




Quantum anonymous collision detection for quantum networks

Awais Khan¹ , Uman Khalid¹ , Junaid ur Rehman¹ , Kyesan Lee^{1*} and Hyundong Shin^{1*} 

*Correspondence: hshin@khu.ac.kr;
kyesan@khu.ac.kr

¹Department of Electronics and
Information Convergence
Engineering, Kyung Hee University,
Yongin-si, 17104, Korea

Abstract

Quantum mechanics offers new opportunities for diverse information processing tasks in communication and computational networks. In the last two decades, the notion of quantum anonymity has been introduced in several networking tasks that provide an unconditional secrecy of identity for the communicating parties. In this article, we propose a quantum anonymous collision detection (QACD) protocol which detects not only the collision but also guarantees the anonymity in the case of multiple senders. We show that the QACD protocol serves as an important primitive for a quantum anonymous network that features tracelessness and resource efficiency. Furthermore, the security analysis shows that this protocol is robust against the adversary and malicious participants.

Keywords: Collision detection; Quantum anonymity; Quantum communication; Quantum entanglement; Quantum networks

1 Introduction

Quantum information science has enabled outstanding improvement in security for communication [1], cryptography [2], metrology [3] and computation [4]. Such tasks include quantum secret sharing [5, 6], blind quantum computation [7, 8], secure quantum clock synchronization [9], and distributed secure quantum computation [10]. These technologies pave way for the vision of a secure quantum internet [11, 12]. However, these protocols are mostly developed to protect the content of the messages, which means that the encoded information can be accessed only by the sender and the intended receiver. On the other hand, in many real-life applications, it is more desirable to hide the identity of the sender and receiver than the information itself. Thus, the secrecy of identity was coined as anonymity which should be guaranteed without making any assumption on the computational power of the adversary. This property is the main enabler of several interesting applications such as anonymous quantum voting [13–15], anonymous quantum key agreement [16], quantum anonymous multi-data ranking [17], and anonymous quantum private comparison [18].

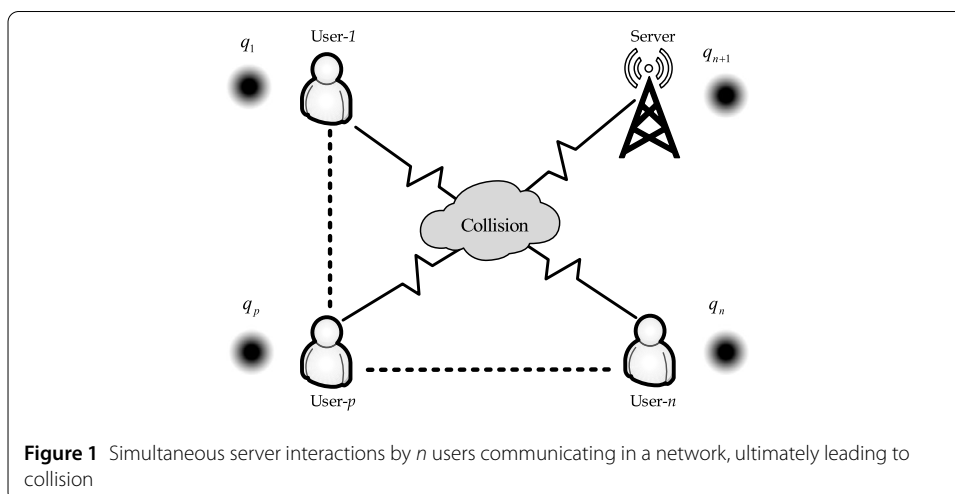
The first-ever quantum anonymous transmission protocol was proposed in [19]. This proposal consisted of two protocols—namely—the quantum anonymous broadcast for classical information and sharing entanglement between sender and receiver anonymously.

© The Author(s) 2021. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

These two protocols were combined to send a quantum message via quantum teleportation [20]. However, it was assumed that a perfect n -partite GHZ state is shared among the participants. This work was followed by several other proposals for anonymous network-based tasks. For example, anonymous quantum communication with disruption detection [21], anonymous entanglement generation from EPR pairs [22], and anonymous quantum communication via a noisy channel [23]. More recently, the protocol for anonymity in quantum networks was presented [24]. In this protocol, their main aim was the anonymous verification of GHZ state that is shared via protocols in [25, 26]. However, all these protocols have to detect multiple senders prior to their own run of the protocol. Thus, an anonymous collision detection protocol seems indispensable for a truly anonymous execution of these anonymous networking tasks.

A quantum anonymous collision detection (QACD) protocol was proposed in [19] that utilizes $O(\lceil \log n \rceil + 1)$ n -partite GHZ qubit states in an n -node network as a resource. This protocol was proposed under the assumption of semihonest participants, i.e., all participants are honest but curious. However, in real life, anonymous network is usually built among the mutually untrusted participants. Hence, the protocols designed under the semihonest model assumption are impractical. It was also proved that a quantum source cannot securely evaluate any two-party classical deterministic function [27, 28]. This result also applies to the QACD protocols since these protocols can be viewed as a manifestation of two-party classical deterministic function. The motivation for our work lies in the securely and resourcefully collision detection for multiple senders among mutually untrustworthy participants.

In this paper, we propose the quantum anonymous collision detection protocol to detect the collision in the case of multiple senders with the help of the server, as depicted in Fig. 1. The server is almost dishonest which means that it is allowed to misbehave on its own without conspiring with the participants. This protocol guarantees the anonymity of the sender and also features tracelessness property, i.e., the identity of the sender remains hidden even if the adversary gains access to the encoded state. Our protocol is more efficient than the previously proposed protocol and utilizes $O(1)$ n -partite GHZ qudit state. We also show the correctness and robustness against both external and internal adversaries of the protocol.



The rest of the paper is organized as follows. First, we present the quantum anonymous collision detection protocol for multiple senders. Then the security and correctness of the protocol is shown. In the end, we conclude the paper.

2 Quantum anonymous collision detection (QACD)

In this section, we provide the QACD protocol for any quantum anonymous network where collision is detected anonymously with the help of the server. The server in our protocol is allowed to misbehave through active and passive attack but cannot conspire with the participants. However, it is unable to match the identity of the participants with the encoded data. This protocol will also work under untrustworthy participants.

Communication Scenario—Our protocol consist of n agents and the server that can perform local operation and classical communication (LOCC) as graphically illustrated in Fig. 2. Each user is connected to the server via a quantum and a classical authenticated channel. The d -dimensional GHZ state

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_1 |j\rangle_2 \cdots |j\rangle_n |j\rangle_{n+1} \quad (1)$$

is shared among the agents and the server, where $d > n$. The server prepares and distributes the GHZ state by utilizing the entanglement distribution and verification protocol of [17]. After the sharing of the GHZ state, each user applies the quantum Fourier transform to

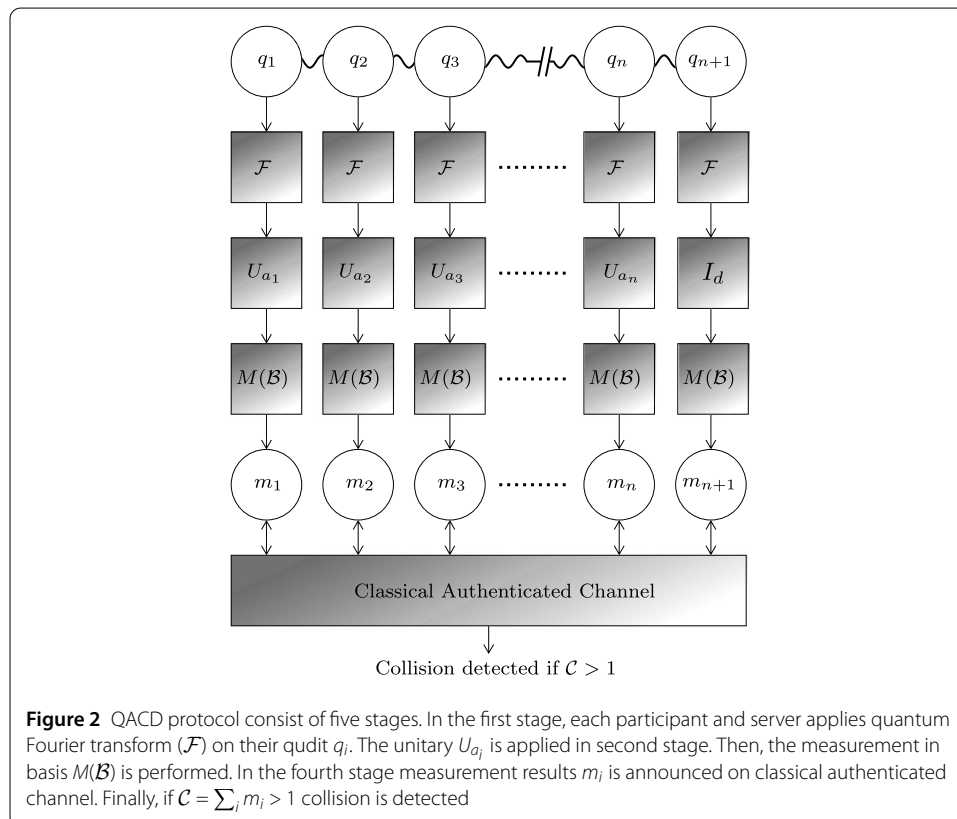


Figure 2 QACD protocol consist of five stages. In the first stage, each participant and server applies quantum Fourier transform (\mathcal{F}) on their qudit q_i . The unitary U_{a_i} is applied in second stage. Then, the measurement in basis $M(\mathcal{B})$ is performed. In the fourth stage measurement results m_i is announced on classical authenticated channel. Finally, if $\mathcal{C} = \sum_i m_i > 1$ collision is detected

their qudit

$$\mathcal{F}_d |j\rangle = \frac{1}{\sqrt{d}} \sum_{w=0}^{d-1} \exp\left(\frac{2\pi i j w}{d}\right) |w\rangle. \quad (2)$$

If any participant wants to be the sender, then it applies the shift operator

$$U_s |j\rangle = |j \oplus 1\rangle \quad (3)$$

to their qudit, where \oplus represents addition mod d . Then, measurements is performed and result is communicated via classical authenticated channel.

Here, the communication objective is to detect the collision anonymously in the case of multiple senders. The protocol is anonymous until the communication does not change the uncertainty about the identity of the sender. The objective of the adversaries and malicious agents t is to break the anonymity or security of the protocol. Eve has access to the public communication occurring through authenticated channels. In a practical scenario, she may have certain network resources beyond public communication. For example, she may have support from $t < n$ malicious parties and has access to all their classical and quantum resources denoted by Q_t . Finally, in an unlikely but possible scenario, she may hijack the quantum channel and gain access to the joint quantum state of k parties, denoted by R_k . Note that these parties are acting honestly and do not conspire with her. Now we can formally idealize the QACD protocol features, provided that the GHZ state is shared correctly.

Correctness: Each party should be notified with certainty if there are multiple senders in a run of the protocol.

Anonymity: The identity of the senders remain hidden regardless of their announced data.

Traceless: Even with access to all network resources including the encoded quantum state and classical communication, the status (sender/ non sender) of all parties remain hidden.

Security: The participants private data should be protected against adversarial (outside/inside) attacks.

In the following, we present the quantum anonymous collision detection protocol with tracelessness.

3 Security analysis

Here we provide the security analysis of the protocol. QACD protocol has to satisfy two condition for security: (1) correctness, (2) secrecy. First, we show the correctness of the protocol.

3.1 Correctness

Here, we prove the correctness of Protocol 1. Initially, an $(n + 1)$ -partite GHZ state (1) is shared between the agents and the server. Each participant encodes operation on its qudit using the unitaries. If the participants want to be a sender, they apply U_s otherwise they

Protocol 1 Quantum Anonymous Collision Detection

Prerequisite: Preshared $(n + 1)$ -partite d -dimensional GHZ.

Protocol Parameters

- A server and n participants.
- Total l senders, where $0 \leq l \leq n$.

The Protocol

- (1) All parties including the server apply \mathcal{F}_d to their qudits.
- (2) Each party $1 \leq i \leq n$ applies U_{a_i} on q_i according to the rule:

$$U_{a_i} = \begin{cases} U_s, & \text{if party } i \text{ wants to be the sender,} \\ I_d, & \text{otherwise.} \end{cases}$$

Here,

$$U_s = \sum_k |k \oplus 1\rangle \langle k|,$$

with \oplus being the modulo d addition and I_d is the identity operator on d -dimensional Hilbert space.

- (3) All parties including the server measure their qudits in the computational basis $\mathcal{B} = \{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$.
 - (4) Each party i announces the measurement results m_i on a classical authenticated channel to the server.
 - (5) Server calculates $\mathcal{C} = \sum_{i=1}^{n+1} m_i \pmod{d}$ where $\mathcal{C} \in \{0, 1, 2, \dots, n\}$ and announces \mathcal{C} . If $\mathcal{C} > 1$ then collision is detected.
-

apply I_d . Each participant and server is given one qudit q_i from the GHZ state

$$|\Phi\rangle = |\text{GHZ}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_1 |j\rangle_2 \cdots |j\rangle_n |j\rangle_{n+1}. \quad (4)$$

After the first and second step, participants apply $U_{a_i} \mathcal{F}$ on (4). Consequently, state transforms

$$\begin{aligned} |\hat{\Phi}\rangle &= U_{a_1} \mathcal{F}_d \otimes U_{a_2} \mathcal{F}_d \otimes \cdots \otimes U_{a_n} \mathcal{F}_d \otimes I_d \mathcal{F} |\text{GHZ}\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} U_{a_1} \mathcal{F}_d |j\rangle_1 \otimes U_{a_2} \mathcal{F}_d |j\rangle_2 \otimes \cdots \otimes U_{a_n} \mathcal{F}_d |j\rangle_n \otimes I_d \mathcal{F}_d |j\rangle_{n+1} \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \left[\bigotimes_{i=1}^n \left(U_{a_i} \frac{1}{\sqrt{d}} \sum_{w_i=0}^{d-1} \exp\left(\frac{2\pi i j w_i}{d}\right) |w_i\rangle \right) \right. \\ &\quad \left. \otimes \left(I_d \frac{1}{\sqrt{d}} \sum_{w_{n+1}=0}^{d-1} \exp\left(\frac{2\pi i j w_{n+1}}{d}\right) |w_{n+1}\rangle \right) \right] \\ &= d^{-1/2} \sum_{j=0}^{d-1} d^{-(n-2)/2} \sum_{w_1, \dots, w_{n+1}} \exp\left[\frac{2\pi i j}{d} (w_1 + \cdots + w_{n+1})\right] \end{aligned}$$

$$\begin{aligned} & \times |w_1 \oplus a_1\rangle \otimes \cdots \otimes |w_n \oplus a_n\rangle \otimes |w_{n+1} \oplus 0\rangle \\ & = d^{-\frac{n}{2}} \sum_{W=0(\bmod d)} |w_1 \oplus a_1\rangle \otimes \cdots \otimes |w_n \oplus a_n\rangle \otimes |w_{n+1} \oplus 0\rangle, \end{aligned}$$

where $W = \sum_{i=1}^{n+1} w_i$ and $a_i \in \{0, 1\} \Rightarrow U_{a_i} \in \{I_d, U_s\}$. After this, each participant and the server measure their qudit in \mathcal{B} basis. Each participants announces the measurement result m_i to the server via a classical authenticated channel. The server calculates $\mathcal{C} = \sum_{i=1}^{n+1} m_i(\bmod d)$. If there are multiple senders, then $\mathcal{C} > 1$ and a collision is detected.

3.2 Secrecy

In this subsection, we analyze the secrecy of Protocol 1. If an eavesdropper wants to know the sender's identity, they should get the specific value of the participant's classified input. We characterize the security in two different scenarios: (i) the adversary or server attacks the protocol alone without any collaboration with the participants, and (ii) the adversary collaborates with t malicious participants to attack the anonymity of the honest participants.

In the first scenario, we assume the preshared GHZ qudit state and its method of sharing as mentioned in [17]. Any misadventure by the server or adversary can be detected easily during the distribution of GHZ state. Since there is no further communication on quantum channel in our protocol. So, Eve or server cannot perform the active attack. She has to rely on the passive attacks. The participants encode their information on their respective qudit states and then perform the measurements. The announced result by the participant has no information regarding the identity of the sender. Therefore, Eve or server cannot deduce any useful information about the identity of the sender. We can say that this protocol is robust against outside adversaries since Eve is unable to gain any information and the sender remains anonymous.

In the second scenario, Eve collaborates with t malicious participants to extract the honest participants' classified inputs. A malicious participant already has some information about the protocol. So, this kind of attack is more powerful and deserves more attention. Eve has access to the resources Q_t of malicious participants t . To gain useful information about honest participant's k private inputs, she can only utilize the resources Q_t of malicious participants and classical information announced by the honest participants k . However, this resource Q_t is not useful. Intuitively, the secret string possessed by the n parties satisfy $w_1 + w_2 + \cdots + w_n + w_{n+1} = 0(\bmod d)$. Since the honest participant's resource R_k is only known to them, we can conclude that Eve cannot get any one of the honest participant's string. In other words, she is unable to get the private inputs of honest participants with the resources of the malicious participants t .

Now we consider an unlikely scenario in which an adversary, after the encoding process, hijacks the quantum channel and gets the honest participants' resources R_k as well. She has the encoded state

$$|\hat{\Phi}\rangle = d^{-\frac{n}{2}} \sum_{W=0(\bmod d)} \bigotimes_{i=1}^n |w_i \oplus a_i\rangle \otimes |w_{n+1} \oplus 0\rangle.$$

As we know that after Fourier transform, the GHZ state transforms into a random string satisfying $w_1 + \cdots + w_n + w_{n+1} = 0(\bmod d)$. The private inputs are encrypted on these random strings. Since these conditions are similar to the quantum one-time pad scheme [1]

and provide the same unconditional security to this protocol. So even if the adversary has the honest participant's resources R_k , she cannot track the senders. This shows the tracelessness of the protocol. The only possibility for Eve is to know the sender's identity if all parties behave as senders at the same time. This event only happens with $1/2^{n-t}$ probability and this probability decreases as t decreases.

4 Conclusion

In this work, we have proposed a quantum anonymous collision detection (QACD) protocol, which is a prerequisite for quantum anonymous networks. This protocol efficiently detects the collision in case of multiple senders with the help of a server. The QACD protocol provides sender anonymity. This protocol also features tracelessness, which means that the encoding operation cannot be traced back to the encoding parties. Our proposed protocol is more efficient in terms of quantum resources than previously proposed protocols. Furthermore, security analysis showed that the proposed QACD protocol is robust against malicious participants and adversaries.

Acknowledgements

Not applicable.

Funding

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1A2C2007037) and the MSIT (Ministry of Science and ICT) ITRC (Information Technology Research Center) support program (IITP-2021-0-02046) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

AK contributed the idea. AK, UK, and JR developed the theory and wrote the manuscript. HS and KL improved the manuscript and supervised the research. All the authors contributed in analyzing and discussing the results and improving the manuscript. All authors read and approved the final manuscript.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 29 July 2021 Accepted: 22 November 2021 Published online: 07 December 2021

References

1. Deng F-G, Long GL. Secure direct communication with a quantum one-time pad. *Phys Rev A*. 2004;69(5):052319.
2. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Rev Mod Phys*. 2002;74(1):145.
3. Huang Z, Macchiavello C, Maccone L. Cryptographic quantum metrology. *Phys Rev A*. 2019;99(2):022314.
4. Ladd TD, Jelezko F, Laflamme R, Nakamura Y, Monroe C, O'Brien JL. Quantum computers. *Nature*. 2010;464(7285):45–53.
5. Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. *Phys Rev A*. 1999;59(3):1829–34.
6. Bell B, Markham D, Herrera-Martí D, Marin A, Wadsworth W, Rarity J, Tame M. Experimental demonstration of graph-state quantum secret sharing. *Nat Commun*. 2014;5(1):1–12.
7. Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation. In: 50th annual IEEE symposium on foundations of computer science. Los Alamitos: IEEE Comput. Soc.; 2009. p. 517–26.
8. Barz S, Kashefi E, Broadbent A, Fitzsimons JF, Zeilinger A, Walther P. Demonstration of blind quantum computing. *Science*. 2012;335(6066):303–8.
9. Dai H, Shen Q, Wang C-Z, Li S-L, Liu W-Y, Cai W-Q, Liao S-K, Ren J-G, Yin J, Chen Y-A, Zhang Q, Xu F, Peng C-Z, Pan J-W. Towards satellite-based quantum-secure time transfer. *Nat Phys*. 2020;16:848–52.
10. Ben-Or M, Crépeau C, Gottesman D, Hassidim A, Smith A. Secure multiparty quantum computation with (only) a strict honest majority. In: 47th annual IEEE symposium on foundations of computer science (FOCS'06). Los Alamitos: IEEE Comput. Soc.; 2006. p. 249–60.

11. Kimble HJ. The quantum Internet. *Nature*. 2008;453(7198):1023.
12. Wehner S, Elkouss D, Hanson R. Quantum Internet: a vision for the road ahead. *Science*. 2018;362:6412.
13. Vaccaro JA, Spring J, Chefles A. Quantum protocols for anonymous voting and surveying. *Phys Rev A*. 2007;75(1):012333.
14. Jiang L, He G, Nie D, Xiong J, Zeng G. Quantum anonymous voting for continuous variables. *Phys Rev A*. 2012;85(4):042309.
15. Bao N, Halpern NY. Quantum voting and violation of arrow's impossibility theorem. *Phys Rev A*. 2017;95(6):062306.
16. Hahn F, de Jong J, Pappa A. Anonymous quantum conference key agreement. *PRX Quantum*. 2020;1(2):020325.
17. Huang W, Wen Q-Y, Liu B, Su Q, Qin S-J, Gao F. Quantum anonymous ranking. *Phys Rev A*. 2014;89(3):032325.
18. Khan A, ur Rehamn J, Shin H. Quantum anonymity for quantum networks. 2020. [2007.11176](https://doi.org/10.21203/rs.3.rs-11176).
19. Christandl M, Wehner S. Quantum anonymous transmissions. In: International conference on the theory and application of cryptography and information security. Berlin: Springer; 2005. p. 217–35.
20. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys Rev Lett*. 1993;70(13):1895.
21. Bouda J, Sprocar J. Anonymous transmission of quantum information. In: 2007 first international conference on quantum, nano, and micro technologies (ICQNM'07). 2007. p. 12–12.
22. Yang W, Huang L, Song F. Privacy preserving quantum anonymous transmission via entanglement relay. *Sci Rep*. 2016;6:26762.
23. Lipinska V, Murta G, Wehner S. Anonymous transmission in a noisy quantum network using the W state. *Phys Rev A*. 2018;98(5):052320.
24. Unnikrishnan A, MacFarlane IJ, Yi R, Diamanti E, Markham D, Kerenidis I. Anonymity for practical quantum networks. *Phys Rev Lett*. 2019;122(24):240501.
25. Pappa A, Chailloux A, Wehner S, Diamanti E, Kerenidis I. Multipartite entanglement verification resistant against dishonest parties. *Phys Rev Lett*. 2012;108(26):260502.
26. McCutcheon W, Pappa A, Bell B, McMillan A, Chailloux A, Lawson T, Mafu M, Markham D, Diamanti E, Kerenidis I et al. Experimental verification of multipartite entanglement in quantum networks. *Nat Commun*. 2016;7(1):1–8.
27. Lo H-K. Insecurity of quantum secure computations. *Phys Rev A*. 1997;56(2):1154.
28. Buhrman H, Christandl M, Schaffner C. Complete insecurity of quantum protocols for classical two-party computation. *Phys Rev Lett*. 2012;109(16):160501.

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► [springeropen.com](https://www.springeropen.com)