PHYS.ORG

Practical anonymous communication protocol developed for quantum networks

August 21 2019, by Lisa Zyga

Credit: Laurentiu Robu, pexels.com

The ability to securely transmit information over the internet is extremely important, but most of the time, eavesdroppers can still generally determine who the sender and receiver are. In some highly confidential situations, it is important that the sender's and receiver's identities remain anonymous.

Over the past couple of decades, researchers have been developing protocols for anonymously transmitting messages over classical networks, but similar protocols for quantum networks are still in much earlier stages of development. The anonymity methods that have been proposed for quantum networks so far face challenges such as implementation difficulties or require that strong assumptions be made about the resources, making them impractical for use in the real world.

In a new paper, Anupama Unnikrishnan, Ian MacFarlane, Richard Yi, Eleni Diamanti, Damian Markham, and Iordanis Kerenidis, from the University of Oxford, MIT, Sorbonne University, the University of Paris and CNRS, have proposed the first practical protocol for anonymous communication in quantum networks.

"Our protocol brings anonymous quantum communication closer to being actually demonstrated in the lab," Unnikrishnan told *Phys.org*. "We can guarantee anonymity in the most paranoid scenario: without needing to trust the honesty or computational power of players in the network, or even the entanglement they share."

The new protocol works in the following way. To start, the player who wants to send a message anonymously notifies the receiver. Then, in each round of the protocol, an untrusted source creates an entangled quantum state called the Greenberger-Horne-Zeilinger (GHZ) state, and distributes it between the players.

The players then have two options: They can either check if the state is actually the GHZ state by running a verification test, or they can use the state for anonymous quantum communication. Most of the time, the players test the state. If a test fails, indicating a possible breach, the players stop the protocol. In this way, a misbehaving source is likely to get caught.

If the players chose to use the state for anonymous communication, they perform certain operations and measurements on their part of the GHZ state in order to create "anonymous entanglement" between the sender and receiver, so that they are now connected by an anonymous quantum channel. Using this channel, the sender can then use quantum teleportation to anonymously send a quantum message to the receiver.

The ability of the protocol to achieve perfect anonymity depends on the players performing perfect actions and sharing a perfect GHZ state. The researchers showed that, even in realistic networks with imperfections, the players can still communicate close to anonymously—within a security parameter epsilon, leading them to call their method an "epsilon-anonymous protocol."

In the future, the ability to anonymously transmit messages will be critical for many of the potential applications of a future quantum internet. However, much more work needs to be done in the meantime.

"We are looking into the experimental demonstration of the protocol in our lab and also in parallel into the conception of further protocols that can enrich the toolbox of applications offered by quantum networks," Diamanti said.

More information: Anupama Unnikrishnan, Ian J. MacFarlane, Richard Yi, Eleni Diamanti, Damian Markham, and Iordanis Kerenidis. "Anonymity for Practical Quantum Networks." *Physical Review Letters*. DOI: 10.1103/PhysRevLett.122.240501

Also at arXiv:1811.04729 [quant-ph]

Citation: Practical anonymous communication protocol developed for quantum networks (2019, August 21) retrieved 5 April 2024 from https://phys.org/news/2019-08-anonymous-protocol-quantum-networks.html