Revolutionary quantum breakthrough paves way for safer online communication

Press release issued: 2 September 2020

The world is one step closer to having a totally secure internet and an answer to the growing threat of cyber-attacks, thanks to a team of international scientists who have created a unique prototype which could transform how we communicate online.

The quantum physics experiment has demonstrated an important step towards quantum cryptography between many users, an essential requirement for a secure quantum internet.

Image Credit: Copyright ÖAW /Klaus Pichler

The invention led by the University of Bristol, revealed today in the journal *Science Advances*, has the potential to serve millions of users, is understood to be the largest-ever quantum network of its kind, and could be used to secure people's online communication, particularly in these internet-led times accelerated by the COVID-19 pandemic.

By deploying a new technique, harnessing the simple laws of physics, it can make messages completely safe from interception while also overcoming major challenges which have previously limited advances in this little used but much-hyped technology.

Lead author Dr Siddarth Joshi, who headed the project at the university's Quantum Engineering Technology (QET) Labs, said: "This represents a massive breakthrough and makes the quantum internet a much more realistic proposition. Until now, building a quantum network has entailed huge cost, time, and resource, as well as often compromising on its security which defeats the whole purpose."

"Our solution is scalable, relatively cheap and, most important of all, impregnable. That means it's an exciting game changer and paves the way for much more rapid development and widespread rollout of this technology."

The current internet relies on complex codes to protect information, but hackers are increasingly adept at outsmarting such systems leading to cyber-attacks across the world which cause major privacy breaches and fraud running into trillions of pounds annually. With such costs projected to rise dramatically, the case for finding an alternative is even more compelling and quantum has for decades been hailed as the revolutionary replacement to standard encryption techniques.

So far physicists have developed a form of secure encryption, known as quantum key distribution, in which particles of light, called photons, are transmitted. The process allows two parties to share, without risk of interception, a secret key used to encrypt and decrypt information. But to date this technique has only been effective between two users.

“Until now efforts to expand the network have involved vast infrastructure and a system which requires the creation of another transmitter and receiver for every additional user. Sharing messages in this way, known as trusted nodes, is just not good enough because it uses so much extra hardware which could leak and would no longer be totally secure,” Dr Joshi said.

The team’s quantum technique applies a seemingly magical principle, called entanglement, which Albert Einstein described as ‘spooky action at a distance.’ It exploits the power of two different particles placed in separate locations, potentially thousands of miles apart, to simultaneously mimic each other. This process presents far greater opportunities for quantum computers, sensors, and information processing.

“Instead of having to replicate the whole communication system, this latest methodology, called multiplexing, splits the light particles, emitted by a single system, so they can be received by multiple users efficiently,” Dr Joshi said.

The team created a network for eight users using just eight receiver boxes, whereas the former method would need the number of users multiplied many times – in this case, amounting to 56 boxes. As the user numbers grow, the logistics become increasingly unviable – for instance 100 users would take 9,900 receiver boxes.

To demonstrate its functionality across distance, the receiver boxes were connected to optical fibres via different locations across Bristol and the ability to transmit messages via quantum communication was tested using the city’s existing optical fibre network.

“Besides being completely secure, the beauty of this new technique is its streamline agility, which requires minimal hardware because it integrates with existing technology,” Dr Joshi said.

The team’s unique system also features traffic management, delivering better network control which allows, for instance, certain users to be prioritised with a faster connection.

Whereas previous quantum systems have taken years to build, at a cost of millions or even billions of pounds, this network was created within months for less than £300,000. The financial advantages grow as the network expands, so while 100 users on previous quantum systems might cost in the region of £5 billion, Dr Joshi believes multiplexing technology could slash that to around £4.5 million, less than 1 per cent.

In recent years quantum cryptography has been successfully used to protect transactions between banking centres in China and secure votes at a Swiss election. Yet its wider application has been held back by the sheer scale of resources and costs involved.

“With these economies of scale, the prospect of a quantum internet for universal usage is much less far-fetched. We have proved the concept and by further refining our multiplexing methods to optimise and share resources in the network, we could be looking at serving not just hundreds or thousands, but potentially millions of users in the not too distant future,” Dr Joshi said.

“The ramifications of the COVID-19 pandemic have not only shown importance and potential of the internet, and our growing dependence on it, but also how its absolute security is paramount. Multiplexing entanglement could hold the vital key to making this security a much-needed reality.”

The research received funding from the Quantum Communications Hubs of the Engineering and Physical Science Research Council (EPSRC), Ministry of Science and Education (MSE) of Croatia, and the Austrian Research Promotion Agency (FFG).

Collaborating institutions with the University of Bristol are the University of Leeds, Croatia's Ruder Boskovic Institute (RBI) in Zagreb, Austria's Institute for Quantum Optics and Quantum Information (IQOQI), in Vienna, and China's National University of Defence Technology (NUDT) in Changsha.

Paper:

'A trusted node-free eight-user metropolitan quantum communication network,' by Siddarth Koduru Joshi et al in *Science Advances.*