Securing communication in quantum anonymous networks

The demand for secure network communication is increasing as online fraud and cybercrime pose threats to users' security and data confidentiality. Awais Khan, Dr Junaid ur Rehman and Professor Hyundong Shin, from the Kyung Hee University, Korea, have developed two key protocols for quantum anonymous network communication: the quantum anonymous collision detection (QACD) protocol and quantum anonymous notification (QAN) protocol. This research paves the way for secure quantum anonymous communication across quantum networks.

With the continuing proliferation of the internet comes the vast demand for secure communication across networks. The troubling upsurge in online fraud and cybercrime pose threats to users' security and data confidentiality. A good deal of attention has been paid to protecting the contents of messages to ensure that encrypted information can only be accessed by the sender and recipient. On the other hand, less consideration has been given to the users' anonymity, even though concealing the identities of both sender and receiver is a sought-after requirement for communication networks.

Communication using classical computers involves sending data and keys as bits, but these transmissions are vulnerable as hackers can read and copy them without leaving a trace. Quantum mechanics presents novel opportunities for an assortment of information-processing tasks in both communication and computational networks. Quantum information science makes it possible to significantly improve security for communication, with quantum communication systems offering many benefits – derived from their use of the laws of quantum physics – to protect data. A key advantage from a cybersecurity perspective is that if a hacker attempts to tamper with quantum bits, also known as qubits, that represent many combinations of 1s and 0s, their fragile quantum state collapses to 1 or 0, leaving evidence of the activity.

sakkmesterke/Shutterstock.com

Quantum network-based applications, such as quantum secret sharing and quantum conference key agreements, have been proposed with the inviting prospect of an ultra-secure quantum internet. A challenging requirement of quantum networks, however, is establishing the anonymity of both the sender and the receiver when they communicate through the network. Classical communication protocol anonymity is either predicated on the scheme's computational complexity or the limit of the adversary's computational power when compared with what is classically achievable. The algorithmic acceleration afforded by quantum computers presents a colossal threat to computational complexity-based anonymity.

Through their innovative research into anonymity in quantum networks, Awais Khan, Dr Junaid ur Rehman, and Professor Hyundong Shin, from the Department of Electronics and Information Convergence Engineering at the Kyung Hee University in Korea, are aiming to build a quantum anonymous network that can provide anonymity without putting any constraints on the adversaries computing power. So far, they have developed two key protocols for quantum anonymous communication: the quantum anonymous collision detection protocol and the quantum anonymous notification protocol.

QUANTUM ANONYMOUS COLLISION DETECTION PROTOCOL

Network collisions occur when two or more devices try to transmit over a network at the same time. Without a suitable protocol in place, the data will collide, becoming corrupted and rendering the transmission unsuccessful. Over the past two decades, the concept of quantum anonymity has been proposed for several networking tasks with the goal of providing complete secrecy for those sending and receiving communications. Existing protocols for anonymity in quantum networks, developed prior to this research, all require the detection of multiple senders. The researchers draw attention to the fact that to perform an anonymous execution of these anonymous networking tasks, an anonymous collision detection protocol is required.


Lightspring/Shutterstock.com

Concealing the identities of sender and receiver is a desired requirement for communication networks.

The researchers have developed the first quantum anonymous notification protocol that can deliver anonymity for both senders and receivers.

The researchers have developed a quantum anonymous collision detection (QACD) protocol that can detect collisions when simultaneous server interactions are performed by multiple users communicating over a network. The QACD protocol both detects collisions and guarantees anonymity for each of the many senders using the server. In addition, it has a tracelessness property that ensures that even if the adversary manages to gain access to the encoded state, the sender's identity remains hidden. It is important to note that tracelessness is not possible with regular network communication.

The QACD protocol can be implemented for any quantum anonymous network and will anonymously detect collisions with the help of the server. The researchers explain that the server in the QACD protocol 'is allowed to misbehave through active and passive attack but cannot conspire with the participants'. The server, however, is not able to match the identity of the senders or the receivers with the encoded data.

QACD PROTOCOL FEATURES

A Greenberger–Horne–Zeilinger (GHZ) state is an entangled quantum state made up of at least three subsystems that possesses extremely non-classical properties. The research team has established that while the GHZ state is shared correctly the QACD protocol has the following four attributes: correctness in that each party is notified when there are multiple senders involved in a run of the protocol; anonymity so that the senders' identities are always kept secret; tracelessness, ensuring that even if an adversary has access to all the network resources, including the encoded communication both in its classical and quantum states, the sender/recipient status of all participants remains


sdecoret/Shutterstock.com

Quantum information science promises to significantly enhance online security.

The research lays the foundation for enhanced security across quantum networks.

concealed; security, making sure that the private data pertaining to all involved parties is safeguarded against attacks.

The research team show how their new QACD protocol is more efficient than the previous protocols in terms of quantum resources. Moreover, their security analysis demonstrates the security and correctness of the QACD protocol together with its robustness against both internal and external adversaries.

QUANTUM ANONYMOUS NOTIFICATION PROTOCOL

The researchers have developed the first ever quantum anonymous notification (QAN) protocol that can deliver anonymity for both senders and receivers using practical quantum networks. The QAN protocol lets an anonymous sender notify another anonymous party about an upcoming communication task without revealing their identity. It is impossible to trace the notifier once the notification is encoded. Like the QACD protocol, QAN includes tracelessness, so even if all the network resources become available to an adversary, the encoding operations cannot be traced back to the encoding party.

PRACTICAL DEMONSTRATION OF THE QAN PROTOCOL

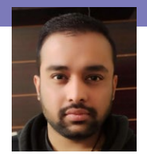
In addition to proving the anonymity and traceless properties of the QAN protocol, the research team provide a practical demonstration. They employ an IBM quantum computer with a five-qubit noisy intermediate-scale quantum (NISQ) processor to benchmark the protocol's performance. Using a four-node network where the fourth node can receive notifications sent by any of the other three parties, they execute the QAN protocol 8,192 times and calculate the probability for each of the experimental outcomes. Then they compared the results with their theoretical calculations and the results produced by an IBM QASM simulator, a high-performance quantum simulator for quantum circuits. The simulation confirmed the theoretical results, with both producing a success probability of 1. In the realistic noisy conditions of the experiment the probability of success is 0.862; the shortfall is due to device error since quantum processors are very sensitive to the environment and can lose their quantum state in noisy situations.

Over the past two decades, the concept of quantum anonymity has been proposed for several important networking tasks.

SECURE QUANTUM ANONYMOUS COMMUNICATION

This is the first quantum anonymous notification protocol that introduces anonymity and lays the foundations for secure quantum anonymous communication across quantum networks, paving the way towards an ultra-secure quantum internet. The research team has shown that the QAN protocol provides anonymity for both the sender and the receiver. Furthermore, it is easy to modify the protocol so that only the sender, or the receiver, is afforded anonymity based on the application's requirements. The security analysis verifies that the QAN protocols are robust against malicious attacks from both within and outside the networks. The practical application of the QAN protocol on IBM NISQ computing devices confirms the protocol's performance in realistic scenarios. The QAN protocol will be of interest to other researchers and developers as a powerful component for many network applications, ranging from multiparty quantum computation to quantum internet.

Behind the Research



Awais Khan

Dr Junaid ur Rehman

Professor Hyundong Shin

E: hshin@khu.ac.kr **T:** +82 31 201 3812

Research Objectives

Awais Khan, Dr Junaid ur Rehman, and Professor Hyundong Shin research the field of quantum information science; specifically, the development and applications of quantum anonymous network protocols.

Detail

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

Bio

Awais Khan is a PhD student at the Department of Electronics and Information Convergence Engineering, Kyung Hee University, Korea. His research interests include quantum anonymous networks, quantum communications and computation, and quantum information science.

Junaid ur Rehman, PhD is a research professor in the Department of Electronics and Information Convergence Engineering, Kyung Hee University, Korea. His research interests include general quantum channel models, quantum communications, and quantum process tomography techniques.

Hyundong Shin, PhD is a professor in the Department of Electronics and Information Convergence Engineering, Kyung Hee University, Korea. He is the director and founder of Communication and Coding Theory Laboratory (CCTLAB). His research interests include quantum information science, wireless communication, and machine intelligence.

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

References

Khan, A, ur Rehman, J, Shin, H, (2021) Quantum anonymous notification for network-based applications. *Quantum Inf Process*, [online] 20, 397. doi.org/10.1007/s11128-021-03339-y

Khan, A, Khalid, U, ur Rehman, J, Lee, K, Shin, H (2021) Quantum anonymous collision detection for quantum networks. *EPJ Quantum Technology*. [online] 8, 27. doi.org/10.1140/epjqt/s40507-021-00116-9

Personal Response

What other applications of quantum anonymous communication are you currently working on?

" Privacy means ensuring confidentiality while gathering, storing, and transferring data over the network. The requirement for user data privacy in network queries motivated the field of private information retrieval (PIR). Classical PIR gave the security definition of classical single-server PIR protocols in terms of computational complexity. Incorporating quantum resources in PIR protocols significantly reduces communication and computational complexity. However, such inclusions still lack absolute information-theoretic security in single-server cases. Anonymity might provide a security layer in such single-server, multi-user network scenarios. Currently, we are developing the quantum anonymous private information retrieval (QAPIR) protocol which entails both privacy and anonymity as a security instrument in distributed networks. "