Report from NCSC/Quantum Communications Hub workshop

on Cyber Security and Quantum Communications

Held online on 24 November & 8 December 2020; report published in March 2021

Background

A virtual workshop was hosted by the National Cyber Security Centre (NCSC) and the Quantum Communications Hub, to consider the scope for quantum communications within the wider cyber security landscape and framework. The workshop was held over two part-days (24 November and 8 December 2020), with the gap designed for participants to reflect on presentations and prepare input for subsequent discussions. The objectives of the workshop were: (i) for NCSC and cyber security experts to present their perspectives on approaches to cyber security; (ii) to identify and assess challenges for new quantum communications technologies; and (iii) to identify future events and activities to be undertaken to start addressing these challenges.

The background and motivation for this workshop comprise various factors. The growing threat to current, widely-used, public-key cryptography from quantum computers is one factor – generating a need to develop, assess and integrate new approaches, in order to render the cyber security infrastructure "quantum safe" – that is, safe in a future, fully quantum-enabled world. The current NCSC position [1] is to pursue quantum safety through new quantum-resistant cryptography – new mathematical cryptography known to be immune to enhanced attack from existing quantum computer algorithms (notably Shor's algorithm) and thought to be immune to other quantum algorithms that will emerge. Such quantum-resistant cryptography is being selected from numerous submitted candidates, through an intensive, multi-stage process run by NIST in the US [2][1]. Another approach for quantum safety is through quantum communications. Here the safety arises through new quantum enabled hardware. For the most technologically advanced example, quantum key distribution (QKD)[2], as long as the hardware satisfies specified criteria there exist security proofs of quantum safety, against any possible attack by quantum computers or other quantum technologies. At present, NCSC do not endorse QKD for government and military applications [3]. However, there is now scope for initial trials in commercial scenarios, supported with suitable authentication [4]. Clearly all this background provides motivation for increased discussion and collaboration between the cyber security and quantum technology communities, as also recommended in the 2016 Blackett review for quantum technologies [5]. For example, it is obvious that security proofs have appeal, but then integration of new hardware, as opposed to software, generates significant new challenges. Thus, quantum safe solutions could vary according to the scenarios in which they are deployed and the flexibility required.

To provide context for the workshop discussions, various cyber security perspectives were presented under (i). Important takeaways from these presentations were: consider the whole system and what evidences system security; identify threats and adversaries and their attack surfaces; know what you

[1] China has run their own internal process to select new quantum-resistant cryptography.

[2] More precisely this should be called quantum key expansion, as separate authentication is required [3,4].

trust; understand the security architecture and system requirements; understand the cryptographic architecture, all its components and any limitations; address the challenges to integrate technologies into systems with assurance; identify where vulnerabilities arise due to human factors. Clearly there is a common thread to many of these perspectives, which is to adopt a system-level approach. In order to focus workshop discussions (ii) and the development of next steps to be taken (iii), six separate topics were identified. For each, an expert cyber security, quantum and industry group (containing both NCSC and Hub representatives) produced the following key points and suggested next steps. Note that although produced from focused discussions, many of the key points and next steps identified below apply much more widely than just for the topic under which they were produced and are listed.

Topic 1: Implementation challenges in technology take-up

Key points:

- Quantum communications technologies need to reduce significantly in cost, address the requirements of the networks into which they seek integration and ensure their non-quantum hardware is also secure ("classical hardening").
- Key management across networks and integration into the cryptographic and trust architectures is important.
- Security assurance must be at two levels, device/sub-system level but also fully deployed system level.

Suggested next steps:

- Undertake further R&D on "classical hardening" and system-level security, including vulnerability testing – all from a multi-disciplinary team perspective. Promote wider understanding of all this.
- Continue with R&D into new quantum protocols and technologies, beyond QKD and quantum random number generation (QRNG).
- Leverage NCSC and the cyber security community to better connect the quantum community to existing UK-approved security assurance companies.
- Continue international work on standards (e. g. through ETSI, ISO, ITU, IEEE …), both for the technologies but also for the higher level and wider approaches to quantum safety and cyber security.

Topic 2: Hybrid Systems

Key points:

- Hybrid systems mean different things (classical and quantum, hardware and software, fibre and free space) to different communities, so defining the particular hybrid is important.
- Graceful failure of (all, not just hybrid) systems is highly desirable when an element of the system fails.
- Assurance and certification (for Government and commercial markets) are clearly important and even more so now, post-Brexit. The UK position and approach needs to be clarified.

Suggested next steps:

- Undertake further R&D into combinations of hybrid systems.
- Increased clarity of approach is required; there are distinct differences in applications for government, commerce and consumers.
- Avoid silos by devising mechanisms to encourage a genuine mix of skills and expertise in groups. There is a skills (and training) issue at national level that needs to be addressed to better connect the cyber and quantum communities. The UK National Quantum Technologies Programme (UKNQTP) and its stakeholders should play a role here; the Hub can contribute to specific activities.
- Produce more White Papers – in particular ones highlighting strength in depth.
- Convene a workshop focused on assurance and certification for UK markets.

Topic 3: Demonstrators, incl. field trials

Key points:

- Future access to and participation in EU projects and activities (Galileo, the Quantum Communications Initiative, OpenQKD, etc.) is at best unclear and may be limited or non-existent, so UK quantum strategy needs to include large-scale UK demonstrators.
- Any future UK participation in major international demonstrators and initiatives would benefit from UKNQTP coordination.
- Demonstrating (added) value and capability is key. Demonstrators and other (e.g. Industrial Strategy Challenge Fund - ISCF) projects should show **operational security**, not just use of quantum technology.
- Think wider than purely quantum demonstrations, so consider e. g. quantum technologies with 6G, 7G, conventional satellite communications.

Suggested next steps:

- Develop roadmaps for the various technologies, identifying gaps in current provisions and the pathways to maturity and filling these gaps. The Hub can contribute here, but industry should push the road-mapping, if the end goals are technologies and systems with target markets and applications.
- Further leverage and expand the existing demonstrator – the UK Quantum Network [6] (while being aware that communications are free-space as well as fibre).
- More (e.g. Innovate UK-type of) funding is needed, for projects to build new demonstrators (and to support the appropriate skills and training). Industry should shape/lead these demonstrators, informed by their target markets and adoption requirements.

Topic 4: Sector specificity

Key points:

- There can be a tension between requirements for high security assurance and the flexibility required in some commercial applications.
- Risk appetites and thresholds vary among different sectors and markets, and there may be acknowledged trade-offs between security and performance or other operating constraints.
- A rigid set of requirements for security is very hard to specify in isolation. A more realistic approach is to be risk-driven – that is, for a sector / application to define security goals,

perceived threats and the trade-offs that can be made, so security assurance, including integration within a wider system, fits with the risk profile.

Suggested next steps:

- Capture potential sector-specific use cases and an analysis of potential threats, risks, and integration challenges:
    - draw on the Catapults to provide input (satellite, digital, connected places, compound semi-conductor);
    - directly from companies in the ecosystem sharing what they can from their engagements;
    - relevant recent and current Innovate UK projects;
    - NCSC and the wider cyber security sector.
- Articulate (without hype) the benefits of QKD-based systems, including:
    - functionality
    - low operational costs of QKD such as power consumption, ease of use, latency, etc.

Topic 5: Future directions of new technologies

Key points:

- Next generation measurement-device-independent (MDI) and device-independent (DI) quantum technologies will constitute major advances, closing side-channel attacks that exist in current technologies and assuring security independent of hardware specifications.
- Protocols beyond QKD and QRNG (see Topic 6) expand the capabilities of quantum communications. Hardware development and security testing should prioritise applications that can utilise quantum advantage and do so where there is potential market pull.
- Quantum-literate contacts in user companies/institutions and security-literate people in quantum companies are highly desirable. Such experts can act as both advocates within their companies and informed critics for research. Such a network would significantly enhance the quantum-cyber dialogue for current as well as future technologies.

Suggested next steps:

- Undertake further R&D on MDI and DI technologies.
- Continue to generate ISCF and other Innovate UK industry-led projects on new technologies and applications, including security assessment that involves cyber security expertise and NCSC consultancy (e.g. like the current ISCF project on QRNG assurance).
- Explore other funding and project potential for enhancing the quantum-cyber dialogue, including some of NCSC's own industry and academic calls.

Topic 6: Future directions on new protocols

Key points:

- In addition to security, quantum advantage can impact other communications tasks such as fingerprinting and applications of secret-sharing, teleportation and summoning.
- Quantum position authentication and signature protocols exist with application potential.

- New protocols continue to emerge. Pre-commercial examples include: quantum commitments to private data; quantum money and secure tokens for high-sensitivity financial transactions; mistrustful random number generation between two or more parties (secure coin tossing).

Suggested next steps:

- Beyond QKD and QRNG, quantum protocols still seek real-world application. Organise a workshop explaining these to the wider security community: for feedback, discussion and identification of possible application areas where quantum could really add advantage.
- Produce a sequence of White Papers on quantum protocols and their potential applications (possibly starting with signatures).
- Undertake further R&D on new protocols, composable security of quantum primitives and scope and limitations of quantum security.
- Produce a roadmap for hardware-specific implementations of practical and commercially applicable new protocols.
- Support the development of standards for implementations of new post-QKD protocols.

Conclusion: Increased dialogue and collaboration between the quantum and cyber security communities will support further advances in quantum safe security. The Quantum Communications Hub is well placed to support this. Numerous next steps for delivery have been identified, bringing in industry, partners and stakeholders as appropriate.

Appendix: Workshop Participants

The workshop included participants from the EPSRC Quantum Communications Hub and the National Cyber Security Centre, including representatives from BEIS, Imperial College London, Innovate UK, National Physical Laboratory, Royal Holloway College, University of London, Satellite Applications Catapult, the Universities of Bristol and York, and the following companies: Adelard, ADVA, ArQit, BT, Cambridge Quantum Computing, Crypta Labs, ID Quantique, KETS, NCC Group, Quantum Dice, Senetas, and Toshiba Europe Ltd.

References

[1] https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

[2] https://csrc.nist.gov/projects/post-quantum-cryptography

[3] https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[4] https://www.quantumcommshub.net/wp-content/uploads/2020/09/Response-to-NCSC-QSC-WP-Issue-1.1-27_5_2020-1.pdf

[5] https://www.gov.uk/government/publications/quantum-technologies-blackett-review

[6] https://www.quantumcommshub.net/industry-government-media/our-technologies/fibre-based-qkd/