Quantum holds the key to secure conference calls

The world is one step closer to ultimately secure conference calls, thanks to a collaboration between Quantum Communications Hub researchers and their German colleagues, enabling a quantum-secure conversation to take place between four parties simultaneously.

The demonstration, led by Hub researchers based at Heriot-Watt University and published in *Science Advances,* is a timely advance, given the global reliance on remote collaborative working, including conference calls, since the start of the C19 pandemic.

There have been reports of significant escalation of cyber-attacks on popular teleconferencing platforms in the last year. This advance in quantum secured communications could lead to conference calls with inherent unhackable security measures, underpinned by the principles of quantum physics.

Senior author, Professor Alessandro Fedrizzi, who led the team at Heriot-Watt said:

"We've long known that quantum entanglement, which Albert Einstein called 'spooky action at a distance' can be used for distributing secure keys. Our work is the first example where this was achieved via 'spooky action' between multiple users at the same time — something that a future quantum internet will be able to exploit."

Secure communications rely upon the sharing of cryptographic keys. The keys used in most systems are relatively short and can therefore be compromised by hackers, and the key distribution procedure is under increasing threat from quickly advancing quantum computers. These growing threats to data security require new, secure methods of key distribution.

A mature quantum technology called Quantum Key Distribution (QKD), deployed in this demonstration in a network scenario for the first time, harnesses the properties of quantum physics to facilitate guaranteed secure distribution of cryptographic keys.

QKD has been used to secure communications for over three decades, facilitating communications of over 400km over terrestrial optical fibre and recently even through space, however, crucially, these communications have only ever occurred exclusively between two parties, limiting the practicality of the technology used to facilitate secure conversations between multiple users.

The system demonstrated by the team here utilises a key property of quantum physics, entanglement, which is the property of quantum physics that gives correlations – stronger than any with which we are familiar in everyday life – between two or more quantum systems, even when these are separated by large distances.

By harnessing multi-party entanglement, the team were able to share keys simultaneously between the four parties, through a process known as 'Quantum Conference Key Agreement', overcoming the limitations of traditional QKD systems to share keys between just two users, and enabling the first quantum conference call to occur with an image of a Cheshire cat shared between the four parties, separated by up to 50 km of optical fibre.

Entanglement-based quantum networks are just one part of a large programme of work that the Quantum Communications Hub is undertaking to deliver future quantum secured networks.

The technology demonstrated here has potential to drastically reduce the resource costs for conference calls in quantum networks when compared to standard two-party QKD methods. It is one of the first examples of the expected benefits of a future quantum internet, which is expected to supply entanglement to a system of globally distributed nodes.

Notes to editors:

Quantum Communications Hub

The EPSRC Quantum Communications Hub is a synergistic partnership of ten UK universities, numerous private sector companies and public sector bodies that have come together in a unique collaboration to exploit fundamental laws of quantum physics for the development of secure communications technologies and services. The overall vision of the Hub is to deliver quantum secured communication technologies at all distance scales, offering a range of applications and services with the potential for integration with existing infrastructure. The project is part of a major national initiative, the UK National Quantum Technologies Programme, which aims to ensure the successful transition of quantum technologies from laboratory to industries. For more information about the work of the Hub, please visit https://www.quantumcommshub.net/.

UK National Quantum Technologies Programme

The National Quantum Technologies Programme (NQTP) was established in 2014 and has EPSRC, IUK, STFC, MOD, NPL, BEIS, and GCHQ as partners. Four Quantum Technology Hubs were set up at the outset, each focussing on specific application areas with anticipated societal and economic impact. The Commercialising Quantum Technologies Challenge (funded by the Industrial Strategy Challenge Fund) is part of the NQTP and was launched to accelerate the development of quantum enabled products and services, removing barriers to productivity and competitiveness.

The NQTP is set to invest £1B of public and private sector funds over its ten-year lifetime.

For more information about the NQTP, please visit https://uknqt.ukri.org/.