Introducing Quantum Cryptography: The What, When and How

At a time when technological advances have created an almost constant state of data proliferation, the need for the secure transmission of sensitive information has never been more significant. In fact, Cisco predicts mobile data traffic to increase sevenfold between 2016 and 2021. IT decision-makers evidently recognise this challenge, with the latest research from Toshiba revealing that, for over half (52%) of businesses in Europe, data security is a top three investment priority for the year ahead. Yet despite this, businesses often fall behind in keeping themselves aware and ahead of cyber-security trends and developments.

Enter quantum cryptography, which, by harnessing the principles of quantum physics, has the ability to usher in a new age of secure online communication. But what exactly is quantum cryptography, what problems does it solve, and how can it fill the gaps in online defences to enable businesses to stay one step ahead of any complex threats, now and in the future?

How does quantum cryptography work?

“Simply put, quantum cryptography provides a secure means for generating and distributing secret keys between two parties on an optical network,” says Dr. Andrew Shields, Assistant Managing Director at Toshiba’s Research Laboratory in Cambridge. “By harnessing the inherent unpredictability in the state of particles, like electrons or photons, quantum cryptography can be used to generate the random numbers needed for cryptographic applications. Furthermore, by sending streams of encoded single photons through an optical communication network, it is possible to share a secret digital key that can be used for encrypting or authenticating information.”

Why do we need it? Quantum cryptography now and in the future

It is widely considered today that public key encryption is an essential part of data security, but that’s being challenged by new attack strategies and the emergence of quantum computers that will ultimately render much of today’s encryption unsafe. Today’s security challenges and tomorrow’s security fears are driving the adoption of reliable quantum cryptography solutions and services to enable better data security.

As a result, the global quantum cryptography market is forecast to grow from USD 285.7 Million in 2017 to USD 943.7 Million by 2022, a CAGR of 27%. Yet quantum cryptography’s arrival is not as close to fruition nor as widely acknowledged within relevant fields. This doesn’t detract from its essential and unparalleled value as we move into the quantum age, so how far away from quantum cryptography are we, and what needs to be progressed in order to achieve this?

When will it reach the mainstream?

While not yet commercially available, scientists are now at the stage of being able to deploy the technology and demonstrate its benefits. Toshiba’s Cambridge Research Laboratory recently published a paper explaining a breakthrough made using a protocol known as Twin-Field QKD, extending the range of QKD to over 500 kilometres of standard telecom fibre.

“This opens up the potential for secure communication between cities such as London, Paris, Dublin, Manchester and Amsterdam. Beyond this, a number of large collaborative projects such as the Innovate UK EQUIP project and the EU Commission’s Horizon 2020 programme are also working to develop the technology and make QKD an accessible, valuable tool for the enterprise,” Dr. Shields said.

Beyond the desire for IT decision makers to keep their data secure when in transit from A to B, so too is legislation changing to make it the law that data concerning a person’s identity is kept safe, with the General Data Protection Regulation (GDPR) a prime example of this. Coupled with growing and diversifying cyber threats and the difficulties associated with data security, as well as the need for a new standard in protecting such information, QKD can be the pivotal tool in making sure data is kept safe and secure.

Planning for the future

Quantum cryptography has great potential to become the key technology for protecting communication infrastructure from cyber-attacks and putting businesses on the front foot when it comes to protecting operation-critical information. Unlike other existing security solutions, quantum cryptography is secure from all future advances in mathematics and computing, even from the number crunching abilities of a quantum computer. Standardisation of QKD protocols remains essential for commercialised quantum cryptography. The need to enable interoperability of technologies, develop the components market as well as processes and technology, will reduce the costs of creation and deployment of QKD and see the commencement of a more secure future for all of us.