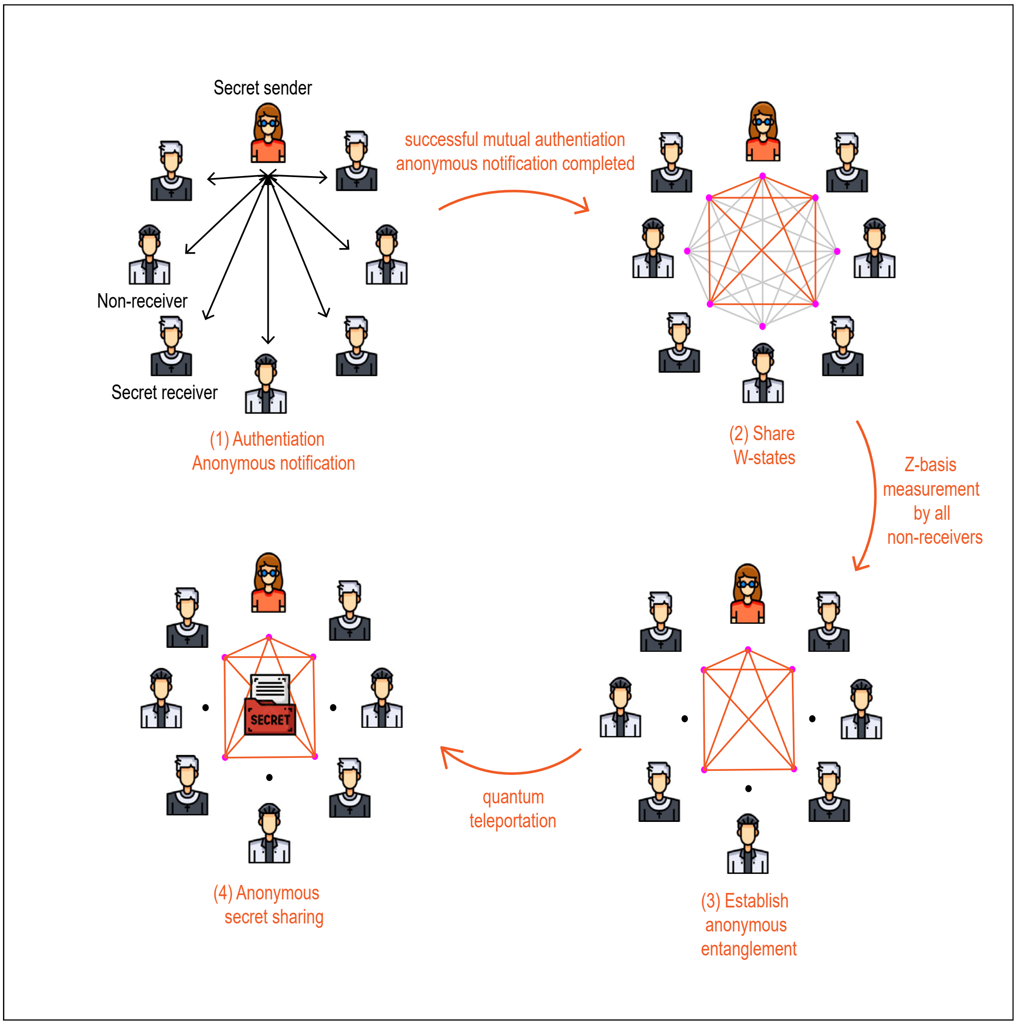
iScience

CellPress
OPEN ACCESS

Article

Enhanced quantum secret sharing protocol for anonymous secure communication utilizing W states



Guo-Dong Li, Wen-Chuan Cheng, Qing-Le Wang, Long Cheng, Ying Mao, Heng-Yue Jia

wqle519@gmail.com

Highlights

A quantum protocol for anonymous sharing of classical and quantum information is proposed

A secret sharing protocol constructing W state anonymous entanglement is proposed

A quantum protocol for anonymous notification to secret receivers is designed

A noise-resistant quantum secret sharing scheme is introduced

Li et al., iScience *27*, 109836
June 21, 2024 © 2024 The Author(s). Published by Elsevier Inc.
https://doi.org/10.1016/j.isci.2024.109836

iScience

CellPress
OPEN ACCESS

Article

Enhanced quantum secret sharing protocol for anonymous secure communication utilizing W states

Guo-Dong Li,[1] Wen-Chuan Cheng,[1] Qing-Le Wang,[1,2,6,*] Long Cheng,[1] Ying Mao,[3] and Heng-Yue Jia[4,5]

SUMMARY

Quantum secret sharing (QSS) represents the fusion of quantum mechanics principles with secret information sharing, allowing a sender to distribute a secret among receivers for collective recovery. This paper introduces the concept of quantum anonymous secret sharing (QASS) to enhance the practicality of such protocols. We propose a QASS protocol leveraging W states, ensuring both recover-security and anonymity of shared secrets. Our protocol undergoes rigorous evaluation verifying their accuracy and fortifying their security against scenarios involving the active adversary. Additionally, acknowledging the imperfections inherent in real-world communication channels, we conduct a comprehensive analysis of protocol security and efficacy in noisy quantum networks. Our investigations reveal that W states exhibit good performance in mitigating noise interference, making them apt for practical applications.

INTRODUCTION

Anonymity is an important cryptographic property. With an increasing emphasis on personal privacy by communication users, the anonymity of user identities, and the confidentiality of information[1–4] should hold equal importance. There are various classical cryptographic applications emphasizing anonymity, such as anonymous voting,[5,6] anonymous key distribution,[7,8] and anonymous private information retrieval,[9,10] have been developed. The anonymous secret sharing (ASS)[11] technique, which we discuss, is also applicable across many cryptographic domains, such as secure key management, multiparty secure conferences, and more. However, while classical ASS schemes have substantial practical value, they rely on the computational complexity of classical encryption, making them potentially vulnerable to adversaries with strong computational capabilities, especially the upcoming quantum computers and fast quantum algorithms.[12,13] Fortunately, QASS addresses this issue while ensuring information-theoretic security.

In 2023, Li et al. proposed the first authenticated ASS protocol based on *d*-dimensional quantum systems, aiming to address the anonymity issue of receiver identities in the secret sharing process.[14] In this protocol, secret senders authenticate participants using Greenberger-Horne-Zeilinger (GHZ) states and construct anonymous entanglement among a specified set of anonymous receivers, ultimately sharing classical information. The constructed anonymous entanglement provides dual protection for secret sharing tasks, ensuring both message confidentiality and receiver identity anonymity.

Anonymous entanglement is the core of QASS, achieved by performing local operations at nodes in the network to create entanglement links between senders and anonymous receivers. It also plays a crucial role in protecting user identity anonymity in quantum cryptography, with many protocols proposed for various tasks such as anonymous ranking,[15–17] voting,[18–20] and communication.[21–23] Among these, GHZ states are the most commonly used anonymous entanglement resource. However, in noisy scenarios, the fidelity of the anonymous entanglement GHZ state may be poor, requiring high channel demands. Victoria Lipinska's research suggests that using W states to construct anonymous entanglement has advantages in terms of operational simplicity, performance in noisy channels, and more.[24] Besides, anonymous entanglement constructed using W states can tolerate an unresponsive node. For example, if one of the qubits of a multipartite state gets lost.

In this paper, leveraging the advantages of W states in constructing anonymous entanglement, we design a QASS protocol based on W states capable of accomplishing tasks involving the sharing of classical or quantum information. We elaborate on the process of anonymously sharing secret information and present corresponding sub-protocols. These sub-protocols include quantum identity authentication, quantum notification, anonymous entanglement, ASS, and anonymous secret recovery protocols. Our research demonstrates that W states can be applied to the ASS process. Additionally, we thoroughly prove the security of the protocol in an active adversary scenario, covering message

[1] School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China
[2] Key Lab of Information Network Security, Ministry of Public Security, Shanghai 200031, China
[3] Department of Computer and Information Science, Fordham University, New York City, NY 10458, USA
[4] School of Information, Central University of Finance and Economics, Beijing 102206, China
[5] Engineering Research Center of State Financial Security, Ministry of Education, Central University of Finance and Economics, Beijing 102206, China
[6] Lead contact
*Correspondence: wqle519@gmail.com

https://doi.org/10.1016/j.isci.2024.109836

confidentiality, identity information privacy, and participant identity anonymity. We emphasize that the security of our protocol remains unchanged when all particles experience the same type of noise interference. Importantly, we consider the feasibility of ASS in noisy quantum networks, quantifying the performance of our protocol through the fidelity of transmitted quantum states.

RESULTS

Definitions

Our (n, n) quantum secret sharing (QSS) scheme necessitates the collaborative effort of all receivers for secret reconstruction. This scheme is specifically designed for high-security requirements, incorporating anonymous entanglement to ensure robust protection, especially in applications where recipient anonymity is crucial.

Before presenting a comprehensive definition, it is essential to introduce the concept of an access structure. In a secret sharing protocol, participants can be categorized into three roles: the secret sender, potential receivers, and secret restorer. The qualified subset refers to the group of receivers capable of effectively recovering the secret. Let $[\mathcal{B}] = Bob_1, Bob_2, \ldots, Bob_n$ represents the set of potential receivers. A monotone access structure, denoted as $\Gamma \subseteq 2^{\mathcal{B}}$, encompasses all qualified subsets within $[\mathcal{B}]$.[11,25] Our (n, n) QASS scheme can be defined in conjunction with its properties based on the access structure as follows.

Definition 1: (n, n) quantum anonymous secret sharing

In a (n, n) QASS, $[\mathcal{B}]$ is the set of potential receivers, the secret sender chooses m of them to be receivers. Let $[\mathcal{R}] = \{Bobr_1, Bobr_2, \cdots, Bobr_m\} \subseteq [\mathcal{B}]$ be the set of anonymous receivers, access structure $\Gamma = \{\mathcal{R}\}$. Then we can say a perfect (n, n) QASS scheme is a collection of distribution rules that satisfy the following three properties:

- Recover-ability: For a random participant subset $[\mathcal{B}'] \subseteq [\mathcal{B}]$, $[\mathcal{B}'] \in \Gamma$, if all of the participants in $[\mathcal{B}']$ pool their shares, they can determine the value of the secret K.
- Recover-security: For a random participant subset $[\mathcal{B}'] \subseteq [\mathcal{B}]$, $[\mathcal{B}'] \notin \Gamma$, then the participants in $[\mathcal{B}']$ can determine nothing about the value of the secret K (in an information-theoretic sense), even with infinite computational resources.
- Receiver-anonymity: The secret sharing and secret recovering processes can guarantee the receiver-anonymous.

In Definition 1, we explore the concept of receiver anonymity, a fundamental component in the realm of anonymous communications. Consider an entity, denoted as $Bobr_i$ $(i \in [1, m])$, symbolizing an unidentified anonymous receiver within the network. This network includes an adversary aiming to unveil the identity of $Bobr_i$ among a myriad of potential receivers. The adversary controls a subset of these potential receivers, designated as dishonest, denoted by $[\mathcal{D}] \subseteq [\mathcal{B}]$. Concurrently, $[\mathcal{H}] \subseteq [\mathcal{B}]$ represents the cohort of honest potential receivers.

The protocol is deemed receiver-anonymous if the adversary's probability of correctly identifying $Bobr_i$ does not exceed the initial uncertainty regarding $Bobr_i$'s identity before the protocol's initiation. This initial uncertainty is quantified by the prior probability, expressed as $P[Bobr_i = Bob_j | Bobr_i \notin \mathcal{D}]$. To elucidate, receiver anonymity can be formally defined as follows.

Definition 2: Receiver-anonymity

Given that the sender *Alice* is honest, we say that an ASS protocol is receiver-anonymous if, the probability of the adversary guessing that $Bobr_i$ to be Bob_j is,

$$P_{guess}\left[Bobr_i \middle| \mathcal{W}^{\mathcal{D}}, \mathcal{C}, Bobr_i \notin \mathcal{D}\right] \leqslant \max_{Bob_j \in [\mathcal{H}]} P\left[Bobr_i = Bob_j \middle| Bobr_i \notin \mathcal{D}\right]. \tag{Equation 1}$$

Here, $\mathcal{W}^{\mathcal{D}}$ denotes the adversary's quantum states distributed by *Alice*, $\mathcal{C}$ denotes all classical and quantum side information accessible to the adversary. In words, the protocol is receiver-anonymous if the probability that the adversary guesses the identity of any anonymous receiver $Bobr_i$ at the end of the protocol is not larger than the probability that an honest Bob_j is a receiver, maximized over all the honest potential receivers.

Definition 2 articulates anonymity within the context of either a perfect channel model or a noise model where each qubit is uniformly affected by an identical noisy channel. However, this definition requires modification when addressing receiver anonymity under conditions of variable network noise. In practical quantum networks, it is plausible that qubits traversing a noisy channel experience non-uniform noise effects. This study aims to examine scenarios wherein each qubit is subject to marginally distinct noise, a concept we term as ε-receiver security.

Definition 3: ε-receiver anonymity

Given that the sender *Alice* is honest, an ASS protocol is ε-receiver-anonymous if, the probability of the adversary guessing that $Bobr_i$ to be Bob_j is,

$$P_{guess}\left[Bobr_i \middle| \mathcal{W}^{\mathcal{D}}, \mathcal{C}, Bobr_i \notin \mathcal{D}\right] \leqslant \max_{Bob_j \in \mathcal{H}} P\left[Bobr_i = Bob_j \middle| Bobr_i \notin \mathcal{D}\right] + \varepsilon.$$

Table 1. The use of PIN_i^{aj} in this protocol

PIN_i^{aj}	00	01	10	11
Alice's generation	$\|0\rangle$	$\|1\rangle$	$\| + \rangle$	$\| - \rangle$
Bob_j's measurement basis	$\mathcal{Z}$	$\mathcal{Z}$	$\mathcal{X}$	$\mathcal{X}$

Here, ε is a parameter used to characterize the channel noise perturbation. This is to say, if the perturbation is small, the guessing probability in a noisy channel with perturbation is ε-close to the guessing probability in a perfect channel or a noisy channel without perturbation, then it can be said that the protocol is ε-receiver-anonymous.

System model

Investigate a quantum network involving three entities: a publicly known secret sender, denoted as *Alice*; an honest secret restorer, referred to as *Charlie*; and n potential receivers, labeled as $Bob_1, Bob_2, \cdots, Bob_n$. The secret sharing phase involves *Alice* transmitting a confidential message to a specific subset of receivers within the network, symbolized as $[\mathcal{R}]$. Each selected receiver acquires a fragment of the secret. It is hypothesized that any subset of the potential receivers, including non-receivers and even some receivers, may exhibit corrupt behavior. This corruption could manifest as individual or collective attempts to illicitly access additional secret information or infer the identities of other honest receivers.

Alice functions as the secret sender whose identity is public. *Charlie*, designated as the secret restorer, is responsible for reconstructing the secret during the recovering phase. This reconstruction is based on the measurement outcomes disclosed by *Alice* and the data shared by other potential receivers. This study excludes the possibility of *Alice* and *Charlie* participating in active sabotage or disclosing the identities of others.

Protocols

Under the model, we present a QASS protocol, comprising various sub-protocols.

Quantum identity authentication protocol

To resist impersonation attacks, *Alice* and each Bob_j ($j \in [1,n]$) use their personal identification number (PIN) to prepare a single photon token for mutual identity authentication. Before authentication, *Alice* generates a one-time PIN^{aj}, sent to Bob_j via QKD[26] or a face-to-face way. At the same time, Bob_j generates PIN^{bj} and sends it to *Alice* in the same way. The form of PIN^{aj} and PIN^{bj} are as follows:

$$PIN^{aj} = \left\{PIN_1^{aj}, PIN_2^{aj}, \cdots, PIN_l^{aj}\right\}; PIN^{bj} = \left\{PIN_1^{bj}, PIN_2^{bj}, \cdots, PIN_l^{bj}\right\}; \qquad \text{(Equation 2)}$$

Here $PIN_i^{aj}, PIN_i^{bj} \in \{00, 01, 10, 11\}$, $i \in [1,l]$, $j \in [1,n]$, $2l$ is the length of PIN^{aj}, PIN^{bj}. The authentication process between them is shown in Protocol 1. The guidelines for photon generation in the protocol are presented in Table 1, and the operational rules are specified in Table 2.

Protocol 1: Quantum identity authentication protocol

Goal: *Alice* and Bob_j perform mutual authentication.

Input: Private $\{PIN_i^{aj}, PIN_i^{bj}\}_{i=1}^{l}$ shared by *Alice* and Bob_j in advance.

Output: Authentication success mark U_j.

(1) *Alice* generates l authentication photons as a token based on PIN^{aj}. She then performs operations according to PIN^{bj}.

(2) *Alice* transmits the token to Bob_j.

(3) Upon receiving the token, Bob_j executes a unitary operation on each photon, following the instructions of PIN^{bj}, and employs the measurement basis indicated by PIN^{aj} for each particle.

(4) If Bob_j's measurement results align with the indication of PIN^{aj}, he confirms *Alice* is trustworthy. Otherwise, he issues an alert regarding the illegitimacy of *Alice*'s identity.

(5) If the results conveyed by Bob_j are same to the token prepared by *Alice*, she acknowledges Bob_j's legal identities and sets $U_j = 1$. Otherwise, *Alice* alerts about the illegitimacy of Bob_j's identity and sets $U_j = 0$.

Note that, $\mathcal{Z}$-basis and $\mathcal{X}$-basis are rectilinear basis and diagonal basis commonly used in quantum communication. $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Table 2. The use of PIN_i^{bj} in this protocol

PIN_i^{bj}	00	01	10	11
Alice's operation	I	X	Y	Z
Bob_j's operation	I	X	Y	Z

Quantum anonymous notification protocol

Quantum anonymous notification protocol is designed to solve the problem that *Alice* secretly informs each anonymous receiver of his identity. *Alice* will take advantage of Protocol 2 and use n notification states to separately inform each Bob_i whether he is a receiver or not. The process is shown in Protocol 2.

Protocol 2: Quantum anonymous notification protocol

Goal: *Alice* separately notifies $Bob_1, Bob_2, \cdots, Bob_n$ whether he is a receiver or not in an anonymous way.

Input: *Alice*'s choice of m receivers.

Alice performs n rounds to notify $Bob_1, Bob_2, \cdots, Bob_n$. For the i-th ($i \in [1, n]$) round:

(1) *Alice* generates a notification W state, whose form is as described in Equation 3. If Bob_i is a receiver, she selects a random but odd number of particles in this W state and performs the X operator in turn. Otherwise, she selects a random but even number of particles in this W state and performs the X operator in turn.

(2) *Alice* separately sends the first particle, the second particle, $\cdots$, and the n-th particle to $Bob_1, Bob_2, \cdots, Bob_n$, and keeps the $(n + 1)$-th particle. Then she measures her qubit in the $\mathcal{Z}$-basis. The measured result is denoted as N_i^{n+1}.

(3) For each participant Bob_j ($j \neq i$), he measures his qubit in the $\mathcal{Z}$-basis, and publishes his measured result, denoted as N_i^j. Bob_i also measures and records, but not publishes.

(4) Bob_i calculates $N_i = \oplus_{j=1}^{n+1} N_i^j$. If $N_i = 0$, then he identifies himself as a secret receiver. If $N_i = 1$, then he identifies himself as a non-receiver.

Note that, the $(n + 1)$-particle W state used in this protocol is as follows:

$$|W^{n+1}\rangle = \frac{1}{\sqrt{n+m}}\left(\sqrt{m}\,|0_1 0_2 \cdots 0_n 1_{n+1}\rangle + |0_1 0_2 \cdots 1_n 0_{n+1}\rangle + \cdots + |1_1 0_2 \cdots 0_n 0_{n+1}\rangle\right). \quad \text{(Equation 3)}$$

For convenience, let $W_{i,j}$ be the j-th particle in the i-th $|W^{n+1}\rangle$.

Quantum anonymous entanglement protocol

In the proposed system, the key to sharing secrets anonymously without being known by the adversary is the establishment of an anonymous entanglement state between the sender and the intended receivers. This approach in Protocol 3 is different from the methods of anonymously generating Bell states or GHZ states as discussed in ref.[27,28] It is a novel scheme for anonymously establishing W states. Here, *Alice* prepares and shares $|W^{n+1}\rangle$ with potential receivers in advance and wants to anonymously construct an entanglement state $|\overline{W}^{m+1}\rangle$ with secret receivers.

Protocol 3: Quantum anonymous entanglement protocol

Goal: $|\overline{W}^{m+1}\rangle$ shared anonymously between *Alice* and m secret receivers.

Input: $|W^{n+1}\rangle_i$ shared between *Alice* and all potential receivers.

Output: Anonymous entanglement success mark E_i.

(1) *Alice* generates $|W^{n+1}\rangle_i$, separately sends $|W^{n+1}\rangle_{i,1}, |W^{n+1}\rangle_{i,2}, \cdots, |W^{n+1}\rangle_{i,n}$ to $Bob_1, Bob_2, \cdots, Bob_n$, and keeps $|W^{n+1}\rangle_{i,n+1}$.

(2) Each non-receiver $Bob_j \notin [\mathcal{R}]$ measures in the $\mathcal{Z}$-basis and publishes his result e_j; receivers do not perform any measurement but publishes $e_j = 0$.

(3) *Alice* calculate $E_i = \Sigma_{j=1}^{n} e_j$. $E_i = 0$ means that *Alice* and receivers successfully construct a W-state anonymous entanglement $|\overline{W}^{m+1}\rangle$.

Note that, the $(m + 1)$-particle anonymous entangled W-states are of the following form:

$$|\overline{W}^{m+1}\rangle = \frac{1}{\sqrt{2m}}\left(\sqrt{m}\,\overbrace{|00\cdots01\rangle}^{m+1} + |00\cdots10\rangle + \cdots + |10\cdots00\rangle\right). \quad \text{(Equation 4)}$$

The state $|\overline{W}^{m+1}\rangle$ is referred to as the 'perfect W state,[29] which is an asymmetric W state. This state is capable of facilitating perfect quantum teleportation and superdense coding. In contrast, symmetric W states are characterized by their ability to enable teleportation only with a certain probability.

Quantum anonymous secret sharing protocol

Based on the corresponding sub-protocols proposed in the previous subsections, the complete protocol for the anonymous sharing of a t-bit secret $K = \{|k\rangle_1, |k\rangle_2, \cdots, |k\rangle_t\}(|k\rangle_i = \alpha|0\rangle + \beta|1\rangle, |\alpha|^2 + |\beta|^2 = 1, i \in [1,t])$ among m anonymous receivers is given in Protocol 4, whose flowchart is shown in Figure 1.

Before the execution of the protocol, the corresponding preparations must be completed. *Alice* initiates the process by generating x $|W^{n+1}\rangle$ $(x > t \cdot \frac{n-m}{2m} + n)$, with n of these states designated as notification states. These notification states are preprocessed according to the guidelines specified in step (1) of Protocol 2. The remaining $(x - n)$ states are utilized for constructing anonymous entanglement, adhering to the distribution guidelines specified in step (2) of Protocol 2 and step (1) of Protocol 3. *Alice* segregates all particles into sequences $Q_1, Q_2, \cdots, Q_n, Q_{n+1}$, where Q_j $(j \in [1, n + 1])$ contains the j-th particles in each W state. After that, she prepares n single photon tokens for mutual authentication ruled by Protocol 1, step (1). Then she randomly inserts the j-th token corresponding to Bob_j into Q_j, resulting in the modified sequence $Q'j$. *Alice* does not need to insert the token into Q_{n+1}, which is kept in her hand. Finally, *Alice* separately sends $Q'_1, Q'_2, \cdots, Q'_n$ to $Bob_1, Bob_2, \cdots, Bob_n$.

When the protocol is executed, the authentication and notification of each Bob_j is done in order. *Alice* can determine a random order and publish it before proceeding to the corresponding step.

Protocol 4: Quantum anonymous secret sharing protocol

Goal: *Alice* shares $K = \{|k\rangle_i\}_{i=1}^{t}$ between m anonymous receivers.

Input: $\{PIN^{aj}, PIN^{bj}\}_{j=1}^{n}$; $\{Q'_j\}_{j=1}^{n}$ and Q_{n+1} distributed in advance; secret $\{|k\rangle_i\}_{i=1}^{t}$.

(1) Identity authentication.

Alice executes identity authentication with $Bob_1, Bob_2, \cdots, Bob_n$ in order. For each Bob_j, she notifies the location of l authentication photons in Q'_j, and executes Protocol 1. If outputs $U_j = 0$, the protocol is terminated. If $U_1 = U_2 = \cdots = U_n = 1$, the legal identity of all potential receivers is authenticated, perform the next step.

(2) Notification.

Alice broadcasts the location of n notification states in $Q'_1, Q'_2, \cdots, Q'_n$, then executes protocol inform each Bob_j whether he is a secret receiver or not in turn.

(3) Anonymous entanglement.

Alice and $Bob_1, Bob_2, \cdots, Bob_n$ try to establish t W state anonymous entanglement for secret sharing. For the i-th round, *Alice* inputs $|W^{n+1}\rangle_i$ and perform Protocol 3. If protocol outputs $E_i = 0$, then a new anonymous entanglement is established. Otherwise, execute the next round until getting t anonymous entanglement.

(4) Secret sharing.

Alice use t $|\overline{W}^{m+1}\rangle$ to share t bits of quantum information. For the i-th round, *Alice* performs a joint Bell state measurement of $|k\rangle_i$ and $|\overline{W}^{m+1}\rangle_{i,n+1}$ in her hand. She announces her measurement result $p_{i,n+1}$ (possible results contain $|\Psi^+\rangle$, $|\Psi^-\rangle$, $|\Phi^+\rangle$, $|\Phi^-\rangle$). All secret receivers measure the $|\overline{W}^{m+1}\rangle_{i,1}, |\overline{W}^{m+1}\rangle_{i,2}, \cdots, |\overline{W}^{m+1}\rangle_{i,n}$ in their hands on $\mathcal{Z}$-basis and keep the measurement results $p_{i1}, p_{i2}, \cdots, p_{im}$. This round is completed, *Alice* turns to share the next bit.

This protocol primarily addresses the methodology for sharing quantum information. The sharing of classical information can be regarded as a specific instance within the broader context of quantum information sharing. For example, sharing $|k\rangle_i$ under the conditions where either $\alpha = 0,\ \beta = 1$ or $\alpha = 1,\ \beta = 0$. Under these parameters, it becomes feasible to share classical binary information 1 or 0.

Quantum anonymous secret recovering protocol

In this protocol, Charlie serves as the pre-appointed secret restorer. In the secret recovering phase, he will recover the secret based on the measurement results published by *Alice* and the information published by other potential receivers. Significantly, the identification of secret receivers remains undisclosed to Charlie during this phase. Here, we propose the secret recovering scheme in Protocol 5, and the flowchart in Figure 2.

Before recovering, *Charlie* generates t W states $|W^{n+1}\rangle_1,\ |W^{n+1}\rangle_2, \cdots, |W^{n+1}\rangle_t$, following the similar preparation and distribution rule in section 3.4, but without preparing notification states. This process produces sequences $O_1, O_2, \cdots, O_n, O_{n+1}$. After that, he prepares authentication single photons token for mutual authentication with other potential receivers and randomly inserts these photons corresponding to Bob_j into O_j, which is converted to O'_j. Denote his personal identity number used in this process as $\{PIN^{cj}\}_{j=1}^{n}$. O_{n+1} does not need to insert the token, *Charlie* keeps this sequence in his hand. Finally, *Charlie* separately sends $O'_1, O'_2, \cdots, O'_n$ to $Bob_1, Bob_2, \cdots, Bob_n$.

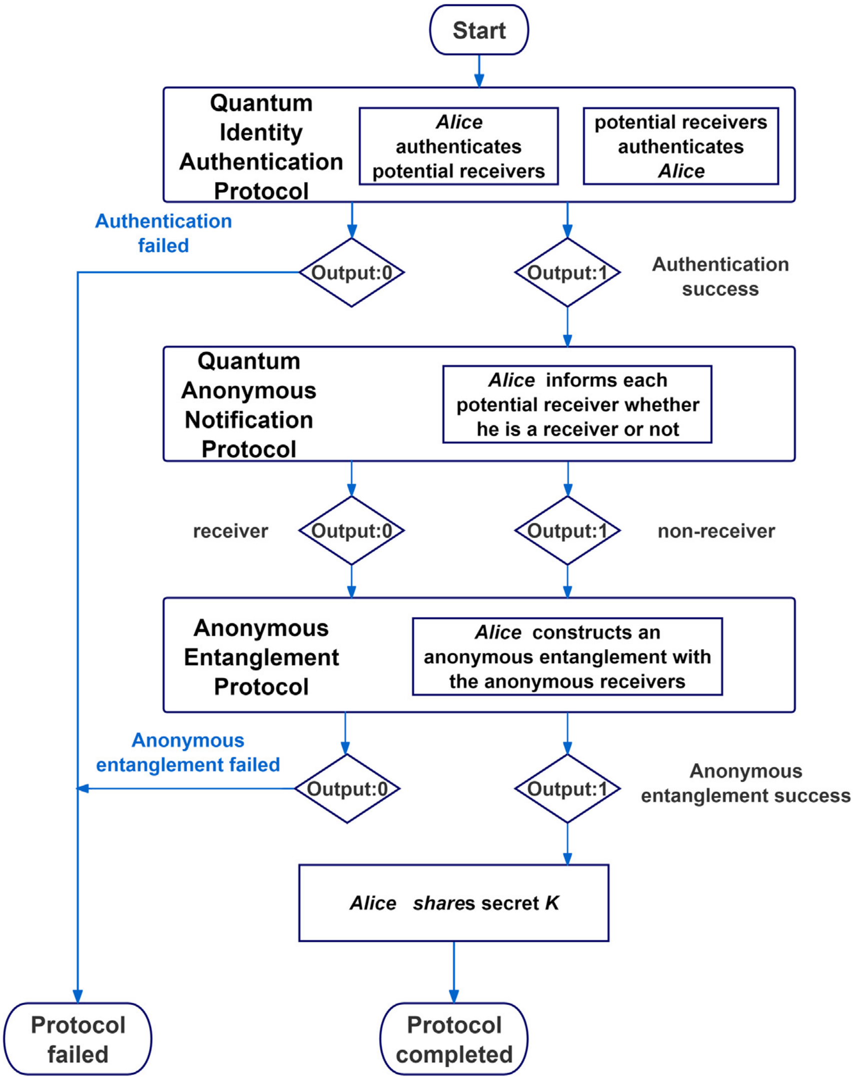

Start
Quantum Identity Authentication Protocol
Alice authenticates potential receivers
potential receivers authenticates Alice
Authentication failed
Output:0
Output:1
Authentication success
Quantum Anonymous Notification Protocol
Alice informs each potential receiver whether he is a receiver or not
receiver
Output:0
Output:1
non-receiver
Anonymous Entanglement Protocol
Alice constructs an anonymous entanglement with the anonymous receivers
Anonymous entanglement failed
Output:0
Output:1
Anonymous entanglement success
Alice shares secret K
Protocol failed
Protocol completed

Figure 1. Flowchart of constructing an anonymous secret sharing protocol

Same to *Alice*, *Charlie* can determine a random order for authentication on his own, and announce it before proceeding to step (1). In addition, the operation rules in the protocol are shown in Table 3.

Protocol 5: quantum anonymous secret recovering protocol

Goal: Bob_n recovers the secret shared by *Alice*.

Input: $\{PIN^{bj}, PIN^{cj}\}_{j=1}^{n}$; $O'_1, O'_2, \cdots, O'_n$ and O_{n+1} distributed in advance.

(1) Identity authentication.

Charlie executes identity authentication with $Bob_1, Bob_2, \cdots, Bob_n$ in order. For each Bob_j ($j \in [1, n]$), he notifies the location of l authentication photons in O'_j, and executes Protocol 1. If the protocol outputs $U_j = 0$, terminate the protocol and consider Bob_j illegal. If $U_1 = U_2 = \cdots = U_n = 1$, the legal identity of all potential receivers is authenticated, perform the next step.

(2) Secret recovering.

Charlie use $t\,|W^{n+1}\rangle$ to recover t bits of quantum information. For the i-th round, secret receivers perform a unitary operation based on the measurement result in Protocol 4, step (4). Take $Bobr_j$ as an example, if $p_{ij} = 0$, he performs an I operation; if $p_{ij} = 1$, he performs an X operation. Then, $Bob_1, Bob_2, \cdots, Bob_n$ measure the particles in their hands on $\mathcal{Z}$-basis and report their results $p'_{i1}, p'_{i2}, \cdots, p'_{in}$ to *Charlie* in order. *Charlie* can perform corresponding unitary operations on his particle according to $p_{i,n+1}$ and $p'_1, p'_2, \cdots, p'_n$ to get $|k\rangle_i$.

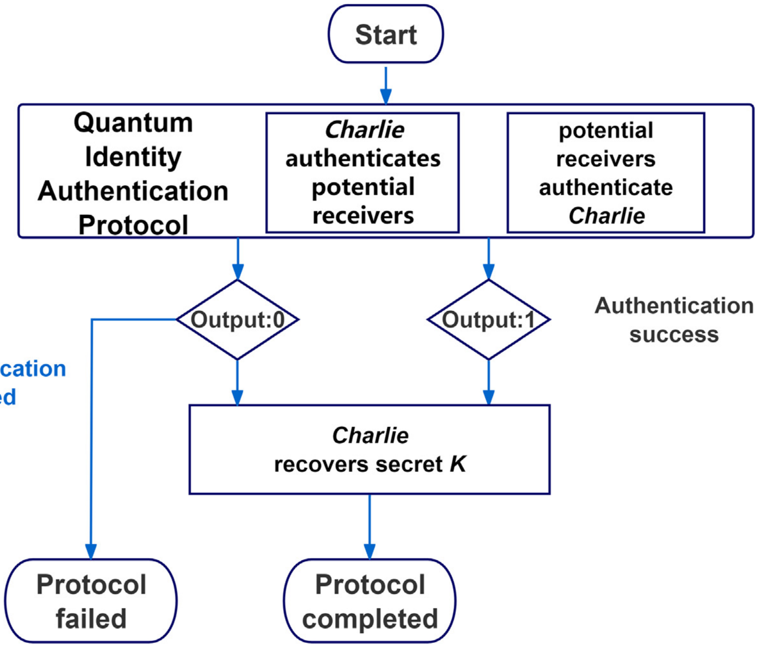

Start
Quantum Identity Authentication Protocol
Charlie authenticates potential receivers
potential receivers authenticate Charlie
Output:0
Output:1
Authentication failed
Authentication success
Charlie recovers secret K
Protocol failed
Protocol completed

Figure 2. Flowchart of constructing an anonymous secret recovering protocol

If $Bob_1, Bob_2, \cdots, Bob_n$ execute the protocol honestly, there are two possible measurement results for $p'_{i1}, p'_{i2}, \cdots, p'_{in}$. One is that $(n - 1)$ potential receivers' measurement results are 0 and one potential receiver's measurement result is 1, we denote it as "measurement result 1", or "MR1" for short. The other is that n potential receivers' measurement results are all 0, we denote it as "measurement result 2", or "MR2" for short.

Analysis

As delineated in Definition 1, the primary aim of QASS is to ensure recover-ability, recover-security, and recover-anonymity. The core of QASS is anonymous entanglement. It is pertinent to note that the construction of anonymous W state entanglement within this framework is probabilistic. Specifically, there is a possibility of construction failure of the W state when $E_i \neq 0$ in Protocol 3. The first subsection will focus on the probability of successful anonymous entanglement, quantified as a function of parameters m and n in the network. This will be followed by an analysis of the protocol's correctness and security.

Entanglement probability

Theorem 1 (Probability of successful anonymous entanglement). In a noise-free channel, assume a sender, denoted as *Alice*, aims to establish anonymous entanglement with m undisclosed receivers utilizing the state $|W^{n+1}\rangle$. Within this system, there are n potential receivers, and all parties involved adhere to honest protocols. Under these conditions, the probability of successfully generating an anonymous entangled state, represented as $|\overline{W^{m+1}}\rangle_i$, is calculated to be $\frac{2m}{n+m}$.

Proof. Let $\left|\vec{0}\rangle\langle\vec{0}\right|_{n-m}$ denote the projection on the $|0\rangle$ state of $(n - m)$ non-receivers. The probability $P_{|\overline{W^{m+1}}\rangle_i}$ of obtaining this state can be expressed as,

$$P_{|\overline{W^{m+1}}\rangle_i} = Tr\left[|W\rangle\langle W|_{n+1} \cdot \left(I_A \otimes I_{m+1} \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_{n-m}\right)\right] = \frac{2m}{n+m}. \qquad \text{(Equation 5)}$$

Theorem 1 states that in the honest implementation, the probability of successful anonymous entanglement in Protocol 3 is based on the proportion of the number of receivers and non-receivers. The success rate is higher when the number of secret receivers is large.

Protocol correctness

Theorem 2 (Correctness of secret sharing). In a noise-free channel, provided that all participants act honestly and Protocol 4 proceeds without termination, the objective of distributing the secret quantum state $|k\rangle_i$ in an anonymous manner is achieved with precision.

Proof. We examine the accuracy of the secret sharing protocol, including an assessment of the individual sub-protocols. During the initial phase, designated as step (1), *Alice* runs Protocol 1 with each potential receiver separately to finish authentication. Specifically, in an authentication sequence involving Bob_i, *Alice* prepares a quantum state denoted as q_i, applies a unitary operation U_i, and transmits the transformed

Table 3. Rules for Charlie to perform unitary operations

$p_{i,n+1}$	$\lvert\Psi^+\rangle$	$\lvert\Psi^+\rangle$	$\lvert\Psi^-\rangle$	$\lvert\Psi^-\rangle$
$p'_{i1},p'_{i2},\cdots,p'_{in}$	MR_1	MR_2	MR_1	MR_2
$\lvert W^{n+1}\rangle_{i,n+1}$	$\alpha\lvert 1\rangle + \beta\lvert 0\rangle$	$\alpha\lvert 0\rangle + \beta\lvert 1\rangle$	$\alpha\lvert 1\rangle - \beta\lvert 0\rangle$	$\alpha\lvert 0\rangle - \beta\lvert 1\rangle$
Charlie's unitary operation	X	I	Y	Z
$p_{i,n+1}$	$\lvert\Phi^+\rangle$	$\lvert\Phi^+\rangle$	$\lvert\Phi^-\rangle$	$\lvert\Phi^-\rangle$
$p'_{i1},p'_{i2},\cdots,p'_{in}$	MR_1	MR_2	MR_1	MR_2
$\lvert W^{n+1}\rangle_{i,n+1}$	$\alpha\lvert 0\rangle + \beta\lvert 1\rangle$	$\alpha\lvert 1\rangle + \beta\lvert 0\rangle$	$\alpha\lvert 0\rangle - \beta\lvert 1\rangle$	$\alpha\lvert 1\rangle - \beta\lvert 0\rangle$
Charlie's unitary operation	I	X	Z	Y

state $q'_i = U_i \cdot q_i$ to Bob_i. Based on the properties of unitary transformation, for any unitary transformation U, it follows $U \cdot U^T = 1$. In other words, for any unitary transformation U, if $U|\varphi\rangle = |\psi\rangle$, then it must hold that $U|\psi\rangle = |\varphi\rangle$. Consequently, if Bob_i possesses a legal identity, he will apply U_i to receive $q''_i = U_i \cdot q'_i = q_i$. This allows both parties to verify the authenticity of each other's identity.

In step (2), the potential receivers are notified one after another anonymously according to Protocol 2. The notification state shared by them is obtained by applying several X operators on $|W^{n+1}\rangle$. If *Alice* selects Bob_i as one of her unique receivers, the number of X operators is random but odd. Bob_i does not publish his measurements, so only he knows his receiver identity by calculating N_i after others publish their measurement results.

The analysis of step (3) and Protocol 3 follows the correctness of the anonymous entanglement protocol presented in ref.[24], which provides a method for constructing anonymous entangled EPR pairs. Differently, we aim to build anonymous W state entanglement instead of EPR pairs between multiple participants. If we partition the $|W^{n+1}\rangle$ state depicted in Equation 3 into two subsystems in the way: $i/\ (1,\cdots,i-1,\ i+1,\cdots,n+1)$, then when $i \neq n+1$ it can be rewritten in the Schmidt decomposition form:

$$|W^{n+1}\rangle = \sqrt{\frac{n+m-1}{n+m}}|\psi^n\rangle|0\rangle_i + \frac{1}{\sqrt{n+m}}|00\cdots0\rangle|1\rangle_i, \tag{Equation 6}$$

where,

$$|\psi^n\rangle = \frac{1}{\sqrt{n+m-1}}\left(\sqrt{m}\,\overbrace{|00\cdots01\rangle}^{n} + |00\cdots10\rangle + \cdots + |10\cdots00\rangle\right). \tag{Equation 7}$$

Thus, after Bob_i's $\mathcal{Z}$-basis measurement on particle i, the total state will collapse into $|\psi^n\rangle$. If we decompose the state in the same way in the case that the measurement results of all non-receivers are all 0, then the total state will collapse into $|\overline{W}^{m+1}\rangle_i$. Then *Alice* can perfectly transmit a quantum state to the receivers.

In step (4), *Alice* conducts a Bell State measurement on the quantum states $|k\rangle_i$ and $|\overline{W}^{m+1}\rangle_{i,n+1}$. Subsequently, she discloses the measurement outcome. Following this, $Bobr_1, Bobr_2, \ldots, Bobr_m$ proceed to measure their own particles using the $\mathcal{Z}$-basis. Upon the completion of these measurements, the process of quantum teleportation is considered finalized. The entangled state resulting from these operations can be reformulated as:

$$|k\rangle_i|\overline{W}^{m+1}\rangle_i \tag{Equation 8}$$

$$= (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|\tilde{W}^m\rangle|0\rangle + |00\cdots0\rangle|1\rangle)$$

$$= \frac{1}{\sqrt{2}}(\alpha|00\rangle|\tilde{W}^m\rangle + \alpha|01\rangle|00\cdots0\rangle + \beta|10\rangle|\tilde{W}^m\rangle + \beta|11\rangle|00\cdots0\rangle)$$

$$= \frac{1}{2}[|\psi^+\rangle(\alpha|\tilde{W}^m\rangle + \beta|00\cdots0\rangle) + |\psi^-\rangle(\alpha|\tilde{W}^m\rangle - \beta|00\cdots0\rangle) + |\varphi^+\rangle(\alpha|00\cdots0\rangle + \beta|\tilde{W}^m\rangle) + |\varphi^-\rangle(\alpha|00\cdots0\rangle - \beta|\tilde{W}^m\rangle)],$$

where,

$$|\tilde{W}^m\rangle = \frac{1}{\sqrt{m}}(|0\cdots01\rangle + |0\cdots10\rangle + \cdots + |10\cdots0\rangle). \tag{Equation 9}$$

which is an m-particle symmetric W state.

After $\mathcal{Z}$-basis measurement, each receiver acquires an equitable portion of the confidential information. This action culminates in the substantiation of Theorem 2. Subsequently, the validation of Protocol 5 is established through the ensuing result.

Theorem 3 (Correctness of secret recovering). If all participants adhere to the protocol with integrity and Protocol 5 proceeds without termination, the secret restorer is capable of achieving anonymous recovery of the quantum information denoted by $|k\rangle_i$.

Proof. Step (1) adheres to the guidelines established in Protocol 1; therefore, the verification of its accuracy is aligned with the relevant section in the proof of Theorem 2. During step (2), Bob_n employs one of the unitary operators (I, X, Y, Z) to transform his particle into the state $|k\rangle_i$. This process is described below, which is divided into four cases, each contingent upon the variance in *Alice*'s measurement result:

(1) *Alice*'s BSM result is $|\psi^+\rangle$.

$$\left|W^{n+1}\right\rangle = \frac{1}{\sqrt{2}}\left(|\tilde{W}^n\rangle|0\rangle + |00\cdots0\rangle|1\rangle\right) \quad \text{(Equation 10)}$$

$$= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|\tilde{W}^{n-1}\rangle|0\rangle + |00\cdots0\rangle|1\rangle\right)|0\rangle + |00\cdots0\rangle|1\rangle\right]$$

$$\left|W^{n+1}\right\rangle \rightarrow \left(\alpha I^{\otimes m-1} \otimes X + \beta I^{\otimes m}\right)\left|W^{n+1}\right\rangle \quad \text{(Equation 11)}$$

$$\left|W^{n+1}\right\rangle = \frac{1}{2}\left[|\tilde{W}^{n-1}\rangle(\alpha|1\rangle + \beta|0\rangle) + \left|00\cdots0\right\rangle(\alpha|0\rangle + \beta|1\rangle)\right]\left|0\right\rangle + \frac{1}{\sqrt{2}}|00\cdots0\rangle(\alpha|1\rangle + \beta|0\rangle)|1\rangle \quad \text{(Equation 12)}$$

$$= \frac{1}{\sqrt{2}}\left[\left|\tilde{W}^n\right\rangle(\alpha|1\rangle + \beta|0\rangle) + |00\cdots0\rangle(\alpha|0\rangle + \beta|1\rangle)\right]$$

(2) *Alice*'s BSM result is $|\psi^-\rangle$.

$$\left|W^{n+1}\right\rangle \rightarrow \left(\alpha I^{\otimes m-1} \otimes X - \beta I^{\otimes m}\right)\left|W^{n+1}\right\rangle \quad \text{(Equation 13)}$$

$$\left|W^{n+1}\right\rangle = \frac{1}{\sqrt{2}}\left[|\tilde{W}^n\rangle(\alpha|1\rangle - \beta|0\rangle) + |00\cdots0\rangle(\alpha|0\rangle - \beta|1\rangle)\right] \quad \text{(Equation 14)}$$

(3) *Alice*'s BSM result is $|\varphi^+\rangle$.

$$\left|W^{n+1}\right\rangle \rightarrow \left(\alpha I^{\otimes m} + \beta I^{\otimes m-1} \otimes X\right)\left|W^{n+1}\right\rangle \quad \text{(Equation 15)}$$

$$\left|W^{n+1}\right\rangle = \frac{1}{\sqrt{2}}\left[|\tilde{W}^n\rangle(\alpha|0\rangle + \beta|1\rangle) + |00\cdots0\rangle(\alpha|1\rangle + \beta|0\rangle)\right] \quad \text{(Equation 16)}$$

(4) *Alice*'s BSM result is $|\varphi^-\rangle$.

$$\left|W^{n+1}\right\rangle \rightarrow \left(\alpha I^{\otimes m} - \beta I^{\otimes m-1} \otimes X\right)\left|W^{n+1}\right\rangle \quad \text{(Equation 17)}$$

$$\left|W^{n+1}\right\rangle = \frac{1}{\sqrt{2}}\left[|\tilde{W}^n\rangle(\alpha|0\rangle - \beta|1\rangle) + |00\cdots0\rangle(\alpha|1\rangle - \beta|0\rangle)\right] \quad \text{(Equation 18)}$$

Here, $|\tilde{W}^n\rangle$ corresponds to the case of MR_1 in Table 3; $|00\cdots0\rangle$ corresponds to the case of MR_2 in Table 3. It follows from Equations 10, 11, 12, 13, 14, 15, 16, and 17 that the particle in *Charlie*'s hand is the same as revealed in Table 3. Thus *Charlie* can obtain $|k\rangle_i$ after performing the corresponding operation according to the rules of Table 3. This completes the proof of Theorem 3.

Authentication security

Within the scope of our security framework, we consider the presence of the active adversary. This entity can execute any quantum operation and may target some participants in the system, as discussed in the referenced literature.[30]

Regarding the identity authentication protocol, utilizing a one-time *PIN*-based token renders any attempt by an adversary to intercept this token futile. The robustness of the single-photon Quantum Identity Authentication (QIA) protocol has been rigorously analyzed and its resilience against various attack methodologies has been affirmed.[31] Consequently, our analysis primarily focuses on the scenario where an active adversary attempts to impersonate a designated receiver, Bob_j, or the sender, *Alice*.

We denote $\mathcal{D}$ as the subset comprising dishonest potential receivers. In cases of impersonating *Alice*, let $\mathcal{W}^1$ represent the adversaries' source of quantum single photons, generated independently of the legitimate PIN^{aj} and PIN^{bj}. Since each participant does not share their PIN with others, the adversary can only randomly prepare the authentication states. He may randomly pick particles to try to evade authentication, but the probability of him making a correct pick is less than 1/2. Then the probability of the adversary successfully passing the authentication process is quantified as

$$P_{pass1}\left[\mathcal{C},\mathcal{W}^1\right] = \frac{1}{2^l}. \qquad \text{(Equation 19)}$$

Here, l denotes the length of the authentication sequence. When impersonating Bob_i, let $\mathcal{W}^2$ denote the adversaries' quantum register of the state distributed by *Alice*; $\mathcal{U}^2$ denote the random unitary operation since adversaries operate without the true PIN^b. Similarly, the adversary can only randomly choose the $\mathcal{Z}$-basis or the $\mathcal{X}$-basis to measure with probability 1/2. Then, the probability of him passing authentication is given by,

$$P_{pass2}\left[\mathcal{C},\mathcal{W}^2,\mathcal{U}^2\right] = \frac{1}{2^l}. \qquad \text{(Equation 20)}$$

Thus, for l large enough, it can be considered that $P_{pass1} = P_{pass2} \approx 0$. Therefore, it can be considered that the adversary cannot pass the identity authentication, and the authentication part can ensure its security.

Receiver anonymity

It should be noted that the honesty of potential receivers does not preclude the possibility of the malicious adversary obstructing the shared secret between *Alice* and secret receivers. Consequently, the reliability of both Protocol 4 and Protocol 5 is vulnerable to such malicious interventions. This issue could be addressed through the implementation of quantum message authentication techniques. A pertinent question arises: does this approach compromise the anonymity of the secret receivers? In the subsequent analysis, it is demonstrated that our protocols maintain receiver anonymity. Even in scenarios where the adversary controls some dishonest potential receivers, the anonymity of the receivers remains intact.

Theorem 4 (Receiver anonymity in the active adversary scenario). Consider the noise-free perfect channel, our quantum anonymous secure sharing protocol with W states, is receiver-anonymous in the active adversary scenario.

Proof. In section 2, we introduce the security definition of the guessing probability in Equation 1. In our protocol, for the ideal case, $P[br_i = b_j | br_i \notin \mathcal{D}]$ should be $\frac{m_{\mathcal{H}}}{n-|\mathcal{D}|}$. Here $m_{\mathcal{H}}$ represents the number of honest receivers. Besides, the *guessing probability*,[24] in our QASS protocol is (in the following section, br_i is short for $Bobr_i$, represent a anonymous receiver, b_j is short for Bob_j)

$$P_{guess}\left[br_i \middle| \mathcal{W}^{\mathcal{D}},\mathcal{C}, br_i \notin \mathcal{D}\right] = \max_{M^j} \sum_{b_j \in \mathcal{H}} P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right] Tr\left[M^j \cdot \rho_{\mathcal{W}^{\mathcal{D}},\mathcal{C}|br_i = b_j}\right], \qquad \text{(Equation 21)}$$

where the guessing probability is the maximum taken over the set of positive operator-valued measures M^j for the adversaries, and $\rho_{\mathcal{W}^{\mathcal{D}},\mathcal{C}|br_i = b_j}$ is the reduced quantum state of dishonest participants at the end of the protocol given that Bob_j is the receiver $Bobr_i$. The premise of achieving receiver security is that the adversary cannot distinguish the honest non-receiver from the receiver.

We prove anonymity for all involved sub-protocols separately. The outcome of Protocol 2 confidentially informs each potential receiver of their status as a receiver or not, without divulging additional information. The adversary's reduced quantum state upon completion of this protocol remains uncorrelated with the identity of the receiver. Specifically, for any Bob_i not included in the subset $\mathcal{D}$ of adversaries, the condition $\rho_{\mathcal{W}^{\mathcal{D}},\mathcal{C},br_i} = \rho\mathcal{W}^{\mathcal{D}},\mathcal{C}$ holds true. In practical terms, this implies that in scenarios where the adversary controls all entities except for $Bobr_i$ and acquires the measurement outcomes of the notification state, the probability of correctly guessing the identity of $Bobr_i$, denoted as $P_{guess}[Bobr_i]$, remains at 1/2. This satisfies Equation 1, that the receiver identity about $Bobr_i$ remains inaccessible to the adversary.

An active adversary might target all quantum sequences to ascertain whether $Bobr_i$ is the intended receiver. While Protocol 2 does not solely thwart such an attack, in Protocol 4, *Alice* reveals the positions of all notification states only after successful authentications. If the adversary indiscriminately compromises all particles, this mode of attack will be detected during the authentication phase, a scenario substantiated in our analysis of Protocol 1. Furthermore, selectively attacking a specific notification particle is not feasible. To elucidate this, we introduce P_{attack}:

$$P_{attack} = \frac{n}{x+l}. \qquad \text{(Equation 22)}$$

Thus, for x and l large enough, it can be considered that $P_{attack} \approx 0$. In other words, it is impossible for the adversary to only attack the designated notification state particles to obtain the identity information of a receiver by guessing.

If some or all potential receivers except $Bobr_i$ are governed by an active adversary, the worst case would be that the parity of broadcast results changes from even to odd or vice versa, which prevents the receiver from being notified or makes the sender aware of the presence of an adversary. Nevertheless, it reveals no information on the identities of $Bobr_i$. In summary, we have progressively analyzed the possibilities of various types of adversaries and proved the proposed quantum protocol is perfectly receiver-secure.

In steps (3) or (4), each participant performs local operations and measurements in sequence. The key to the protocol to ensure anonymity is to establish secure anonymous entanglement. To achieve this, a feasible prerequisite is to guarantee that the measurement results published by non-receivers are random and indistinguishable. Therefore, in our protocol, this is equivalent to,

$$P_{measure}\left[b_i \middle| \mathcal{W}^{\mathcal{D}}, \mathcal{C}, b_i \notin \mathcal{D}\right] = P_{measure}\left[b_j \middle| \mathcal{W}^{\mathcal{D}}, \mathcal{C}, b_j \notin \mathcal{D}\right], \tag{Equation 23}$$

where $P_{measure}$ represents the probability of a possible measurement result, $i \neq j$. According to the conditions for the successful anonymous entanglement, we consider its probability of 0.

Considering the presence of active adversaries, the shared W state in the protocol should be,

$$\left|\omega_{n+1}\right\rangle = \frac{1}{\sqrt{n+m}}\left(\sqrt{m}\,|00\cdots01\rangle_{\mathcal{AH}} \otimes |\varphi_0\rangle_{\mathcal{D}} + |00\cdots10\rangle_{\mathcal{AH}} \otimes |\varphi_1\rangle_{\mathcal{D}} + \cdots + |10\cdots00\rangle_{\mathcal{AH}} \otimes |\varphi_n\rangle_{\mathcal{D}}\right). \tag{Equation 24}$$

Denote $\sqrt{m}|00\cdots01\rangle_{\mathcal{AH}}$ as $|\psi_0\rangle$, $|00\cdots10\rangle_{\mathcal{AH}}$ as $|\psi_1\rangle$, $\cdots$, $\sqrt{m}|10\cdots00\rangle_{\mathcal{AH}}$ as $|\psi_n\rangle$, then,

$$\left|\omega_{n+1}\right\rangle = \frac{1}{\sqrt{n+m}}\sum_{x=0}^{n}\left(|\psi_x\rangle \otimes |\varphi_x\rangle\right). \tag{Equation 25}$$

By tracing out $P_{measure}[b_i]$, after measurement,

$$\begin{aligned} P_{measure}[b_i] &= Tr_{n-m}\left[\left(|\omega_{n+1}\rangle\langle\omega_{n+1}|\right) \cdot \left(I_n \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_i\right)\right] \\ &= \frac{1}{n+m}\sum_{y=0}^{n}\sum_{z=0}^{n} Tr\left[|\psi_y\rangle\langle\psi_z|\right] Tr\left[|\varphi_y\rangle\langle\varphi_z|\right] \cdot \left(I_n \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_i\right)\Bigg]. \end{aligned} \tag{Equation 26}$$

Since the I operation does not change the trace, we can rewrite and simplify Equation 26 as,

$$\begin{aligned} P_{measure}[b_i] &= \frac{1}{n+m}\left[\left(m\left\langle\vec{0}_i\middle|\varphi_0\right\rangle\right) + \sum_{x=1}^{j-1}\left(\left\langle\vec{0}_i\middle|\varphi_x\right\rangle\right) + \sum_{x=j+1}^{n}\left(\left\langle\vec{0}_i\middle|\varphi_x\right\rangle\right)\right] \\ &= \frac{n+m-1}{n+m}. \end{aligned} \tag{Equation 27}$$

Therefore, $P_{measure}[b_i]$ is independent of the identity of Bob_i, or $P_{measure}[b_i] = P_{measure}[b_j]$, Equation 23 holds. Then we can calculate

$$P_{guess}\left[br_i \middle| \mathcal{W}^{\mathcal{D}}, \mathcal{C}, br_i \notin \mathcal{D}\right] \tag{Equation 28}$$

$$\begin{aligned} &= \max_{M^j}\sum_{b_j \in \mathcal{H}} P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right] Tr\left[M^j \cdot \rho_{\mathcal{W}^{\mathcal{D}},\mathcal{C}|br_i = b_j}\right] \\ &\nleqq \max_j P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right] Tr\left[\sum_{b_j \in \mathcal{H}} M^j \cdot \rho_{\mathcal{W}^{\mathcal{D}},\mathcal{C}}\right] \\ &= \max_j P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right]. \end{aligned} \tag{Equation 29}$$

It can be seen that the guessing probability P_{guess} satisfies our anonymity requirement in Definition 2. However, due to the attacks from malicious potential receivers, their broadcast results would be changed, which causes Protocol 4 to abort or pass. Even so, no adversary obtains any information about the identity of the receivers, since all honest potential receivers exhibit the same. Thus, the anonymity of the receivers is guaranteed regardless of how many potential receivers are controlled by the active adversary. But we remark that the malicious parties can prevent *Alice* and receivers from sending and sharing the desired secret. For example, the dishonest parties can measure the W state on a different basis affecting the resulting anonymous entanglement. In this sense, Protocol 4 is not robust to malicious attacks. The reliability of this part can be ensured by quantum message authentication. Thus, even in the presence of dishonest parties, the anonymity of receivers is preserved. So Theorem 4 is proven.

The anonymity of Protocol 5 is similar to that of Protocol 4. The known recovering W state is distributed to all participants, and the secret receiver behaves the same as the non-secret receiver except for the local measurement and unitary operation, and only transmits the measurement results through a secure classical channel with the secret restorer. Thus, the completion of Protocol 5 does not break the recipient's anonymity either.

Secret security

Theorem 5 (Secret security in the active adversary scenario). Consider the noise-free perfect channel, our quantum anonymous secure sharing protocol with W states, can protect secret security in the active adversary scenario.

Proof. In Protocol 4, the security of the secret sharing part can be guaranteed by the authentication mentioned above. The authentication of the potential receivers' identity ensures that the illegal external adversary cannot obtain the secret information. Therefore, in this subsection, we will focus on the case where the adversary controls the dishonest potential receivers.

Considering that *Alice* uses quantum teleportation based on perfect W state to share the quantum information $|k\rangle_i$, which is information-theoretic secure.[29] So it is not practical to launch the attack in this step. A feasible way is in step (3), to try to join the anonymous entanglement $|\overline{W}^{m+1}\rangle_i$. There are two possibilities. The first is to make a measurement and publish the wrong result. That is, publish 0 when the measurement is 1. Only one dishonest potential receiver can publish a false measurement result to complete step (3). Otherwise, there will be a measurement result that violates the property of W state and will be found. Suppose the dishonest potential receiver is Bob_j. Follow Equation 6, in this case, the actual shared anonymous entangled state is given by

$$|\varphi^{m+2}\rangle_i = |00\cdots0\rangle|1\rangle. \qquad \text{(Equation 30)}$$

Equation 30 shows that the final shared $|\varphi^{m+2}\rangle_i$ is a direct product state instead of an entangled state. Consequently, teleportation is not achievable, leading to the failure of ASS. Thus, the adversary naturally cannot recover the shared secret information of *Alice*.

The second possibility is not to measure but to complete steps (3) and (4) in the same way as a secret receiver. In this case, the actual shared anonymous entangled state is given by

$$|W^{m+1+d}\rangle_i = \frac{1}{\sqrt{2m+d}}\left(\sqrt{m}|00\cdots01\rangle + |00\cdots10\rangle + \cdots + |10\cdots00\rangle\right), \qquad \text{(Equation 31)}$$

where d denotes the number of dishonest non-receivers. This state is not a perfect W state, and the teleportation is a probabilistic success, which is detailed in.[32] The combined state can be rewritten as,

$$|k\rangle_i|W^{m+1+d}\rangle_i \qquad \text{(Equation 32)}$$

$$= (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2m+d}}\left(\sqrt{m}\left|\tilde{W}^{m+d}\right\rangle\left|0\right\rangle + \sqrt{m+d}|00\cdots0\rangle|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(\alpha\sqrt{m}|00\rangle\left|\tilde{W}^{m+d}\right\rangle + \alpha\sqrt{m+d}|01\rangle\left|00\cdots0\right\rangle + \beta\sqrt{m}|10\rangle\left|\tilde{W}^{m+d}\right\rangle + \beta\sqrt{m+d}|11\rangle|00\cdots0\rangle\right)$$

$$= \frac{1}{2}\left[\left|\psi^{+}\right\rangle\left(\alpha\sqrt{m}\left|\tilde{W}^{m+d}\right\rangle + \beta\sqrt{m+d}\left|00\cdots0\right\rangle\right) + \left|\psi^{-}\right\rangle\left(\alpha\sqrt{m}\left|\tilde{W}^{m+d}\right\rangle - \beta\sqrt{m+d}\left|00\cdots0\right\rangle\right)\right.$$

$$\left. + \left|\varphi^{+}\right\rangle\left(\alpha\sqrt{m+d}|00\cdots0\rangle + \beta\sqrt{m}\left|\tilde{W}^{m+d}\right\rangle\right) + \left|\varphi^{-}\right\rangle\left(\alpha\sqrt{m+d}|00\cdots0\rangle - \beta\sqrt{m}\left|\tilde{W}^{m+d}\right\rangle\right)\right].$$

This results in the secret restorer getting a wrong state in Protocol 5, that is, failing to recover $|k\rangle_i$. We take one of these cases as an example, where *Alice*'s BSM result is $|\psi^{+}\rangle$. Assuming that subsequent steps execute normally, the secret restorer has already distributed $|W^{n+1}\rangle$ and attempted to recover $|k\rangle_i$.

$$\left|W^{n+1}\right\rangle = \frac{1}{\sqrt{2}}\left(|\tilde{W}^{n}\rangle|0\rangle + |00\cdots0\rangle|1\rangle\right) \qquad \text{(Equation 33)}$$

$$= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|\tilde{W}^{n-1}\rangle|0\rangle + |00\cdots0\rangle|1\rangle\right)|0\rangle + |00\cdots0\rangle|1\rangle\right]$$

$$\left|W^{n+1}\right\rangle \to \left(\alpha\sqrt{m}\,I^{\otimes m-1}\otimes X + \beta\sqrt{m+d}\,I^{\otimes m}\right)\left|W^{n+1}\right\rangle \qquad \text{(Equation 34)}$$

$$\left|W^{n+1}\right\rangle = \frac{1}{2}\left[\left|\tilde{W}^{n-1}\right\rangle\left(\alpha\sqrt{m}\left|1\right\rangle + \beta\sqrt{m+d}\left|0\right\rangle\right) + \left|00\cdots0\right\rangle\left(\alpha\sqrt{m}\left|0\right\rangle + \beta\sqrt{m+d}\left|1\right\rangle\right)\right]\left|0\right\rangle$$

$$+\frac{1}{\sqrt{2}}\left|00\cdots0\right\rangle\left(\alpha\sqrt{m}\left|1\right\rangle + \beta\sqrt{m+d}\left|0\right\rangle\right)\left|1\right\rangle \quad \text{(Equation 35)}$$

$$=\frac{1}{\sqrt{2}}\left[\left|\tilde{W}^{n}\right\rangle\left(\alpha\sqrt{m}\left|1\right\rangle + \beta\sqrt{m+d}\left|0\right\rangle\right) + \left|00\cdots0\right\rangle\left(\alpha\sqrt{m}\left|0\right\rangle + \beta\sqrt{m+d}\left|1\right\rangle\right)\right]$$

Therefore, when the measurements of other potential receivers are MR1, the particles held in *Charlie*'s hand is $\alpha\sqrt{m}\left|1\right\rangle + \beta\sqrt{m+d}\left|0\right\rangle$, instead of $\alpha|1\rangle + \beta|0\rangle$. *Charlie* does not know this, so after he follows the rule and performs the unitary operation, the resulting particle is $\alpha\sqrt{m}\left|0\right\rangle + \beta\sqrt{m+d}\left|1\right\rangle$. The adversary cannot obtain more information than *Charlie*, and even *Charlie* himself cannot get the correct secret, so the adversary cannot obtain the secret illegally by using this attack method.

In addition, it is also possible that a dishonest secret receiver will try to obtain the secret shares of other receivers. But this is not realistic in our protocol, because the measurement of the anonymous entangled particles is done locally, and there is no possibility of being attacked within the considered category.

In Protocol 5, we assume that at least the secret retriever is honest since he is already able to have all participants' *PIN* and the full secret. In a real scenario, this participant may be a public trusted control center that assists anonymous receivers in recovering the final secret according to their additional information. Two kinds of channels are used in Protocol 5. One is the secure classical channel, which transmits the measurement results. The second is the quantum channel, which distributes the recovery W states. The security of the quantum channel is also guaranteed by the randomly inserted identity authentication single photon, and the analysis of this part is similar to that in Protocol 4. So the attack on the channel cannot obtain valid information about the secret. In summary, we analyze the possible attack means of the adversary and exclude the possibility of a successful attack, so Theorem 5 is proved.

Secret integrity

In secret sharing, the integrity of information is also a part of its security. It should be mentioned that in our protocol, the secret restorer can correctly recover *Alice*'s shared secret, but the authenticity of the secret cannot be guaranteed. Whether to give him the ability to authenticate messages depends on the requirements of real applications, because the verification process consumes additional resources. The way to do this is through quantum message authentication, which we will describe shortly.

To implement message authentication, *Alice* creates several instances of Bell state $|\Phi^{+}\rangle$. She keeps one qubit of each pair, calls ρ as the kept qubit and γ as the other qubit. In Protocol 4, before step (4) (secret sharing), *Alice* creates a random classical key δ, and computes $\gamma' = \mathbf{authenticate}(\gamma,\delta)$. These particles will be randomly inserted into the t-bit secret sequence and transmitted to the secret receivers in the same way as the secret particle $|k\rangle_i$ is transmitted. In detail, she performs a joint Bell state measurement on γ' and $\left|\overline{W}^{m+1}\right\rangle_{i,n+1}$ in her hand.

After secret recovering in Protocol 5, *Alice* can use an anonymous message transmission protocol to send δ as well as the kept qubit ρ to the restorer *Charlie*, and inform the location of all message authentication particles. *Charlie* completes the secret sharing, restores the particles transmitted by *Alice*, and computes $\gamma = \mathbf{decode}(\gamma',\delta)$. Then he performs a joint Bell state measurement on ρ and γ to confirm it is $|\Phi^{+}\rangle$. If the error rate is higher than expected, *Charlie* considers the shared secret to be wrong. Otherwise, he can accept that he has the correct secret.

Security in the presence of noise

We consider a noise model wherein each qubit is subject to an identical, individual noisy channel. This channel not only pertains to the qubits themselves but also extends to include the noise associated with local measurements conducted on the quantum state.[33] To preserve the anonymity of the receiver during the recovery phase, it becomes imperative to involve a non-secret receiver, to make it impossible for an outside adversary to distinguish which people are the real receivers. However, the potential for this non-secret receiver to be under the influence of an adversarial entity necessitates careful consideration.

In the noise model mentioned above, suppose each qubit is individually affected by a noise map Λ while being transmitted to the nodes. If $|W\rangle\langle W|_{n+1}$ is the $(n + 1)$-particle W state prepared by *Alice*, then after transmitting,

$$\omega_{n+1}^{\Lambda} = \Lambda^{\otimes n+1}\left(|W\rangle\langle W|_{n+1}\right) \quad \text{(Equation 36)}$$

is the actual state distributed to the parties at step (3) of Protocol 4. In what follows we will show that our protocol is perfectly secure in the active adversary scenario in the noisy network defined by the above equation.

According to the definition of the Permutational-invariance preserving map,[24] the noise channel of our interest, $\Lambda^{\otimes n+1}$, preserves permutational invariance due to the tensor structure. Accordingly, we will prove the following Theorem:

Theorem 6. Our QASS protocol is receiver-anonymous in the active adversary situation in the noisy quantum network modeled by ω_{n+1}^{Λ}.

Proof. Following the definition of a permutational-invariance-preserving map, the noise channel introduced in our protocol, preserves permutational invariance due to the tensor structure. So the proof of Theorem 5 follows the same steps as the proof of Theorem 4, the difference is that the state $|W\rangle\langle W|_{n+1}$ is replaced by ω_{n+1}^{Λ}. The guessing probability of a receiver $Bobr_i$ is given by

$$P_{guess}\left[br_i\middle|\mathcal{W}^{\mathcal{D}},\mathcal{C},br_i\notin\mathcal{D}\right] \quad \text{(Equation 37)}$$

$$= \max_{M^j} \sum_{b_j \in \mathcal{H}} P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right] Tr\left[M^j \cdot \rho^{\Lambda}_{\mathcal{W}^{\mathcal{D}},\mathcal{C}|br_i = b_j}\right]$$

$$\nleq \max_{b_j \in \mathcal{H}} P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right].$$

Therefore, P_{guess} satisfies our anonymity requirement in Definition 2, and Theorem 6 is proved.

In a realistic quantum network, it is impossible to ensure that all qubits are subjected to the action of the same noise channel. So we would like to analyze in the sense that each qubit experiences a slightly different noise, following Definition 3. Then the total state of the noisy channels is given by

$$\widehat{\omega}^{\hat{\Lambda}}_{n+1} = \bigotimes_{i=1}^{n+1} \Lambda_i(|W\rangle\langle W|_{n+1}), \qquad \text{(Equation 38)}$$

where $\|\Lambda - \Lambda_i\|_1 \leq \varepsilon_i$, $\|\cdot\|_1$ represents the 1-norm of a matrix, $\varepsilon_i \rightarrow 0$, which is the parameter in ε-receiver anonymity.

Theorem 7. Our QASS protocol is ε-receiver-anonymous in the active dishonest participant situation in the noisy quantum network modeled by $\widehat{\omega}^{\hat{\Lambda}}_{n+1}$.

Proof. Follows the same steps as the proof of Theorem 4 and Theorem 5, we can calculate,

$$P_{guess}\left[br_i \middle| \mathcal{W}^{\mathcal{D}}, \mathcal{C}, br_i \notin \mathcal{D}\right] \qquad \text{(Equation 39)}$$

$$= \max_{M^j} \sum_{b_j \in \mathcal{H}} P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right] Tr\left[M^j \cdot \widehat{\rho}^{\hat{\Lambda}}_{\mathcal{W}^{\mathcal{D}},\mathcal{C}|br_i = b_j}\right]$$

$$\nleq \max_{b_j \in \mathcal{H}} P\left[br_i = b_j \middle| br_i \notin \mathcal{D}\right] + (n+1)\varepsilon_{max},$$

where $\widehat{\rho}^{\hat{\Lambda}}_{\mathcal{W}^{\mathcal{D}},\mathcal{C}|br_i = b_j}$ is the state of the adversaries at the end of the protocol, $\varepsilon_{max} = \max_{i \in [\mathcal{H}+\mathcal{R}_{\mathcal{H}}]} \varepsilon_i$, $(n+1)\varepsilon_{max} \rightarrow \varepsilon$. Therefore, P_{guess} satisfies our ε-anonymity requirement in Definition 3, Theorem 5 is proved.

Performance in a noisy network

In this section, we analyze the performance of Protocol 4 in a noisy quantum network. To complete this task reliably, we assume that all the participants follow the protocol honestly. After step (3), the resultant anonymous entangled state between *Alice* and $[\mathcal{R}]$ is given by

$$\omega_{m+1} = \frac{1}{\mathcal{N}} Tr_{n-m}\left[\Lambda^{\otimes n+1}(|W\rangle\langle W|_{n+1}) \cdot \left(I_{m+1} \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_{n-m}\right)\right], \qquad \text{(Equation 40)}$$

where $|W\rangle\langle W|_{n+1}$ is the $(n+1)$-particle W state shared in advance, $\left|\vec{0}\right\rangle\left\langle\vec{0}\right|_{n-m}$ is a projection onto the $|0\rangle$ state of $(n-m)$ parties and $\mathcal{N}$ is a normalization factor that can be calculated as,

$$\mathcal{N} = Tr_{n+1}\left[\Lambda^{\otimes n+1}(|W\rangle\langle W|_{n+1}) \cdot \left(I_{m+1} \otimes \left|\vec{0}\right\rangle\left\langle\vec{0}\right|_{n-m}\right)\right]. \qquad \text{(Equation 41)}$$

In the noiseless case, *Alice* and $[\mathcal{R}]$ can obtain a perfect W state anonymously. However, the states shared in the noisy channel may deviate from what is expected. Next, we will discuss the performance of the ASS protocol over two types of noisy channels:

1. Λ is the dephasing channel, which is modeled by,

$$\Lambda(\rho) = q\rho + (1-q)Z\rho Z, \qquad \text{(Equation 42)}$$

where ρ is a single qubit state, Z is the Pauli-Z gate, and $q \in [0,1]$ is the noise parameter.

2. Λ is the depolarizing channel, which is modeled by,

$$\Lambda(\rho) = q\rho + (1-q)\frac{I}{2}, \qquad \text{(Equation 43)}$$

where ρ is a single qubit state, $\frac{I}{2}$ is a maximally mixed state in two-dimensional Hilbert space, and $q \in [0,1]$ is the noise parameter.

To confirm the performance of our protocols, we fix the figure of merit to be the fidelity of the obtained anonymous entangled (AE) state with the ideal state that is obtained in the protocol when no noise is present,

$$F_{AE}(\omega_{m+1}) = Tr[\omega_{m+1} \cdot |W\rangle\langle W|_{m+1}] \qquad \text{(Equation 44)}$$

where ω_{m+1} is the anonymous entangled states between *Alice* and $[\mathcal{R}]$ arising from measuring W states subjected to the network noise, and $|W\rangle\langle W|_{m+1}$ is the $(m + 1)$-particle perfect W state.

In what follows we explain what it means for an anonymous entangled state to be useful. According to ref.[34], not all states are entangled enough to be a resource for teleportation. Besides, the quality of a low-fidelity anonymous entanglement could be further improved by performing entanglement distillation.[35] However, entanglement distillation protocols for W states et al. can be carried out only when fidelities of initial states are larger than $\frac{1}{2}$. So we can extend the definition of what it means to say that a resource state is useful for anonymous transmission to multi-particle entangled states. We say that the anonymous entangled state is a useful resource for quantum teleportation if its fidelity is larger than $\frac{1}{2}$, i.e., $F_{AE} > \frac{1}{2}$.

To evaluate the behavior of the protocols, we calculate the fidelity of anonymous entanglement as a function of the noise parameter q, the number of participants n, and the number of secret receivers m, for the depolarizing and dephasing channels. Let $tr_{xy} = Tr[\Lambda(|x\rangle\langle y|)\cdot|0\rangle\langle 0|]$. Then the state ω_{m+1} shared between *Alice* and all receivers in the noisy implementation of our protocol is

$$\omega_{m+1} = \frac{1}{\mathcal{N}}\Big[(n - m)\cdot tr_{00}^{n-m}\cdot(vaa1 + vaa2 + vaa3 + vaa4 + vaa5)$$

$$+ 2m\cdot tr_{00}^{n-m-1}\cdot tr11\cdot tr_{00}^{m-1}\cdot\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|)\Big] \qquad \text{(Equation 45)}$$

$$vaa1 = (m - 1)\cdot(m - 2)\cdot tr_{01}\cdot tr_{10}\cdot tr_{00}^{m-3}\cdot\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) \qquad \text{(Equation 46)}$$

$$vaa2 = m\cdot(m - 1)\cdot tr_{10}\cdot tr_{00}^{m-2}\cdot[\Lambda(|0\rangle\langle 1|)\otimes\Lambda(|0\rangle\langle 0|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 1|)] \qquad \text{(Equation 47)}$$

$$vaa3 = m\cdot(m - 1)\cdot tr_{01}\cdot tr_{00}^{m-2}\cdot[\Lambda(|1\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|1\rangle\langle 0|)] \qquad \text{(Equation 48)}$$

$$vaa4 = (m - 1)\cdot tr_{11}\cdot tr_{00}^{m-2}\cdot\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) \qquad \text{(Equation 49)}$$

$$vaa5 = m\cdot m\cdot tr_{00}^{m-1}\cdot\big[\Lambda(|0\rangle\langle 1|)\otimes\Lambda(|1\rangle\langle 0|)$$

$$+ \Lambda(|1\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 1|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|1\rangle\langle 1|) + \Lambda(|1\rangle\langle 1|)\otimes\Lambda(|0\rangle\langle 0|)\big] \qquad \text{(Equation 50)}$$

Using the explicit form of Λ for the depolarizing and dephasing noise, after calculations, one obtains explicit fidelity expressions derived from Equations 51 and 52.

1. Dephasing channels.

$$F_{AE}(\omega_{m+1}) = 2q^2 - 2q + 1 \qquad \text{(Equation 51)}$$

2. Depolarizing channels.

$$F_{AE}(\omega_{m+1}) = \frac{(q+1)\left\{n(q - 1)^2 - m(n+3)(q - 1)^2 + m^3(6q^2+2) + m^2\left[(q - 1)^2 - 2n(3q^2+1)\right]\right\}}{4\left\{n+m(n+3)(q - 1) - nq+2m^3(q+1) - m^2[q - 1+2n(q+1)]\right\}} \qquad \text{(Equation 52)}$$

We start by looking at the dephasing noise. Observe that in this case the fidelity of anonymous entanglement created with the W state $F_{AE}(\omega_{m+1})$ is irrelevant with n and m. Specifically, this implies that when fixed dephasing noise is present in the network, the quality of the anonymous link only depends on the noise parameter, regardless of the number of participants or secret receivers. This results in great performance when there are a large number of participants in the system. The performance of our protocol for dephasing noise is shown in Figure 3.

When depolarizing noise is present in the network, unlike the dephasing noise, the fidelity of the anonymous entanglement generated by our protocol depends on the numbers m and n. We first analyze the fidelity affected by m when n is constant. It can be seen in Figure 4 that except for the case $n = m$, the fidelity images coincide.

After analyzing more cases of n and m, we can know that the fidelity of anonymous entanglement is relatively stable and greater than $\frac{1}{2}$ when $q > \frac{1}{2}$ independent of m, except for the case of $n = m$, where the protocol does not meet the requirements of usefulness. In fact, the case $n = m$ corresponds to the case where all participants are secret receivers, which is not common in general.

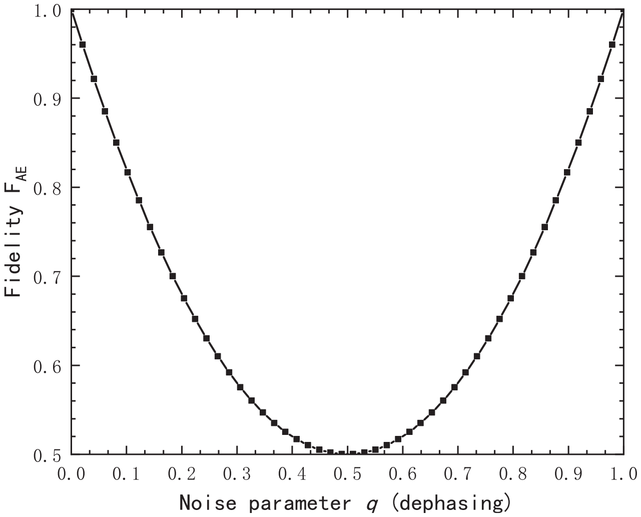


Figure 3. Fidelity of anonymous entanglement as a function of the noise parameter *q* for dephasing noise

Then we analyze the fidelity affected by *n* when *m* is constant. It can be seen in Figure 4 that the function images coincide even though *n* is increasing. Thus, we can draw a similar conclusion as for dephasing noise, that is, the protocol can still maintain good performance when there are a large number of potential receivers in the system.

DISCUSSION

Conclusion

In this research, we have pioneered the integration of quantum mechanics with the realm of QSS, culminating in the development of a QASS protocol utilizing W states. This development represents an essential exploration in quantum information processing, facilitating the secure and anonymous distribution of quantum secrets. It can effectively resist attacks on anonymous receivers and quantum secret information from malicious external adversaries and dishonest authenticated participants. The application of W states within QASS demonstrates substantial efficacy in counteracting noise interference, which is a useful step toward bridging the theoretical constructs of quantum mechanics with their practical implementation in quantum networks. Two interesting future research are the pursuit of more efficient quantum resources to enhance the functionality of QASS, and the exploration of the broader utility of quantum advantages in addressing other practical challenges.

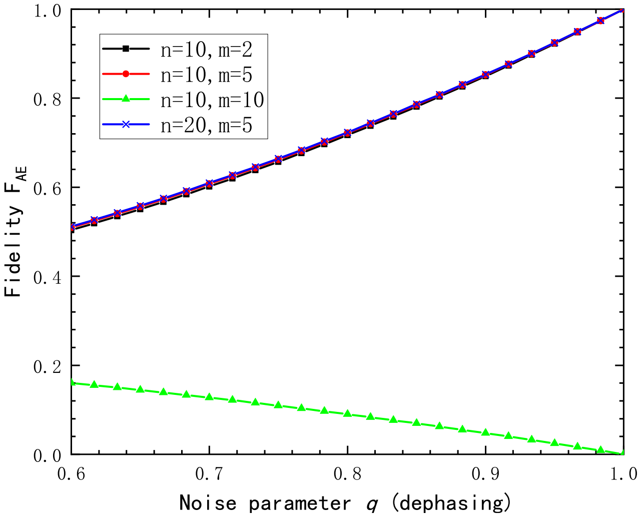


Figure 4. Fidelity of anonymous entanglement as a function of the noise parameter *q* for depolarizing noise

Limitations of the study

In the preceding discussions, this study examined the efficacy of the protocol within the context of noisy quantum networks, relying predominantly on numerical simulations for analysis. However, it is important to acknowledge that the intricacies of noise in genuine application environments could surpass the complexity accounted for in these simulations. Consequently, there is a notable imperative for future research to implement and assess proposed quantum protocols on actual quantum devices, thereby providing a robust verification of their practical applicability and feasibility.

STAR★METHODS

Detailed methods are provided in the online version of this paper and include the following:

- KEY RESOURCES TABLE
- RESOURCE AVAILABILITY
  - Lead contact
  - Materials availability
  - Data and code availability
- EXPERIMENTAL MODEL AND SUBJECT DETAILS
- METHOD DETAILS
- QUANTIFICATION AND STATISTICAL ANALYSIS

ACKNOWLEDGMENTS

This research was supported by the Key Lab of Information Network Security, Ministry of Public Security (C21605).

AUTHOR CONTRIBUTIONS

Study conception and design: G.-D.L. and W.-C.C. Writing of the manuscript: W.-C.C. and Q.-L.W. Analysis and discussion: L.C., Y.M., and H.-Y. J. All authors reviewed the manuscript.

DECLARATION OF INTERESTS

All authors declare no competing interests.

Received: February 21, 2024
Revised: April 9, 2024
Accepted: April 25, 2024
Published: April 29, 2024

REFERENCES

1. Gu, J., Xie, Y.-M., Liu, W.-B., Fu, Y., Yin, H.-L., and Chen, Z.-B. (2021). Secure quantum secret sharing without signal disturbance monitoring. Opt Express *29*, 32244–32255.
2. Senthoor, K., and Sarvepalli, P.K. (2022). Theory of communication efficient quantum secret sharing. IEEE Trans. Inf. Theory *68*, 3164–3186.
3. Yang, Y.-H., Gao, F., Wu, X., Qin, S.-J., Zuo, H.-J., and Wen, Q.-Y. (2015). Quantum secret sharing via local operations and classical communication. Sci. Rep. *5*, 16967.
4. Shi, R.-H., and Fang, X.-Q. (2023). Edge-assisted Quantum Protocol for Secure Multiparty Logical AND and its Applications. iScience *26*, 106990.
5. Toma, C., Popa, M., Boja, C., Ciurea, C., and Doinea, M. (2022). Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology. Electronics *11*, 1895.
6. Song, J.-G., Moon, S.-J., and Jang, J.-W. (2021). A scalable implementation of anonymous voting over ethereum blockchain. Sensors *21*, 3958.
7. Abbasinezhad-Mood, D., and Nikooghadam, M. (2018). An anonymous ECC-based self-certified key distribution scheme for the smart grid. IEEE Trans. Ind. Electron. *65*, 7996–8004.
8. He, D., Wang, H., Khan, M.K., and Wang, L. (2016). Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun. *10*, 1795–1802.
9. Yang, Y.-G., Liu, B.-X., Xu, G.-B., Zhou, Y.-H., and Shi, W.-M. (2023). Practical Quantum Anonymous Private Information Retrieval Based on QuantumKey Distribution. IEEE Trans. Inf. Forensics Secur. *18*, 4034–4045.
10. Khan, A., Khalid, U., Ur Rehman, J., and Shin, H. (2022). Quantum anonymous private information retrieval for distributed networks. IEEE Trans. Commun. *70*, 4026–4037.
11. Blundo, C., and Stinson, D.R. (1997). Anonymous secret sharing schemes. Discrete Appl. Math. *77*, 13–28.
12. Liang, J.-M., Lv, Q.-Q., Wang, Z.-X., and Fei, S.-M. (2023). Assisted quantum simulation of open quantum systems. iScience *26*, 106306.
13. Klassert, R., Baumbach, A., Petrovici, M.A., and Gärttner, M. (2022). Variational learning of quantum ground states on spiking neuromorphic hardware. iScience *25*, 104707.
14. Li, G., Xu, Y., Wang, Q., Zhuang, Z., and Cheng, W. (2023). Authenticated anonymous secret-sharing protocol based on a high-dimensional quantum system. Sci. Sin. *53*, 110313.
15. Lin, S., Guo, G.-D., Huang, F., and Liu, X.-F. (2016). Quantum anonymous ranking based on the Chinese remainder theorem. Phys. Rev. *93*, 012318.
16. Huang, W., Wen, Q.-Y., Liu, B., Su, Q., Qin, S.-J., and Gao, F. (2014). Quantum anonymous ranking. Phys. Rev. *89*, 032325.
17. Li, Y.-R., Jiang, D.-H., and Liang, X.-Q. (2021). A novel quantum anonymous ranking protocol. Quant. Inf. Process. *20*, 342.
18. Xu, X., Shi, R.-H., and Ke, W. (2023). Decentralized quantum anonymous veto voting scheme based on measurementdevice-independence. Phys. Scr. *98*, 095116.
19. Ruan, X., Zhang, H., Mao, Y., Wang, Z., Zuo, Z., and Guo, Y. (2022). Multiparty quantum anonymous voting with discrete modulated coherent states and an optical frequency comb. Opt Express *30*, 41204–41218.

20. Jiang, L., He, G., Nie, D., Xiong, J., and Zeng, G. (2012). Quantum anonymous voting for continuous variables. Phys. Rev. *85*, 042309.
21. Yang, W., Huang, L., and Song, F. (2016). Privacy preserving quantum anonymous transmission via entanglement relay. Sci. Rep. *6*, 26762.
22. Thalacker, C., Hahn, F., de Jong, J., Pappa, A., and Barz, S. (2021). Anonymous and secret communication in quantum networks. New J. Phys. *23*, 083026.
23. Unnikrishnan, A., MacFarlane, I.J., Yi, R., Diamanti, E., Markham, D., and Kerenidis, I. (2019). Anonymity for practical quantum networks. Phys. Rev. Lett. *122*, 240501.
24. Lipinska, V., Murta, G., and Wehner, S. (2018). Anonymous transmission in a noisy quantum network using the W state. Phys. Rev. *98*, 052320.
25. Zhang, Z.-J., Li, Y., and Man, Z.-X. (2005). Multiparty quantum secret sharing. Phys. Rev. *71*, 044301.
26. Huang, W., Wen, Q.-Y., Liu, B., and Gao, F. (2015). Multi-user quantum key distribution with collective eavesdropping detection over collective-noise channels. Chin. Phys. B *24*, 070308.
27. Horoshko, D., and Kilin, S. (2011). Quantum anonymous voting with anonymity check. Phys. Lett. *375*, 1172–1175.
28. Hahn, F., de Jong, J., and Pappa, A. (2020). Anonymous quantum conference key agreement. PRX Quantum *1*, 020325.
29. Li, L., and Qiu, D. (2007). The states of W-class as shared resources for perfect teleportation and superdense coding. J. Phys. A: Math. Theor. *40*, 10871–10885.
30. Yang, Y.-G., Liu, X.-X., Gao, S., Zhou, Y.-H., Shi, W.M., Li, J., and Li, D. (2021). Towards practical anonymous quantum communication: A measurement-deviceindependent approach. Phys. Rev. *104*, 052415.
31. Hong, C.H., Heo, J., Jang, J.G., and Kwon, D. (2017). Quantum identity authentication with single photon. Quant. Inf. Process. *16*, 236.
32. Joo, J., Park, Y.-J., Oh, S., and Kim, J. (2003). Quantum teleportation via a W state. New J. Phys. *5*, 136.
33. Niu, P.-H., Zhou, Z.-R., Lin, Z.-S., Sheng, Y.-B., Yin, L.-G., and Long, G.-L. (2018). Measurementdevice- independent quantum communication without encryption. Sci. Bull. *63*, 1345–1350.
34. Horodecki, M., Horodecki, P., and Horodecki, R. (1999). General teleportation channel, singlet fraction, and quasidistillation. Phys. Rev. *60*, 1888–1898.
35. Rozpędek, F., Schiet, T., Elkouss, D., Doherty, A.C., and Wehner, S. (2018). Optimizing practical entanglement distillation. Phys. Rev. *97*, 062333.

STAR★METHODS

KEY RESOURCES TABLE

REAGENT or RESOURCE	SOURCE	IDENTIFIER
Other		
Single photon	Hong et al.[31]	N/A
W state	Li et al.[29]	N/A
Pauli Operator	Li et al.[14]	N/A
Noisy channel	Lipinska et al.[24]	N/A

RESOURCE AVAILABILITY

Lead contact

Further information and requests for resources should be directed to the lead contact Qing-le Wang (wqle519@gmail.com).

Materials availability

This study did not generate new unique reagents.

Data and code availability

- All data reported in this paper will be shared by the lead contact upon request.
- This paper does not use new code that needs to be reported.
- Any additional information required to reanalyze the data reported in this paper is available from the lead contact upon request.

EXPERIMENTAL MODEL AND SUBJECT DETAILS

Our study does not use experimental models typical in the life sciences.

METHOD DETAILS

The method details refer to the anonymous quantum secret sharing protocol utilizing W states. All relevant methods are presented in the body of the article.

QUANTIFICATION AND STATISTICAL ANALYSIS

It is not applicable for this study.