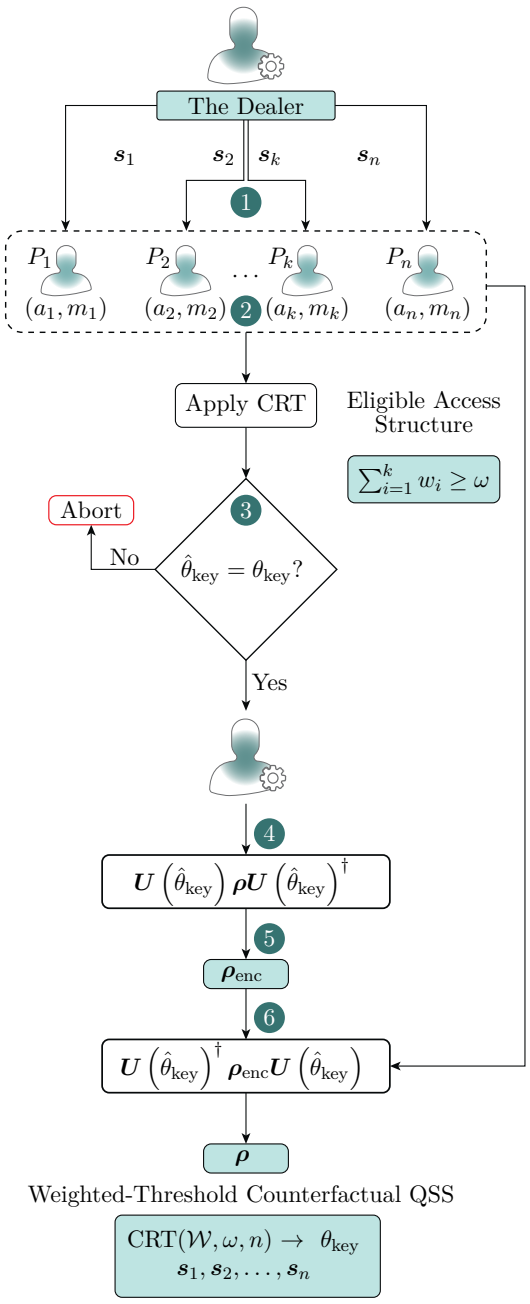


Fig. 3. A verifiable $(\mathcal{W}, \omega, n)$-multiparty weight-threshold counterfactual QSS protocol. 1) The dealer distributes the partial keys $\boldsymbol{s}_i$, $i = 1, 2, \ldots, k$ to participants following the counterfactual QSS protocol, ensuring security through counterfactual QSDC. 2) Participants collaborate to reconstruct the key using their shares via CRT and verify the threshold condition $\sum_{i=1}^{k} w_i \geq \omega$. 3) The reconstructed key is validated using Algorithm 3. 4) Upon successful verification, the dealer encrypts the secret quantum information $\boldsymbol{\rho}$ using the shared key $\hat{\theta}_{\text{key}}$. 5) The encrypted state $\boldsymbol{\rho}_{\text{enc}}$ is transmitted to the participants via counterfactual QST. 6) Participants decrypt the state using the Hermitian conjugate of the unitary transformation, provided they possess the correct key.

state sequences, with the dealer possessing a record of their positions. Subsequently, the dealer sends these sequences to the participants. To intercept the dealer's state, Eve sits between the dealer and the ith participant P_i. She impersonates P_i by sending her photon through the H-CQZ gate to the dealer while simultaneously acting as the dealer for the incoming photon from P_i. Suppose the initial joint state of the dealer, P_i, and Eve as follows:

$$|\psi_0\rangle_{\text{AEB}} = (\alpha\,|0\rangle + \beta\,|1\rangle)_{\text{A}}\,(\gamma\,|\text{H}0\rangle_{\text{E}} + \delta\,|\text{H}1\rangle_{\text{E}})\,|\text{H}\rangle_{\text{B}} \quad (6)$$

where A, B, and E denote the qubits of the dealer (Alice), P_i (Bob), and Eve, respectively. After passing through the H-CQZ gate, this initial state transforms to

$$|\psi_1\rangle_{\text{AEB}} = |i\rangle_{\text{A}}\,(\alpha\,|\text{H}j\rangle_{\text{E}} \pm \beta\,|\text{V}j\rangle_{\text{E}})\,(\gamma\,|\text{H}\rangle_{\text{B}} \pm \delta\,|\text{V}\rangle_{\text{B}}) \quad (7)$$

where $i, j \in \{0, 1\}$. Note that when Alice and Bob declare their measurement results, they are inconsistent. For d decoy particles, Eve is detected with a probability of $1 - 1/4^d$. As d increases, the probability of detecting Eve approaches one, ensuring robust security against eavesdropping.

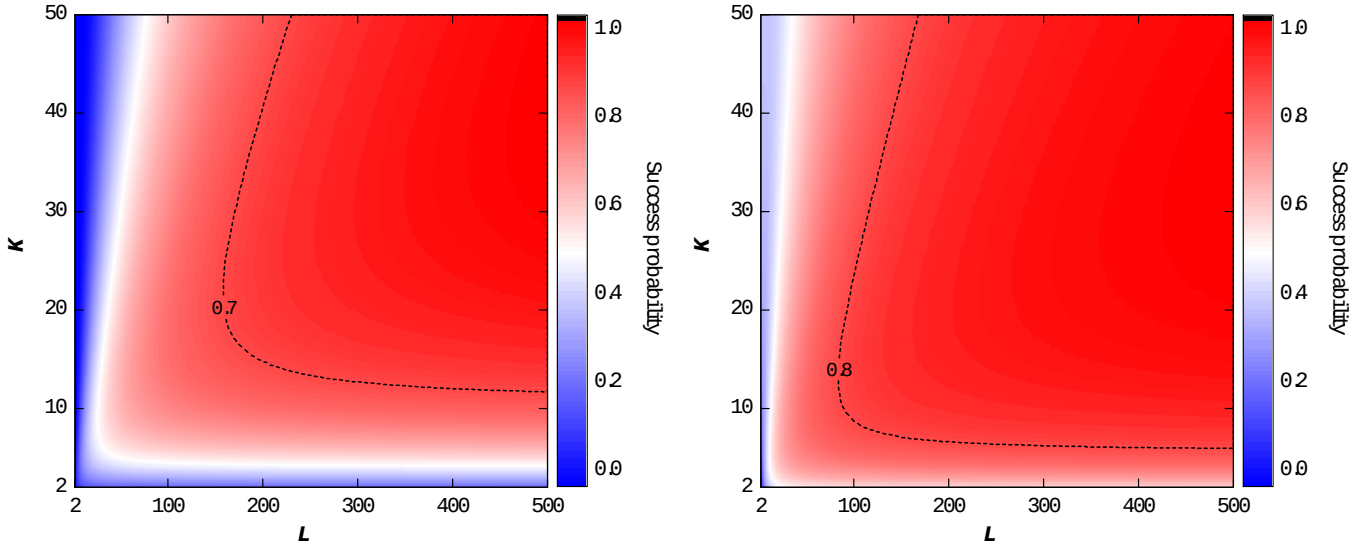
2) Entangle-and-Measure Attacks: Eve can attempt to steal the QAO state of the dealer by applying a unitary operation to entangle the transmitted particle with her own qubit and then measuring her qubit. However, her measurement collapses the entangled state shared between the dealer and P_i, leading to discrepancies in their measurement outcomes. To counter this attack, the dealer and P_i can introduce decoy particles at random positions during quantum state transmission. The more decoy particles incorporated, the higher the probability of detecting Eve's presence, thereby enhancing the protocol's security.

B. Security of Shared Secret Keys

The designed protocol includes a key verification stage to prevent internal attacks before quantum information is shared. Since the proposed scheme follows a weighted-threshold model, the key is determined by the range between the minimum value from the set $\mathcal{A}$ and the maximum value from the set $\mathcal{B}$. Hence, only participants who satisfy the weighted threshold ω can reconstruct the key. If any participant fails to comply with this requirement, the secret key shared by the dealer cannot be retrieved. Once the threshold condition is met, each legitimate participant obtains the secret key from the dealer. To verify the secret key, participants generate arbitrary quantum state sequences, encode them using the received secret key, and send them back to the dealer. Since the dealer already knows the secret key, he can decode the states and compare them with the states declared by the participants. Some errors may occur due to channel noise. However, if the error rate exceeds an acceptable threshold, the dealer immediately detects potential dishonesty among participants and restarts the secret sharing protocol. Therefore, the protocol can proceed only if all the participants are honest.

V. Numerical Analysis

This section presents the numerical analysis, evaluating success probabilities of counterfactual QSDC and QST protocols, assessing the security of quantum encryption, and analyzing the IBMQ implementation results.



(a) Counterfactual QSDC (b) Counterfactual QST

Fig. 4. Success probabilities (a) P_{cqsdc} and (b) P_{cqst} of the counterfactual QSDC and QST protocols as a function of inner cycles L and outer cycles K. For counterfactual QSDC, we set $J = K$ MQZ operations.

A. Success Probability of Counterfactual QSDC and QST

The success probability of counterfactual communication is mainly influenced by the numbers of inner and outer cycles—denoted as L and K, respectively—used in the CQZ gate. As detailed in [40], [46], and [47], the success probabilities of the counterfactual QSDC and QST protocols can be expressed respectively as follows:

$$P_{\text{cqsdc}} = \lambda_J \lambda_K^2 P_{K,L}^2 \left[1 - \frac{1}{2}\cos^2\left(\frac{\pi}{2J}\right)\sin^2\left(\frac{\pi}{2L}\right)\right]^{LJ} \quad (8)$$

$$P_{\text{cqst}} = \frac{1}{2}\left[\cos^{2K}\left(\frac{\pi}{2K}\right) + P_{K,L}\right] \quad (9)$$

with

$$\lambda_K = \left[1 - \frac{1}{2}\sin^2\left(\frac{\pi}{2K}\right)\right]^K \quad (10)$$

$$P_{K,L} = \prod_{k=1}^{K}\left[1 - \sin^2\left(\frac{k\pi}{2K}\right)\sin^2\left(\frac{\pi}{2L}\right)\right]^L \quad (11)$$

where J denotes the number of modified quantum Zeno (MQZ) operations used in the counterfactual QSDC protocol. Fig. 4 shows the success probabilities P_{cqsdc} and P_{cqst} as a function of inner cycles L and outer cycles K. For the counterfactual QSDC protocol, we set $J = K$ MQZ operations. For both counterfactual protocols, the success probabilities asymptotically approach one as the cycle numbers L and K increase, ensuring that no physical particle passes through the channel while transmitting both the classical and quantum information. Subsequently, the proposed QSS protocol leverages the inherent security advantages of CQC [32], [48].

Implementing CQC within the QSS framework introduces an inherent tradeoff between enhanced security benefits from no information-carrier transmission and the detrimental effects of photonic loss. This photonic loss primarily arises from absorption or scattering in optical components, as well as weak measurements performed within the interferometer, governed by the nested MZIs and the QZE [34], [49]. Such photonic loss can significantly degrade the fidelity of both classical and quantum information transmission, thereby compromising the overall efficiency of the proposed protocol. Moreover, an excessive number of inner L and outer K cycles intensifies these losses, potentially lowering the success probability of counterfactual transmission and increasing the risk of transmission failures. To counteract these deleterious effects, high-quality optical components and rigorous resource optimization for L and K are imperative [50]. Such optimization aims to minimize photonic losses while preserving both the integrity and counterfactuality of the communication protocol, ensuring a robust and efficient implementation of counterfactual QSS.

Furthermore, previous two-qubit-based QSS protocols [30], [31] are susceptible to increased noise due to entangling operations such as controlled-NOT (CNOT) gates and quantum state teleportation. These entanglement-based protocols suffer from decoherence and fidelity degradation due to multi-qubit interactions, making their practical implementation more challenging. In contrast, CQC protocols fundamentally differ from entanglement-based schemes, as the counterfactual protocols do not rely on quantum entanglement in the traditional sense. Instead, the protocol leverages quantum interference and the QZE to control photon transmission, enabling counterfactual information transfer. The absence of entangling operations in CQC eliminates the noise and decoherence issues associated with entangling gates, distinguishing it from two-qubit-based QSS protocols. However, the counterfactual QSS protocol remains vulnerable to counterfactual channel imperfections, including photonic loss, dispersion, and phase instability within the optical medium. Although there is no fault-tolerant implementation

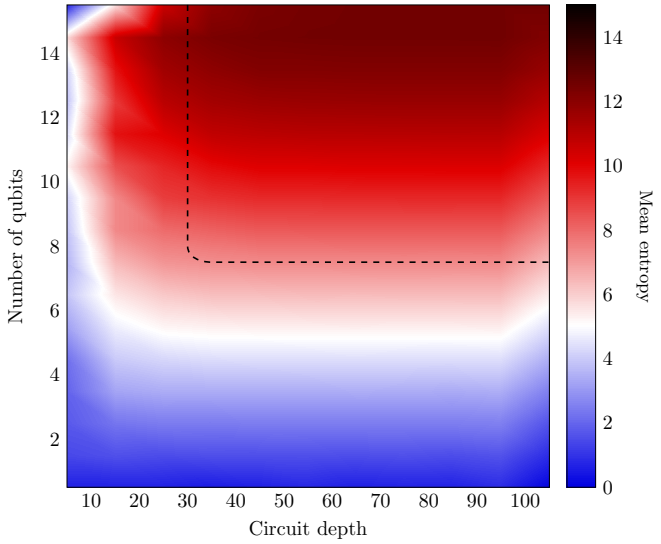


Fig. 5. Mean entropy $\langle \mathcal{H} \rangle$ of encrypted 15-bit sequences as a function of the quantum circuit depth and the number of qubits for `qasm_simulator`. The heatmap illustrates the relationship between qubit count per chunk, encrypting circuit depth, and mean entropy values. These entropy values are obtained by averaging over 10 trials for each depth and qubit count combination with 2^{12} shots per trial. Bit sequences are randomly generated for each trial and a seed (secret key) of 836 is used for reproducibility.

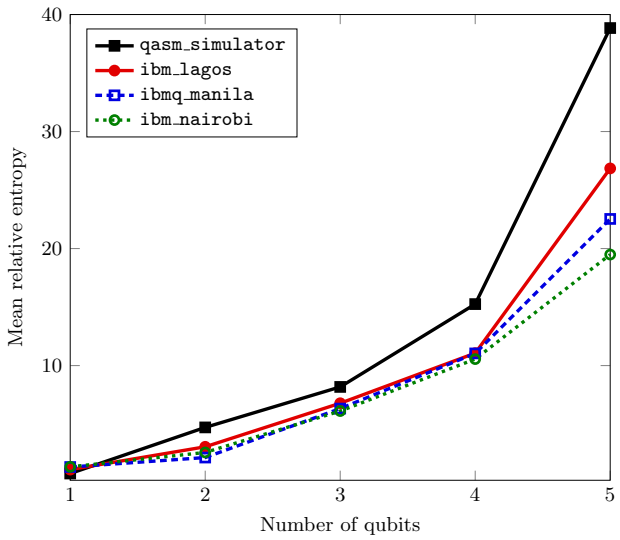


Fig. 6. Comparative analysis of encoding a q-qubit Hadamard state $\boldsymbol{\rho} = \boldsymbol{H}^{\otimes q}$ using the `qasm_simulator`, `ibm_lagos`, `ibmq_manila`, and `ibm_nairobi` quantum devices. A single-depth encoding circuit is generated with a seed (secret key). Quantum state tomography reconstructs the encoded state $\boldsymbol{\rho}_{\text{enc}}$ and the relative entropy $D(\boldsymbol{\rho} \| \boldsymbol{\rho}_{\text{enc}})$ is calculated as a metric for uninterpretability. The mean relative entropy is obtained from $1,000$ trials for `qasm_simulator` and 10 trials for `ibm_lagos`, `ibmq_manila`, and `ibm_nairobi` (each with a random seed). All experiments employ 2^{12} shots per trial.

of the nested MZI, the quantum error correction and phase stabilization techniques can minimize errors introduced by different noise sources in the counterfactual setup.

B. Security of Quantum Encryption

In this subsection, we present the specific metrics used to assess the security of quantum encryption in terms of its capability to obfuscate information by incorporating randomness into the encrypted data. These metrics are utilized in Section V-C to analyze the implementation of the encryption scheme on actual quantum computers. For classical information, we use entropy $\mathcal{H} = -\sum_i p_i \log_2(p_i)$ spanning all possible outcomes where p_i denotes the probability of observing the ith bit sequence chunk. In encryption schemes, entropy measures the unpredictability or randomness of the concealed information. An increased entropy value corresponds to enhanced security and resistance to attacks, making it increasingly difficult to extract the original information from the encrypted data. For quantum information, we employ the Kullback-Leibler (KL) divergence, defined as [51]:

$$D(\boldsymbol{\rho} \| \boldsymbol{\rho}_{\text{enc}}) = \text{tr}(\boldsymbol{\rho} \log_2 \boldsymbol{\rho}) - \text{tr}(\boldsymbol{\rho}_{\text{enc}} \log_2 \boldsymbol{\rho}_{\text{enc}}) \tag{12}$$

where $\text{tr}(\boldsymbol{\rho})$ and $\text{tr}(\boldsymbol{\rho} \log_2 \boldsymbol{\rho})$ denote the trace operator and the von Neumann entropy of the quantum state $\boldsymbol{\rho}$, respectively. In quantum information encryption, the KL divergence quantifies the difference or relative entropy between two quantum states, measuring the inefficiency of assuming one quantum state when the actual state is different.

C. IBMQ Implementation Analysis

The IBMQ cloud platform [52] is an invaluable experimental testbed for studying and validating quantum information science concepts. This platform enables users to perform quantum computations by remotely accessing physical quantum computers via cloud services, using a Python-based framework known as `Qiskit`. The primary focus of IBMQ systems is to simulate small-scale quantum circuits, with performance benchmarked using key metrics such as the quantum volume (QV), circuit layer operations per second (CLOPS), median CNOT error rate, and median readout error rate. Additionally, the noiseless simulator, `qasm_simulator`, can be employed to validate hypotheses and compare results against real quantum hardware, which inherently exhibits noise and imperfections. In this paper, we utilize `qasm_simulator` to investigate the mean entropy $\langle \mathcal{H} \rangle = -\frac{1}{T} \sum_{j=1}^{T} \sum_i p_{i,j} \log_2(p_{i,j})$ of encoding a k-bit sequence as a function of varying encryption circuit depths and the number of qubits where $p_{i,j}$ denotes the probability of observing the ith outcome in the jth trial from a total of T trials. Fig. 5 illustrates a heatmap depicting the mean entropy $\langle \mathcal{H} \rangle$ of encrypted 15-bit sequences as a function of the quantum circuit depth and the number of qubits, obtained using `qasm_simulator`. The heatmap reveals a clear increasing behavior in the mean entropy as the number of qubits and circuit depth increase, highlighting their effect on encryption security. However, some deviations from this pattern can be attributed to statistical noise, as only the 2^{12} shots used per trial may not be sufficient to eliminate entropy fluctuations fully.

To evaluate the security of the proposed quantum encoding scheme in terms of the relative entropy defined in (12), we utilize three different quantum computers: `ibm_nairobi` (7 qubits), `ibm_lagos` (7 qubits), and `ibmq_manila` (5

TABLE I
COMPARISON OF QSS METHODS

Method		**Counterfactual QSS**	**CRT-based QSS [30], [31]**	**Traditional QSS [15]**
Verification		Verified the original key with the reconstructed key	N/A	N/A
Security	**Internal attacks**	Resistant when $\sum_{i=1}^{k} w_i < \omega$	Resistant when $\sum_{i=1}^{k} w_i < \omega$	Resistant when a single participant lacks all divided parts of the information
	External attacks	Resistant to intercept-and-resend, man-in-the-middle, Trojan horse, and entangle-and-measure attacks	Resistant to intercept-and-resend and entangle-and-measure attacks	N/A
Quantum resources		N qubits	N qubits	N qubits
Scalability	**Noise robustness**	Robust against dephasing noise	N/A	N/A
	Efficiency	Probabilistic (M, N)	N/A	N/A

qubits). These computers share the same QV of 32 and have computational capacities of $2,600$, $2,700$, and $2,800$ CLOPS, respectively. The complete backend specifications are publicly available on the IBMQ cloud platform. For our experiment, we prepare a q-qubit Hadamard state $\boldsymbol{\rho} = \boldsymbol{H}^{\otimes q}$, which exhibits a low circuit depth of 1. We then employ a single-depth logical encoding circuit generated using a `secret_key` as the seed (see Algorithm 1). This circuit is used solely for secret key generation and does not implement a physical bosonic channel. Note that after transpilation, the circuit depth increases, as logical gates are converted into physical gates supported by the quantum hardware. The rationale for maintaining a low circuit depth stems from the inherently noisy nature of current quantum computers and their limited QV. For example, a QV of 32 implies that a quantum circuit can reliably execute on 4 qubits with a depth of 8. To compute the mean relative entropy, we generate random secret keys as seeds within the range from 0 to $1,000$, producing corresponding quantum encoding circuits. The prepared state $\boldsymbol{\rho}$ is then evolved through these circuits, and once it is encoded as $\boldsymbol{\rho}_{\text{enc}}$, we assess its effectiveness by reconstructing $\boldsymbol{\rho}_{\text{enc}}$ using quantum state tomography—the gold standard for benchmarking quantum computers. Using built-in tomography techniques in `Qiskit`, which are based on the least-square algorithm, we reconstruct $\boldsymbol{\rho}_{\text{enc}}$. We then calculate the relative entropy $D\left(\boldsymbol{\rho} \| \boldsymbol{\rho}_{\text{enc}}\right)$ and determine the mean value over all trials. Finally, as shown in Fig. 6, we plot this mean relative entropy as a function of the number q of qubits, demonstrating the enhanced security of encoded quantum information as q increases.

VI. DISCUSSION AND CONCLUSION

In conclusion, the designed QSS protocol based on CQC provides a practical and secure solution for hierarchical communication systems. By utilizing counterfactual QSDC and counterfactual QST in the initial phases and incorporating a key verification step, the protocol offers both internal and external security while effectively identifying dishonest parties. Moreover, our scheme outperforms existing QSS methods by ensuring robustness against internal and external attacks, enabling secure key reconstruction through weighted-threshold validation, and enhancing scalability with noise-resistant properties, as shown in Table I. The low-depth quantum circuit used in our protocol for encryption and decryption reduces the number of gate operations, rendering it ideal for implementation on the current NISQ devices. By mitigating the noise effect and increasing entropy, the designed protocol demonstrates near-term applicability in fields such as quantum cloud computing and secure communication within organizations with diverse security clearance levels.

To optimize the performance of quantum computers, both the sender and receiver must employ the same basis gates, with a priority given to single-qubit-based circuits. Additionally, the number of qubits and encryption circuit depth should not exceed the QV of the device to prevent information loss caused by gate and readout errors. Before implementing such a system, it is essential to conduct benchmark tests on state reconstruction fidelity using quantum state tomography and to assess entropy levels. These security metrics provide valuable insights into the applicability of the proposed protocol. We can develop pulse-efficient algorithms and utilize low-level hardware manipulation techniques to further optimize resource efficiency and reduce error rates. Ultimately, the proposed protocol strikes an effective balance between security and practicality, making it a viable candidate for deployment in the current NISQ devices and a wide range of applications requiring secure hierarchical communication.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, Mar. 2002.

[2] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022.

[3] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019.

[4] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins *et al.*, "Quantum computational advantage with a programmable photonic processor," *Nature*, vol. 606, no. 7912, pp. 75–81, Jun. 2022.

[5] S. N. Paing, J. W. Setiawan, T. Q. Duong, D. Niyato, M. Z. Win, and H. Shin, "Quantum anonymous networking: A quantum leap in privacy," *IEEE Netw.*, vol. 38, no. 5, pp. 131–145, Sep. 2024.

[6] C. Thalacker, F. Hahn, J. de Jong, A. Pappa, and S. Barz, "Anonymous and secret communication in quantum networks," *New J. Phys.*, vol. 23, no. 8, p. 083026, Aug. 2021.

[7] S. Tariq, U. Khalid, B. E. Arfeto, T. Q. Duong, and H. Shin, "Integrating sustainable big AI: Quantum anonymous semantic broadcast," *IEEE Wireless Commun.*, vol. 31, no. 3, pp. 86–99, Jun. 2024.

[8] A. Shamir, "How to share a secret," *Commun. ACM.*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[9] K. Meng, F. Miao, Y. Ning, W. Huang, Y. Xiong, and C.-C. Chang, "A proactive secret sharing scheme based on Chinese remainder theorem," *Front. Comput. Sci.*, vol. 15, pp. 1–10, Apr. 2021.

[10] X. Li, C.-C. Chang, and Y. Liu, "A generalized Chinese remainder theorem-based proactive multi-secret sharing scheme for global wide area network," *Telecommun Syst.*, vol. 78, no. 1, pp. 49–56, Sep. 2021.

[11] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electron. Commun. Jpn.*, vol. 72, no. 9, pp. 56–64, Jan. 1989.

[12] E. Karnin, J. Greene, and M. Hellman, "On secret sharing systems," *IEEE Trans. Inf. Theory*, vol. 29, no. 1, pp. 35–41, Jan. 1983.

[13] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Commun. ACM.*, vol. 24, no. 9, pp. 583–584, Sep. 1981.

[14] A. Beimel, "Secret-sharing schemes: A survey," in *Proc. International Conference on Coding and Cryptology (ICCC)*, Berlin, Heidelberg, May 2011, pp. 11–46.

[15] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, p. 1829, Mar. 1999.

[16] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, p. 648, Jul. 1999.

[17] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A*, vol. 59, no. 1, p. 162, Jan. 1999.

[18] L. Xiao, G. L. Long, F.-G. Deng, and J. W. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Phys. Rev. A*, vol. 69, no. 5, p. 052307, May 2004.

[19] Z.-J. Zhang and Z.-X. Man, "Multiparty quantum secret sharing of classical messages based on entanglement swapping," *Phys. Rev. A*, vol. 72, no. 2, p. 022303, Aug. 2005.

[20] Z.-J. Zhang, Y. Li, and Z.-X. Man, "Multiparty quantum secret sharing," *Phys. Rev. A*, vol. 71, no. 4, p. 044301, Apr. 2005.

[21] G. G. Ping and G. G. Can, "Quantum secret sharing without entanglement," *Phys. Lett. A*, vol. 310, no. 4, pp. 247–251, Apr. 2003.

[22] F.-L. Yan and T. Gao, "Quantum secret sharing between multiparty and multiparty without entanglement," *Phys. Rev. A*, vol. 72, no. 1, p. 012304, Jul. 2005.

[23] L.-Y. Hsu, "Quantum secret-sharing protocol based on Grover's algorithm," *Phys. Rev. A*, vol. 68, no. 2, p. 022306, Aug. 2003.

[24] K. Meng, F. Miao, Y. Xiong, and C.-C. Chang, "A reversible extended secret image sharing scheme based on Chinese remainder theorem," *Signal Process. Image Commun.*, vol. 95, p. 116221, Jul. 2021.

[25] K. Randy and P. Maria, "Quantum encryption with quantum permutation pad in IBMQ systems," *EPJ Quantum Technol.*, vol. 9, p. 26, Dec. 2022.

[26] J. Zeuner, I. Pitsios, S.-H. Tan, A. N. Sharma, J. F. Fitzsimons, R. Osellame, and P. Walther, "Experimental quantum homomorphic encryption," *npj Quantum Inf.*, vol. 7, no. 1, p. 25, Feb. 2021.

[27] U. Khalid, J. ur Rehman, S. N. Paing, H. Jung, T. Q. Duong, and H. Shin, "Quantum network engineering in the NISQ age: Principles, missions, and challenges," *IEEE Netw.*, vol. 38, no. 1, pp. 112–123, Jan. 2024.

[28] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018.

[29] S. Tariq, A. Farooq, J. ur Rehman, T. Q. Duong, and H. Shin, "Efficient quantum state estimation with low-rank matrix completion," *EPJ Quantum Technol.*, vol. 11, no. 1, p. 50, Aug. 2024.

[30] Y. H. Chou, G. J. Zeng, X. Y. Chen, and S. Y. Kuo, "Multiparty weighted threshold quantum secret sharing based on the Chinese remainder theorem to share quantum information," *Sci. Rep.*, vol. 11, no. 1, p. 6093, Mar. 2021.

[31] F. Li, M. Luo, and S. Zhu, "A new (w, t, n)-weighted threshold quantum secret sharing scheme based on two-qubit system," *Physica A*, vol. 607, p. 128229, Dec. 2022.

[32] Z.-H. Li, L. Wang, J. Xu, Y. Yang, M. Al-Amri, and M. S. Zubairy, "Counterfactual Trojan horse attack," *Phys. Rev. A*, vol. 101, no. 2, p. 022336, Feb. 2020.

[33] H. Salih, Z.-H. Li, M. Al-Amri, and M. S. Zubairy, "Protocol for direct counterfactual quantum communication," *Phys. Rev. Lett.*, vol. 110, no. 17, p. 170502, Apr. 2013.

[34] M. A. Ullah, S. N. Paing, and H. Shin, "Noise-robust quantum teleportation with counterfactual communication," *IEEE Access*, vol. 10, pp. 61 484–61 493, Jun. 2022.

[35] A. C. Elitzur and L. Vaidman, "Quantum mechanical interaction-free measurements," *Found. Phys.*, vol. 23, no. 7, pp. 987–997, Jul. 1993.

[36] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, "Interaction-free measurement," *Phys. Rev. Lett.*, vol. 74, no. 24, p. 4763, Jun. 1995.

[37] F. Zaman, U. Khalid, T. Q. Duong, H. Shin, and M. Z. Win, "Quantum full-duplex communication," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 9, pp. 2966–2980, Sep. 2023.

[38] S. N. Paing, J. W. Setiawan, M. A. Ullah, F. Zaman, T. Q. Duong, O. A. Dobre, and H. Shin, "Counterfactual quantum Byzantine consensus for human-centric Metaverse," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, pp. 905–918, Apr. 2024.

[39] W. M. Itano, D. J. Heinzen, J. J. Bollinger, and D. J. Wineland, "Quantum Zeno effect," *Phys. Rev. A*, vol. 41, no. 5, p. 2295, Mar. 1990.

[40] S. N. Paing, F. Zaman, J. ur Rehman, T. Q. Duong, and H. Shin, "Counterfactual quantum protocols for dialogue, teleportation and comparison," *IEEE Trans. Commun.*, vol. 73, no. 2, pp. 874–888, Feb. 2025.

[41] Z.-H. Li, M. Al-Amri, X.-H. Yang, and M. S. Zubairy, "Counterfactual exchange of unknown quantum states," *Phys. Rev. A*, vol. 100, no. 2, p. 022110, Aug. 2019.

[42] F. Zaman, S. N. Paing, A. Farooq, H. Shin, and M. Z. Win, "Concealed quantum telecomputation for anonymous 6G URLLC networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 7, pp. 2278–2296, Jul. 2023.

[43] N. Earnest, C. Tornow, and D. J. Egger, "Pulse-efficient circuit transpilation for quantum applications on cross-resonance-based hardware," *Phys. Rev. Res.*, vol. 3, p. 043088, Oct. 2021.

[44] S. N. Paing, F. Zaman, J. ur Rehman, and H. Shin, "Counterfactual universal logic gates," in *Proc. Korea Information and Communication Society (KICS) Summer Conference*, Pyeongchang, Korea, Aug. 2020.

[45] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in e-voting," *Electronic Notes in Theor. Comput. Sci.*, vol. 186, pp. 67–84, Jul. 2007.

[46] S. N. Paing, T. Q. Duong, and H. Shin, "Counterfactual long-distance quantum communication," in *Proc. International Conference on Quantum Communications, Networking, and Computing (QCNC)*, Kanazawa, Japan, Jul. 2024, pp. 253–258.

[47] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, "Counterfactual quantum-information transfer without transmitting any physical particles," *Sci. Rep.*, vol. 5, no. 1, Feb. 2015.

[48] Z. Q. Yin, H. W. Li, W. Chen, Z. F. Han, and G. C. Guo, "Security of counterfactual quantum cryptography," *Phys. Rev. A*, vol. 82, p. 042335, Oct. 2010.

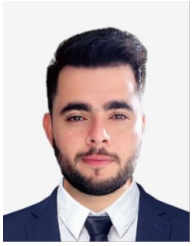
[49] R. Demkowicz-Dobrzański, M. Jarzyna, and J. Kołodyński, "Quantum limits in optical interferometry," *Prog. Opt.*, vol. 60, pp. 345–435, Jan. 2015.

[50] F. Zaman, K. Lee, and H. Shin, "Information carrier and resource optimization of counterfactual quantum communication," *Quantum Inf. Process.*, vol. 20, no. 5, p. 168, May 2021.

[51] B. Qi, Z. Hou, L. Li, D. Dongi, G. Xiang, and G. Guo, "Quantum state tomography via linear regression estimation," *Sci. Rep.*, vol. 3, no. 1, p. 3496, Dec. 2013.

[52] G. García-Pérez, M. A. Rossi, and S. Maniscalco, "IBM Q experience as a versatile experimental testbed for simulating open quantum systems," *npj Quantum Inf.*, vol. 6, pp. 1–10, Jan. 2020.

Nomi Lae received the B.E. degree in Electronic Engineering from Yangom Technology University (YTU), Myanmar, in 2020. She is currently pursuing the Ph.D. degree in quantum information science with the Department of Electronics and Information Convergence Engineering, Kyung Hee University (KHU), South Korea. Her research interests include quantum communication, quantum information science, and quantum security.



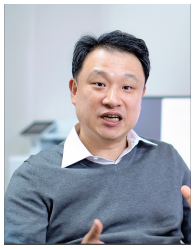
Shehbaz Tariq received the B.S. degree in electrical engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2020. He is currently pursuing the Ph.D. degree with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, Seoul, South Korea. His research interests include quantum machine learning, quantum information science, and artificial intelligence for 6G and beyond.

Saw Nang Paing received the B.E. degree in Computer Engineering and Information Technology from Mandalay Technology University (MTU), Myanmar, in 2019. She is working towards the Ph.D. degree in quantum information science with the Department of Electronics and Information Convergence Engineering, Kyung Hee University (KHU), South Korea. Her research interests include distributed quantum networks, quantum communication, and quantum security.

Jason William Setiawan received the B.S. degree in electrical engineering from Bandung Institute of Technology, Indonesia, in 2020. He is currently pursuing the Ph.D. degree in quantum information science with the Department of Electronics and Information Convergence Engineering, Kyung Hee University (KHU), South Korea. His research interests include quantum information science, quantum communication, and quantum networks.

Sunghwan Kim (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees from Seoul National University, Seoul, South Korea, in 1999, 2001, and 2005, respectively. From 2005 to 2007, he was a Postdoctoral Visitor at the Georgia Institute of Technology, Atlanta, GA, USA. From 2007 to 2011, he worked as a Senior Engineer at Samsung Electronics, Suwon, South Korea. From 2011 to 2024, he was a Professor in the Department of Electrical, Electronic, and Computer Engineering, University of Ulsan, Ulsan, South Korea. He is currently a Professor in the School of Electronic Engineering, Kyonggi University, Suwon, South Korea. His research interests include 5G/6G communications, multiple access, IoT communications, deep learning, transformers, DNA-based storage, and quantum comunications.

Trung Q. Duong (Fellow, IEEE) is a Canada Excellence Research Chair (CERC) and a Full Professor at Memorial University, Canada. He is also an adjunct professor at Queen's University Belfast, UK, a visiting professor at Kyung Hee University, South Korea, and an adjunct professor at Duy Tan University, Vietnam. His current research interests include wireless communications, quantum machine learning, and quantum optimization. He is the Editor-in-Chief of IEEE Communications Surveys & Tutorials and an IEEE ComSoc Distinguished Lecturer. He has received the two prestigious awards from the Royal Academy of Engineering (RAEng): RAEng Research Chair and the RAEng Research Fellow. He is the recipient of the prestigious Newton Prize 2017. He is a Fellow of the Engineering Institute of Canada (EIC), the Canadian Academy of Engineering (CAE), the Institution of Engineering and Technology (IET), and Asia-Pacific Artificial Intelligence Association (AAIA).



Hyundong Shin (Fellow, IEEE) received the B.S. degree in Electronics Engineering from Kyung Hee University (KHU), Yongin-si, Korea, in 1999, and the M.S. and Ph.D. degrees in Electrical Engineering from Seoul National University, Seoul, Korea, in 2001 and 2004, respectively. During his postdoctoral research at the Massachusetts Institute of Technology (MIT) from 2004 to 2006, he was with the Laboratory for Information Decision Systems (LIDS). In 2006, he joined the KHU, where he is currently a Professor in the Department of Electronic Engineering. His research interests include quantum information science, wireless communication, and machine intelligence. Dr. Shin received the IEEE Communications Society's Guglielmo Marconi Prize Paper Award and William R. Bennett Prize Paper Award. He served as the Publicity Co-Chair for the IEEE PIMRC and the Technical Program Co-Chair for the IEEE WCNC and the IEEE GLOBECOM. He was an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS.