Quantum networking technologies

A white paper outlining the NCSC's approach to quantum security technologies.

In recent years, the NCSC has released several documents covering security technologies that rely on quantum mechanics:

- in 2016, we published a white paper about **Quantum Key Distribution (QKD)**
- in 2020, we published a white paper about **Quantum Security Technologies**, which included thoughts on **Quantum Random Number Generation (QRNG)** in addition to refined positions on QKD

Since then, there have been national and international developments.

The National Quantum Strategy was published in 2022, and implementation of that strategy is underway. The NIST post-quantum cryptography process has defined standards for algorithms that will help manage the threat to cryptography from quantum computing, and standards for common cryptographic protocols are following close behind. And there is a growing consensus among our international cyber security partner agencies around the future direction for quantum communications.

In this paper, we provide an updated analysis of QKD as a security technology, and the development of QRNGs. We also consider the future of quantum networking technologies.

Quantum Key Distribution

Quantum Key Distribution provides a mechanism to generate and share cryptographic keys in a way that guarantees detection against eavesdroppers and is resistant to a future quantum computer. It offers provable security (in the sense that – given a model of operation – there is a set of security guarantees that it upholds) that is underpinned by the laws of physics.

Establishment of cryptographic keys between communicating parties in a network is only one of a number of necessary steps needed to ensure secure communications. A critical additional mechanism is **authentication**; that is, establishing the identity of those parties. QKD does not provide authentication, nor do any other quantum techniques. Therefore, in practice, QKD must be combined with other cryptographic services to provide security against the threat from quantum computing, and therefore should not be relied on as a mechanism that provides substantial security value.

This means taking one of two options to protect against the quantum computing threat.

The first of these is using post-quantum cryptography (PQC) to provide authentication. PQC algorithms have been through a rigorous standardisation process run by NIST (the US national standards body) with extensive global scrutiny from experts in academia, industry and governments. Implementations are already being developed and deployed in some operational systems, and PQC will continue to be integrated into security protocols and widely used libraries. As well as offering authentication, PQC also includes mechanisms for agreeing cryptographic keys. The NCSC recommends PQC as the primary mitigation to the threat to cryptography from quantum computing, and has issued guidance on timelines for PQC migration.

The second option is to use QKD in systems based only on symmetric-key authentication (which is resistant to quantum computing) with pre-shared keys to support authentication. This can work in some controlled environments, but such systems do not have general purpose applicability as the distribution and management of these authentication keys makes scaling and managing systems difficult in practice.

Alongside the need for authentication, it is also important to consider broader cyber risks. Implementation of any security mechanism without inadvertently introducing vulnerabilities needs care. A good design principle is to minimise unnecessary complexity in both the system design and engineering, and hence constrain the potential attack surface. Managing complexity is a challenge when combining, for example, multiple software components. The NCSC's view is that it is much harder when integrating quantum and classical components, and combining specialised hardware with existing networking infrastructure. Developing implementations of QKD that will themselves be secure against 'elevated threats' (where adversaries are prepared to develop sophisticated attacks involving long-term research effort and significant resources) is an ongoing challenge, albeit one that the quantum industry and assurance community will continue to address.

For these reasons:

- The NCSC will not support the use of QKD for government or military applications. PQC is the best mitigation to the threat to cryptography from quantum computers.
- For other sectors, the NCSC recommends that QKD should not be solely relied upon for generating and distributing cryptographic keys. The use of QKD systems should not constitute evidence towards assessments of security of data-in-transit under the NCSC's Cyber Assessment Framework.
- Where organisations are considering using QKD, they should ensure that robust quantum-resistant mechanisms for authentication are implemented alongside them, and that they take appropriate steps to ensure they manage any additional cyber security risks arising from the increased complexity.

Quantum Random Number Generators

Quantum Random Number Generators (QRNG) use the inherent unpredictability in the measurement of quantum states to produce random numbers. In principle, this provides a truly random source of entropy.

Random numbers have several important uses in cyber security. They are used to generate cryptographic secrets and session identifiers, and as part of the computation in post-quantum algorithms. They are also used within many machine learning algorithms in AI systems. In all these cases, unpredictability is important, as is assurance in the behaviour of the random number generator.

Classical RNGs have met these needs for many years, and continue to do so. Although they do not provide ‘perfect’ randomness, we know how to characterise their performance and condition the output to give the security guarantees we need.

However, QRNGs have the potential to offer other properties that could be of value, in addition to ‘perfect randomness’. One important feature is the rate of generation. Quantum sources can – in theory – generate entropy at a significantly higher rate than classical sources. This could be useful in, for example, modern simulation algorithms.

A second property is the ability to rapidly detect degradation of the source through precise modelling of the quantum components, something that classical sources do not routinely offer.

In short, we are keen that research on QRNGs continues to progress. The NCSC would like to see a focus on the assurance of the raw sources, their integration into fully-engineered devices, and their role in larger, mostly classical systems.

Quantum networking

We have seen the term ‘quantum networking’ used to cover a range of possible future deployments of quantum communications technologies. Broadly, these fall into three classes.

1. Replacing classical security functionality with quantum technologies. We can view QKD as an instance of this, replacing classical key generation and agreement with a quantum approach.
2. Extending classical networks to include new functionality that can only be provided by quantum components (for example, integrating quantum sensors into larger networks).

3. Inherently quantum networks, distributing entangled quantum states between quantum devices.

The latter two of these have the most interesting applications. Entanglement between distant nodes of quantum sensor networks can provide greater sensitivity and precision. Local-scale networking (or transfer of state) is an enabler for scaling-up of quantum computers, to help realise the economic potential they offer. In the longer-term, we may expect to see quantum computers sharing information at longer distances to enable distribution of some tasks.

For each of these applications, building the networking technology that enables the secure distribution of quantum state is a substantial challenge; a quantum-specific approach (combined with cyber security expertise) appears to be a natural fit.

It is possible that the technologies underpinning QKD could play some part in future quantum networks. However, these technologies will be just one of a number that are needed to address broader network security challenges. The skills used to develop existing quantum communications technologies, as well as recent progress on assurance of quantum technologies, are likely to be relevant in meeting these challenges. This includes foundational research to develop and instantiate quantum network protocols, and engineering expertise to design and build the various components (such as quantum memories and repeaters) that will enable such functionality.

Closing thoughts

The implementation of the National Quantum Strategy includes five missions. One of these includes the target that by 2035, the UK will have deployed the world's most advanced quantum network at scale. A number of the planned outcomes of that mission focus on use cases described in this paper. We believe there is an ideal opportunity for industry and academic groups in the quantum communications and cyber security sectors to work in partnership to the benefit of the UK, with a focus on envisioning secure network architectures, defining the components that may be needed, and thinking about the assurance of these components and the wider system.

PUBLISHED

5 August 2025

VERSION

1.0

WRITTEN FOR

Cyber security professionals