Quantum Anonymity for Quantum Networks

Awais Khan, Junaid ur Rehman, Hyundong Shin

Department of Electronic Engineering, Kyung Hee University, Yongin-si, 17104, Korea

Abstract

We present the first quantum anonymous notification (QAN) protocol that introduces anonymity and paves the way for anonymous secure quantum communication in quantum networks. QAN protocol has applications ranging from multiparty quantum computation to quantum internet. We utilize the QAN protocol to propose an anonymous quantum private comparison protocol in an $n$-node quantum network. This protocol can compare private information of any $2 \leq k \leq n$ parties with the help of the remaining $n-k$ parties and a semi-honest third party. These protocols feature a traceless property, i.e., encoding operations cannot be traced back to their originating sources. Security analysis shows that this protocol is robust against external adversaries and malicious participants.

Keywords: Quantum anonymity, quantum anonymous notification, quantum network, quantum private comparison, quantum information

1. Introduction

Development of quantum communication systems provides potential benefits to carry out the information processing tasks in a quantum network. Many quantum network based applications such as quantum secret sharing [1, 2], quantum voting [3], and quantum conference key agreement [4] have been proposed with the vision of quantum internet [5].

One practical application of quantum networks is quantum private comparison (QPC) protocols [6]. The main objective of QPC is to allow two parties to compare their private information with the help of a semi-honest third party (TP) (which can be almost dishonest [7]), without leaking the information to participants and the TP. QPC has been generalized to compare secrets of multiple parties and is called multiparty QPC (MQPC) [8]. MQPC has many applications such as quantum voting [9], quantum bidding [10], and quantum auctions [11].

One of the challenging requirements of quantum networks is to provide anonymity of the sender and the receiver when they wish to communicate through the network. Anonymity should be guaranteed without making any assumption on the computational power of malicious participants who might have quantum computers. The introduction of anonymity provides security against maliciously behaved participants and potential adversaries.

In the classical scenario, Broadbent et. al. showed how to transmit a message anonymously with information-theoretic security in the absence of an honest majority [12]. The key enabler for the anonymity in their proposal is an anonymous notification protocol, which utilizes authenticated pairwise private channels and simultaneous classical broadcast channels.

In the case of quantum communication, the first work related to an anonymous message was proposed by Christandl and Wehner [13]. They proposed the protocols with perfect anonymity for quantum broadcast and the creation of an EPR pair between two remote parties. More recently, the protocol for anonymity in
a practical quantum network was proposed [14]. The main ingredient of the protocol which introduces the anonymity in the network is a classical notification protocol. However, this classical notification protocol can be vulnerable to quantum computers. That means communicating parties are no longer anonymous against a sufficiently powerful quantum adversary.

We present the first quantum anonymous notification (QAN) protocol to introduce anonymity in a practical quantum network. This protocol guarantees the anonymity of communicating parties and also features traceless property, i.e., once the receiver is notified there is no way to trace the notifier. We exemplify the application of QAN on a new MQPC, where the QAN acts as the main ingredient for providing the anonymity. Our MQPC protocol compares private information anonymously of any \( 2 \leq k \leq n \) parties with the help of the remaining \( n - k \) parties and the semi-honest TP. In contrast to previous MQPC protocols, our proposed protocol removes the requirement of use of hash function, quantum key distribution, quantum secure direct communication, or multiple TPs [15, 7, 16, 17]. We prove the security against common attacks launched by the participants, TP, and outsiders.

2. Quantum Anonymous Notification

Here we provide the QAN protocol for a quantum network where any of the participants can anonymously notify another participant for any upcoming targeted communication task.

**Communication scenario.**—Our network consists of \( n \) agents that can perform local operations and classical communication (LOCC). GHZ states are shared between these \( n \) agents using the protocol in [18, 19]. We also require pairwise classical authenticated channels between agents. The communication objective is to allow any honest party to anonymously notify any other party in the network. The adversaries and malicious agents aim is to break the anonymity or security of the protocol.

**Protocol 1 Quantum Anonymous Notification**

**Prerequisite:** \( n \) \((n)\)-partite GHZ states.

**Protocol Parameters**

- Sender choice of the receiver is party \( r \)
- \( U_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad U_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \)

**The Protocol**

![Figure 1: Anonymous quantum notification protocol.](image-url)
1. GHZ states and the constituent particles of all GHZ states are numbered such that $q^j_i$ is the $i$th particle in the $j$th GHZ state. Each party $i$ is given $n$ particles, $q^j_i$, $1 \leq j \leq n$.

2. Each party $i$ applies $U^j_i$ on the $q^j_i$ according to the rule:

$$U^j_i = \begin{cases} U_Z, \text{ with probability } P_Z, \\ U_I, \text{ with probability } 1 - P_Z, \end{cases}$$

(1)

if $j = r$ is the intended party to be notified. Otherwise $U^j_i = U_I$ with probability 1.

3. Each party applies $H$ to all of the held particles and measures them in the computational basis. The measurement results on $q^j_i$ is $m^j_i \in \{0, 1\}$.

4. Each party $i$ announces the measurement results $m^j_i \forall j \neq i$ on a classical authenticated channel.

5. Each party calculates $m_j = \bigoplus_{i=1}^n m^j_i$ for their allotted GHZ state.

6. Steps 1–5 are repeated $K$ times. Party $j$ is notified if $m_j = 1$ for any run of the protocol.

Here we analyze the Protocol 1. We assume that $(n)$-partite GHZ states are shared between the network,

$$|GHZ\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle^\otimes n + |1\rangle^\otimes n \right).$$

In step 1), each party is allotted with a GHZ state. 2) The sender simply notifies by applying $U_Z$ on the receiver related particle of GHZ state with a probability of $P_Z$. This introduces the phase on the receiver GHZ state with a probability $P_Z$. 3) After the $H$ gate state changes into the superposition of all strings $E_j \in \{0, 1\}^n$ with an odd number of 1’s if $j = r$ else even number of 1’s:

$$H^\otimes n |GHZ\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{E_j \in \{0, 1\}^n} \left( 1 + (-1)^{v \oplus |E_j|} \right) |E_j\rangle,$$

where $|E_j|$ is the hamming weight of string $E_j$. After step 4 & 5, each party calculates $m_i$ for their allotted GHZ state. If the party is notified then she will get odd number of 1’s and $v = 1$ else she is not notified and $v = 0$. This result $m_i$ is only available to the party $i$. Our protocol gives the perfect anonymity to the receiver and the sender. Malicious participants cannot obtain the identity of the notifier and the notified party even if they collaborate as long as the total number of collaborating parties is less than $n - 2$.

Fig. I shows the QAN protocol for $n = 4$ on $q^4_i$ where any of the parties can notify the fourth party $A - 4$.

3. Anonymous Multiparty Quantum Private Comparison

In this section, we provide an application for quantum anonymity in multiparty computation protocol. We consider the problem of multiparty quantum private comparison. First, we provide the protocol for resource sharing, which will be used as a sub-protocol for the anonymous MQPC protocol. In this protocol, agents are connected via the quantum channel and classical authenticated channel.

**Protocol 2** Resource sharing and security check

**Protocol Parameters**

- $n$: Total number of participants
- $L$: Total number of $(n)$-partite GHZ states shared at the end of the protocol
Figure 2: Modified anonymous quantum notification protocol.

- **S**: Security parameter, the number of GHZ states utilized in the security check and verification.

**The Protocol**

1. **State Preparation**: All parties in the network are indexed with \( i \in \{1, 2, \cdots, n\} \). A randomly designated player (e.g., Alice, with index \( a \)) prepares \( K = L + S \) GHZ states and labels them as \( F^i_j \), \( i \in \{1, 2, \cdots, n\} \), \( j \in \{1, 2, \cdots, K\} \). Here \( F^i_j \) is the \( i \)th particle in the \( j \)th GHZ state.

2. **State Distribution**: Alice sends \( F^i_j \), \( 1 \leq j \leq K \) particles to \( i \)th party in the network through quantum channel and keeps \( F^a_j \) for herself.

3. **Security Check & Verification**: Participants repeat the following steps \( S \) number of times:

   (i) One of the party \( i' \neq a \) randomly announces \( j' \in \{1, 2, \cdots, K\} \), and \( h = 0, 1 \). Each party \( i \) applies \( H^h \) on \( F^i_{j'} \) where \( H \) is the Hadamard gate.

   (ii) Alice measures \( F^a_{j'} \) in the computational basis and announces the outcome on the classical authenticated channel. After Alice’s announcement, the rest of the parties perform the same measurement on their respective particles and announce their measurement results.

   (iii) The protocol aborts if 1) any party refuses to announce the measurement results, or 2) the measurement results are not consistent with the GHZ state.

4. If the protocol does not abort, they have shared \( L \) (\( n \))-partite GHZ states with probability \( 1 - 2^{-S} \).

After the resource sharing protocol, we move towards the first step of anonymous quantum private comparison. We use Protocol 1 to introduce the quantum anonymity in quantum private comparison network. In the quantum private comparison network, TP performs the comparison between competing parties and is already known as the notifier. Therefore, only the receiver’s anonymity is required. Protocol 1 can be easily modified to provide receiver anonymity.

In Protocol 1, small changes are made in steps 1-4. 1) \( (n+1)\)-partite GHZ states are shared instead of \( (n)\)-partite where the \( (n+1)\)th particle is held by the TP. 2) The TP only applies \( U^TP \) on the \( q^TP \) particle to notify the competing parties. 3) The TP also performs this step similarly on her held particle. 4) Each party announces the measurement result \( m^i_j \forall j \neq i \) to TP via a classical authenticated channel. TP calculates \( m^i_i = \bigoplus_{j=1}^{n} m^i_j \oplus m^TP_j, \forall i \neq j \) for each party and sends it to the respective parties on a classical authenticated channel. After this procedure, if a party obtains \( m_j = 1 \) for any run of the protocol then she is a competing party. Else she will assist the TP for the comparison. The simplified setup of this protocol is
Protocol 3 Anonymous Quantum Private Comparison (For two parties in an $n$-partite network)

**Prerequisite:** From Protocol 2. $M$ ($n + 1$)-partite and $M$ ($n$)-partite GHZ states whose particles are labelled as $G_{j}^{n+1}$ and $F_{j}^{n}$, respectively. $G_{j}^{n+1}$, $1 \leq j \leq M$ are held by the TP.

**Protocol Parameters**
- $M$: Total number of secret bits of each party
- $n$: Total number of parties in the network

**The Protocol**

1. Each notified party (e.g., Alice and Bob, labelled with indexes $a$ and $b$, respectively) encode their secrets as follows. For $1 \leq j \leq M$:
   - (i) Alice and Bob measure $F_{a}^{j}$ and $F_{b}^{j}$, respectively, in the computational basis. Let $k_{a}^{j}$ and $k_{b}^{j}$ be their measurement outcomes.
   - (ii) If $k_{a}^{j} = k_{b}^{j} = 0$, Alice and Bob encode their secret messages by applying $U_{I}(U_{Z})$ for the message bit $0(1)$ on $G_{j}^{a}$ and $G_{j}^{b}$, respectively. Else if $k_{a}^{j} = k_{b}^{j} = 1$, they reverse the role of $U_{I}$ and $U_{Z}$.

2. After the encoding, each participant including Alice, Bob, and TP apply $H$ to their $G_{j}^{a}$, qubits.

3. Each participant and TP measure their $G_{j}^{a}$ qubits in the computational basis and send their measurement outcomes $m_{j}^{a}$ to the TP via the classical authenticated channel.

4. The TP calculates the $m_{j} = \oplus_{a=1}^{n+1} m_{j}^{a}$ for each secret bit $j$. The secrets of Alice and Bob are equal if $m_{j} = 0$, $1 \leq j \leq M$, otherwise they are not equal. The TP announces whether or not the secrets are equal.

This protocol is also based on the LOCC only. For example, the notified competing participants are Alice and Bob have a secret bit $b_{1}$ and $b_{2}$, respectively, where $b_{1}, b_{2} \in \{0, 1\}$. 

---

Figure 3: Example run of anonymous quantum private comparison protocol for two comparing parties in a four-node network.
In step 1, Alice and Bob apply the unitaries $U_I$ or $U_Z$ on the particles of $(n + 1)$-partite GHZ state for the message bit $b_1$ and $b_2$. This encoding depends upon the measurement outcome of their $(n)$-partite GHZ state particle. After the encoding, the change of phase in global GHZ state depends upon the secret bits,

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle^\otimes (n+1) + (-1)^{b_1 \oplus b_2} |1\rangle^\otimes (n+1) \right).$$

If the secret bits $b_1 \neq b_2$, then the phase of the global GHZ state changes else it remains the same. Each participant and the TP applies the $H$ gate to their particles in step 2. This changes the GHZ state into the superposition of all strings $E_j \in \{0, 1\}$ with an even number of 1’s for $b_1 = b_2$ or an odd number of 1’s for $b_1 \neq b_2$. After $H$, state becomes:

$$H^\otimes (n+1) |\text{GHZ}\rangle = \frac{1}{\sqrt{2}^{n+2}} \sum_{E_j \in \{0,1\}^{n+1}} \left( 1 + (-1)^{b_1 \oplus b_2 \oplus |E_j|} \right) |E_j\rangle,$$

where $|E_j|$ is the hamming weight of string $E_j$. TP computes the phase of the GHZ state after step 3. If the result is $m_j = 0$ for each secret bit $j$ then secret is equal else secrets are not equal. In the Fig. 3 & 4 simplified example of the experimental setup for a four-partite case is shown. Fig. 4 explains the inside of the device of participants. Fig. 3 explains that A-2 and A-4 laboratories are comparing secrets anonymously with the help of the remaining parties and the TP.

In the following, we present the protocol of private comparison between more than two parties. This protocol is similar to the Protocol 3 with a slight modification. In this protocol, both the unitaries are utilized for a single secret bit.

**Protocol 4 Anonymous Quantum Private Comparison (For $n > 2$)**

**Prerequisite:**
- $K$ $(n + 1)$-partite GHZ states, where $K = (2^\lceil \log(n) \rceil + 2) M$. The particle held by the $i$th party, which will be utilized for comparing the $m$th bit of the message is labeled as $Q_{i,k,m}$. The role of $k \in \{0, 1\}$, and $g \in \{0, 1, \cdots, \lceil \log(n) \rceil \}$ will be explained in the protocol. $Q_{k,g}^{m,n+1}, \forall (m, k, g)$ are held by the TP.
- $M n$-partite GHZ states. The particle held of the $j$th state held by the $i$th party is labeled as $F_{i,j}^m$.

**Protocol Parameters**
- $M$: Total number of secret bits of each party
- $n$: Total number of parties in the network
- $U_g(\phi) = \cos(\phi/2)U_I + i \sin(\phi/2)U_Z$, where $\phi = \pi/2^g$ and $0 \leq g \leq \lceil \log(n) \rceil$.

**The Protocol**
1. Each notified party (e.g. Alice, Bob, and Charlie, labelled with indexes $a$, $b$, and $c$, respectively) encode their secrets as follows.

Steps (i)–(ii) are repeated for $1 \leq m \leq M$:

(i) Alice, Bob, and Charlie measure $F^a_m$, $F^b_m$ and $F^c_m$, respectively, in the computational basis. Let $k^a_m = k^b_m = k^c_m = k$ be their measurement outcomes.

Step (ii) is repeated for $0 \leq g \leq \log(n)$:

(ii) Alice, Bob, and Charlie encode their secret bits by applying $U^g I$, $U^g g$, and $U^g c$, respectively. Then, they reverse the role of $U^g$ and $U^g$ and perform the encoding on $Q^{m,a}_{-k,g}$, $Q^{m,b}_{-k,g}$ and $Q^{m,c}_{-k,g}$, where $\neg$ denotes the logical NOT.

2. All participants including the TP apply $H$ to their $Q^{m,i}_{k,g}$ qubits.

3. All participants including the TP measure their $Q^{m,i}_{k,g}$ qubits in the computational basis and send the respective measurement outcomes $z^{m,i}_{k,g}$ to the TP via the classical authenticated channel.

4. For each message bit $1 \leq m \leq M$, the TP calculates $D^m_{k,g} = \oplus_{i=1}^{n+1} z^{m,i}_{k,g}$, $\forall (k,g)$. The $m$th message bit of all participants are equal if $D^m_{k,g} = 0, \forall g$ when $k$ is fixed to either 0 or 1. The TP announces whether the secrets are equal or not.

The correctness of this protocol can be deduced from the correctness of Protocol 3.

4. Security Analysis

The security of quantum private comparison protocols is hard to prove due to the participant’s and the TP’s attacks. Previously, these protocols were vulnerable to participants’ attacks. However, the secrecy of protocol increases due to the induction of anonymity and traceless properties. For security, we analyze the quantum communication between the participants and the TP.

- **Outside attacks**: A designated player (e.g., Alice) shared the GHZ states via the quantum channel with the parties and TP. After receiving the GHZ states, one party randomly selects GHZ state for security check and also announces a random bit $h$. The value of $h$ determines that all parties and TP should perform Hadamard transformation or not. This process not only detects the adversaries but also inquires about Alice’s honesty, whether she prepared the GHZ states correctly. After the selection of GHZ state and value of $h$, Alice measures her particle in the computational basis and announces the results. Then, each party and the TP measure their qubits and announce the result to check the security of the communication. The attacker does not know in advance the value of $h$ and the GHZ state chosen by the random party. This process will prevent well-known attacks such as intercept-resend attacks, entangled-resend attacks, and correlation elicitation attacks. The detection of the adversary is $P_d = 1 - 2^{-S}$, where $S$ is the security parameter.

- **Participants attacks**: The TP anonymously notifies the competing participants. To get the secret information, the participants have to identify first the competing parties. To reveal the identity of competitors is impossible for a single participant. After the encoding, the only communication between participants and the TP is via the classical authenticated channel. This information does not reveal any information to the participants. This communication only helps the TP to compute the comparison results. Therefore, cheating and collusion attacks are not possible for the proposed protocol. The private information is still not available for the adversaries if the $n - 1$ parties collude against the one. The only option left for malicious parties is to adopt Eve’s strategies to steal private information. These strategies are known as outside attacks. As discussed earlier, the protocol is secure against these attacks.
• **TP’s attacks**: Malicious TPs can also threaten the security of the private comparison protocols. The TP can attack to gain useful information using her resources. Our procedure has a unique traceless property to tackle the TP’s attacks. Firstly, with the assumption that semi-honest TP is not allowed to collude with the participants. To prove the security, assume that competing parties (e.g., Alice and Bob) have secrets of 0 and 1, respectively. After applying the unitaries, the GHZ state has a phase, which means that the secrets are not equal. The TP computes the phase of the GHZ state with her and each participant’s measurement outcomes. The TP cannot identify the party which introduced the phase. So this protocol is secure against the TP’s attack as well.

5. **Conclusion**

Anonymity can be a useful but challenging requirement of any communication network. In this work, we proposed the QAN protocol which can be implemented in quantum networks where anonymity is required (e.g., accessing the quantum internet without revealing the identity). QAN provides both sender and receiver anonymity. However, this protocol can be easily modified to provide receiver anonymity only. We used this protocol as an application and introduced the anonymity in the MQPC. Firstly, TP notifies the participants via the QAN protocols. Then, the MQPC protocol is executed to anonymously and securely perform the comparison of secrets of different remote parties. Our framework allows two or more parties to compare their secrets with the help of the remaining parties and a semi-honest TP. Security analysis shows that this protocol is robust against malicious participants and the TP.

**Conflict of interest**

The authors declare that they have no conflict of interest.

**Acknowledgments**

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1A2C2007037).

**Author contributions**

A.K contributed the idea. A.K and J.R developed the theory and wrote the manuscript. H.S improved the manuscript and supervised the research. All the authors contributed in analyzing and discussing the results and improving the manuscript.

**References**

[1] Cleve, R., Gottesman, D., Lo, H.K.. How to share a quantum secret. Phys Rev Lett 1999;83(3):648.

[2] Bell, B., Markham, D., Herrera-Martí, D., Marin, A., Wadsworth, W., Rarity, J., et al. Experimental demonstration of graph-state quantum secret sharing. Nat Commun 2014;5(1):1–12.

[3] Bao, N., Halpern, N.Y.. Quantum voting and violation of arrow’s impossibility theorem. Phys Rev A 2017;95(6):062306.

[4] Ribeiro, J., Murta, G., Wehner, S.. Fully device-independent conference key agreement. Phys Rev A 2018;97(2):022307.

[5] Kimble, H.J.. The quantum internet. Nature 2008;453(7198):1023.

[6] Yang, Y.G., Wen, Q.Y.. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A: Math and Theor 2009;42(5):055305.

[7] Hung, S.M., Hwang, S.L., Hwang, T., Kao, S.H.. Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf Process 2017;16(2):36.

[8] Chang, Y.J., Tsai, C.W., Hwang, T.. Multi-user private comparison protocol using ghz class states. Quantum Inf Process 2013;12(2):1077–1088.

[9] Jiang, L., He, G., Nie, D., Xiong, J., Zeng, G.. Quantum anonymous voting for continuous variables. Phys Rev A 2012;85(4):042309.

[10] Muhammad, S., Tavakoli, A., Kurant, M., Pawłowski, M., Żukowski, M., Bourennane, M.. Quantum bidding in bridge. Phys Rev X 2014;4(2):021047.
[11] Hogg, T., Harsha, P., Chen, K.Y.. Quantum auctions. Int J Quantum Inf 2007;5(05):751–780.
[12] Broadbent, A., Tapp, A.. Information-theoretic security without an honest majority. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer; 2007, p. 410–426.
[13] Christandl, M., Wehner, S.. Quantum anonymous transmissions. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer; 2005, p. 217–235.
[14] Unnikrishnan, A., MacFarlane, I.J., Yi, R., Diamanti, E., Markham, D., Kerenidis, I. Anonymity for practical quantum networks. Phys Rev Lett 2019;122(24):240501.
[15] Ye, T.Y.. Multi-party quantum private comparison protocol based on entanglement swapping of bell entangled states. Commun Theor Phys 2016;66(3):280.
[16] Abulkasim, H., Alsouqaih, H.N., Hamdan, W.F., Hamad, S., Farouk, A., Mashatan, A., et al. Improved dynamic multi-party quantum private comparison for next-generation mobile network. IEEE Access 2019;7:17917–17926.
[17] Abulkasim, H., Farouk, A., Hamad, S., Mashatan, A., Ghose, S.. Secure dynamic multiparty quantum private comparison. Sci Rep 2019;9(1):1–16.
[18] Pappa, A., Chailloux, A., Wehner, S., Diamanti, E., Kerenidis, I.. Multiparty entanglement verification resistant against dishonest parties. Phys Rev Lett 2012;108(26):260502.
[19] McCutcheon, W., Pappa, A., Bell, B., McMillan, A., Chailloux, A., Lawson, T., et al. Experimental verification of multipartite entanglement in quantum networks. Nat Commun 2016;7(1):1–8.