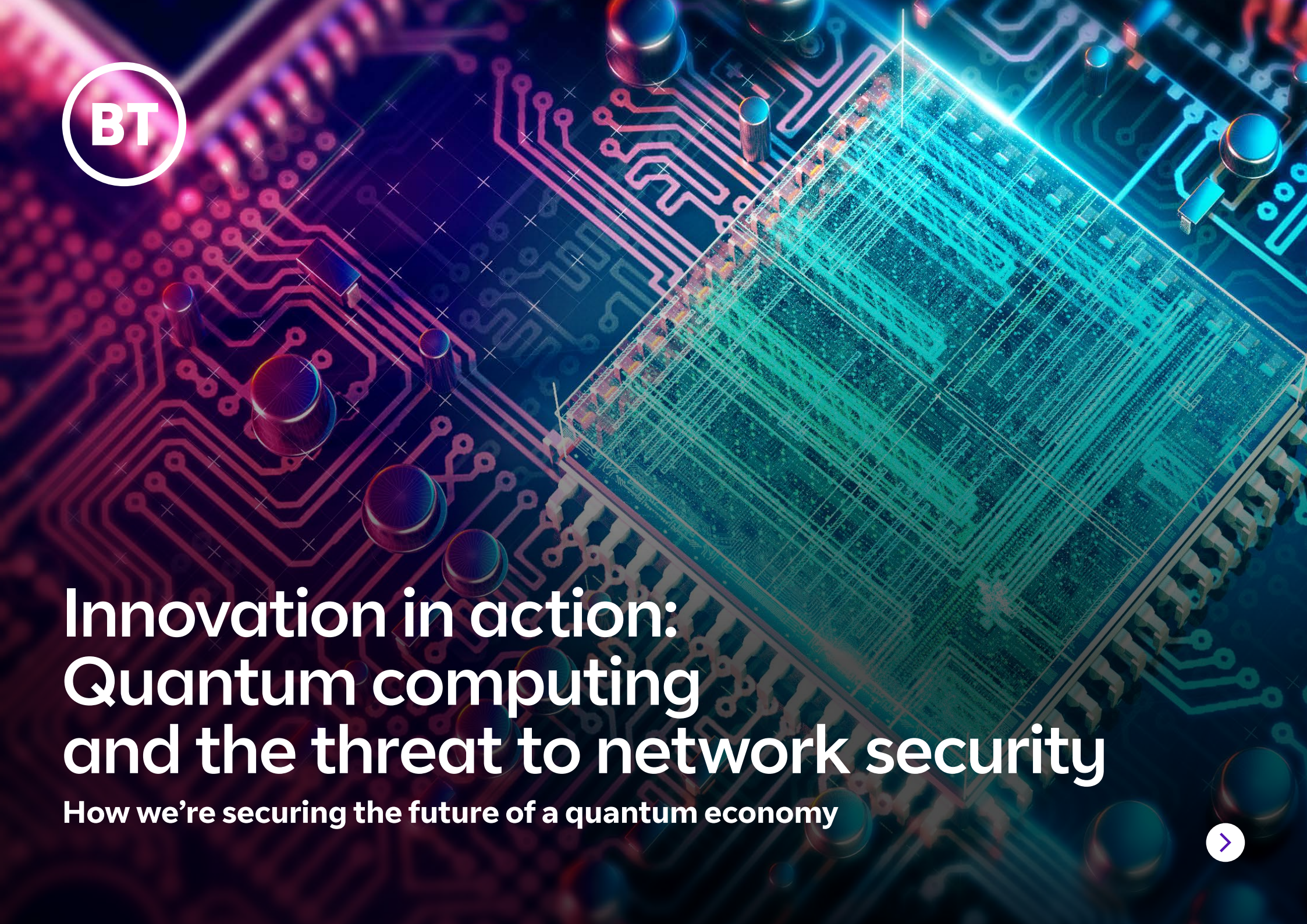


Innovation in action: Quantum computing and the threat to network security

How we're securing the future of a quantum economy

Preparing for an evolving quantum environment

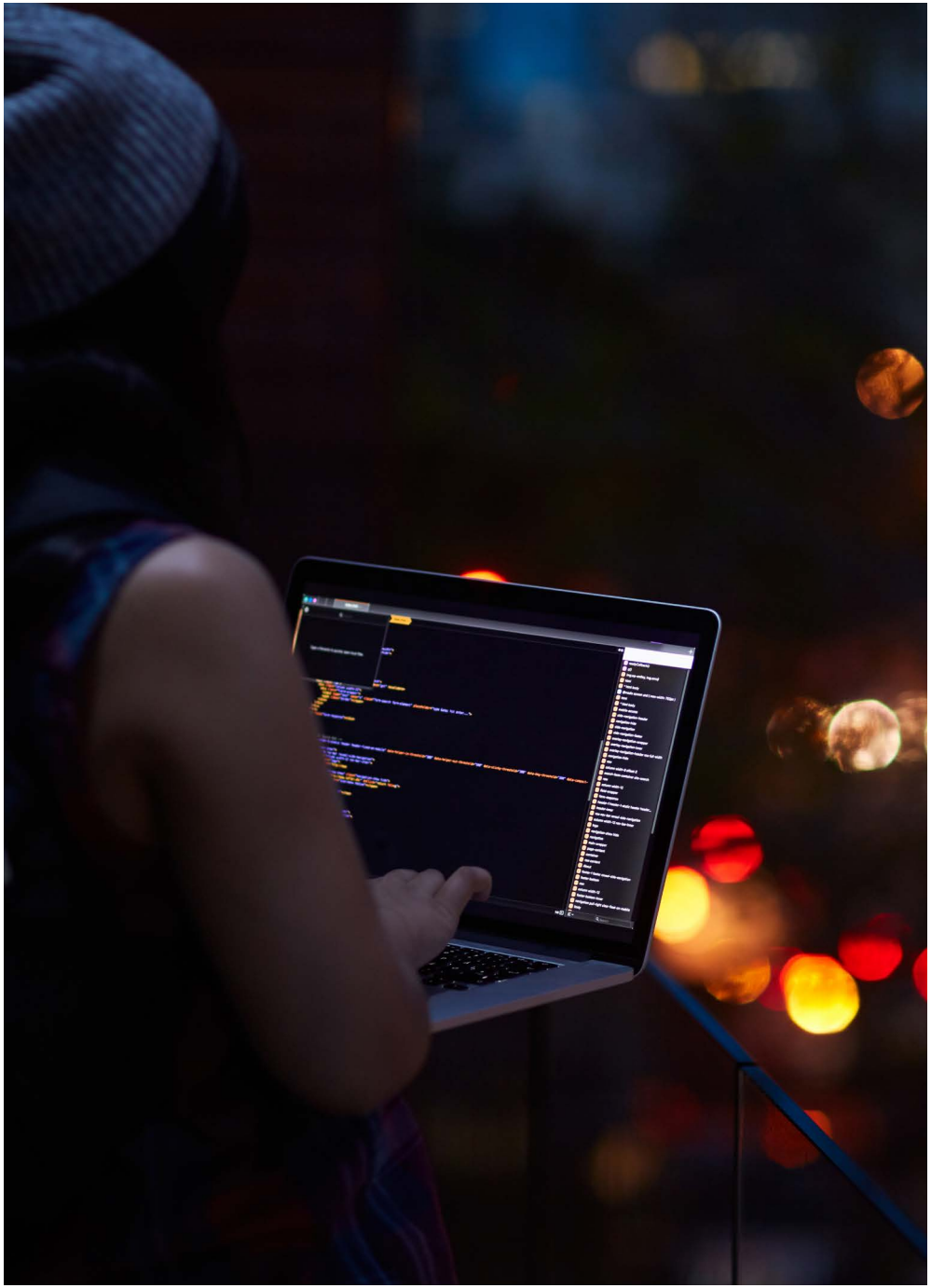
We're now at a point where companies and research institutions are announcing plans that make the prospect of capable, real-world quantum computers a likely development. So, it's time to talk about our purposeful innovation, centred on quantum technology, that we've been quietly working on since 2013.

Our ambition is to be the world's most trusted connector, and part of achieving that goal is taking an active role in determining the future of connections. However, because the future has yet to evolve into definite scenarios, we keep a watching brief over all possible avenues, as well as the balance between hype versus reality.

This way we'll always be ready to turn challenger technologies into the next generation of connection, future-proofing our business, our infrastructure and our customers' organisations.

We're actively exploring a range of new solutions that address current and future threats and a secure digital infrastructure is at the heart of our plan for quantum technologies. Our quantum technology approach brings together the best of UK and international collaboration, and sees us working as a key contributor to the UK National Quantum Technologies Programme (NQTP).

At this point, quantum computing has significant potential for a broad range of industries, including financial services, professional services, health and life sciences, government and manufacturing. Our focus now is on turning quantum innovation into services that secure data in the long term for our customers, to protect connections and digital communications.



Why quantum computing is one to watch

Quantum computing uses the laws of quantum mechanics to solve problems that are too complex for conventional computers.

Quantum bits (or qubits) are the basic unit of information in quantum computing but, unlike the traditional bit, it can be a one, a zero or both at the same time. Furthermore, these qubits can be entangled into multi-qubit states, enabling powerful quantum computation. A quantum computer is capable of solving certain mathematical problems which cannot be efficiently processed on a conventional computer.

For certain types of problem, quantum computers have the potential to be more powerful than a conventional computer could ever be, enabling organisations to solve some of their largest and most complex business problems.

Quantum computing is one to watch because it has the potential to be able to crack the mathematics that underpin much of the current cryptography that's used to secure networks. The type of algorithms that are most affected are 'asymmetric' algorithms used in key exchange, digital signatures and Public Key Infrastructure (PKI) certificate-based authentication.

There's a risk of 'hack-today, crack-tomorrow' attacks, where key exchanges and digital signatures made today could be at risk of retrospective attacks, even after the key has been used, or certificate has expired, once capable quantum computers are available.

For key delivery, the key exchange process together with encrypted traffic could be eavesdropped and stored, and a quantum computer could later extract the key and decrypt the traffic involved.

For digital signatures, an adversary could reverse engineer the private key used to sign a digital asset in the past, and be able to make changes to that digital asset or create a new signed digital asset apparently from the past.

Developing Post-Quantum Cryptography (PQC)

Global action is underway

The threat of large-scale quantum computers is well understood and has been emphasised by many national cybersecurity and defence authorities. It's high on the agenda of the National Cyber Security Centre, the Defence Science and Technology Laboratory, and international governmental and standards organisations like standards organisation ETSI, the Internet Engineering Task Force and the National Institute of Standards and Technology (NIST).

The urgency to plan for post-quantum defences is also evident. In January 2022, the US President signed an Executive Order that included a requirement for all US federal agencies to launch preparation for replacing quantum-vulnerable asymmetric algorithms from their IT systems with PQC alternatives, within 180 days.

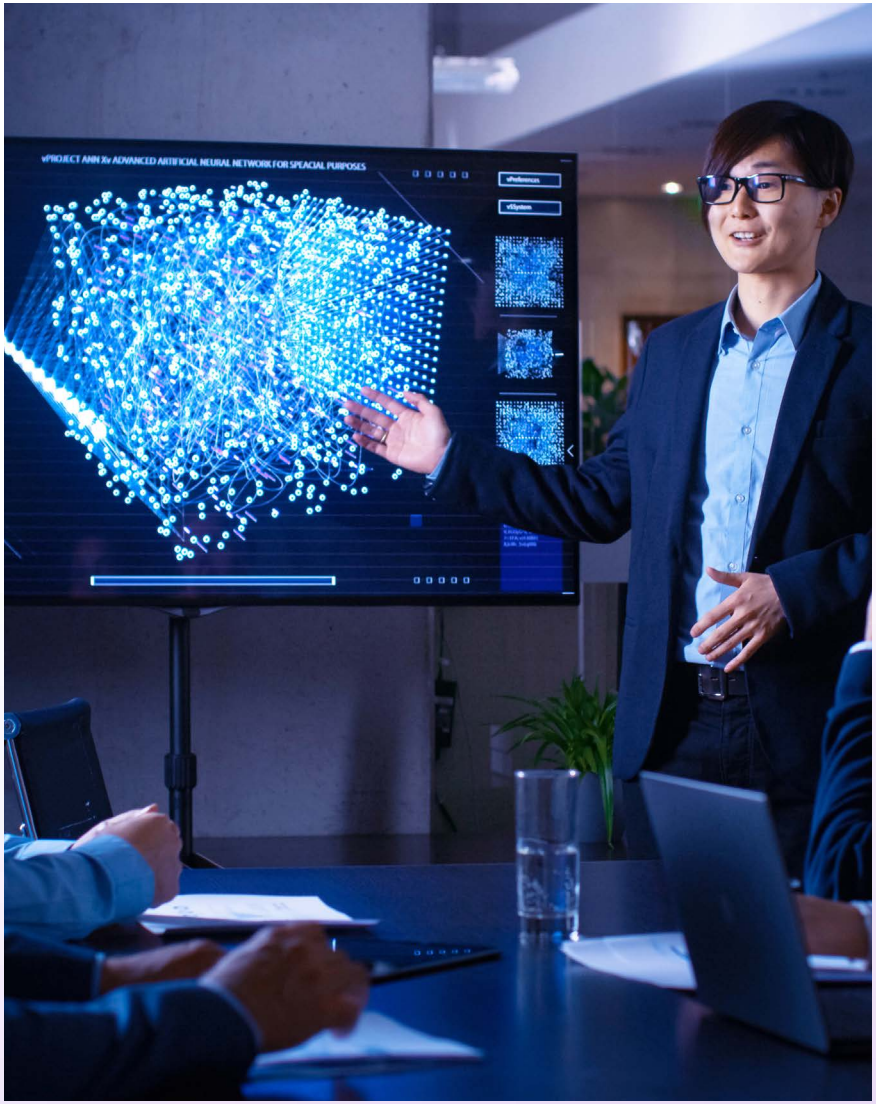
Many international standards organisations now have working programmes for PQC standardisation. Front runner, NIST, plans to publicly release its standardised specifications for PQC algorithms by 2024.

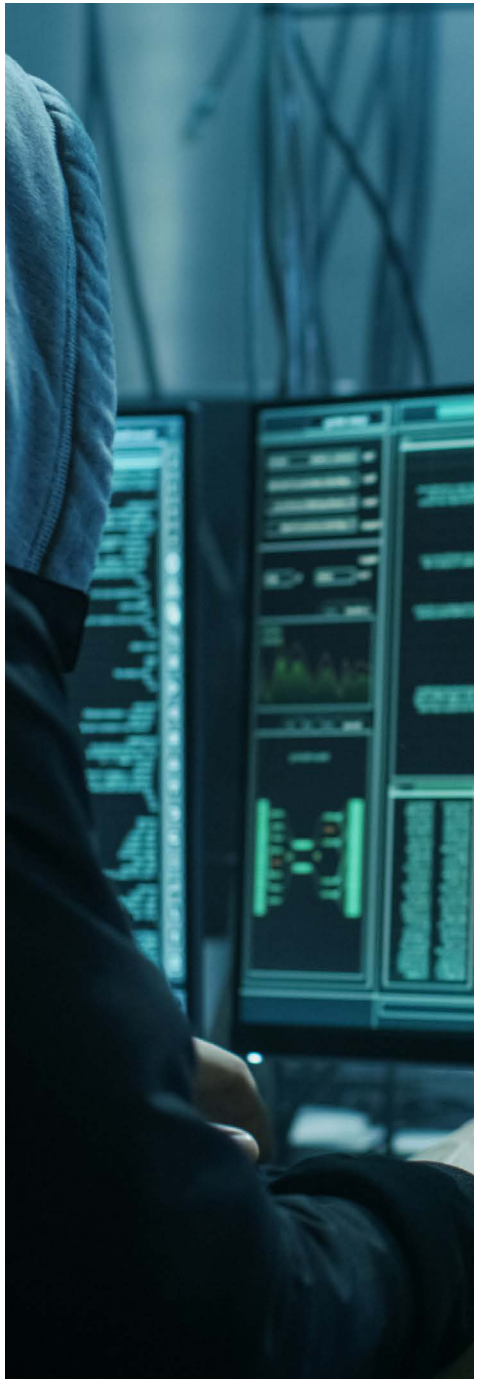
The first line of defence

Quantum Key Distribution (QKD) is the most secure key establishment technology available today, other than using a physical courier to move keys.

QKD provides a secure communication method for exchanging encryption keys only known between shared parties, across an authenticated but insecure channel. Its security relies on distributing information as qubits that can't be read accurately without being disturbed, unless you have knowledge about how they were prepared.

At BT, we deploy QKD in parallel with a standard classical mathematical key exchange, for dual resilience against any emergent cryptographic breaks.





Our latest research into PQC

In BT Applied Research, we've been incorporating and evaluating some of the more promising PQC algorithms for the past few years in internal and collaborative research projects.

Post-quantum VPN

In collaboration with the Nuclear Engineering Group at Imperial College London, we extended an existing VPN solution by adding two PQC alternative algorithms for authentication and key establishment into it. We successfully identified an algorithm that only caused a manageable increase in latency of 15%.

Post-quantum remote attestation

Remote Attestation is a method that ensures that the hardware and software configurations of a client device are correct before letting the device connect to a network. It includes making sure connected devices aren't running any modified or malicious code.

We implemented two quantum-safe digital signature algorithms in a remote attestation application we had developed for an internal project. We identified two algorithms that were faster than a standard asymmetric algorithm, taking 75% and 55% less time for the attestation.

Post-quantum PKI

We designed and developed a private PKI solution with automated certificate management and used PQC algorithms from NIST PQC Round 3 candidates, instead of using classical asymmetric cryptographic algorithms.

We established root and intermediate Certificate Authorities, creating a service that can be used to requisition post-quantum digital certificates, as well as verification of these certificates and code signing services. The PQ certificates it issues can be used widely, including by web servers and VPN servers to verify the identities of users, devices or services.

QKD in live trials

In recent years, we've worked with partners such as the Aquasec consortium and the UK Quantum Communications Hub to trial encrypted links. These links use QKD in combination with classical cryptography for key exchange.

Establishing the UK's ultra-secure Quantum Network Link (UKQNtel)

In collaboration with government and industry, we opened a commercial-grade quantum test network link between the BT Labs in Suffolk and Cambridge University in 2019.

The link forms part of the UK Quantum Network (UKQN) built by the Quantum Communications Hub, and is used for testing and demonstrating new quantum technologies, such as QKD. This includes trials of how these technologies can be used to secure critical and sensitive data across vertical industry sectors such as healthcare, financial services, defence and logistics.

A first for smart manufacturing

In partnership with Toshiba Europe Ltd, we built an industrial quantum-secure network between the National Composites Centre (NCC) and the Centre for Modelling & Simulation (CFMS), near Bristol, using BT Openreach's 'standard' fibre optic infrastructure.

The NCC was able to use QKD in combination with a standard classical algorithm for dual resilience during the trial, to transfer sensitive data relevant to the design and performance of a large-scale industrial component. It proved the suitability of QKD for real-world manufacturing applications, accelerating the shift to smart factories.

Launching a London Quantum Secure Metronet

In April 2022, continuing our partnership with Toshiba Europe Ltd, we launched the London Quantum Secure Network - a trial London area network able to deliver key material to customer sites, incorporating high-speed, high-performance encryption and data transmission.

EY became our first commercial customer to connect quantum secure data transmission between its major London offices. The Metronet is demonstrating how data secured using QKD can move between sites, in a way that's future-proofed against the threat of an adversary equipped with a quantum computer.

It’s a case of ‘when’, not ‘if’

Quantum-enabled security attacks are likely to be here within 10 years, so we can’t rely on current encryption technology in the medium term.

Quantum computers have the potential to attack certain very vital tasks in cryptography, one of which is Public Key Infrastructure. PQC allows us to keep all the functionality of existing cryptography, at the same time as upgrading it to be much harder for quantum computers to crack.

However, the algorithms used in PQC are still fairly new, and caution and practicality mean that most customers may not want or need to rush to upgrade. Instead, they may choose to wait until the new algorithms (as implemented in protocols) have been further standardised and have undergone more testing in the field.

It’s also worth remembering that quantum computers are not the only threat that networks are facing, and that upgrading this aspect of security is only one part of maintaining security.

Right now, some types of links and tasks can benefit from new quantum-based services. High-speed encryption supported by QKD has great potential for dedicated fibre links between large sites and data centres carrying data that must be secure in transit. This is a critical step forward in understanding where data and assets are across a network – an essential part of protecting them against mounting risks.

We’ll continue investing in quantum-based services as part of our ongoing commitment to innovation. BT Labs at Adastral Park is a globally recognised centre for communications research, and it’s the centre of our £2.5bn investment in research and development.

We’ve a particular focus on technologies that will shape the future of business, and take an open approach to pushing boundaries with customers, strategic partners and specialist innovators. We’re taking an active role in the quantum field and will continue to bring you accessible, quantum-based services as we build out our offering.

Visit our webpage to find out more about how global, end-to-end fraud protection can meet your security needs.

Creating a quantum-based future with Toshiba

In partnership with Toshiba, we’re exploring practical use cases for quantum technology to power and secure the next generation of connections.

Leading the market, we’ve already created a quantum secured network pilot, connecting London with the M4 business corridor. We’ll continue to push the boundaries of what’s possible, to turn quantum innovation into services for customers.

“Both Toshiba and BT have demonstrated world-class technology development and leadership through decades of innovation and operation. Combining BT’s leadership in network technologies and Toshiba’s leadership in quantum technologies has brought this network to life, allowing businesses across London to benefit from quantum-secured communications for the first time.”

Shunsuke Okada, Corporate Senior Vice President and Chief Digital Officer, Toshiba

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

December 2022