

"Quantum Holds the Key to Secure Conference Calls"

Submitted by grigby1 on Mon, 06/07/2021 - 4:03pm

A collaboration between Quantum Communications Hub researchers based at Heriot-Watt University and their German colleagues has brought the world a step closer towards ultimately secure conference calls. Their work has enabled a quantum-secured conversation to happen between four parties at the same time. This advancement is timely, given the rise in remote collaborative work, including conference calls, during the COVID-19 pandemic. This increase in remote collaborative work has come with a significant escalation of the launch of cyberattacks on popular teleconferencing platforms. The advancement in quantum-secured communications could enable unhackable security measures for conference calls, supported by quantum physics principles. The system demonstrated by the team employs entanglement, an essential property of quantum physics. Entanglement is a quantum physics property that provides correlations between two or more quantum systems, even when they are separated by large distances. By harnessing multi-party entanglement, the team was able to share cryptographic keys between four parties simultaneously, using a process called Quantum Conference Key Agreement. This allowed the team to overcome the limitations associated with traditional Quantum Key Distribution (QKD) that only allow the sharing of keys between two users. The defeat of these limitations enabled the first quantum conference call in which an image of a Cheshire cat was shared between four parties separated by up to 50 kilometers of optical fiber. This article continues to discuss the advancement that could lead to quantum-secured conference calls.

[Heriot-Watt University reports "Quantum Holds the Key to Secure Conference Calls"](#)
