Community Response to the NCSC 2020 Quantum Security Technologies White Paper

Issue 1.1 27th May 2020

*ADVA, BT, ID Quantique, KETS, Quantum Communications Hub, M Squared Lasers, Senetas, Thales, Toshiba Europe Limited

1 Executive Summary

The QKD community* welcomes the NCSC's revised White Paper on Quantum Security Technologies [7] published March 2020. We are pleased that the NCSC has updated its guidance to allow the use of QKD in Industry and Critical National Infrastructure. We believe this significant change from the 2016 position, whilst cautioning against sole reliance, is recognition of the considerable progress made in QKD technologies over recent years.

It is widely recognised that businesses must prepare now for the emergence of quantum computers. Retrospective decryption is a very real threat and critical information which requires long-term security should be protected now. Quantum Key Distribution and quantum-resistant algorithms[1] (QRA) are critical technologies that businesses concerned with long-term data protection should begin deploying with urgency.

The NCSC does not currently endorse QKD for use in Government & military applications. We believe early engagement in trials and testing however will enable the development of QKD systems for this specialist sector.

The NCSC rightly observes that QKD (as a means of securely distributing encryption keys) is a component of a secure system which must be securely integrated with authentication mechanisms and quantum-resistant algorithms. The industry has well-established approaches for authentication with QKD and we fully agree that QKD should be used alongside quantum-safe cryptography as that technology matures.

Assurance is essential and we are pleased the NCSC has recognised the significant research and standards activity that is underway. We would welcome the NCSC's endorsement of key programmes e.g. through ETSI and encourage direct involvement in this important work.

[1] The NCSC White Paper uses the term quantum-safe cryptography which includes QKD. For clarity this paper uses the term quantum-resistant algorithms to refer specifically to *cryptographic algorithms believed to be secure against attack by quantum computers*.

2 Authentication in Quantum Key Distribution

QKD is a secure method of key distribution, in that two users can share a key which they can determine is secure from eavesdropping based on direct measurement. QKD should always be implemented with authentication of the discussion channel (and in addition to any other classical interfaces, such as management). In cases where the QKD devices already share "pre-loaded" secret seed keys, there exist recognised unconditionally secure authentication schemes that can be utilised, such as Wegman-Carter. This "key expansion" capability of a pre-seed authentication secret using QKD is known to be secure against adversaries armed with quantum computers, or indeed any other new quantum technologies. In this sense it is therefore future-proofed against any emergent new technologies.

In dynamic or rapidly expanding communication networks there may be no "pre-shared" secret seed key. To avoid an adversary operating a man-in-the-middle attack in this situation, the QKD devices require some form of authentication infrastructure e.g. a public key infrastructure (PKI) or trusted 3rd party such as Kerberos. Given the vulnerability of current PKI to quantum computers, there is thus a requirement to use new, quantum-safe PKI for authentication in this situation.

It should be noted that in the latter case of using PKI, the algorithm need only be resistant to quantum attacks during the initial device authentication as the QKD system is not vulnerable to retrospective attack.

3 Quantum-safe cryptography: Quantum-Resistant Algorithms & QKD

It is widely accepted in the community that QKD will be deployed alongside quantum-resistant algorithms (QRA). There is a range of algorithms being evaluated under the NIST programme [8] leading to Draft Standards in two to four years.

Meanwhile, retrospective decryption is a very real threat; intercepting encrypted data today, storing this data, and decrypting it at a later date once access to a quantum computer, or other hacking methods, becomes available. QKD is the only known concept of circumventing this indefinitely as QRA is based on the believed hardness of certain problems, which could be compromised as understanding of quantum computers increases.

We stress that wherever possible QKD should be used in tandem with QRA to future-proof quantum-safety and to offer the widest spectrum of secure communications technologies. Indeed, we believe that an approach suggesting a need to choose between QKD and QRA is based on a false dichotomy. Increased system security is possible because quantum-resistant algorithms can have access to the secure shared key material from QKD, with applications beyond point-to-point encryption and authentication, and can also (where necessary) support new authentication for QKD. There are various research efforts across the world focussing on this. Examples in the UK include the EPSRC Quantum Communications Hub [3] and the Innovate UK AQuaSeC [1] project, with Queen's University Belfast (QUB) working alongside Royal Holloway University of London and Toshiba, KETS Quantum Security, BT and other industry leads.

4 Assurance and standards

There is a clear assurance need for all elements of QKD systems including QKD endpoints, trusted nodes and for the interfaces between QKD devices, hardware security module (HSM) key stores and the encryption function. International study groups such as the ITU, ISO, and ETSI have created both published and draft standards with recommendations for QKD components, systems and networks. ISO 23837-1 and ISO 23837—2 [5] are particularly important as a basis for an assurance framework document, and the ETSI QKD Industry Specification Group [4] is coordinating the development of a Common Criteria Protection profile, with support from the German BSI. BT are leading efforts through the EU's OpenQKD [9] project for pen-testing of QKD systems, trusted nodes and other auxiliary classical network devices to address the concerns about the security of these elements. We encourage active involvement from across industry and the NCSC to ensure these standards provide the necessary assurance required for the Cyber Assessment Framework.

National metrology institutes, such as the UK's National Physical Laboratory (NPL), are working with the Quantum Communications Hub to develop the standardised high-precision measurements required to support the process of assessing the security level of QKD systems.

5 Quantum Random Number Generation

There are two key requirements for Random Number Generators (RNG):

1. some specified distribution of the outcomes (usually a string of uniform and independent random bits) and
2. the outcomes cannot be predicted by any other party.

Quantum RNGs provide a way to ensure both these properties. Since simple quantum processes provide a way to generate fundamental randomness, by careful modelling we can quantify the amount of quantum randomness produced. Other processes that influence the raw outcomes can be accounted for and randomness extraction used to remove these so that the final output randomness is based only on the quantum component.

There are a number of UKRI activities addressing the development and evaluation of Quantum RNGs. The Innovate UK funded project AQuaSeC [1] is developing Quantum RNGs integrated on a semiconductor chip, allowing cost effective integration into a wide range of security products. Meanwhile, a newly funded Innovate UK project, led by NPL and involving industry and academia, will leverage work from the EPSRC Quantum Communications Hub [3] to develop methods for the security evaluation of quantum RNGs. This new project will engage with NCSC on how to establish a security assurance process for quantum technology in the UK, as recommended in the GO Science Blackett Report [2]. In addition, a joint activity by the Hub and NPL is already looking at newer protocols. New "device-independent" QRNGs that exploit quantum entanglement can, in principle, allow random numbers to be generated without assumptions on the inner

workings of the devices used, hence providing an enhanced and uniquely quantum route to QRNGs and their assessment.

6 Conclusion

It is essential that industry prepares now for the emergence of quantum computers. Retrospective decryption is a very real threat and critical information which requires long-term security should be protected now. Quantum Key Distribution and quantum-resistant algorithms are critical technologies which we should begin deploying with urgency.

We are delighted that the NCSC has withdrawn its restriction on the use of QKD. This reflects the significant progress made in QKD technologies. We are confident that the QKD industry can address outstanding concerns so that in time the NCSC will endorse its use in Government and military applications.

References

1. AQuaSeC
   https://gtr.ukri.org/projects?ref=104615
2. Blackett Review: Quantum Technologies
   https://www.gov.uk/government/publications/quantum-technologies-blackett-review
3. EPSRC Quantum Communications Hub
   https://www.quantumcommshub.net/
4. ETSI ISG-QKD
   https://www.etsi.org/technologies/quantum-key-distribution
5. ISO/IEC JTC 1/SC 27
   https://www.iso.org/committee/45306.html
6. ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)
   https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx
7. NCSC White Paper: Quantum Technologies
   https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
8. NIST
   https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline
9. OPENQKD
   https://openqkd.eu/