RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

SWEDISH ARMED FORCES

Position Paper on Quantum Key Distribution

French Cybersecurity Agency (ANSSI)

Federal Office for Information Security (BSI)

Netherlands National Communications Security Agency (NLNCSA)

Swedish National Communications Security Authority, Swedish Armed Forces

Executive summary

Quantum Key Distribution (QKD) seeks to leverage quantum effects in order for two remote parties to agree on a secret key via an insecure quantum channel. This technology has received significant attention, sometimes claiming unprecedented levels of security against attacks by both classical and quantum computers.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. In light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying.

This paper is aimed at a general audience. Technical details have therefore been left out to the extent possible. Technical terms that require a definition are printed in italics and are explained in a glossary at the end of the document.

Contents

1 The quantum threat

If large-scale fault-tolerant *quantum computers* become available in the future, due to Shor's algorithm [17], they will be able to break most of the *public-key cryptography* that our digital infrastructure is currently built upon. Even if such cryptographically relevant *quantum computers* are not yet available, the confidentiality of our communication is under threat today as adversarial actors may store encrypted messages in order to decrypt them in the future. This threat is known as the store-now-decrypt-later scenario.

To mitigate the quantum threat, one option is to use pre-shared *symmetric* keys in combination with *classically secure public-key cryptography* in situations where the secure distribution of *symmetric* keys is feasible. An alternative option is to develop *public-key cryptography* that can be considered secure against attacks from both classical computers and *quantum computers*. Over the past few years, such so-called *post-quantum cryptography* has undergone a rigorous standardisation process at NIST and is also the subject of ISO standardisation efforts. As a result, a first selection of NIST standards will be available sometime in 2024. Many national cybersecurity and communication security agencies have made recommendations [1, 4, 5, 6, 13, 14, 18] and governments have announced their intentions and plans for a timely migration to *post-quantum cryptography*.

Another proposed solution for quantum-safe *key agreement* is Quantum Key Distribution (QKD). QKD comprises protocols which exploit quantum-physical phenomena for secure *key agreement*. It is quite different from *post-quantum* and *classically secure public-key cryptography*, regarding both the principles its security is based on and the way it is implemented. Large national and European projects are currently working on the development of QKD systems and the construction of large-scale quantum communication networks; most prominently the EuroQCI project initiated by the European Commission. Several national cybersecurity and communication security agencies have published their position on the use of QKD or aspects of QKD security [2, 4, 5, 12, 15].

2 What QKD can provide

In order for two parties, say Alice and Bob, to agree on a shared secret key using a QKD protocol, they are typically connected via a quantum channel (such as fibre-optic cables or, in the case of satellite-based QKD, free-space) and a classical communication channel. In order to prevent man-in-the-middle attacks, the messages sent via the classical communication channel need to be authenticated. One common way to achieve this is for Alice and Bob to share a secret key in advance and use it to authenticate messages sent over the channel. In a QKD protocol, quantum states (for example as polarised photons) are exchanged or distributed and measured; then after post-processing, using classical communication over the authenticated channel, a secret key is derived from the measurements. Alice and Bob may detect an eavesdropper by comparing parts of their measurement results since a quantum state changes if there is any non-trivial interaction with it.

The theoretical security of QKD protocols is based on quantum-physical principles, whereas *post-quantum* and *classically secure public-key cryptography* are based on the assumed hardness of certain mathematical problems. This implies that, at least in theory, QKD protocols are secure even against computationally unbounded attackers or in the event of future algorithmic breakthrough. In particular, they claim to be secure against the store-now-decrypt-later scenario.

To be secure against computationally unbounded attackers, the actual data has to be protected by an absolutely secure encryption mechanism (i.e. the *one-time pad* scheme); which in turn requires a QKD channel with a bandwidth equal to that of the classical data channel. For most realistic applications, such bit-rates are far from what QKD can achieve today. This means that the secrets shared through quantum

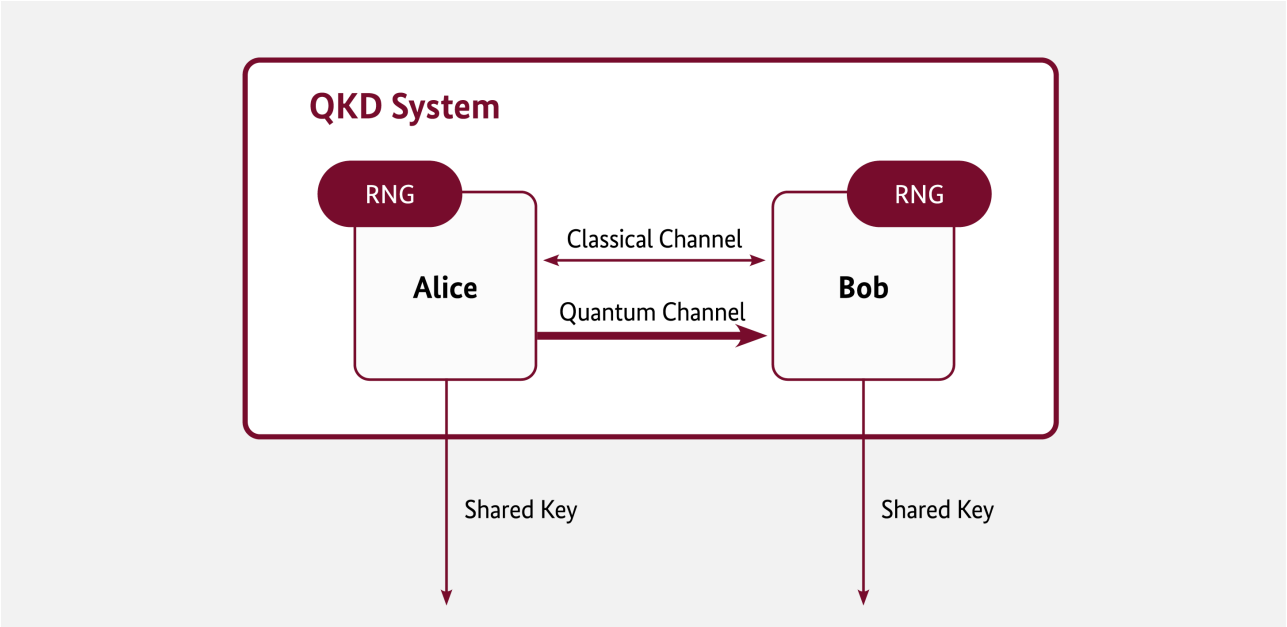

Figure 1 Schematic illustration of a QKD system. As part of the QKD protocol, Alice and Bob communicate via the classical and the quantum channel. At the end of the protocol, they obtain shared secret keys that can then be used for encryption, for example. Typically, random number generators (RNGs) are part of Alice's and/or Bob's QKD module.

channels will need to be used as keys for established *symmetric cryptographic schemes* without absolute security such as AES. Such a scheme would invalidate the claim of absolute security against computationally unbounded adversaries.

It is also important to emphasise that the security guarantees of QKD protocols can only hold and be proven in a theoretical model. Any practical implementation of a QKD protocol, just like any other cryptographic implementation, will have imperfections and deviate from the theoretical model. In fact, several QKD systems have been demonstrated to be insecure due to attacks depending on the physical properties of the concrete devices used to implement QKD protocols, see for example [11]. Thus, rigorous evaluation of QKD systems is required to obtain an assurance about the security of concrete implementations. Claims about "absolute" or "unconditional" security allegedly offered by QKD can never apply to actual implementations.

3 How QKD is technologically limited

Current QKD technology has a number of limitations. Therefore, for the time being, QKD can in practice only be considered for some niche use cases and *post-quantum cryptography* and *symmetric* keying (with pre-shared symmetric keys) must be the primary solutions for *quantum-safe cryptography*. In the following, we briefly explain some of the limitations of QKD.

Need for specialised hardware and high costs

In contrast to *post-quantum* and *classically secure public-key cryptography*, QKD cannot be implemented on classical computing hardware. It requires specialised hardware such as single-photon sources and detectors. Currently, the acquisition of this equipment as well as the maintenance of a QKD system or network over its entire life cycle is associated with very large costs. Needless to say, such equipment cannot be deployed to every individual user that needs secure communication, nor is it suitable for use with mobile devices. Moreover, the basic claim of QKD, namely that any attempt at eavesdropping is detected, turns each such attempt into a denial-of-service attack. More generally, any interference with the communication channel (even if not explicitly measured by an adversary) will lead in practice to denial of service. This threat has not been thoroughly studied yet and the costs of protecting quantum channels against such attacks are still unknown.

Distance limitations and *end-to-end security*

Signal losses in fibre-optic cables grow exponentially as a function of distance. Therefore, it is currently not possible to reliably transmit quantum states via fibre-optic cables over longer distances. QKD demonstrations at present can reach at most a few hundred kilometres and commercial QKD systems typically reach about one hundred kilometres [8]. Over longer distances, trusted nodes must be introduced so that a key is agreed between each pair of neighbouring nodes at a time. Thus, at present, *end-to-end security* cannot be achieved over long distances using fibre-based QKD.

One possible solution to reach longer distances is the use of quantum repeaters based on quantum entanglement. Quantum repeaters are still the subject of fundamental research and not practical at present. An alternative is to use satellite-based QKD. However, current implementations mostly target non-geostationary orbits so that the availability of these satellites, which is also sensitive to weather conditions, is limited to a short timeframe per day. This further limits the practical key rate. Furthermore, the satellites themselves constitute trusted nodes in most current implementations. A satellite infrastructure for QKD naturally adds very significant costs.

Reliance on classical cryptography for peer authentication

As explained before, QKD requires a classical authenticated channel between the communicating parties. There are several options for how to implement an authentication mechanism. One option is the use of pre-shared keys with *symmetric* message authentication. To this end, a secret shared key must already be present at both ends wishing to communicate with each other before running a QKD protocol. Consequently, secret keys must be distributed and then periodically renewed in a secure manner before being able to perform QKD. Another option is to use post-quantum *signature schemes* with an associated *public-key infrastructure*. However, in this case, the authentication relies on the security of the post-quantum scheme.

4 Why QKD is not sufficiently mature

Because of its technological limitations, QKD is currently not suitable for use in most practical cases. Due to the high costs of current QKD technology, it would only be relevant to implement in situations where the specific security requirements can justify such costs and where, at the same time, less expensive options would not be feasible. Even in cases where QKD might be identified as a good fit, a lot more work is required to have confidence in the security of concrete QKD devices. The following aspects are some of the most important ones that still need a significant amount of work. However, this is not an exhaustive list and there are other issues which also require attention.

QKD protocol standards

Developing secure cryptographic algorithms and protocols is hard and even experts make mistakes in designing these. Therefore, in the cryptographic community, there is a consensus about the importance of standardising cryptographic algorithms and protocols. Besides enabling interoperability, standardisation is crucial for security because it allows experts to rigorously scrutinise the cryptographic mechanisms. Such a process, for example the NIST process for *post-quantum cryptography*, usually runs for several years, and can yield a high level of confidence in the schemes that are standardised in the end.

The same should hold for QKD protocols. However, to the best of our knowledge, no QKD protocol has undergone such a standardisation process.

QKD security proofs

As explained above, on a theoretical level, QKD protocols can provide security based on quantum-physical principles without requiring assumptions about the hardness of mathematical problems. To be confident that a given QKD protocol provides this kind of security and to quantify the level of security, rigorous security proofs are required. A security proof should describe the QKD protocol in a precise mathematical

model with well-stated assumptions, and derive a precise statement expressing and quantifying the security of the protocol in this model. In order for a security proof, which is purely theoretical and conducted in an abstract model, to relate to the security of an actual implementation in a meaningful way, the security statement should be proved in a model that reflects realistic conditions as much as possible.[1] Furthermore, it is important that all aspects of the protocol be formalised in the model so that the proof is sufficiently rigorous and gaps or errors are avoided. There have in fact been commercially used QKD protocols which lacked a sufficient security proof and later turned out to be insecure [7].

Over the past years, a lot of research has been carried out on the subject of QKD security proofs and the field has advanced significantly [16]. However, to the best of our knowledge, no security proof for a practically relevant protocol has been written up in a cohesive and comprehensive way that satisfies the requirements outlined above. To have confidence in the theoretical security of QKD protocols, standardised QKD protocols with matching precise and comprehensive security proofs that take a realistic model into account are required. These need to be widely available and accessible to be scrutinised by various experts.

Evaluation criteria and methodology

Standardised QKD protocols with matching security proofs alone are not sufficient. The existence of broad families of physical attacks against QKD devices [3] implies that all the physical devices used to implement them must also undergo a rigorous evaluation procedure. Recognised evaluation criteria and methodologies are required in order to provide an assurance that QKD protocols have been correctly implemented in concrete devices and that the implementation is not susceptible to physical attacks. Some work has been done in this regard. A Common Criteria Protection Profile for one important class of QKD protocols, so-called prepare-and-measure QKD, was funded by the BSI and developed in collaboration with ETSI. Additionally an ISO/IEC standard on security requirements and test and evaluation methods for QKD [9, 10] has been published. However, a lot of work remains. For example, QKD-related standards as well as an evaluation methodology for physical attacks against QKD systems still need to be developed. This may also require additional research in this area.

5 Conclusion

QKD is an interesting technology and research on this topic should be continued in order to investigate if there are ways to overcome some of the limitations of the current technology. Furthermore, the underlying technology may be useful for other applications.

Due to current and inherent limitations, QKD can however currently only be used in practice in some niche use cases. For the vast majority of use cases where classical *key agreement schemes* are currently used it is not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently mature from a security perspective. A lot more work is required to build sufficient confidence in QKD protocols and in QKD devices that implement such protocols – including but not limited to work on protocol standards, on other QKD-related standards, on security proofs, and on evaluation methodologies.

Post-quantum cryptography, on the other hand, can be implemented on classical hardware and thus be deployed in classical communication infrastructures; standardisation of schemes and their integration in protocols and data formats is quite advanced and several schemes based on different mathematical assumptions are available, thus minimising the risk. In light of the urgent need to stop relying only on quantum-vulnerable *public-key cryptography* for key establishment, the clear priority should therefore be the migration to *post-quantum cryptography* in hybrid solutions with traditional *symmetric* keying or *classically secure public-key cryptography*.

[1] For example, the attack model should be as general as possible, loss in the quantum channel as well as imperfections in the detectors should be considered, and the security statement should hold for finite key sizes and not only asymptotically, i.e. not only in the limit of infinitely many exchanged signals.

6 Glossary

Term	Definition
Classically secure public-key cryptography	Public-key cryptographic mechanisms which are, in contrast to post-quantum cryptography, not secure against attacks by large-scale quantum computers. This includes RSA and elliptic-curve cryptography.
End-to-end security	Ensures that only the communicating parties, and no passive or active intermediaries, can gain access to the plaintext of the messages exchanged in a communication protocol.
Key agreement scheme	A mechanism or protocol allowing two parties to agree on a shared secret key via an insecure communication channel. Typically these secret keys are then used to encrypt plaintext messages using symmetric cryptography.
One-time pad	A symmetric encryption scheme which provides perfect secrecy, in the sense that no information about the plaintext can be derived from the ciphertext (except for an upper bound on its length). The scheme requires every encryption key to be used at most once and to be the same length as the plaintext or longer. Therefore, it is rarely used.
Post-quantum cryptography	Public-key cryptographic mechanisms which are secure against attacks by both classical and quantum computers. Post-quantum cryptography can be implemented on classical computers.
Public-key cryptography	Also known as asymmetric cryptography. A form of cryptography where a key pair, consisting of a public key and a private key, is used for all operations. For instance, anyone can encrypt plaintext messages using the public key, but only the private key can be used to decrypt the resulting ciphertext messages, when public-key cryptography is used to provide confidentiality. Similarly, the private key is used to generate signatures whereas the public key can be used by anyone to verify the resulting signatures when public-key (asymmetric) cryptography is used for authentication or non-repudiation. For this to work in practice, the public and private keys in the key pair must of course be strongly related. The security of public-key cryptography is therefore typically based on the hardness of very specific mathematical problems.
Public-key infrastructure	A system that can create, distribute, store, verify and revoke digital certificates and that is generally used for the management of public keys to enable the use of public-key cryptography.
Quantum computer	A computer that leverages quantum-mechanical phenomena to perform computations, in contrast to the classical computers of today that instead leverage classical phenomena to perform computations. Quantum computers are capable of solving some problems faster than classical computers.
Quantum-safe cryptography	Cryptographic mechanisms and protocols that are secure against attacks by both classical and quantum computers. This includes both post-quantum cryptography and quantum key distribution.
Signature scheme	A form of public-key cryptography that can be used to generate and verify signatures, for instance for the purpose of authenticating messages.
Symmetric cryptography	A form of cryptography where the same key is used for all operations. For instance, the same key is used both to encrypt plaintext messages and to decrypt the resulting ciphertext messages when symmetric cryptography is used to provide confidentiality. Similarly, the same key is used both to generate and to verify authentication tags when symmetric cryptography is used for message authentication.

7 References

[1] ANSSI: ANSSI views on the Post-Quantum Cryptography transition (2023 follow up), https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography (29/08/2023)

[2] ANSSI: Should Quantum Key Distribution be Used for Secure Communications? (ANSSI – Technical Position Paper: QKD v2.1), https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications

[3] BSI: Implementation Attacks against QKD Systems, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.html (21/12/2023)

[4] BSI: Quantum-Safe Cryptography, www.bsi.bund.de/dok/pqmigration-en (18/05/2022)

[5] M. Ekerå, Swedish NCSA, Swedish Armed Forces, "The quantum threat to cryptography, our mitigation strategy, and our stance on quantum key distribution", keynote at the NATO IST-SET-198 Symposium, Amsterdam, the Netherlands, October 3–4, 2023.

[6] M. Ekerå, Swedish NCSA, Swedish Armed Forces, "Advice on mitigating the quantum threat to cryptography", presentation at the ESA workshop, Noordwijk, the Netherlands, June 27, 2022.

[7] Javier González-Payo, Róbert Trényi, Weilong Wang, and Marcos Curty. Upper security bounds for coherent-one-way quantum key distribution. Phys. Rev. Lett., 125:260510, Dec 2020.

[8] Huttner, B., Alléaume, R., Diamanti, E. et al. Long-range QKD without trusted nodes is not possible with current technology. npj Quantum Inf 8, 108 (2022). https://doi.org/10.1038/s41534-022-00613-4

[9] ISO/IEC 23837-1:2023. “Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements”, https://www.iso.org/standard/77097.html

[10] ISO/IEC 23837-2:2023. “Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods”, https://www.iso.org/standard/77309.html

[11] Lydersen, L., Wiechers, C., Wittmann, C. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon 4, 686–689 (2010). https://doi.org/10.1038/nphoton.2010.214

[12] NCSC: Quantum security technologies, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies (24/03/2020)

[13] NLNCSA: Prepare for the threat of quantum computers, https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers (18/01/2022)

[14] NSA: Announcing the Commercial National Security Algorithm Suite 2.0, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF (07/09/2022)

[15] NSA: Quantum Key Distribution (QKD) and Quantum Cryptography (QC), https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[16] Christopher Portmann and Renato Renner. Security in quantum cryptography. Rev. Mod. Phys., 94:025008, Jun 2022.

[17] Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press. pp. 124–134.

[18] TNO, CWI, AIVD: The PQC Migration Handbook, https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook (03/2023)