Version 1.0, May 2024

Quantum Assurance Introductory Foreword

By Christopher Chunnilall & Tim Spiller

In 2021, NCSC introduced a major new approach to technology assurance in the UK. In 2022, this approach was applied in detail to the assurance of security products, and other relevant products which, because of their use, would negatively impact security if compromised.[1] This new assurance approach is based on the provision of principles and guidance which providers of security products should follow in order to deliver security assurance to users and customers. Clearly, the NCSC strategy and approach should be applied to all security products – quantum and non-quantum, or systems including both.

The purpose of these Quantum Communications Hub documents is to highlight, with comments and examples, particular aspects of the NCSC principles that should be considered, or expanded upon, for **quantum security products.** These Hub documents present the NCSC text verbatim, interspersed with identifiable comments or additions specifically focussed on the "quantum layer", or quantum aspects of the products. Note that all the NCSC principles should still be followed in the quantum case, not just those identified for commentary.

The new feature of quantum security products is that their security relates to hardware, with the physical properties and behaviour of the hardware or technology components of the products governed by the laws of quantum physics, which is how Nature works in the quantum domain. There will be non-quantum hardware and software in these products as well, but these are already addressed by the original NCSC principles.

The "quantum advantage" of quantum security products is that their operation is underpinned by a security proof, which can be validated through measurements that evidence and verify their quantum behaviour. This quantum advantage is the additional and desirable feature of quantum security products; it is potentially very important, because (unless explicitly qualified) a security proof will hold into the future, even when any new quantum technologies (such as large quantum computers) become available. This future-proof aspect is very appealing, and potentially commercially advantageous.

However, it is also important to understand that a quantum security proof is a mathematical proof, based on a physical model of the system.[2] This model is constructed to be as accurate as possible, but it can neither be complete (it cannot capture every detail of the system), nor perfectly accurate (physical devices have imperfections, not all of which can be modelled accurately). There will thus be discrepancies between what is assumed in the model and the behaviour of the physical hardware. These discrepancies can provide so-called quantum side channels, which could be used to circumvent the proven security. Therefore, many of the comments and additions provided to the original NCSC principles text raise the important matter of quantum side channels, as identification and understanding of these is crucial for quantum-security-product assurance. The physical nature of quantum side channels implies that a newly uncovered side channel, not previously known, does

[1] From now on, we will use the term "security products" to cover hardware, software, technologies and services that are supplied to provide security. Our particular focus will be quantum security products, which contain some quantum hardware or technology to support their security.

[2] This is fundamentally different to a security proof in conventional cryptography, which applies purely to the cryptography, thus requiring completely separate considerations of the technology implementation. In the quantum case the two are intimately linked, with the proof applying to any technology implementation satisfying the set of physical assumptions upon which the model is based.

not invalidate earlier security. However, an associated quantum security proof may then require improvement, for future security of the relevant product.

To date, quantum security proofs have generally been developed and improved within an open scientific environment (an "open source" approach), with publications placed in the public domain. There is strong motivation for this approach to continue. Having such proofs open to widespread scrutiny means that they provide a very strong foundation for the assurance of commercial products that utilise them. A similar philosophy has been applied with the development of new post-quantum cryptography (PQC), where the new PQC candidates are open to widespread scrutiny.[3] A highly desirable feature of conventional security is that of "universally composable security" [1]. In this framework, security is still maintained for a protocol composed of any set of protocols, or more generally when the protocol is used as a component in any composite system. Thus, security can be maintained in complex and uncertain environments, like the Internet. Composable security is similarly desirable in the quantum case.

Conventional, i.e. non-quantum, side channels can also arise in all (quantum and non-quantum) secure products and services. Unintended effects (in conventional software or hardware) can leak sensitive information when a secure protocol is realised with actual technology (e.g. accidental electromagnetic radiation of secret key material by a device). These side channels have to be addressed for all security products. However, established methods exist for dealing with such side channels. Otherwise, conventional assured security products would not currently be available.

It should also be noted that there is significant scope for improvement of quantum advantage in next-generation quantum security products, with the introduction of "device independence". This feature will eliminate many of the current quantum side channels, along with very significantly simplifying assurance measurements, by making these independent of the internal physical details of the quantum hardware. Practical device-independent technologies don't yet exist, but there has been significant research progress accompanied with experimental demonstrations of both randomness expansion [2] and quantum key distribution (QKD) [3-5,6].

In order to widely benefit from quantum advantage, it is essential that end users are not required to have or acquire quantum knowledge. Assurance and certification provide this for them. Developers/manufacturers of quantum security products, along with service providers who deploy and incorporate such products into their infrastructure, will need the relevant quantum knowledge and understanding appropriate to their role. This distinction, between the (lack of) requirements on end users and the requirements on developers and service providers, is reflected in the comments and additions to the NCSC principles.

The full list of NCSC principles is detailed and carefully constructed. Following these principles and providing evidence to support this will be a demanding task, especially for a start-up or small company. Quantum security products – that will very likely also contain non-quantum hardware and software – will increase the evidence workload requirement above that for a non-quantum security product. While UK companies or bodies already exist to support or aid the assurance of non-quantum security products (and thus could be leveraged for their non-quantum aspects by companies producing quantum security products), such comparable support or aid does not yet exist in the quantum sector.

Therefore, there is a strong case for a body being established to support (particularly small) companies with assurance of the quantum-specific aspects of their products. This support could be

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

provided by the National Physical Laboratory (NPL), given the expertise that exists there, or delivered by another organisation in partnership with NPL.[4] Without such a body, UK companies focused on quantum secure products will individually encounter a very substantial assurance workload to gain market entry.

Christopher Chunnilall is a Principal Scientist at the National Physical laboratory (NPL) and co-investigator in the Quantum Communications Hub. He leads NPL's work on Quantum Photonics metrology, which includes the evaluation of quantum communication technologies.

Tim Spiller is Professor of Quantum Information Technologies at the University of York and Director of the Quantum Communications Hub. He leads the Hub activities at the interface of Cyber Security and Quantum Communications, which have previously included a joint workshop with NCSC on this topic.

References

1. R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. Proceedings 42nd IEEE Symposium on Foundations of Computer Science, Newport Beach, CA, USA, 136-145, (2001). https://doi.org/10.1109/SFCS.2001.959888 .
2. Liu, WZ., Li, MH., Ragy, S. et al. Device-independent randomness expansion against quantum side information. Nat. Phys. 17, 448–451 (2021). https://doi.org/10.1038/s41567-020-01147-2 .
3. Nadlinger, D.P., Drmota, P., Nichol, B.C. et al. Experimental quantum key distribution certified by Bell's theorem. Nature 607, 682–686 (2022). https://doi.org/10.1038/s41586-022-04941-5 .
4. Zhang, W., van Leent, T., Redeker, K. et al. A device-independent quantum key distribution system for distant users. Nature 607, 687–691 (2022). https://doi.org/10.1038/s41586-022-04891-y .
5. Liu, WZ., Zhang, YZ. Et al. Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution. Phys. Rev. Lett. 129, 050502 (2022). https://doi.org/10.1103/PhysRevLett.129.050502 .
6. For a review see: Zapatero, V., van Leent, T., Arnon-Friedman, R. et al. Advances in device-independent quantum key distribution. npj Quantum Inf 9, 10 (2023). https://doi.org/10.1038/s41534-023-00684-x .

[4] For example, the IUK ISCF project AQuRand (led by NPL) has taken preliminary steps for assurance of QRNGs.