QUANTUM KEY DISTRIBUTION:

What is the opportunity in ICT?

Quantum computers will one day be able to crack current data encryption, creating major security risks to the world's information. Quantum safe approaches – Quantum Key Distribution (QKD) and post-quantum algorithms - will be needed for many secure communications. In order to ensure that business and government can continue to securely use electronic communications, the ICT industry needs to develop real world capabilities in QKD, and so support the world's businesses to make this transition to post-quantum security.

Why does QKD matter to the ICT sector?

Companies and governments rely on being able to encrypt data for secure information sharing, from financial transactions, to sharing health records, to managing smart grids. They turn to the ICT industry to install and manage the systems that deliver this encryption. In a post-quantum world, it will be vital that the ICT industry has quantum safe encryption, including QKD, as part of its arsenal.

QKD will need physical integration into network infrastructure, as well as accompanying software to deploy it effectively. The ICT industry will be required to both develop new QKD products, and to deliver them as part of an integrated network solution. Those that get involved early will find themselves leading the sector when QKD reaches commercial maturity.

> **"It has taken almost two decades to deploy our modern public key cryptography infrastructure. Regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing."**
>
> *The US National Institute of Standards and Technology (NIST)*

Where are we now and where are we going?

Companies including Toshiba and ID Quantique have already developed photon emitters and detectors capable of communicating using encoded photons over fibre. Bristol-based KETS is developing chip-scale QKD which could be integrated into handheld devices. The UK Quantum Network provides fibre links within and between Cambridge and Bristol, allowing quantum technologies to be tested on real world infrastructure.

Commercial offerings are already viable in highly secure applications, where the benefit of securing information from future hacking outweighs the current cost. A number of projects are exploring QKD links between secure corporate networks and data centres, for example.

Over the next five years significant work will go into improving transmission rates and reducing size, weight and power - and of course cost - of quantum devices, bringing QKD solutions closer to market, and leading to the first commercial use cases.

WHAT IS QKD?

In conventional encryption, data is encrypted using an algorithm, making it unintelligible to anyone who steals it. The algorithm also generates a key – a long string of random numbers – which allows the intended receiver to decrypt the data. This is secure for now, but such algorithms could be cracked in future by quantum computers.

In QKD, this key is physically distributed using a sequence of photons, whose quantum state is assigned randomly to represent a 0 or a 1. The physical approach means the key cannot be cracked mathematically. It is also impossible to copy or steal the key in transit, since quantum mechanics dictates that any observation will change the quantum state – which can be detected by the receiver.

WHO'S INNOVATING IN ICT?

BT is making a big drive into QKD, which it sees as a potentially revolutionary technology that could transform network security.

BT is developing systems based on commercial fibre, with extra channels for sending the QKD key. Medium term, it sees opportunities to sell Openreach access solutions with integrated QKD to provide highly secure communications between sites, or bespoke links such as those between a bank and a datacentre. Through partnerships with technology providers, BT hopes to eventually offer complete managed network solutions.

Ultimately QKD could be at the heart of ubiquitous Quantum-Safe Cryptography that underpins the world's secure communications, so BT wants to be ahead of the game.

How to get involved

The UK Quantum Network launched in 2019, connecting Cambridge, Bristol and BT's Adastral Park. This provides a testbed, comparable to national communications infrastructure, on which ICT companies can test and validate new quantum communications devices such as transmitters and receivers, and work with current innovators to learn about the practicalities of real-world deployment.

Significant investment is being made to support industry led projects that advance QKD and related technologies. The Industrial Strategy Challenge Fund (ISCF), is investing £153million in the *Commercialising Quantum Technologies* challenge. This includes areas of focus on Secure Encryption and Keeping Data Safe[1].

It is important that eventual commercial products meet the needs of end users. By talking to us about their challenges, and engaging with the companies in our network, the ICT industry can help ensure QKD meets the needs of its customers.

Those interested in being involved in these projects, receiving updates, or finding out more should contact:

enquiries@quantumcommshub.net
www.quantumcommshub.net

QUANTUM COMMUNICATIONS HUB

1 https://www.ukri.org/innovation/industrial-strategy-challenge-fund/quantum-technologies/