The debate over QKD: A rebuttal to the NSA's objections

Renato Renner^{1,2} and Ramona Wolf^{1,2}

A recent publication by the NSA assessing the usability of quantum cryptography has generated significant attention, concluding that this technology is not recommended for use. Here, we reply to this criticism and argue that some of the points raised are unjustified, whereas others are problematic now but can be expected to be resolved in the foreseeable future.

1 Summary of criticism and replies

The recent publication [Natc] by the National Security Agency (NSA) of the United States assesses the usability and current technical limitations of quantum cryptography and, in particular, quantum key distribution (QKD). It identifies several challenges and concludes that using QKD is not recommended until these challenges are overcome. Similar views have been expressed by the National Cyber Security Center of the UK government [Nata] and the Agence Nationale de la Sécurité des Systèmes d'Information of the French government [Age]. While some of the criticism has been addressed in earlier work (see, for example, [SK14, DLQY16, Qua, All21]), we provide here specific replies to all points raised in [Natc]. We analyze the limitations raised and discuss to what extent the claims are justified and how QKD can overcome these challenges.¹

First, we give an overview of the five technical limitations mentioned in [Natc] and present a high-level summary of our replies. Our detailed answers are shown in the next section. The technical terms throughout this note are explained in the Glossary at the end. The text in italics reproduces the statements in [Natc]. Our assessment of whether these limitations are problematic now, in the medium-term and long-term future, is summarized in Table 1. To avoid providing specific time frames for the terms "medium-term" and "long-term", we have chosen to define them based on technological milestones—the realization of quantum repeaters and universal quantum computers, respectively. This approach is favorable due to the inherent challenge in predicting when these milestones in hardware development will be achieved. By adopting this strategy, we aim to offer an assessment that remains independent of the pace of this development.

Limitation 1: Quantum key distribution is only a partial solution.

(a) QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e., entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication.

Renato Renner: renner@ethz.ch Ramona Wolf: rawolf@phys.ethz.ch

¹Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland

²Quantum Center, ETH Zurich, 8093 Zurich, Switzerland

¹A short version of these replies has already appeared in [RW23].

		Problematic now	Problematic medium term	Problematic long term		
Limitation 1	(a)	not within scope of QKD				
	(b)	see Table 2	no	no		
Limitation 2	(a)	yes	no	no		
	(b)	not specific to quantum (vs. classical) cryptography				
Limitation 3	(a)	yes	to some extent	to some extent		
	(b)	yes	no	no		
Limitation 4		yes	yes	no		
Limitation 5		yes	yes	no		

Table 1: Summary of our assessment of whether Limitations 1-5 are problematic now, in the medium-term, and long-term future. By "medium-term future" we mean the epoch when cheaper optical equipment and quantum repeaters are widely available, whereas "long-term future" refers to the era when universal quantum computers connected by a quantum network are realized.

While correct, this statement cannot be regarded as a limitation specific to quantum cryptography. Authentication always requires either a pre-shared secret or a trusted third party, independently of whether one uses classical or quantum technology. It is not the goal of QKD to solve this problem.

(b) Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better-understood risk profile.

QKD protocols come with a mathematical proof that they are information-theoretically secure. Conversely, the security of post-quantum cryptography (PQC) protocols—referred to as quantum-resistant cryptography above—is only as well understood as that of classical (computationally secure) schemes. The lack of quantitative security proofs for the latter is a significant problem, evidenced by a long history of misjudgments. Hence, regarding its protocol security, QKD arguably has a better-understood risk profile than PQC (see also Fig. 2). The situation is a bit different if one considers implementation security (see Table 2), which is addressed by Limitation 4 (discussed below).

Limitation 2: Quantum key distribution requires special purpose equipment.

(a) QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment.

The requirement of dedicated and, thus, expensive hardware is indeed one of the main reasons why QKD is not widely usable today. Nonetheless, such hardware is expected to become more readily available with future advances in optical communication technology.

(b) Since QKD is hardware-based, it also lacks flexibility for upgrades or security patches.

Any cryptographic scheme, classical or quantum, ultimately runs on hardware, which may be prone to side-channel attacks. The difficulty of patching flawed hardware is thus not a problem specific to quantum cryptography.

Limitation 3: Quantum key distribution increases infrastructure costs and insider threat risks.

QKD networks frequently necessitate the use of trusted relays, entailing

(a) additional cost for secure facilities and

(b) additional security risk from insider threats.

This eliminates many use cases from consideration.

At the current state, QKD protocols indeed require trusted intermediate stations to achieve longer distances. However, this will change once quantum repeaters are developed. These devices work entirely on the quantum level and hence don't need to be trusted. This eliminates any insider threats and point (b) will no longer be an issue. Regarding (a), while QKD hardware costs are expected to decrease in the coming years, they will likely remain more expensive than classical communication infrastructure.

Limitation 4: Securing and validating quantum key distribution is a significant challenge.

The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.

The gap between theoretical and implementation security is a general issue in cryptography, already on the classical level. Since quantum communication is a relatively young field, it lacks experience with these problems and is still prone to side-channel attacks (cf. Table 2). However, this can be resolved by (semi-) device-independent QKD, which requires only minimal (weak) assumptions about the quantum devices and is thus robust against such attacks. Even though this technology is preliminary, it provides a clear path to overcoming this challenge in the long-term future.

Limitation 5: Quantum key distribution increases the risk of denial of service.

The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

Current implementations of QKD are usually individual point-to-point links. An adversary with access to the link may successfully run a denial-of-service attack. However, future quantum cryptographic solutions are expected to run on a network of quantum connections. Like in classical communication networks, information can be rerouted if one of the links fails to function. Once this stage is reached, there will be no fundamental difference between classical and quantum cryptography regarding their vulnerability to denial-of-service attacks.

2 Detailed replies

2.1 Limitation 1

Limitation 1(a)

This limitation concerns the fact that QKD does not provide authentication but instead relies on an already established authentic classical communication channel.

Authentication has its price: A party A who wishes to ensure that a message originates from a party B must either have a pre-shared secret from B or invoke a trusted third party (TTP) who identifies B towards A, as illustrated in Figure 1. (We refer to Chapter 21 of [BS23] for a description of how a TTP can facilitate authentication between parties with no prior relationship.) This price must be paid, independently of whether one uses classical or quantum cryptographic protocols. Hence, the reliance of QKD on authenticated communication is not a problem specific to quantum cryptography.

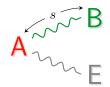
Crucially, the need for authentication does not compromise the information-theoretic security QKD provides. It has been shown that a small initial secret (for example, a password) shared by A and B is sufficient to establish authentication between them that is information-theoretically

No initial information:

Pre-shared secret s:

Trusted third party:





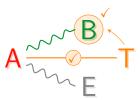


Figure 1: **Authentication.** Without any initial information about Bob (B), there is no way for Alice (A) to distinguish whether a message she receives is from him or from an adversary Eve (E) who pretends to be B (left figure). Any authentication scheme (classical or quantum) must rely on something that breaks the symmetry between B and E (from A's viewpoint). This could be a pre-shared secret s held by A and B (middle figure). Alternatively, A could rely on a trusted third party (T) who can distinguish B from E, which requires some initial authenticated connection between A and T (right figure).

secure [RW04, DW09]. Alternatively, if A and B invoke a TTP, information-theoretically secure authentication between them can be established whenever A and B's initial link to the TTP is information-theoretically secure.¹

Even if the authentication method used in QKD is not information-theoretically secure but instead relies on (computationally secure) asymmetric cryptography, QKD remains future-proof in the sense that "store now decrypt later" attacks do not work. An attacker would have to hack the authentication procedure in real-time to gain access to the generated key. Merely storing the messages exchanged and waiting for more powerful computers to decrypt them would not be sufficient to obtain the key. Once the key generation process is finished, even a complete breach of the authentication procedure does not reveal any information on the generated key.

Limitation 1(b)

In this part of the criticism, it is argued that the confidentiality provided by QKD may as well be achieved with post-quantum cryptography (PQC) [BL17] (also known as quantum-resistant or quantum-safe cryptography), and it is claimed that the latter has a better-understood risk profile.

To be able to compare the risk profiles of quantum cryptography and PQC, we distinguish two aspects (see Table 2):

- 1. Protocol security, which describes the theoretical security of the protocol.
- 2. Implementation security, which describes the security of the actual implementation of a protocol (which can deviate from the theoretical description.)

The protocol security of PQC relies on the assumption that a given mathematical problem is hard to solve for classical and quantum computers. The crux is that evidence for such an assumption is sparse. It depends on how many mathematicians or computer scientists have already tried to solve the problem and for how long. The list of problems considered "hard" is thus generally shrinking over time (Figure 2). Furthermore, while researchers have decade-long experience regarding hard problems for classical computers, quantum computing is relatively young, and it is conceivable that novel quantum algorithms for solving problems that were initially considered hard will be discovered (as was already the case for the factoring problem).

A PQC protocol may thus turn insecure overnight. This is not merely a theoretical concern but a practically relevant threat, as evidenced in the context of the standardization process for PQC of the National Institute of Standards and Technology (NIST) [Natb]. This search spanned several years until some finalists for standardization, as well as some alternatives, were announced in 2022. However, it only took a couple of months until one of the alternatives, called SIKE

¹If A and B each have an authenticated and secure link with the TTP, this can be used to equip A and B with a small shared secret s. Afterwards, the two parties are again in the middle scenario of Figure 1, in which case information-theoretic authentication is possible as argued before.

		now	medium term	long term
PQC -	Protocol security	bad	bad	bad
	Implementation security	reasonably good	reasonably good	reasonably good
QKD —	Protocol security	good	good	good
	Implementation security	bad	increasing	good

Table 2: Comparison of how well protocol security and implementation security of post-quantum cryptography (PQC) and quantum key distribution (QKD) is understood. Protocol security refers to the abstract protocol. For classical protocols, it usually relies on the conjectured hardness of certain mathematical problems, such as factoring, which is difficult to quantify. Conversely, in quantum cryptography, protocol security relies on physical laws. Implementation security depends on the safety of the hardware and software on which the abstract protocols are run, such as their robustness against side-channel attacks. Here classical cryptography has an advantage compared to quantum cryptography due to the experience acquired over many decades, whereas quantum hardware and software engineering is still in the early stages.

(which is short for supersingular isogeny key encapsulation), was broken on a single-core classical computer [CD22].

The history of cryptography is full of other examples that illustrate the difficulty of assessing and quantifying protocol security of computational cryptography in general. For instance, the inventors of the widely-used RSA encryption scheme initially calculated that factoring a 200-digit number would take a few billion years with the best-known factoring method [RSA78, Table 1], which is on the order of the estimated remaining lifespan of the universe. As a result, they recommended the use of 200-digit keys. Nonetheless, in 2020, a 250-digit number was factored [BGG⁺20].

Conversely, the protocol security of QKD is provable based on the laws of physics. It is thus unaffected by algorithmic discoveries or hardware developments. In addition, the protocol security can be quantified in terms of a bound on the probability that the protocol is broken. The risk profile of QKD protocols is thus perfectly understood (see Figure 2). Hence, regarding protocol security, QKD has a clear advantage compared to PQC.

PQC, however, has an advantage compared to QKD in terms of implementation security, although this advantage is temporary. Implementations of PQC can draw on decades of experience with classical computers, which has led to a good understanding of potential side-channel attacks. On the other hand, the implementation security of QKD is still in the exploratory stage. As QKD is a relatively young technology, researchers have only little experience with possible side-channel attacks and countermeasures. Still, this understanding will increase in the coming years. Furthermore, in the medium and long term future, the issue can be resolved with semi-device-independent and fully device-independent QKD, respectively (see the discussion of Limitation 4).

2.2 Limitation 2

This limitation concerns the need for dedicated hardware when implementing QKD.

Limitation 2(a)

The first part of this criticism is that QKD cannot be easily integrated into existing network equipment.

QKD requires a communication link that transports information encoded into one single quantum optical mode from sender to receiver at high fidelity. In today's implementations of quantum cryptography, this is realized by point-to-point optical fiber or free-space connections. Current optical communication networks, however, do not provide such high-fidelity links. Hence, integrating QKD indeed requires expensive special-purpose hardware.

Nonetheless, the steady improvements in the efficiency of classical optical communication are expected to eventually reach a point where one (or even more) bits are encoded per photon [BKJJ20]. In this way, classical technology will naturally approach the requirements for quantum communication, thus facilitating a more straightforward and cheaper integration of QKD.

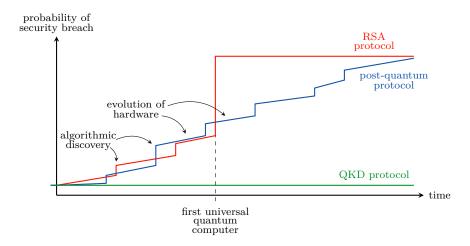


Figure 2: **Protocol security of cryptographic protocols over time.** The diagram shows schematically the development of the probability that an encryption protocol is broken if the adversary has all the computational power in the world as a function of time. Classical protocols (including post-quantum ones), which aim to provide computational security, are becoming increasingly insecure due to the evolution of hardware and algorithmic discoveries. If an efficient quantum algorithm is found for breaking it (which is the case for RSA), the scheme will become insecure once the first universal quantum computer is available. On the other hand, the failure probability of quantum key distribution always remains the same because it only relies on the laws of quantum physics, which don't change over time. This figure is taken from [RW23].

Limitation 2(b)

The second part of Limitation 2 refers to the difficulty of administering security patches.

Here it is again helpful to distinguish protocol and implementation security as in the discussion of Limitation 1 (b). Since QKD comes with a mathematical proof of security, the protocol parameters do not require any updates. This is different in computational cryptography, where algorithmic or hardware breakthroughs may imply that security parameters, such as the key length of RSA [BD15], need to be adapted.

Regarding implementation security, there is no fundamental difference between classical and quantum cryptography. If hardware is found to be flawed or prone to side-channel attacks, patches on the hardware level will be required in both cases.

2.3 Limitation 3

This limitation derives from the claim that QKD networks require trusted relays.

It is correct that current implementations of QKD require trusted relays. The typical information carrier in quantum communication is single photons. Since the loss of photons in optical fibers is typically very high, at the moment, intermediate stations are required to achieve large distances [HAD+22]. The problem of signal losses arises in classical communication, too, requiring the use of repeaters. They measure the incoming signal, copy it, and retransmit it to the other side at higher power, thus effectively amplifying the signal. But the same technique does not work for quantum information, because copying it is prohibited fundamentally, as asserted by the no-cloning theorem [WZ82, Die82]. Therefore, current implementations of QKD are restricted to point-to-point connections that have no repeaters in between. When combining such point-to-point connections to form a network, the communication must be encoded and decoded separately for any link of the network (see Figure 3). But since the intermediate nodes need to store secret *classical* information, they must be trusted.

However, the need for trusted relays is not fundamental—quantum repeaters [BDCZ98, SSdRG11, AEE⁺22] will replace them in the medium-term future. Quantum repeaters work coherently on the quantum level and are thus secured by the laws of quantum theory in the same way as QKD is secured by these laws. Hence, even if they are hacked and controlled by a quantum adversary,

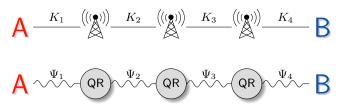


Figure 3: Long-distance QKD via trusted intermediate stations vs. quantum repeaters. The use of trusted intermediate stations, depicted as (\mathbb{Q}) , requires establishing a secret key K_i on each segment. Since these keys are secret classical information, the stations must be trusted. Quantum repeaters (QR), on the other hand, work entirely on the quantum level (illustrated by quantum states Ψ_i). ¡They are hence secured by the laws of quantum theory and don't have to be trusted.

security is still guaranteed. While this method is well-established in theory, it has yet to be experimentally realized. The main obstacle is that a quantum repeater requires quantum memory. The storage time of state-of-the-art quantum memories is insufficient to outperform direct optical links, despite considerable progress in recent years [LHL+21, LRGR+21, RCAW22]. However, since quantum memories are a crucial part of quantum computers, they are being intensively researched on various technology platforms.

Limitation 3(a)

This part of the criticism concerns the costs for trusted relays.

As explained above, current implementations of QKD require trusted relays. These must be placed in secure facilities, which are costly.

In the medium-term future, the trusted relays can be replaced by quantum repeaters. While it is expected that these devices become cheaper as optical technology develops (see also Limitation 2(a)), building a quantum communication network will most likely remain more expensive than the corresponding infrastructure for classical communication.

Limitation 3(b)

This part of the criticism refers to security risks from insider threats.

Security proofs of QKD extend directly to links with intermediate quantum repeaters. Hence, in the medium-term future, when trusted nodes are replaced by quantum repeaters, there do not occur any additional risks from insider threats.

2.4 Limitation 4

This limitation refers to the gap between the security of the theoretical protocol and the security of the practical implementation.²

Devices used within an implementation, such as quantum sources and detectors, often deviate from their theoretical description. This can open up side channel attacks, which exploit such imperfections, both of the quantum source and the detector (see [MAS06, LWW⁺10, GLLL⁺11] for some examples). One approach to prohibit such attacks is to adapt the protocols, or the relevant parameters, in such a way that known imperfections can be tolerated (see, for example, [GLLP04, TCK⁺14, PCLN⁺23]). However, the imperfections are often unknown, especially in real-world implementations, where the devices are exposed to changing environmental conditions.

²One should note that, while for post-quantum cryptography the implementation security is generally better understood (see Table 2), one still has to watch out for new developments regarding side-channel attacks. A recent example that illustrates this fact comes from advances in artificial intelligence (AI) research. Attacks based on machine learning can analyze large amounts of measurable data obtained from a device running the implementation, such as timing and power consumption, possibly recovering the original message. This was, for example, demonstrated for one of the finalists of the NIST standardization process called CRYSTALS-Kyber [DNG22]. Even though this kind of attack does not break the algorithm itself but is a side-channel attack on the *implementation*, it shows that AI-assisted attacks pose a real threat to the practical security post-quantum and classical cryptography can offer.

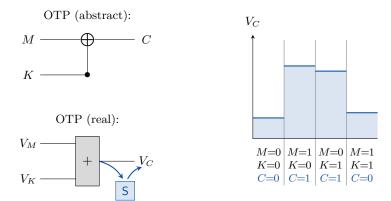


Figure 4: Difference between abstract description and implementation of the OTP. Adding up the voltages V_M and V_K results in a voltage V_C . To ensure the secrecy of the message, this voltage has to be the same regardless of how C was computed (e.g., V_0 should not depend on whether C=0 was the result of adding 0 and 0 or 1 and 1.) In practice, this can never be achieved perfectly. Hence, an adversary could gain access to the key and message by simply measuring the (public) signal V_C . However, it is not an issue in actual implementations because data is usually stored (illustrated by the storage container S) before it is sent over a communication channel, hence noise in the system changes the voltage slightly, effectively disguising the key and message values.

A different approach to ruling out the possibility of side-channel attacks is semi-device-independent or device-independent QKD. Here security is guaranteed from weak or even minimal assumptions about the quantum source and the detector (see, for example, [PAB+09, BP12, LCQ12]), thus narrowing the gap between protocol and implementation security. This high level of security comes, however, at a cost: In the fully device-independent case (where neither the source nor the detectors need to be characterized), the protocols require the demonstration of a loophole-free Bell test, which poses significant challenges to the experimental implementation. In 2021, the first experimental demonstrations of DIQKD have been reported [NDN+22, ZvLR+22, LZZ+22], but the achieved parameters are still far from practical values. On a positive note, once universal quantum computers are available, they will allow for the creation of perfect Bell pairs on their logical (i.e., error-corrected) qubits. Even though this technology is preliminary, it provides a clear path toward fully secure QKD implementations.

Classical cryptography suffers, in principle, the same threat, that is, implementations may be insecure. Indeed, side-channel attacks are a huge topic in classical cryptography and an active area of research (see [AGM16, WGSW18, RD20, PYSJ22] for some examples). One example is the implementation of a one-time pad (OTP) with special-purpose hardware that consists of one gate that computes the XOR between the key and the message (see Figure 4). This gate combines the voltages corresponding to the message bit M and the key bit K, resulting in a voltage representing the ciphertext bit C. There are always two ways in which the value of C could have been created: C = 0 can result from adding M = 0 and K = 0 or M = 1 and K = 1. Similarly, C = 1 can be the result of adding M = 1 and K = 0 or M = 0 and K = 1. The system's security depends on ensuring that the voltage V_C representing the ciphertext bit is identical regardless of which message and key bits have been used. However, perfect equality can never be achieved in practice (as shown on the right-hand side of Figure 4), which means that an adversary who measures the voltage V_C accurately enough can access both the message and the key values.

The example illustrates that the problem arises in implementations where information is encoded very directly (i.e., without further stages, such as the storage of information in memory) into the state of a physical system. While this is the case in current QKD implementations, this is not a problem inherent to the use of quantum information.

2.5 Limitation 5

In this last point, it is claimed that QKD increases the risk of denial of service.

Classical communication networks consist of many connections, allowing for a rerouting of

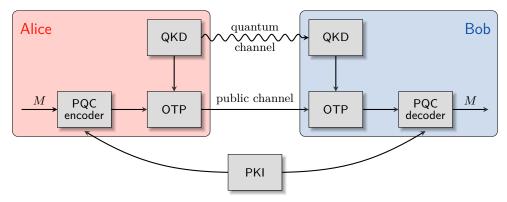


Figure 5: **Hybrid QKD and PQC cryptosystem.** A message M is first encrypted via a PQC scheme, which requires some (quantum-safe) public-key infrastructure (PKI) to distribute the required keys. The ciphertext is then additionally encrypted via a one-time pad (OTP), which uses keys from a QKD scheme.

communication if one of these connections fails to function correctly. This redundancy helps protect them against denial-of-service attacks. Conversely, current implementations of QKD are usually based on individual point-to-point links, and an adversary with access to the link may thus easily interrupt the service. However, this is not a problem that is intrinsic to QKD. Instead, it is a consequence of the high price tag of quantum communication technology, which currently prevents us from building quantum networks with many links (see the discussion of Limitation 2 (a)). In the long-term future, when larger quantum communication networks, or even a quantum internet [WEH18, PHB+21, RCAW22, CWB23], are available, denial-of-service attacks can be countered by rerouting, pretty much the same way as this is done in classical networks.

3 Outlook and recommendation

The issues highlighted in [Natc] are significant and impose severe limitations on the current usability of quantum cryptography. However, it is important to note that these limitations are not inherent to quantum cryptography but rather due to the early stage of the novel hardware required. Some of these limitations can be resolved in the medium-term future with the availability of cheaper and improved quantum technology (see Table 1). Overcoming the remaining limitations, though, will require a long-term investment in developing quantum communication technology.

This, however, is worth the effort: Quantum cryptography has the potential to offer a true advantage over classical cryptography. Unlike traditional encryption schemes, which constantly need to be updated and strengthened to keep up with technological advancements, quantum cryptography breaks this cycle by providing protocol security that is invulnerable to all potential threats, including those posed by quantum computers. Not only do quantum cryptographic protocols gurantee secure communication during their execution, but they also offer everlasting security. Information communicated using quantum cryptography today will remain secure forever, regardless of future developments in software and hardware.

As quantum cryptography is not yet widely available, developing a strategy for securing sensitive data in the interim is essential. While standard encryption schemes such as RSA can still be used for data with a short shelf life (since universal quantum computers are not yet realized), data with a longer lifespan requires protection against "store now, decrypt later" attacks. Therefore, a combination of quantum key distribution (QKD) and post-quantum cryptography (PQC) in hybrid schemes currently offers the most secure approach to data encryption (this approach was, for example, explored in [DHP20, VA20, All21]). A concrete scheme may look as follows (see Figure 5): A message is first encrypted using a PQC scheme, which may rely on public-key infrastructure. In addition, the resulting ciphertext is encrypted using a one-time pad, with cryptographic keys generated via QKD. This combination of PQC and QKD provides future-proof encryption resistant to attacks from both quantum and classical computers. The one-time pad ensures that the encryption remains secure even if the PQC scheme is broken in the long-term future. At the same time, the PQC encryption guarantees that even an adversary able to exploit flaws in the QKD

implementation cannot read secret messages in the short or mid-term future. While this hybrid scheme requires additional infrastructure and thus still suffers from Limitation 3 (a) and 5, it remedies Limitation 4. As such, it can be a viable interim solution for the medium-term future, when Limitation 1 to 3 are (largely) overcome (see Table 1).

Finally, we note that another current limitation of QKD, not mentioned in the NSA report, is its still relatively low key generation rate. While this is unproblematic if one uses QKD to replace an AES key regularly, it imposes severe limits on the communication rate if one uses it for one-time-pad encryption. However, for the same reasons as discussed in our reply to Limitation 2 (a), we expect this shortcoming to be overcome in the medium-term future.

Acknowledgements

This work was supported by the Air Force Office of Scientific Research (AFOSR), grant No. FA9550-19-1-0202, the QuantERA project eDICT, the National Centre of Competence in Research SwissMAP, and the ETH Zurich Quantum Center.

References

- [AEE⁺22] Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin. Quantum repeaters: From quantum networks to the quantum internet. 2022. arXiv:2212.10820.
- [Age] Agence nationale de la sécurité des systèmes d'information (ANSSI). ANSSI views on the post-quantum cryptography transition. https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/. Retrieved on July 26, 2023.
- [AGM16] C. Ashokkumar, Ravi Prakash Giri, and Bernard Menezes. Highly efficient algorithms for AES key retrieval in cache access attacks. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016. 10.1109/eurosp.2016.29.
- [All21] Romain Alléaume. Quantum cryptography and its application frontiers. https://perso.telecom-paristech.fr/alleaume/HDRMainv10final.pdf, 2021. Habilitation, Sorbonne Université.
- [BD15] Elaine B. Barker and Quynh H. Dang. Recommendation for key management part 3: Application-specific key management guidance. Technical report, National Institute of Standards and Technology, 2015. 10.6028/nist.sp.800-57pt3r1.
- [BDCZ98] Hans J. Briegel, Wolfgang Dür, J. Ignacio Cirac, and Peter Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932–5935, 1998, 10.1103/physrevlett.81.5932. arXiv:quant-ph/9803056.
- [BGG⁺20] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, and Paul Zimmermann. Factorization of RSA-250. cado-nfs-discuss (Mailing list), 2020. https://sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html.
- [BKJJ20] Konrad Banaszek, Ludwig Kunz, Michal Jachura, and Marcin Jarzyna. Quantum limits in optical communications. *Journal of Lightwave Technology*, 38(10):2741–2754, 2020, 10.1109/jlt.2020.2973890. arXiv:2002.05766.
- [BL17] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017, 10.1038/nature23461.
- [BP12] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108(13):130502, 2012, 10.1103/physrevlett.108.130502. arXiv:1109.2330.
- [BS23] Dan Boneh and Victor Shoup. A graduate course in applied cryptography. https://toc.cryptobook.us/book.pdf, 2023. Version 0.6.

- [CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. Cryptology ePrint Archive, Paper 2022/975, 2022. https://eprint.iacr.org/2022/975.
- [CWB23] Jacob P. Covey, Harald Weinfurter, and Hannes Bernien. Quantum networks with neutral atom processing nodes. 2023. arXiv:2304.02088.
- [DHP20] Benjamin Dowling, Torben Brandt Hansen, and Kenneth G. Paterson. Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange. In *Post-Quantum Cryptography*, pages 483–502. Springer International Publishing, 2020. 10.1007/978-3-030-44223-1_26.
- [Die82] Dennis Dieks. Communication by EPR devices. Physics Letters A, 92(6):271–272, 1982, 10.1016/0375-9601(82)90084-6.
- [DLQY16] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. npj Quantum Information, 2(1), 2016, 10.1038/npjqi.2016.25. arXiv:1606.05853.
- [DNG22] Elena Dubrova, Kalle Ngo, and Joel Gärtner. Breaking a fifth-order masked implementation of CRYSTALS-Kyber by copy-paste. Cryptology ePrint Archive, Paper 2022/1713, 2022. https://eprint.iacr.org/2022/1713.
- [DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. ACM, 2009. 10.1145/1536414.1536496.
- [GLLL⁺11] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2(1), 2011, 10.1038/ncomms1348. arXiv:1011.0105.
- [GLLP04] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 5:325–360, 2004. arXiv:quant-ph/0212066.
- [HAD⁺22] Bruno Huttner, Romain Alléaume, Eleni Diamanti, Florian Fröwis, Philippe Grangier, Hannes Hübel, Vicente Martin, Andreas Poppe, Joshua A. Slater, Tim Spiller, Wolfgang Tittel, Benoit Tranier, Adrian Wonfor, and Hugo Zbinden. Long-range QKD without trusted nodes is not possible with current technology. npj Quantum Information, 8(1), 2022, 10.1038/s41534-022-00613-4. arXiv:2210.01636.
- [LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503, 2012, 10.1103/physrevlett.108.130503. arXiv:1109.1473.
- [LHL⁺21] Xiao Liu, Jun Hu, Zong-Feng Li, Xue Li, Pei-Yun Li, Peng-Jun Liang, Zong-Quan Zhou, Chuan-Feng Li, and Guang-Can Guo. Heralded entanglement distribution between two absorptive quantum memories. *Nature*, 594(7861):41–45, 2021, 10.1038/s41586-021-03505-3. arXiv:2101.04945.
- [LRGR⁺21] Dario Lago-Rivera, Samuele Grandi, Jelena V. Rakonjac, Alessandro Seri, and Hugues de Riedmatten. Telecom-heralded entanglement between multimode solid-state quantum memories. *Nature*, 594(7861):37–40, 2021, 10.1038/s41586-021-03481-8. arXiv:2101.05097.
- [LWW⁺10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, 2010, 10.1038/nphoton.2010.214. arXiv:1008.4593.
- [LZZ⁺22] Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, Ming-Han Li, Yang Liu, Jingyun Fan, Feihu Xu, Qiang Zhang, and Jian-Wei Pan. Toward a photonic demonstration of device-independent quantum key distribution. *Physical Review Letters*, 129(5):050502, 2022, 10.1103/physrevlett.129.050502. arXiv:2110.01480.

- [MAS06] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006, 10.1103/physreva.74.022313. arXiv:quant-ph/0511032.
- [Nata] National Cyber Security Center (NCSC). Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies. Retrieved on July 26, 2023.
- [Natb] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization. Retrieved on July 26, 2023.
- [Natc] National Security Agency (NSA). Quantum key distribution (QKD) and quantum cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. Retrieved on July 26, 2023.
- [NDN+22] David P. Nadlinger, Peter Drmota, Bethan C. Nichol, Gabriel Araneda, Dougal Main, Raghavendra Srinivas, David M. Lucas, Christopher J. Ballance, Kirill Ivanov, Ernest Y.-Z. Tan, Pavel Sekatski, Rüdiger L. Urbanke, Renato Renner, Nicolas Sangouard, and Jean-Daniel Bancal. Experimental quantum key distribution certified by Bell's theorem. Nature, 607(7920):682–686, 2022, 10.1038/s41586-022-04941-5. arXiv:2109.14600.
- [PAB⁺09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009, 10.1088/1367-2630/11/4/045021. arXiv:0903.4460.
- [PCLN⁺23] Margarida Pereira, Guillermo Currás-Lorenzo, Álvaro Navarrete, Akihiro Mizutani, Go Kato, Marcos Curty, and Kiyoshi Tamaki. Modified BB84 quantum key distribution protocol robust to source imperfections. *Physical Review Research*, 5(2):023065, 2023, 10.1103/physrevresearch.5.023065. arXiv:2210.11754.
- [PHB⁺21] Matteo Pompili, Sophie L. N. Hermans, Simon Baier, Hans K. C. Beukers, Peter C. Humphreys, Raymond N. Schouten, Raymond F. L. Vermeulen, Marijn J. Tiggelman, Laura dos Santos Martins, Bas Dirkse, Stephanie Wehner, and Ronald Hanson. Realization of a multinode quantum network of remote solid-state qubits. *Science*, 372(6539):259–264, 2021, 10.1126/science.abg1919. arXiv:2102.04471.
- [PYSJ22] Max Panoff, Honggang Yu, Haoqi Shan, and Yier Jin. A review and comparison of AI-enhanced side channel analysis. *ACM Journal on Emerging Technologies in Computing Systems*, 18(3):1–20, 2022, 10.1145/3517810.
- [Qua] Quantum Communications Hub. Community response to the NCSC 2020 quantum security technologies white paper. https://www.quantumcommshub.net/news/community-response-to-the-ncsc-2020-quantum-security-technologies-white-paper. Retrieved on July 26, 2023.
- [RCAW22] Julian Rabbie, Kaushik Chakraborty, Guus Avis, and Stephanie Wehner. Designing quantum networks using preexisting infrastructure. npj Quantum Information, 8(1), 2022, 10.1038/s41534-021-00501-3. arXiv:2005.14715.
- [RD20] Mark Randolph and William Diehl. Power side-channel attack analysis: A review of 20 years of study for the layman. *Cryptography*, 4(2):15, 2020, 10.3390/cryptography4020015.
- [RSA78] Ron L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978, 10.1145/359340.359342.
- [RW04] Renato Renner and Stefan Wolf. The exact price for unconditionally secure asymmetric cryptography. In *Advances in Cryptology EUROCRYPT 2004*, pages 109–125. Springer Berlin Heidelberg, 2004. 10.1007/978-3-540-24676-3_7.

- [RW23] Renato Renner and Ramona Wolf. Quantum advantage in cryptography. *AIAA Journal*, 61(5):1895–1910, 2023, 10.2514/1.j062267. arXiv:2206.04078.
- [Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Comput. Soc. Press, 1994, arXiv:quant-ph/9508027. 10.1109/sfcs.1994.365700.
- [SK14] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science*, 560:27–32, 2014, 10.1016/j.tcs.2014.09.015. arXiv:0906.4547.
- [SSdRG11] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33–80, 2011, 10.1103/revmodphys.83.33. arXiv:0906.2699.
- [TCK⁺14] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Physical Review A*, 90(5):052314, 2014, 10.1103/physreva.90.052314. arXiv:1312.3514.
- [VA20] Nilesh Vyas and Romain Alléaume. Everlasting secure key agreement with performance beyond QKD in a quantum computational hybrid security model. 2020. arXiv:2004.10173.
- [WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018, 10.1126/science.aam9288.
- [WGSW18] Meng Wu, Shengjian Guo, Patrick Schaumont, and Chao Wang. Eliminating timing side-channel leaks using program repair. In Proceedings of the 27th ACM SIG-SOFT International Symposium on Software Testing and Analysis. ACM, 2018. 10.1145/3213846.3213851.
- [WZ82] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. Nature, 299(5886):802–803, 1982, 10.1038/299802a0.
- [ZvLR+22] Wei Zhang, Tim van Leent, Kai Redeker, Robert Garthoff, René Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles C.-W. Lim, and Harald Weinfurter. A device-independent quantum key distribution system for distant users. Nature, 607(7920):687-691, 2022, 10.1038/s41586-022-04891-y. arXiv:2110.00575.

Glossary of technical terms

- "store now decrypt later" attacks exploit the fact that encrypted data can be intercepted during transmission and stored in its encrypted form, to be decrypted once more powerful (quantum) computers are available. These attacks pose a high risk to data that has a long shelf life, like medical records or military secrets. 4
- authentication refers to a method for ensuring that the identity of the claimed sender of a message is correct. Authentication requires some initial resources, e.g., a common password held by the sender and the receiver of the message. 2, 14
- computationally secure means that security is based on the assumption that a given mathematical problem is hard to solve on a computer. Cryptosystems that provide this type of security are thus vulnerable to potential future attacks that exploit breakthroughs in software development or novel hardware. 2, 14
- **cryptographic key** refers to a bit string that is uniformly random and secret, i.e., known only to the honest communicating parties. This string may then be used, for example, for one-time pad encryption. 14

- **implementation security** denotes the security of a practical implementation of a protocol (which can differ from the theoretical description). 2
- information-theoretically secure (also called unconditionally secure) means that security is based on information-theoretic principles. In contrast to a computationally secure cryptographic system, an information-theoretically secure system is immune even to attackers with unlimited computational power. 2, 14
- one-time pad (OTP) encryption is a scheme where a message and a cryptographic key are combined via binary addition. The resulting ciphertext does not reveal any information about the encrypted message, but can be decrypted with the same key. This encryption scheme is information-theoretically secure. 8, 13
- post-quantum cryptography (PQC) refers to classical cryptographic algorithms believed to remain secure even when universal quantum computers are available. The security of these algorithms relies on the assumption that a given mathematical problem is hard to solve for any computational device, including future quantum computers. Post-quantum cryptography is thus usually computationally secure but not information-theoretically secure. 2
- **protocol security** describes the theoretical security of a protocol. 2
- public-key cryptography is a cryptosystem that uses pairs of related keys, consisting of a public and a private key. The public key is openly distributed for others to encrypt data, which can only be decrypted by those who know the corresponding private key. Similarly, public-key cryptography enables other functionalities, such as authentication or electronic signatures. Public-key cryptography is usually computationally secure. 14
- **quantitative security proofs** give a quantitative bound on the probability that a security breach happens (cf. Figure 2). 2
- **quantum memory** is the quantum-mechanical analogue of classical computer memory. It stores quantum states for later retrieval. 7
- quantum repeaters allow to establish entanglement over long distances via a procedure called entanglement swapping, effectively enabling the transmission of quantum information over such distances. Since they work entirely on the quantum level, they are secured by the laws of quantum theory and hence don't have to be trusted. 1
- RSA is a classical algorithm for public-key cryptography that is nowadays widely used to encrypt data transmission, named after its inventors Rivest, Shamir, and Adleman [RSA78]. RSA is computationally secure, and the problem it relies on is factoring large numbers into prime factors. Because there exists a quantum algorithm for efficiently solving this problem [Sho94], RSA is vulnerable to attackers with access to a (universal) quantum computer. 5
- side-channel attacks do not target the encryption or key distribution protocol itself, but exploit deviations of the implementation from the theoretical description. This could, for example, be leaked information on timing or power consumption, or imperfections of the devices. 3
- **universal quantum computers** are quantum devices that are able to run any quantum algorithm. 1