Quantum security technologies

This white paper sets out the NCSC position on two security technologies that rely on quantum physics: Quantum Key Distribution and Quantum Random Number Generation.

It replaces the NCSC whitepaper on Quantum Key Distribution.

Quantum Key Distribution

Quantum Key Distribution (QKD) is a mechanism for agreeing encryption keys between remote parties, relying on the properties of quantum mechanics to ensure that key has not been observed or tampered with in transit.

Since traditional public key cryptography algorithms may be vulnerable to a future large-scale quantum computer, new approaches are required that do not share this vulnerability. QKD claims to offer a potential mitigation since its security properties are based on the laws of physics rather than the hardness of some underlying mathematical problems.

QKD protocols provide a mechanism for two remote parties to agree a shared secret key, where the key cannot be observed or tampered with by an adversary without alerting the original parties. However, because QKD protocols do not provide authentication, they are vulnerable to physical man-in-the-middle attacks in which an adversary can agree individual shared secret keys with two parties who believe they are communicating with each other.

For this reason, QKD protocols must be deployed alongside cryptographic mechanisms that ensure authentication. These cryptographic mechanisms must also be secure against the quantum threat.

QKD is not the only mitigation against the threat of quantum computers. Work towards standardising quantum-safe cryptographic algorithms is underway in international standards bodies such as NIST. These algorithms can be implemented on today's classical computers, and, unlike QKD solutions, do not require dedicated or specialist hardware. Quantum-safe cryptographic

algorithms allow two remote parties to agree a shared secret key with authentication, hence without the risk of man-in-the-middle attacks.

Agreeing encryption keys is just one mechanism of many that must be employed to secure a complex system. More research is needed to understand how QKD protocols can be implemented and integrated into these complex systems of classical components, such that the whole system is secure against an appropriate threat model. However, we welcome the ongoing research and assurance work currently underway in this area.

NCSC Position

Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the **NCSC does not endorse the use of QKD for any government or military applications**, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.

In addition, we advise that any other organisations considering the use of QKD as a key agreement mechanism ensure that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them.

NCSC advice is that the best mitigation against the threat of quantum computers is quantum-safe cryptography. Our white paper on quantum-safe cryptography is available on the NCSC website.

The NCSC design principles for high assurance systems, which set out the basis under which products and systems should be designed to resist elevated threats, is also available.

For those organisations using the NCSC Cyber Assessment Framework, a QKD system may not contribute to any assessment of principle B3.b (Data In Transit).

Quantum Random Number Generation

Cryptographic algorithms often require random values; these values may be used, for example, for cryptographic keys, initialisation vectors, salts and nonces. Implementations of these algorithms need access to a Random Number Generator (RNG) which will provide good quality random numbers when required.

A Quantum Random Number Generator (QRNG) is an RNG that relies on constructions based purely on quantum mechanics for its entropy. QRNGs do not provide any new mitigation against the threat from quantum computers to traditional public key cryptography; however, they can generate random numbers at very high speed, and, in their ideal state, the constructions produce truly unpredictable numbers.

QRNGs are often defined in contrast with classical RNGs, where numbers are derived from measurements of the behaviour of higher-level components. However, in many classical RNGs, the dominant hardware noise source is also a consequence of quantum processes. Methods for integrating these RNGs into larger systems and assessing their behaviour are well established.

In practice, the unpredictability that QRNGs can potentially offer is hard to realise. A significant reason for this is that QRNGs will necessarily sit inside classical circuitry for collection and processing, and this classical circuitry adds noise to the measurement of the quantum state.

The embedding within classical circuitry also means that QRNGs are potentially subject to a similar range of implementation-level attacks as classical RNGs, as well as those specific to the quantum technology. This leads to some future research challenges, including (but not exclusively):

- Modelling and evidencing the real-world properties of physical QRNGs.
- Engineering and integration of QRNGs into larger systems.
- Understanding changes in behaviour of QRNGs under various physical stresses and through aging.
- Vulnerability research to explore new technical risks.

NCSC position

The NCSC believes that classical RNGs will continue to meet our needs for government and military applications for the foreseeable future. However, we support continued research into QRNGs, as described above.

PUBLISHED

24 March 2020

VERSION

1.0