Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Semi-Annual Report 2025/1

Quantum Technologies

Trends and Implications for Cyberdefence

Thun, August 19, 2025

Table of contents

1 Introduction and Trend Analysis

Vladimir Pfister, Cyber-Defence Campus, armasuisse
Evan Blezinger, Cyber-Defence Campus, armasuisse

1.1 Introduction

This third semi-annual report explores the field of quantum communications, focusing on technologies that promise to secure information in an era when quantum computers pose a significant threat to classical encryption. It examines quantum threats, quantum key distribution (QKD), and post-quantum cryptography (PQC), highlighting their unique contributions to improving security. The section emphasizes both the current applications and limitations of these technologies, including practical deployment challenges and scalability concerns. Additionally, it examines the ongoing debate between QKD and PQC. By addressing both the advancements and the barriers in these fields, it provides a comprehensive view of the future of quantum-safe communication.

Section 2 of this report explains that recent advances in quantum computing pose a threat to current asymmetric cryptography, which could be compromised by quantum algorithms (e.g., Shor's). In contrast, symmetric encryption and hashing are projected to maintain their resilience. While quantum computers currently lack the processing power to compromise security, the development of a novel quantum algorithm could potentially change this scenario in the coming years.

Section 3 describes QKD technology, which enhances secure communication by leveraging the principles of quantum mechanics to offer security that surpasses that of currently used mathematical approaches. It provides an overview of the current state and trends in QKD, highlighting advancements in single-photon sources and detection, which are driving its gradual adoption. Despite challenges related to cost, integration, and long-range quantum repeaters, QKD remains a promising solution to future quantum threats, complementing secure cryptographic protocols and PQC.

Section 4 explores the impact of large-scale quantum computers on the security of current encryption systems and highlights the urgency of developing solutions that are resistant to quantum attacks. It examines PQC, which provides protection against these threats while remaining compatible with existing infrastructures. The chapter further compares PQC to QKD, highlighting its advantages in terms of practicality and reliability.

The fifth and final section of this study, Section 5, explores the risks that quantum computing poses to conventional encryption systems and the necessity for more resilient solutions. They analyze PQC as a practical short- and medium-term response, while highlighting its limitations with respect to conventional cryptographic principles. Concurrently, an examination of QKD is illustrated, a method that promises superior information security but faces scalability and cost challenges. This article discusses these challenges and explores technological advances that could overcome these limitations.

1.2 Key Updates in Visual Trends Analysis

To offer quantitative trends related to quantum computing, visualizations were developed for the CYD Campus Semi-Annual Report 2024/2 [1] that rely on data from Crunchbase [2], Wikipedia [3], and OpenAlex [4]. These visualizations have been updated to illustrate developments since the publication of the previous report. In this new edition of the report, the visualizations are no longer presented as a single consolidated dashboard. Instead, they have been separated to allow for a more in-depth exploration of the data. The resulting visualizations offer a comprehensive overview of the growth trends in quantum computing from the point of view of research, market development, and technical progress. At the end of this section, a summary table highlights the key updates and differences between the visualizations in the previous edition and those in the current release.

These visualizations illustrate a dual perspective, with one viewpoint offering a comprehensive, global context and the other centered specifically on Switzerland. They offer insights into the rapid growth of quantum computing volume, the increasing number of publications, and the significant investments being made in companies that work in that field. This enables a thorough analysis of Switzerland's standing and its integration within the broader global context.

1.2.1 Quantum Volume Evolution

As illustrated in Figure 1, Quantinuum continues to dominate the field, demonstrating consistent growth in its quantum volume[1] since 2021. Notably, Quantinuum holds the distinction of being the first company to surpass a quantum volume of five digits, a milestone that underscores its pioneering position in the field [5]. In contrast, the volume of other companies, such as Alpine Quantum Technologie GmbH and IQM, has been stagnating since 2023 and 2024, respectively. Of particular interest is the observation that Quantinuum's quantum volume growth appears to have undergone a phase of deceleration since the midpoint of 2023.

[1] “Quantum volume is a metric that measures the capabilities and error rates of a quantum computer. It expresses the maximum size of square quantum circuits that can be implemented successfully by the computer” [3]

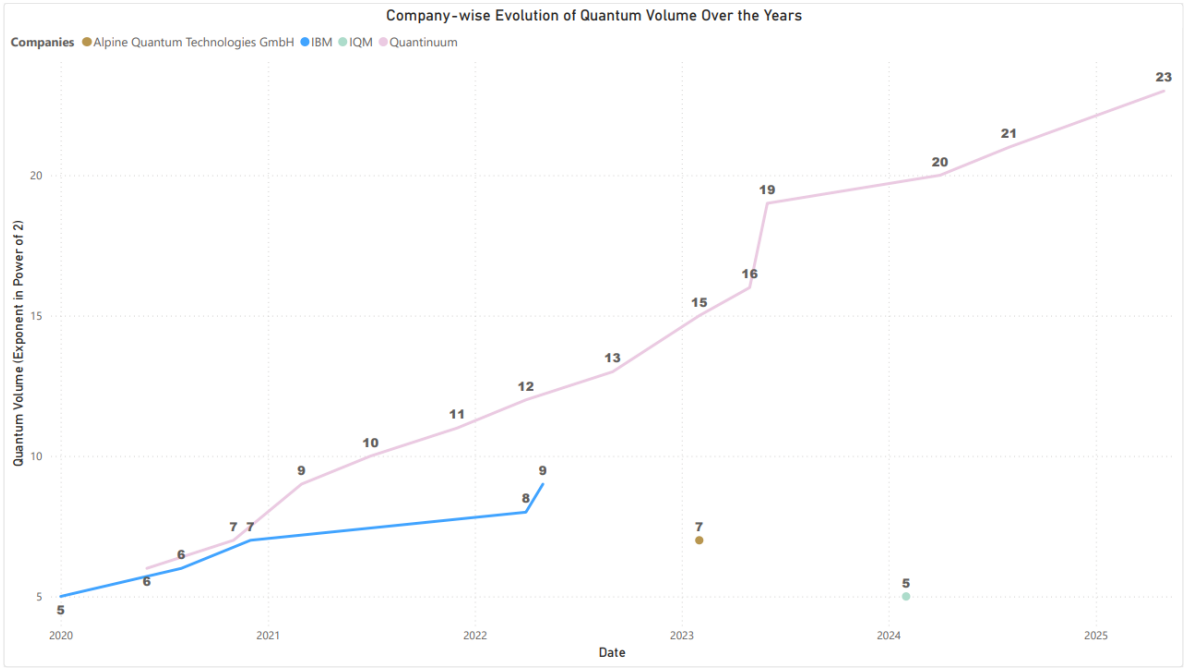

Figure 1 : The visualization shows worldwide quantum volume evolution. The data is from Wikipedia [3].

1.2.2 Number of Scientific Publications

The number of scientific publications related to quantum computing, as illustrated in Figures 2 and 3, reveals a global upward trend since 2000. This upward trend has accelerated sharply since 2018, both in Switzerland and worldwide, as evidenced by the fourfold increase in the number of publications in Switzerland between 2018 and 2023. However, the year 2024 marked a notable halt in this upward trajectory, as evidenced by a decline in global and Swiss publications, accompanied by a modest decrease in publications concerning quantum information and cryptography. A particularly noteworthy development is the substantial decline in publications containing the term ‘post-quantum cryptography’. This transition is further explored upon in the subsequent section, which investigates the shift from research to industry as a potential contributing factor.

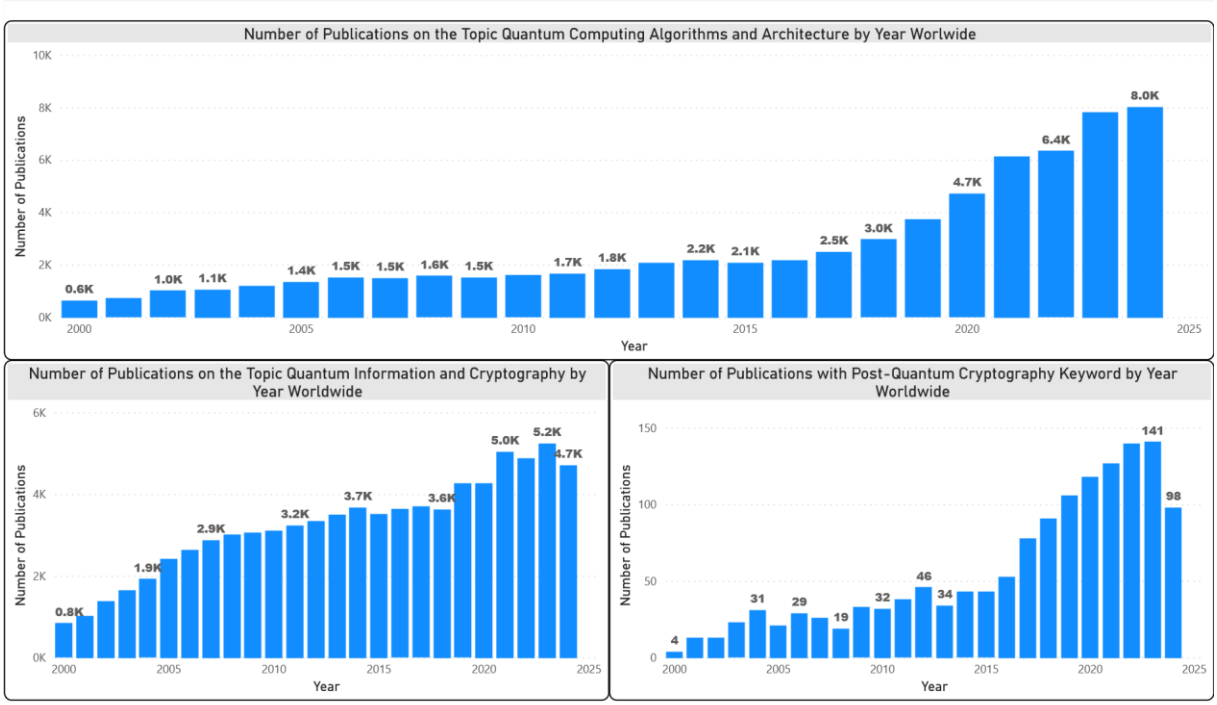

Figure 2 : This visualization shows worldwide publications trends in quantum computing. The data is from OpenAlex [4].

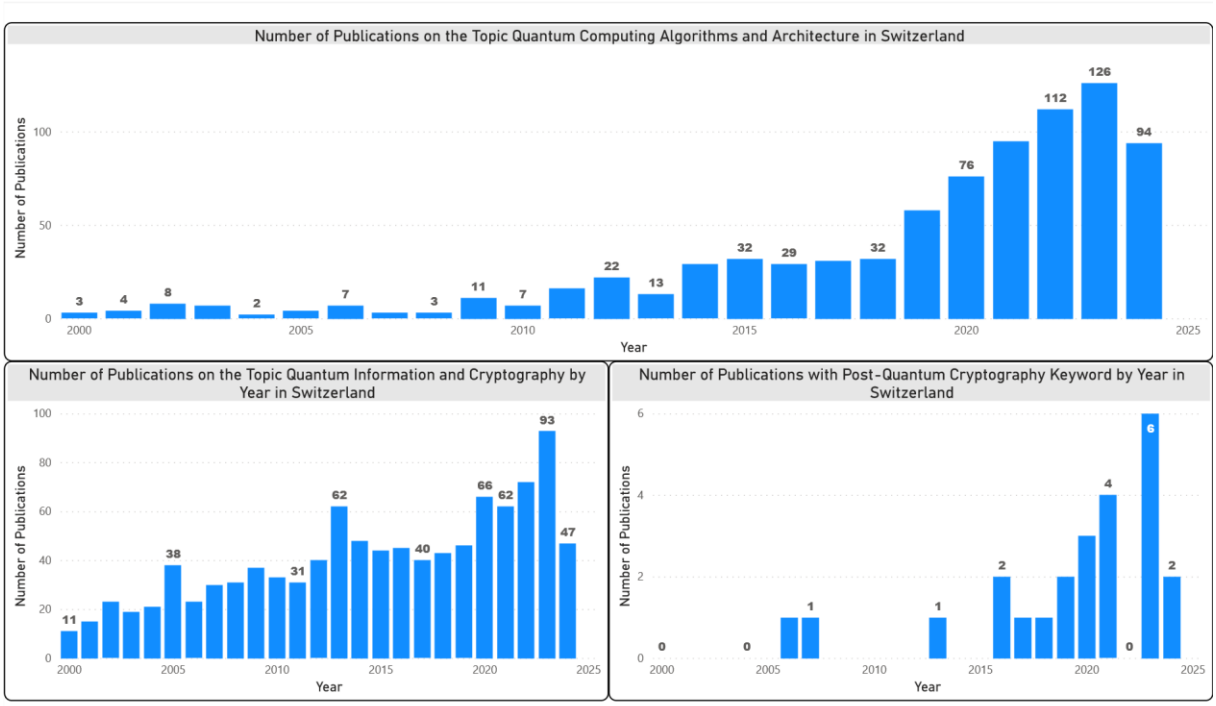

Figure 3 : The visualization shows Swiss publications trends in quantum computing. The data is from OpenAlex [4].

1.2.3 Funding Scale of Quantum Computing-Related Companies

Despite the decreasing number in scientific publications, Figure 4 demonstrates that the aggregate sum of financial resources amassed on a global scale by enterprises functioning within the domain of quantum computing since the previous report in December 2024 [1] and mid-February surpasses USD 1 billion, reaching nearly USD 9 billion. This substantial increase in fundraising was notably driven by Sandbox AQ, which raised USD 300 million during the month of December [6]. In addition, at least USD 400 million investments were amassed between January 1 and mid-February 2025. The most substantial contributions were USD 150 million raised by D-Wave Systems and USD 100 million by Alice and Bob [7] and Quantum Computing, Inc. [8].

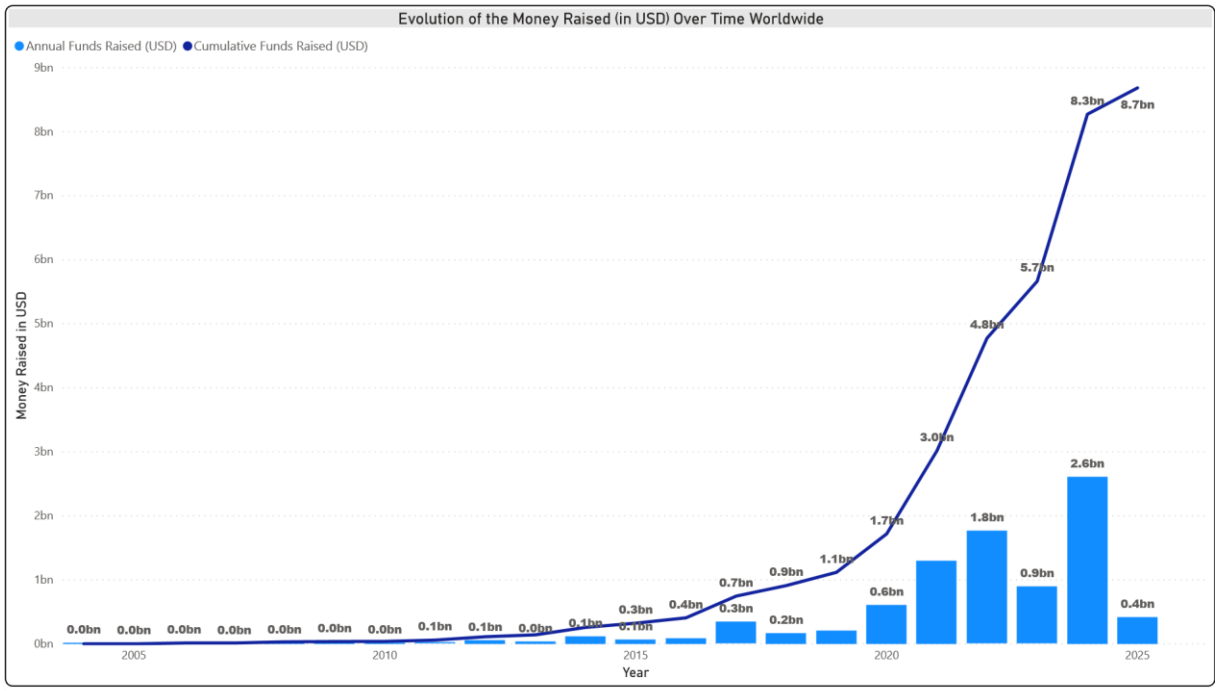

Figure 4 : This visualization shows worldwide fundings trends in quantum computing. The data is from Crunchbase [2].

As illustrated in Figure 5, the aggregate sum of financial resources amassed since 2004 by companies engaged in quantum computing-related operations amounts to USD 96 billion. It has been observed that no financial resources have been raised in the quantum field within Switzerland since 2022. This phenomenon may be due to missing data, likely resulting from the predominantly US-centric focus of Crunchbase [2], the primary data source.

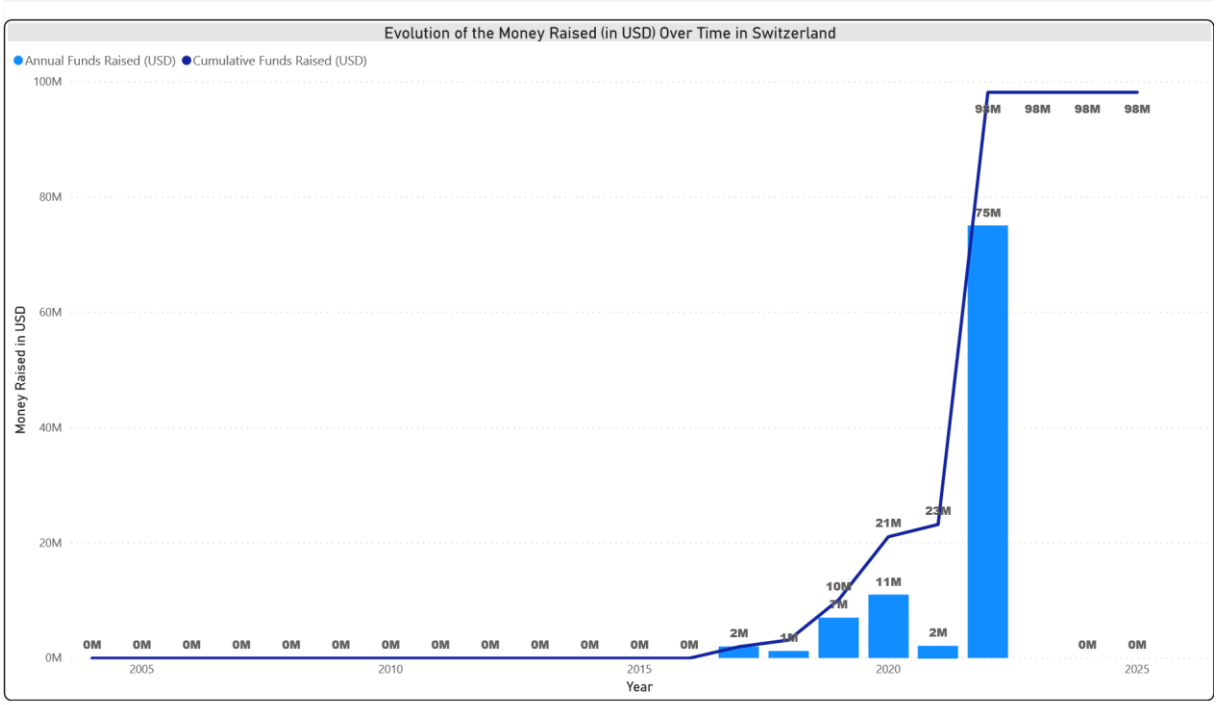

Figure 5 : This visualization shows Swiss fundings trends in quantum computing. The data is from Crunchbase [2].

In conclusion, while academic research in the quantum field appears to be undergoing a period of stagnation in Switzerland and on a global scale, there has been a marked increase in the financial resources allocated to this field in 2024, a trend that appears to persist in the early stages of 2025. This suggests a growing interest in technology and indicates promising development prospects for 2025 and beyond. However, it is crucial to acknowledge that this increase may also signify a lag in research compared to industry and the application of theory. Consequently, the investment in quantum technologies is expected to support substantial progress in the industry soon.

1.2.4 Semester Comparative Analysis

The following section provides a comparative analysis of the semi-annual quantum report (2024/2) and the actual 2025/1, emphasizing the identification of discrepancies or inconsistencies.

Table 1: Comparison table of the most recent Semi-Annual Quantum Report (2024/2) and the actual 2025/1 Worldwide

Comparison table of the most recent Semi-Annual Quantum Report (2024/2) and the actual 2025/1 report.	**Worldwide**
Evolution of Quantum Volume by Company Over Time	The quantum volume has increased from 2^{21} to 2^{23}
Number of Publications on the Topic Quantum Computing Algorithms and Architecture by Year	Trend is now upward, with around 1000 more publications in 2024
Number of Publications on the Topic Quantum Information and Cryptography by Year	Trend is still downward, but there are about 500 more publications in 2024
Number of Publications with Post-Quantum Cryptography Keyword by Year	Trend is still downward
Evolution of the Money Raised (in USD) Over Time	Trend is still upward, with around USD 2 billion more invested

Table 2: Comparison table of the most recent Semi-Annual Quantum Report (2024/2) and the actual 2025/1 in Switzerland

Comparison table of the most recent Semi-Annual Quantum Report (2024/2) and the actual 2025/1 report.	**Switzerland**
Evolution of Quantum Volume by Company Over Time	N/A
Number of Publications on the Topic Quantum Computing Algorithms and Architecture by Year	Trend is still downward, but there are 7 more publications in 2024
Number of Publications on the Topic Quantum Information and Cryptography by Year	Trend is still downward, but there are 3 more publications in 2024
Number of Publications with Post-Quantum Cryptography Keyword by Year	No change
Evolution of the Money Raised (in USD) Over Time	No change

2 Quantum Threats

Rajiv Krishnakumar, QuantumBasel, Arlesheim, Switzerland
Center for Quantum Computing and Quantum Coherence (QC2), University of Basel, Basel, Switzerland

2.1 Introduction

This chapter discusses how quantum computers are on the path to breaking many widely used systems of encryption that exist today and the current state of how this threat is being tackled. However, before delving into the various encryption-breaking algorithms, it is important to establish the basics of the different types of encryption schemes as well as the expected evolution of quantum computers in the near term such that one is aware of exactly which kinds of encryption schemes are at risk and the expected timeline for them to be broken.

2.2 Common Types of Encryption

Encryption is the act of taking some information, whether it is physical or digital, and encoding it in such a way that if a third party intercepts a message containing this information, it is very difficult or even impossible for them to interpret the information in any meaningful way. The three most common types of encryption schemes in the digital space are symmetric encryption, asymmetric encryption, and hashing schemes [9].

2.2.1 Symmetric Encryption

A symmetric encryption scheme uses a single secret key, shared beforehand by two parties, that is used to both encode and decode any transmitted information between them. A typical example of a symmetric key is a randomly generated string of bits. Today's symmetric keys typically use 128, 192, or 256 bits. Even taking the smallest number of 128 bits, this results in over 3×10^{38} different possible keys, a number of combinations that would take even the most powerful supercomputer many times the age of the universe to go through, making it impossible for a third party to decode any intercepted message. This is what makes this method of encryption very secure. However, this way of encryption requires both parties to first share the key through a secure channel before being able to send each other messages. In addition, individual separate keys need to be generated every time a new pair of entities would like to share information using symmetric encryption. Therefore, although symmetric encryption is secure when properly implemented, it is difficult to implement efficiently on global scale. Hence, it is usually used in situations where one needs the information only for oneself (like when encrypting files on one's own computer) or when the secret key generated during the scheme is used to create secure static items that do not change after they have been initialized (e.g., in credit cards). Although there exist quantum algorithms that are more efficient than their classical counterparts at trying to break symmetric encryption schemes, it is explained later in this chapter how symmetric encryption schemes will still remain secure even with the advent of powerful quantum computers in the future.

2.2.2 Asymmetric Encryption

Asymmetric encryption is a form of encryption that uses two types of keys; a public key, and a private key. The public key is used to encode messages, and (as the name suggests) is made public to everyone. However, a private key that is different from the public key is required to decode these messages (and using the same public key to try and decode these messages will not work). This means that any party can create a public key to allow people to send them

secure messages without worrying about malicious parties using this public key to decrypt these messages. The ability to have separate keys to encrypt and decrypt messages comes from the fact that asymmetric encryption schemes are based on mathematical problems that are easy to solve one-way but difficult to solve in reverse. For example, the most common form of asymmetric encryption known as RSA [10] (named after its three inventors Rivest, Shamir and Adleman in 1978[2]) is based on finding prime factors of a large integer. If one were to give you two prime numbers p and q, finding the answer to $(p \times q)$ is a very simple task for any computer to do. On the other hand, if one were to give you a large integer and ask for its two prime factors p and q, this would take even the most powerful supercomputer many lifetimes of the universe to find, as long as that integer in question is large enough (such as the ones composed of 2048 bits, which are typical in today's implementations of RSA).

Compared to symmetric keys, asymmetric keys tend to be more complicated to implement and slower to execute (due to the large key sizes) but are much easier to use at larger scales given that the public key can be shared in an open channel that everyone can have direct access to. This is why most systems on the internet use asymmetric encryption schemes, including website browsing, e-mail systems, mobile text communications, e-banking and any other online systems that require a wide range of people to be able to transfer digital information securely.

Although there exist asymmetric encryption schemes other than RSA, the vast majority of the ones in use today (including RSA, elliptic-curve cryptography [11, 12] and Diffie–Hellman [13]) are actually different variations of the same abstract mathematical problem known the *hidden subgroup problem* (HSP). Hence, any method that can break the RSA encryption scheme can be easily adapted to break any of the other schemes based on the HSP. Therefore, the rest of the chapter focuses on the RSA encryption scheme when discussing the breaking of asymmetric encryption schemes using a quantum computer since everything discussed in this context can also be applied to other HSP-based encryption schemes.

2.2.3 Hashing

Hashing is a scheme used to transform data into a unique serial number of fixed length, similar to how different books, regardless of their length, can be represented by an ISBN number of 13 digits. However, in the case of hashing, it is not possible to retrieve the original information from the hash value, assuming the hashing function is properly implemented. Thus, this encryption scheme, although extremely powerful, is used only for very specific tasks e.g., to store users' passwords without revealing them to the system administrator or as a part of digital signatures creation[3]. To date, there is no evidence that any computer (classical or quantum) will be able to undermine the security of today's most up-to-date hashing algorithms assuming their proper implementations.

[2] An equivalent system was developed secretly four years prior by the mathematician Clifford Cooks at the British Government Communications Headquarters (GCHQ). However, that system was only declassified in 1997, hence why the encryption was not named after Cooks.
[3] It is important to note here that in digital signature schemes, the hashing is only used to verify the integrity of the data, whereas asymmetric encryption is used to verify the authenticity of it, which makes most current digital signature schemes also vulnerable to cryptographic-breaking quantum algorithms.

2.3 The Timeline to Powerful Quantum Computers

Currently, a few different encryption-breaking quantum algorithms exist. However, before discussing them, it is important to have an understanding of the power of the hardware that they will be implemented on, that is, the power of existing and future quantum computers.

In its infancy, the quantum computing industry aimed to demonstrate the ability to build a very basic quantum computer, including creating and controlling a few qubits in a way that allowed for them to interact with each other for a limited amount of time before being measured at the end of those interactions. Having accomplished this task sometime in the late 1990s [14, 15], another big step was to create more robust versions of these small-qubit quantum computers that could be accessed through the cloud. The first instance of such a machine was made in 2016 [16]. Since then, the quantum hardware industry has been focusing on scaling up quantum computers in terms of computing power (i.e., increasing the number of qubits and decreasing noise) and in terms of accessibility through the cloud. This current era is known as the *noisy intermediate scale quantum* (NISQ) era [17], where we now have a handful of quantum computers accessible through the cloud, each with anywhere between 20 and 200 noisy qubits (at least for universal gate-based quantum computers – quantum annealers have thousands of qubits but represent a more specialized form of computing that targets optimization problems). These computers can perform advanced calculations but are limited in two ways: 1) the size of the input data that can be fed into them is limited (due to the limited number of qubits) and 2) the number of operations that can be performed sequentially is minimal due to the noise or *decoherence rate* of the qubits. Currently, it is still unknown whether we will find quantum algorithms (encryption-breaking or otherwise) that are able to run on NISQ computers that can give us an advantage (in speed, accuracy, or energy efficiency) over today's classical algorithms that run on CPUs and GPUs in solving practical problems.

However, the NISQ era is only temporary, and the quantum computing community is now working towards the *fault tolerant* (FT) era, where quantum computers will have over a million qubits and can perform many consecutive operations thanks to the implementation of *quantum error correction* protocols. These protocols propose a way to use many additional redundant physical qubits to continuously correct any errors occurring during the computation. Quantum error correction protocols are different from those in classical error correction as the no-cloning theorem prohibits the cloning of an unknown quantum state. The FT era should allow us to run many more complicated quantum algorithms on real hardware, including the famous Shor's algorithm [18] that can break RSA encryption. The timeline of when FT quantum computers will be readily available is a topic of debate.

2.4 Quantum Algorithms to Break Encryption

Many quantum algorithms, similar to classical algorithms, work in an iterative way. For example, if one had to create a program to search through a list of N colors and find the row which had the color 'orange', the classical algorithm would have to iteratively go through roughly N elements and check if each one matched the word 'orange'. However, if we were told in advance that the list was ordered alphabetically, we could create a much faster binary search algorithm that would only have to look through roughly $\log_2(N)$ items before finding the word 'orange'. In a similar sense, many quantum algorithms have an iterative structure. They start by putting all their input states into an equal superposition such that each answer, including all the incorrect ones, has an equal probability of being measured. Then, they use a specific set of quantum operations in an iterative way until the probability of measuring the correct answer is very high (e.g., more than 2/3) and the probability of measuring one of the wrong answers is heavily suppressed. The specific set of quantum operations to be

implemented iteratively and the number of iterations required to get a sufficiently accurate solution depend on the structure of the problem. Therefore, the way quantum algorithms scale with the size of a problem is use case specific. So, for a given use case, if a quantum algorithm requires many fewer iterations to solve a problem than its most optimal classical counterpart, then it may be said to have achieved a quantum advantage for that problem.

Currently there are several encryption-breaking quantum algorithms that exist that have an advantage over their classical counterparts, leading to a weakening or breaking of different symmetric and asymmetric encryption schemes.

2.4.1 The Robustness of Symmetric Encryption

As discussed earlier, symmetric keys are often produced by randomly generating bit-strings. That means that to break a symmetrically encrypted message, the best way is to randomly try different keys until applying one of them happens to make the encrypted information intelligible. Quantum computing can offer an algorithm that technically can reduce the complexity of this combinatorial task. However, since there is no structure to how the key is generated (as long as the implementation faithfully picks it at random), the best speedup that a quantum computer can offer is a quadratic speedup [19]. This would mean that even if we take keys of only 128 bits, a quantum computer would still have to perform roughly 2×10^{19} iterations of the appropriate set of quantum operations (roughly the square root of 3×10^{48} iterations mentioned earlier), which although technically weakens the symmetric encryption scheme, still requires far too many iterations to run in any practical time frame, even with future quantum computers from the FT era. And even so, one can just double the key size if one really wants to counteract this slight weakening. Therefore, it is unlikely that quantum computers will ever be a real threat to symmetric encryption schemes.

2.4.2 Established Algorithms to Break Asymmetric Encryption

For asymmetric encryption schemes, the situation is different. Focusing on RSA, the task of an encryption-breaking algorithm is to find the prime factors of a large N-bit (typically 2048-bit) integer. The state-of-the-art classical algorithm to solve this problem [20] grows exponentially[5] with N, which makes it unusable to solve this problem in any reasonable time frame. However, the famous Shor's algorithm, discovered in 1994 by Peter Shor [18], is a quantum algorithm that only grows as roughly N^2. This algorithm starts by mapping the prime factors problem onto a corresponding period finding problem before solving the latter with the help of a quantum computer. Still, to fully implement this algorithm to factor a 2048-bit integer, we will need a FT quantum computer. Current estimates suggest that a quantum computer with roughly 6000 error-corrected qubits would be enough to run a version of Shor's algorithm that can break RSA-2048 in several hours [21]. It should be noted that to have 6000 error-corrected qubits, one would require orders of magnitude more redundant qubits to perform the error correction during the running of the algorithm, which leads to a required approximately 20 million physical qubits that are required in total. Therefore, we cannot implement this algorithm on today's NISQ computers for meaningful key sizes.

A more recent quantum algorithm to break RSA was discovered by Oded Regev in 2023 [22]. In this algorithm, the prime factors problem is mapped onto a lattice finding problem, which is then solved efficiently with the help of a quantum computer. This algorithm slightly decreases the required number of qubits and operations by a small polynomial factor. It is estimated that,

[5] Technically it is slightly sub-exponential but regardless it is not practically usable for large integers.

in practice, this translates to a reduction in the number of required qubits and operations by a factor of 2-3 when compared to Shor's algorithm, although this is yet to be confirmed with more rigorous resource estimate calculations. However, even if this were confirmed, Regev's algorithm would still require too many resources to be implementable on today's NISQ computers and will likely only have a small effect on the timeline to when an FT quantum computer could implement an RSA-2048-breaking quantum algorithm. In any case, it is useful to keep an eye on the progress of such algorithms due to their potential to shorten the timeline of when quantum computers will be able to break RSA-2048.

2.4.3 Candidate Algorithms to Break Asymmetric Encryption

In addition to the two algorithms mentioned in the previous section, there is a variety of other 'candidate' algorithms that attempt to break RSA-2048 efficiently using near-term NISQ computers that range from unlikely to succeed to almost certainly failing. Still, it is useful to discuss these algorithms to be aware of them just in case progress on one of them renders it successful, but also to understand how some of them fail.

These algorithms can be split up into a few groups. The first one is the set of algorithms that are able to find prime factors of integers, but do not do it more efficiently than the most efficient classical algorithm, and therefore will not be able to break RSA-2048 in any reasonable time frame. These include the quantum version of Schnorr's algorithm [23], the distributed hybrid Shor's algorithm [24] and algorithms based on today's annealing methodologies [25] which are all shown to scale exponentially with the size of the integer being factored. The second category of these algorithms is when the algorithm attempts to use a variational quantum circuit, where, similar to machine learning algorithms, a parametrized quantum circuit is proposed and iteratively optimized via a cost function until it can factor integers [26]. Although there is no proof of the way these algorithms scale, there is strong evidence to suggest that as you increase the size of the integer that you want to factor, the number of quantum operations required increases exponentially. Finally, for the last category, there are some quantum algorithms that can be used to compute prime factors of large integers efficiently using NISQ devices, with the caveat that the solution is encoded in quantum states that require an exponential number of read-out measurements to extract to a sufficiently high precision [27]. This readout roadblock is likely to be insurmountable given that it is a well-known roadblock that has been studied extensively in many cases. However, if it were circumvented, it would greatly decrease the timeline for when quantum computers could break RSA-2048 encryption.

In addition, the exploration of quantum algorithms could maybe even inadvertently lead to the discovery of efficient classical cryptography-breaking algorithms. Although this is very speculative given the long history of failed attempts at finding such classical algorithms, there may be new ideas arising from the field of quantum algorithms that could be applied to classical algorithms, which slightly increases the chances of the community to find an efficient cryptography-breaking classical algorithm.

2.5 Recommendations for Further Actions

Although today's quantum computers do not have the ability to break asymmetric encryption, it is still imperative that nations, organizations, and individuals around the world start to take appropriate action to defend against this eventuality. For starters, one cannot predict the exact timeline for when this eventuality will occur, so it is recommended to be prepared for it sooner rather than later. In addition, there are likely already initiatives around the world to 'harvest now, decrypt later'. This is when one intercepts encrypted messages, but instead of

immediately trying to decrypt them, one stores them while waiting for quantum computers to become powerful enough to decrypt the messages in the future.

It is always a futile endeavor to try to propose one-size-fits-all solutions or roadmaps, given the diversity of situations in which different countries, organizations, and private citizens find themselves. Therefore, in this section, we will describe the current efforts of the global cybersecurity community to address the threat to cybersecurity posed by quantum computers and then outline some potential directions that some of the aforementioned entities can take to integrate the threat of quantum computers into their cybersecurity strategies. Our only recommendation is that each entity consider the extent to which it wishes to pursue each of these suggested directions based on its individual circumstances.

Currently, there is an ongoing global initiative led by the United States agency of the *National Institute of Standards and Technology* (NIST) to tackle the cybersecurity risks posed by quantum computers. Although this is an evolving process, the overall effort consists of finding new (classical) asymmetric encoding schemes, that are also based on mathematical problems that are easy to solve one-way and difficult to solve in reverse. However, unlike mathematical problems based on the HSP, these new problems should still be difficult to solve in reverse, even with advanced quantum computers. Encryption schemes based on these mathematical problems are known as *post quantum cryptographic* (PQC) schemes. A global competition to find the best new PQC approaches was launched by NIST in 2016, and in 2024, they selected the final encryption standards that are to be used to replace the current ones [28]. The main efforts have now shifted to create guidelines around how to implement these new schemes and disseminate these guidelines, although continuous testing of these new methods and the search for backup schemes are still underway. In addition to PQC schemes (which leverage classical computing to counter the quantum threat), there exists another category of techniques based on quantum communication devices, known as *quantum key distribution* (QKD) schemes. These methods are symmetric encryption schemes, i.e., a scheme in which messages are encoded and decoded with the same key. However, unlike the classical symmetric schemes mentioned in previous sections, QKD methods do not require a secure channel to share the key. This is because the key is generated and shared using a quantum protocol that is in theory, mathematically provably secured against any eavesdroppers, unlike PQC schemes where, although there is strong evidence to suggest that they are resistant to known quantum threats, we have no formal mathematical proof of their security for (current or future) cryptography-breaking quantum algorithms. Nevertheless, QKD requires longer time scales, since it needs a novel hardware infrastructure, and is still very much a field under development. The debate on whether PQC schemes represent the final solution or whether we will eventually need to move to QKD schemes is out of scope for this chapter. In either case, due to the ‘harvest now, decrypt later’ threat, there is a clear need to move to new standards sooner rather than later.

2.5.1 Directions for Governments

One of the directions governments can take is to keep up-to-date with the global initiative led by NIST to tackle this problem and continually evaluate the recommendations and guidelines that come out of this initiative. They can also choose to participate in shaping the solutions and guidelines to the extent desired based proactively to set the standards for PQC or reactively if they find any issues with any of the solutions or recommendations coming out of this initiative. In addition, another possible action of the government is to ensure that the guidelines are being followed and implemented across entities within the country, which includes government offices, private organizations, and private individuals. This involves four main pillars:

1. Ensuring that the encryption standards set by the national standards entity are continuously updated in line with the NIST guidelines.
2. Ensuring that sections of the guidelines that are appropriate to the different entities are being disseminated to them as when there are major updates
3. Monitoring that these entities are performing their recommended actions based on the guidelines
4. Providing assistance in this capacity when required.

2.5.2 Directions for Private and Public Technology Providers

Technology providers, whether they work at a fundamental level like developing internet infrastructure or at a more customer-facing level like providing software services to end users, are the entities that are affected most by this change in encryption guidelines. In addition to considering the directions for organizational end users described in the next section, they can also consider constantly monitoring and evaluating the new guidelines when they come out and bring up any issues they find with the relevant governmental authorities. In parallel, they can already be working on transitioning the encryption schemes present in their products and services to the new PQC ones and be aware of the evolution of these algorithms and their implementations so that they can keep their implementations up-to-date.

2.5.3 Directions for Organizational End Users

There are two main potential actions for organizational end users. The first one is to ensure that their technology providers are indeed keeping their services up-to-date based on the recommended guidelines as mentioned in the previous section. The second is to perform an inventory of their in-house data encryption to understand which parts of it will be affected by the transition to PQC encryption schemes. For example, a change of encryption scheme in the software that they use can affect the speed of their digital operations. In addition, organizations may be required to update any encryption schemes that affect their local data, either by updating third-party software or by upgrading any in-house software with the new PQC schemes in accordance with the latest implementation guidelines.

2.5.4 Directions for Private Individuals

For private individuals, assuming that they are not heavily involved in the cryptography world, the only potential action is to be aware of the ongoing changes and occasionally read up on its progress at a high level. Although there are no technical actions to take, it is always important for the general public to be aware of changes that affect the privacy of their information, especially if they feel that public and private organizations are not acting in their best interest.

2.6 Conclusion

Cryptography-breaking quantum algorithms already exist but the hardware to implement them is not yet available. However, quantum computers could become powerful enough to be able to implement these algorithms. A global effort being led by NIST is underway to tackle this issue, with a focus on upgrading the asymmetric encryption schemes used around the world today. This focus comes from the fact that asymmetric schemes are the most vulnerable to quantum algorithms, as opposed to symmetric encryption and hashing schemes, which will remain robust even with the advent of advanced quantum computers in the future. As long as

the ongoing efforts to tackle this issue continue to progress at the current pace, with the different entities playing their part in the effort, the potential adverse effects of these cryptography-breaking quantum algorithms are likely to be largely mitigated.

3 Trends in Quantum Key Distribution (QKD)

Dr. Seyit Camtepe CSIRO, Canberra, Australia,
Dr. Sebastian Kish CSIRO, Canberra, Australia,
Prof. Josef Pieprzyk Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland and CSIRO, Canberra, Australia

3.1 Introduction

Recent advancements have led to the development of quantum computers, which pose a potential threat to many of the encryption algorithms currently in use. In response, Quantum Key Distribution (QKD) has emerged as a promising technology for secure communication, leveraging the principles of quantum mechanics rather than relying on assumptions about an adversary's computational power. Global efforts are underway to connect individual QKD links into larger testbed networks, paving the way toward practical and commercially viable solutions. Countries such as China and Japan are making significant progress in advancing QKD technology through large-scale research and development initiatives, while Switzerland has distinguished itself in commercializing QKD. However, its implementations remain limited by scalability (suitable for relatively short distances) and cost-effectiveness (requiring dedicated point-to-point links). Overcoming these challenges presents an opportunity for international collaboration between industry and governments to shape the future of secure communications.

3.1.1 Challenges and Opportunities

Quantum computers will soon threaten secure data traffic, necessitating new cryptographic methods. Current cryptography relies on symmetric encryption (e.g., AES) and public-key encryption, with the latter often used to distribute symmetric keys. While symmetric encryption is less vulnerable, Grover's algorithm weakens AES-256 to a 128-bit security level. However, public-key methods like RSA are significantly more at risk due to Shor's algorithm, which provides an exponential speedup for breaking these systems. This highlights the need for quantum-safe solutions, such as Quantum Key Distribution (QKD), which leverages quantum mechanics to securely exchange symmetric keys and detect eavesdropping, making it immune to quantum and classical computational advances. Unlike post-quantum cryptography (PQC), which relies on unproven assumptions about mathematical problem hardness, QKD provides a future-proof solution, mitigating the risk of ‘store now, decrypt later’ attacks and ensuring long-term data confidentiality without dependency on computational assumptions.

3.1.2 Definition of QKD

All QKD protocols are executed by two parties, Alice and Bob, as depicted in Figure 6. Their goal is to establish a common and secret key K. An adversary, Eve, is assumed to have access to the communication channels they use. Alice and Bob are connected by both unidirectional quantum and bidirectional classical channels. The quantum channel can be optical fiber or alternatively free space, which is able to transmit photons. The classical channel is assumed to be authenticated, i.e., a receiver is able to verify if a message comes from an alleged sender. It can be implemented by appending a digital signature or message authentication code (MAC) to the message. A key management system (KMS) is used to manage keys that can also function as a standard based key scheduler for shared randomness. QKD’s security is rooted in two fundamental principles of quantum mechanics: the no-cloning theorem and the quantum uncertainty principle.

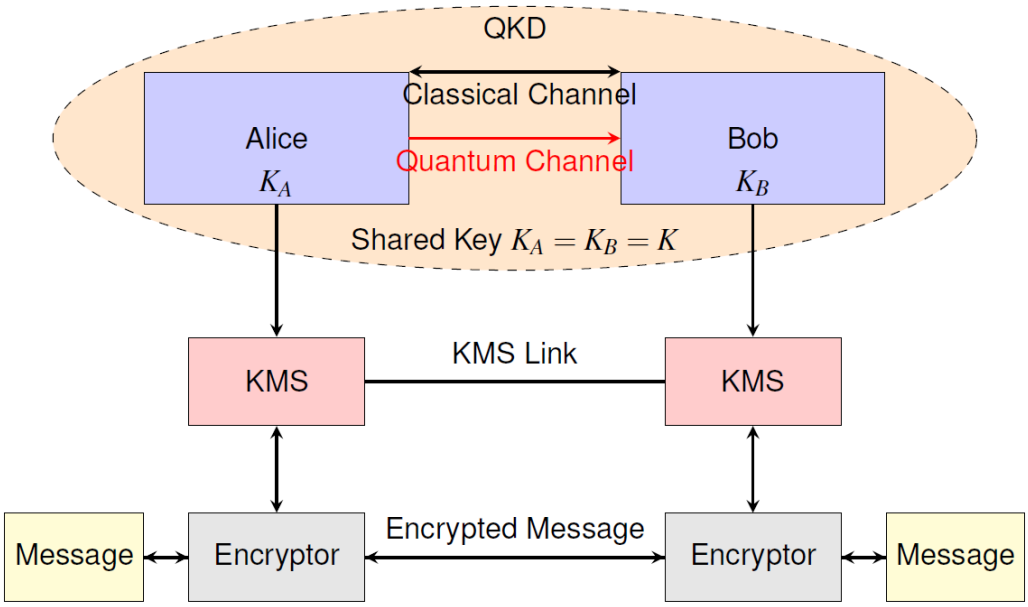

Figure 6 : Quantum Key Distribution (QKD) system

The no-cloning theorem states that it is impossible to create an exact copy of an arbitrary unknown quantum state. This principle underpins the security of QKD because it prevents an eavesdropper like Eve from intercepting photons sent by Alice to Bob and duplicating them to avoid detection. Any attempt by Eve to measure or clone the quantum states will inevitably disturb them, introducing detectable anomalies.

Additionally, the quantum uncertainty principle ensures that certain pairs of properties (e.g., position and momentum, or orthogonal polarization states) cannot be simultaneously measured with perfect accuracy. In the context of QKD, if Eve attempts to intercept and measure the quantum states sent by Alice, her actions will disturb the states in a way that introduces errors in the key generation process. Bob can detect these disturbances by comparing a subset of their measurement results with Alice's through an authenticated public channel. If the error rate exceeds a predefined threshold, Alice and Bob know the communication has been compromised and can discard the affected key.

Through this process, Alice and Bob can ensure that their key is secure, even in the presence of a potential eavesdropper, provided they have an authenticated communication channel for exchanging classical information.

3.2 Maturity of QKD Technology

3.2.1 QKD Systems

The development of QKD systems has reached a level of technical maturity, with multiple vendors producing commercially available products tailored for various applications. Companies like ID Quantique, Toshiba, QuintessenceLabs, and LuxQuanta are leading efforts to commercialize QKD, offering solutions that integrate seamlessly into existing communication infrastructures. These vendors provide systems based on diverse protocols, such as decoy-state BB84, Gaussian-modulated CV-QKD, and Coherent One-Way QKD, each optimized for different use cases, as summarized in Table 1.

Over the past two decades, advancements in single-photon sources and detection technologies have significantly reduced costs, making QKD more accessible. In particular, the development and widespread adoption of avalanche photodiodes (APDs) for the decoy-state QKD protocol have eliminated the reliance on costly superconducting nanowire single-photon detectors (SNSPDs), which require cryogenic cooling. For example, Toshiba's proprietary T12 protocol leverages APDs and other cost-effective single-photon technologies to achieve key distribution over distances of up to 150 km [29]. These innovations are crucial in reducing the cost barriers associated with QKD systems, enabling their deployment in more affordable and scalable configurations, as reflected in the advancements noted in Table 1.

Table 3 : QKD Protocol Security, Implementation Maturity, and Vendors

Protocol	**Aspect**	**Current**	**Future Outlook**	**Vendors**
Decoy-State (includes BB84)	Protocol Security	Proven	Stable	ID Quantique, Toshiba, ThinkQuantum
	Implementation Maturity	Promising	Mature	
Gaussian-Modulated CV-QKD	Protocol Security	Proven	Stable	QuintessenceLabs, LuxQuanta
	Implementation Maturity	Improving	Mature	
Discrete-Modulated CV-QKD (e.g., QPSK)	Protocol Security	Developing	Promising	Huawei, AIT
	Implementation Maturity	Moderate	Improving	
Coherent One-Way	Protocol Security	Developing	Promising	ID Quantique, QNu Labs
	Implementation Maturity	Moderate	Improving	
EntanglementBased Protocols (e.g., E91)	Protocol Security	Proven	Stable	S-Fifteen, Toshiba, ID Quantique
	Implementation Maturity	Challenging	Developing	
Twin-Field QKD	Protocol Security	Promising	Advancing	Toshiba demo (not yet available)
	Implementation Maturity	Challenging	Developing	

Other approaches to reduce costs and enhance compatibility with existing optical communication systems include Continuous-Variable QKD (CV-QKD). QuintessenceLabs Inc., an Australian company, has released a product based on the GG02 protocol and heterodyne detection. These protocols, while less expensive compared to discrete-variable QKD systems, are limited in range due to phase-locking noise. Similarly, LuxQuanta has introduced a CV-QKD system available through the AWS Marketplace, demonstrating growing commercial interest in this cost-effective approach to quantum-secure communication.

To further reduce production costs, ID Quantique has developed a product based on the Coherent One-Way QKD protocol. Although this protocol currently lacks a fully proven

information-theoretic security proof, it leverages off-the-shelf components to provide a more practical and scalable solution. Such advancements make quantum communication systems increasingly accessible to a broader range of users, particularly for enterprise applications.

These QKD protocol developments, as summarized in Table 1, illustrate the ongoing progress in making QKD systems more affordable, scalable, and adaptable to existing communication infrastructure, driving broader adoption across industries.

3.2.2 QKD Activities and Testbeds

QKD activities have advanced significantly, transitioning from purely experimental setups to more sophisticated testbeds and early-stage deployments. Some of the most notable QKD initiatives demonstrating significant progress are shown in Table 2. A notable example is the SwissQuantum testbed in Geneva, launched in 2008. Spanning approximately 20 kilometers, it connected multiple nodes, including corporate offices and data centers, serving as a robust platform for evaluating QKD technology [32]. Such projects highlight the potential for integrating QKD into modern communication systems and pave the way for broader adoption.

The Madrid Quantum Communication Infrastructure (MadQCI) demonstrates significant progress in QKD by integrating quantum communication channels with classical channels for data transmission and network control, managed dynamically through Software-Defined Networking (SDN) [30]. Its architecture includes a Local Key Management System (LKMS) that collects, stores, and manages keys from QKD modules, enabling real-time network monitoring and dynamic reconfiguration. By addressing challenges in hybrid network management, MadQCI highlights the feasibility of scalable QKD systems for real-world applications.

In South Korea, SK Telecom, in partnership with ID Quantique, has developed one of the most advanced QKD testbeds globally, deploying QKD systems over the past five years to connect 48 government organizations [31]. This testbed secures critical communications for government, financial institutions, and enterprises, showcasing the scalability of quantum-safe solutions. Additionally, QKD services have been successfully deployed at Equinix's SL1 data center, offering enterprise clients a subscription-based model that reduces upfront costs, demonstrating the practicality of large-scale QKD implementations.

Singapore has also made significant strides in quantum communication by building a comprehensive QKD testbed in collaboration with ID Quantique. As part of its nationwide quantum security initiative, Singapore has deployed QKD technology to secure its sensitive government and enterprise communications, positioning itself as a leader in quantum-safe communication in Asia. This effort integrates QKD into the broader national infrastructure, demonstrating its commitment to securing critical communications against future quantum threats. With these developments, Singapore is poised to be a hub for quantum innovation in the region.

The European Union's EuroQCI initiative is building a secure quantum communication infrastructure across all 27 EU Member States to enhance security for critical infrastructures and government institutions. As part of this effort, Poland has been advancing its QKD activities through the Poznań Supercomputing and Networking Center (PSNC) in collaboration with ID Quantique, establishing a 380 km intercity QKD link between Poznań and Warsaw within the PIONIER network, and creating the first international QKD link with Czech institutions between Cieszyn and Ostrava. These efforts position Poland as a key contributor to EuroQCI, integrating quantum technologies into secure communication testbeds.

These efforts in South Korea and Singapore, alongside initiatives in Europe with EuroQCI and MadQCI, underscore the global momentum toward quantum-safe communication. They highlight the potential of QKD to transition from isolated demonstrations to integral components of national and enterprise-level cybersecurity strategies.

Table 4 : QKD Activities and Testbeds Worldwide

QKD Activity	Region	Year Commis-sioned	Key Features	Matu-rity	Num-ber of Nodes	Covered Distance	Use
SwissQuantum QKD Network	Switzerland	2008	A notable testbed in Geneva deployed by ID Quantique, a pioneer of commercializing QKD and quantum encryption. Network included 2 Gbps channel fibre and IPSec encryptors.	High	3	20	Research
MadQCI	Spain	2021	Integrated with commercial telecom networks; compatible with IPsec encryption devices; utilizes ID Quantique, Toshiba, AIT & Huawei QKD systems [30] SDN architecture implemented	High	10	200 km	Commercial
SK Telecom	South Korea	2019	Nationwide deployment for government organizations; subscription-based QKD service for enterprises; employs ID Quantique's QKD systems [31] SDN-based control of heterogeneous QKD networks	High	15	150 km	Commercial
Singapore QKD	Singapore	2020	Integrated into national infrastructure for secure communication; positioned as a regional hub for quantum security; collaborates with ID Quantique	High	8	100 km	Commercial
EuroQCI	EU	2023	Developing a quantum network across 27 member states; focus on security for critical infrastructures; involves multiple vendors including Toshiba and ID Quantique, cross-border space links, intracity and inter-city fibre links	High	2–10	10-1000 km	Research
PSNC QKD Link	Poland	2022	380 km intercity QKD link within PIONIER network; includes international QKD links with the Czech Republic; utilizes ID Quantique's systems	High	5	380 km	Research
Cambridge QKD	UK	2023	Operates on dense wavelength division multiplexing (DWDM) networks; demonstrates high-bandwidth quantum communication; vendor information not specified	High	3	25 km	Research

DARPA Quantum Network	USA	2004	Integrated with Internet technologies; used QKD-derived keys for IPsec; one of the first QKD networks deployed; utilized proprietary QKD systems	High	3	50 km	Research
Bristol Quantum Network	UK	2020	QKD provided over 5GUK test network using specially developed Open Source software, also trusted-node free quantum network; University of Bristol	High	4-8	13 km	Research
Tokyo QKD Network	Japan	2010	Multi-node testbed on NICT's JGN-X open fiber network; collaborative research platform for universities and industry; involved multiple vendors	Medium	7	300 km	Research
CSIRO Testbed	Australia	2024	Laboratory-based QKD research environment; focuses on experimental validation and development; employs QuintessenceLabs' QKD system	Low	2	20 km	Research

3.3 Trends and Innovations of QKD

QKD is rapidly advancing through theoretical and practical innovations, offering information-theoretic security based on quantum mechanics. While foundational protocols like BB84 and decoy-state QKD have established security proofs, newer protocols often lack complete analyses, particularly under real-world conditions with finite datasets. Research is focused on addressing these gaps to ensure practical security.

There are additional challenges, as outlined in the following bullet points, that continue to hinder the largescale deployment of QKD technology. For each challenge, we provide an overview, assess its severity in impacting the advancement of QKD, and offer a time estimate for its potential resolution.

- **Implementation Security**

QKD's theoretical promise of 'unconditional security' can be compromised in real-world implementations due to hardware imperfections. These vulnerabilities have been exploited in various side-channel attacks and/or quantum hacking, such as photon-number-splitting (PNS) attacks, detector blinding, and time-shift attacks [33].

Severity: Medium. While vulnerabilities exist, countermeasures like measurement-device-independent QKD (MDI-QKD) and (semi-) device-independent QKD are advancing rapidly and already offer solutions for mitigating these risks.

Timeline for Resolution: Short to medium term (3–7 years). Many countermeasures are being standardized and are expected to integrate seamlessly into commercial systems soon.

- **Limited Role as a Cryptographic Solution**

QKD is often criticized for being a partial solution, as it generates keying material but does not inherently provide source authentication. The authentication of the QKD transmission source

typically relies on pre-placed symmetric keys or asymmetric cryptography [34], which limits its standalone utility.

Potential quantum technologies, such as Quantum Digital Signatures (QDS) and Quantum-Secure Identifiers (QSIs), leverage quantum principles to address this limitation. Hybrid solutions combining QKD with post-quantum cryptography (PQC), such as lattice-based cryptographic algorithms, are also gaining traction. But they come at the cost of breaking the (theoretical) information theoretical security property of the system.

Severity: Medium. Current cryptographic tools and emerging technologies provide adequate solutions, making this a manageable challenge.

Timeline for Resolution: Short term (1–3 years) for hybrid solutions; longer term (5–10 years) for full reliance on quantum-based authentication technologies like QDS and QSIs.

- **Key Extraction Efficiency**

Efficiently extracting secret keys from raw quantum measurement data is critical for real-time operation. The bottleneck in error reconciliation, especially under noisy conditions or high-loss scenarios, has been a challenge. However, modern low-leakage error correction codes and advanced reconciliation techniques already perform well, with minimal delays in key generation.

Severity: Low. While not ideal in all scenarios, backlogged keys can be stored and processed without compromising security.

Timeline for Resolution: Very short term (1–2 years). Existing solutions are already effective and are continuously improving with incremental advancements in algorithms and hardware acceleration.

- **Cost and Scalability**

The cost of deploying QKD infrastructure, particularly for discrete-variable (DV-QKD) systems, remains a barrier due to the specialized hardware required. Continuous-variable (CV-QKD) systems, which are more cost-effective and compatible with standard telecom components, face limitations in range and noise tolerance.

Severity: Medium. Cost and scalability are challenges, but innovative approaches such as Quantum Safe-as-a-Service (QaaS) models and hybrid networks are helping reduce deployment costs.

Timeline for Resolution: Medium term (3–5 years). Market competition and advancements in off-theshelf components are expected to make QKD increasingly affordable and scalable.

Standardization and Interoperability The lack of standardized protocols and evaluation criteria poses a barrier to widespread adoption. However, organizations like ETSI, ISO, and ITU are actively developing global standards.

Severity: Medium. Progress is steady, with global collaboration ensuring cross-vendor compatibility.

Timeline for Resolution: Short to medium term (3–5 years). Certification frameworks are maturing rapidly and will soon establish clear interoperability guidelines.

- **Integration with Classical Systems**

Integrating QKD with existing cryptographic frameworks and networks introduces complexity. However, hybrid systems combining QKD with classical encryption methods are showing promise.

Severity: Low. Integration challenges are manageable with existing technology and ongoing developments in hybrid systems.

Timeline for Resolution: Short term (2–3 years). Active development and testing are already underway.

- **Quantum Repeaters and Long-Distance Communication**

Transmission losses and the absence of practical quantum repeaters limit the achievable distance of QKD without trusted nodes. However, significant advancements in quantum memory and entanglement distribution are being made.

Severity: Medium. While a challenge for global-scale QKD networks, near-term applications can rely on trusted nodes.

Timeline for Resolution: Medium to long term (5–10 years). Progress in quantum repeaters and satellite based QKD is accelerating, making this a solvable issue within the next decade.

- **Comparison with Post-Quantum Cryptography (PQC)**

While PQC provides an alternative to QKD for quantum-safe communication, it relies on computational assumptions. QKD offers (theoretically) the advantage of information-theoretic security based on physical principles. However, a real-world system where this property holds has yet to be designed and hybrid systems (combining QKD and PQC) do not fulfill this property.

Severity: Low. PQC and QKD are complementary rather than competing technologies.

Timeline for Resolution: Short term (1–2 years). Hybrid systems integrating QKD and PQC already could provide practical and robust solutions.

Due to these trends, many countries and defense organizations prefer to monitor QKD's development and adopt it selectively or incrementally as the technology matures and its cost-effectiveness improves.

3.3.1 Vision and Future Outlook

Current QKD developments reflect the dual narrative of QKD's transformative potential and the challenges limiting its scalability. Technological advancements in integrated photonics, cost-effective avalanche photodiodes, and continuous-variable QKD systems are driving down costs, making scalable implementations more feasible [35]. Distance limitations are being addressed through satellite-based QKD, exemplified by China's Micius satellite enabling intercontinental secure communication, and the development of quantum repeaters to extend transmission ranges further [36, 37]. Integration with classical cryptographic systems combines QKD's information-theoretic security with traditional authentication and session management, ensuring compatibility with existing infrastructures. Government agencies, such as the UK's NCSC and the USA's NSA, emphasize the need for cost-benefit analyses given QKD's high costs and scalability constraints, advocating for a cautious approach. In parallel, initiatives like NIST's PQC standardization focus on scalable cryptographic alternatives.

Despite this, private sectors, including finance, telecommunications, and technology, increasingly implement QKD. For instance, JPMorgan Chase has secured financial networks using QKD, BT has deployed quantum-secure industrial networks, and Toshiba has implemented QKD for healthcare data protection. These examples underscore QKD's growing adoption in mission-critical applications as a complementary strategy to PQC.

3.4 Recommendations

Advancing QKD as a potential technology for quantum-secure communication requires addressing key challenges such as implementation security, scalability, and interoperability. Establishing national and regional QKD testbeds could help integrate advanced protocols with existing systems, enabling real-world testing and contributing to standardization efforts. Research into quantum repeaters and satellite-based QKD is needed to address distance limitations, and international collaborations could play a role in accelerating progress. Public-private partnerships may help reduce costs, making QKD more accessible for broader use in enterprise and government applications. Additionally, workforce development through education and training programs will be important for building expertise in quantum technologies. Active engagement in global standardization efforts, such as those by ETSI and ISO, can further support interoperability and promote adoption. These combined efforts could help position QKD as a promising tool for addressing evolving cybersecurity challenges.

3.5 Conclusion

In theory, Quantum Key Distribution (QKD) has the potential to become a foundational technology for securing communications in the quantum era, offering strong information-theoretic security. While challenges remain in scalability, cost, and integration with classical systems, ongoing global investments highlight its strategic significance. Through targeted research, innovation, and collaboration between industry and academia, countries and organizations can advance the adoption of QKD. By addressing these key challenges and promoting international cooperation, QKD could play a significant role in the future cybersecurity landscape, providing robust protection against emerging quantum threats.

4 Post-Quantum Cryptography

Prof. Steven Galbraith University of Auckland, Auckland, New Zealand

4.1 Introduction

4.1.1 Cybersecurity and Cryptography

Cybersecurity is a broad topic that covers a wide range of attacks by a wide range of attackers. Major cybersecurity issues nowadays include ransomware, scams and fraud. These topics are out of scope of this chapter.

The field of cryptography is central to cybersecurity. Cryptography provides tools for privacy and authentication in digital systems. It enables many of the systems and services that we take for granted in modern life, such as online shopping. Many of these systems rely on public key cryptosystems, which are based on hard computational problems in mathematics. Some widely-used examples of systems enabled by cryptography include TLS, secure email, private messaging, e-commerce, cloud storage and computing, VPN, software and firmware updates, e-voting, Internet of Things (IoT), blockchain, etc.

There are two main forms of cryptography. Symmetric key systems require both sender and receiver to hold the same secret key. Asymmetric (also called public-key) algorithms allow a user to make their encryption key public while keeping their decryption key secret. Public key systems enable digital signatures, which have major applications such as software updates, digital currencies, and smart contracts. Another important application of public key cryptography is to set up shared keys using a key exchange or key encapsulation protocol. Each type of cryptography has its strengths and weaknesses, and so large-scale systems usually use a combination of both approaches.

The leading symmetric key cryptosystem for most applications is AES. This is used to encrypt (and ensure integrity) large volumes of data. For example, secure internet sessions protect all data sent between client and server by encrypting it using AES. The shared key for the secure internet session is set up in a handshake protocol, which is built using public-key cryptography.

The RSA cryptosystem was proposed in the 1970s, almost immediately after the invention of public key cryptography. It provides public key encryption and digital signatures. It has been very widely used in practice since the 1980s, and especially with the rapid growth in the internet through the 1990s and early 2000s. The hardness of the integer factoring problem is the basis for RSA encryption and signatures.

Elliptic curve cryptography (ECC) was proposed in 1985. It fits into the discrete logarithm paradigm proposed by Diffie and Hellman, and developed further by Elgamal and others. It provides key exchange, public key encryption, and digital signatures. For the last 20 years, ECC has been the most popular choice for newly built systems. The security of ECC comes from the difficulty of the elliptic curve discrete logarithm problem (ECDLP).

RSA and ECC are used in almost all key exchange, public key encryption, and digital signature algorithms today, and ,hence, are the basis of sessions protected by internet protocols such as TLS. Hence, our security depends on the difficulty of just two computational problems: integer factoring and elliptic curve discrete logarithms. These problems have been studied intensively for at least the last 30 years and have survived sustained public scrutiny and mathematical analysis.

4.1.2 Quantum Threat Revisited

Shor's algorithm, which requires an appropriately general-purpose quantum computer, efficiently solves the two problems underlying almost all currently used public key crypto, namely integer factoring and elliptic curve discrete logarithms. Hence, if large-scale general quantum computers can be built then we immediately lose all security for the current public key cryptosystems that are used to secure a wide range of systems.

For a number of technical reasons, current quantum computers are not powerful enough to run Shor's algorithm on the large numbers needed to break the security systems being used today. In short, they cannot process enough data (i.e., they do not have enough qubits to store large enough numbers) and they cannot yet accurately perform the operations required (due to issues of decoherence and error-tolerance that need to be solved using error-correction). The challenge for quantum computing, at least in the context of breaking cryptography, is to construct a large-scale and error-tolerant quantum computer on which Shor's algorithm can be performed to break the public keys currently in use on the internet.

If a large-scale quantum computer becomes available in 10 to 30 years, what will an attacker be able to do? They will be able to read messages sent using secure end-to-end encrypted messaging systems. They will be able to spoof webpages and hence steal user data without resorting to phishing. They will be able to bypass the security checks on software updates, and, hence, install malware on systems without having to trick users into clicking a link.

Most critically, for some government agencies and institutions, an attacker with a large-scale and error-tolerant quantum computer will be able to decrypt private communications from decades in the past. Suppose an attacker today (or already in the past) intercepts files from your organization that are encrypted using public key cryptography, or with secret keys from an RSA or elliptic curve key exchange protocol. Are there consequences if those files are decrypted in 20 years' time? This is known as a 'store now and decrypt later' attack.

A survey and report were conducted in 2019 by Mosca and Piani for the Global Risk Institute [38] and was updated in 2023 [39]. In particular, they surveyed a wide range of experts to determine estimates for when quantum computers will be a 'significant threat' to public key crypto (where 'significant threat' means being able to factor a 2048-bit RSA integer in less than 1 day of computation). In 2019 the majority of experts believed the risk to be low (less than 5 percent) before 2029, though this still does not exclude the possibility of a breakthrough. About half of the respondents in 2019 considered the risk by 2034 to be at least 50 percent of a significant threat. In the 2023 update the majority considered there to be less than 1 percent chance of a threat before 2028, but almost half considered it more than five percent likely by 2033.

By this measure, a reasonable recommendation would be to migrate to post-quantum crypto within the next 10 years (i.e., to be fully migrated by 2035). Given the standardization and development cycle for security products, it means we need to be acting with urgency now.

4.1.3 Post-quantum cryptography

It has been recognized for the last 10 years that there is an urgent need to develop cryptosystems that can be used today on current computing devices and be incorporated into existing internet protocols, while at the same time withstand an attacker in the future with a quantum computer. Using post-quantum cryptography, we can use today's computers to protect our information against a quantum attacker in the future. However, postquantum

cryptography can be less practical and efficient than current systems, and the process of migration to using new technology is slow, typically 5-10 years.

Post-quantum cryptography is based on mathematical problems that are believed to be intractable even for quantum computers. There are five general areas of mathematics that seem to provide plausible candidates for practical post-quantum cryptosystems.

1. Lattices.

This refers to Euclidean lattices (grids of points in high dimension space). Lattices have been a major topic in algorithmic number theory since the 1980s and were suggested for cryptography in the 1990s. In the last 20 years, they have received a huge amount of research attention from cryptographers, partly due to post-quantum crypto and partly due to other applications in cryptography, such as homomorphic encryption. Lattices are a very versatile tool, and can be used for key exchange, public key encryption, digital signatures, and more.

Overall, lattices seem to be the most mature and trusted of the 5 branches of post-quantum public key cryptography, and NIST has standardized lattice schemes both for key exchange/public key encryption and signatures.

2. Codes.

Error correcting codes are widely used to enable reliable electronic communications, since physical systems are prone to noise and faults. However, it was proposed by McEliece in the late 1970s that one could build cryptosystems from error-correcting codes. This concept was not seriously developed for a long time due to the large key sizes, until the relevance to post-quantum cryptography became understood. Code-based cryptography has become very highly studied in the last 10-15 years and is generally thought to be a mature area. There are several well-known code-based schemes, but they are often perceived as less efficient or less practical than lattice-based systems.

3. Hashing.

This refers to a particular method to build digital signatures from cryptographic hash functions. It is a mature field that is well trusted. The main drawback is that it is only suitable for specific applications and is not a general solution to all the challenges of post-quantum security.

4. Multivariate.

This refers to problems related to solving systems of polynomial equations in a very large number of variables and over a small finite field. While such computational problems are definitely believed to be hard in general, multivariate cryptography is not fully trusted as there is a long history of broken schemes. However, recently there are some digital signature proposals that are gaining greater interest.

5. Isogeny.

This is the most recent of the five branches of post-quantum public key cryptography, and it experienced a major setback in 2022. Currently, isogeny-based cryptography is being developed by several researchers, but it is not clear if it will have major practical applications in the near future.

It is worth noting that post-quantum cryptosystems are typically less efficient than current systems, either in terms of bandwidth/storage or in terms of execution time/computing power required, or both. Hence, the migration to post-quantum cryptography may cause some inconvenience to some businesses and users [40, 41, 42].

4.2 Trends

4.2.1 Standardization

The US National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography Standardization process [43] in 2016 with an open call for algorithms to be submitted and reviewed in a public competitive process. The goal was to standardize and recommend one or more public-key encryption and key-establishment algorithms, and one or more digital signature algorithms, for future use. The initial round attracted 69 submissions. Similar standardization processes are being conducted by other standards bodies internationally.

After multiple rounds of evaluations, on July 5, 2022, NIST announced the first PQC algorithms selected for standardization. CRYSTALS-Kyber was selected as a type of public key encryption or key exchange scheme called a Key Encapsulation Mechanism (KEM), and CRYSTALS-Dilithium, FALCON, and SPHINCS+ were selected as digital signature algorithms. SPHINCS+ is a hash-based signature, and the other three are lattice-based cryptosystems. On August 13, 2024, the standards were published as Federal Information Processing Standards (FIPS):

- FIPS 203: This is intended as the primary standard for general encryption. The standard is based on the CRYSTALS-Kyber algorithm and has been renamed ML-KEM short for Module-Lattice-Based Key-Encapsulation Mechanism.
- FIPS 204: This is intended as the primary standard for protecting digital signatures. The standard uses the CRYSTALS-Dilithium algorithm, which has been renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.
- FIPS 205: This is also a digital signature scheme. The standard employs the SPHINCS+ algorithm, which has been renamed SLH-DSA, short for Stateless Hash-Based Digital Signature Algorithm.

The process of standardizing FALCON (or a variant of it) is ongoing at time of writing this chapter.

Many government and industry groups are required or expected to migrate to the new protocols as soon as practicable. The schemes are already implemented and usable. Indeed, starting from August 2023 the chrome browser has supported the X25519Kyber768 hybrid post quantum key exchange for TLS.

While NIST is a US government agency connected to the NSA, it has a huge influence on other international standards. As with previous NIST standards like AES and SHA-3, most Western governments are expected to approve the NIST standards for their own use. Bodies such as IETF will adopt the NIST standards [42]. A report by the European Union Agency for Cybersecurity (ENISA) [44] only lists algorithms that advanced through the NIST evaluation process. It is also worth noting that the design and development teams for the winning systems CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+ all comprise most European researchers. The use of PQC in hybrid mode with trusted classical systems also helps to reduce any sovereignty or trust issues.

By *hybrid mode* we mean combining two schemes in such a way that the security holds even if one of the two schemes is broken. To take one example, the X25519Kyber768 hybrid post quantum key exchange for TLS combines both classical elliptic curve cryptography and lattice-based post-quantum cryptography. A public key for such a hybrid scheme is a pair of public keys: an elliptic curve public key and a lattice public key. At a high level, the protocol performs in parallel an elliptic curve key exchange protocol and a lattice-based key exchange protocol. At the end of the protocol, the shared key is derived from (e.g., by hashing) both the shared key produced by the elliptic curve protocol and the shared key produced by the lattice-based protocol. Even if one of the schemes is broken, the attacker only knows one of the two keys and so cannot deduce the shared key of the hybrid scheme.

4.3 Analysis

4.3.1 Comparison between post-quantum cryptography (PQC) and quantum key distribution (QKD)

Quantum key distribution (QKD) is another approach to secure communication. It differs from post-quantum cryptography in several important ways. Most importantly, it requires new hardware, while PQC can be used with current computing and networking systems. Further, QKD needs an authenticated classical channel of communication, and the only practical way we know to implement this is using cryptography. To be secure against a quantum computer, the authenticated classical channel will have to be protected using postquantum cryptography. So QKD is not an alternative to PQC, rather PQC is needed to build quantum-secure QKD.

Post-quantum cryptography is a much more mature and thoroughly tested technology than QKD. As noted in [45], there are no published standards for QKD and nor is there a widely accepted evaluation methodology for physical attacks against QKD systems. In contrast, standards for post-quantum cryptography are published and implementations are already being used daily to protect internet communications [40].

In January 2024, the French Cybersecurity Agency (ANSSI), the German Federal Office for Information Security (BSI), the Netherlands National Communications Security Agency (NLNCSA), and the Swedish National Communications Security Authority issued a Position Paper [45] on Quantum Key Distribution. Their findings are clear: '*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*.'

The NSA has published [34] an opinion on QKD for real-world systems. To quote from this document: '*NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations ... are overcome*' and '*NSA views quantum-resistant (or post-quantum) cryptography as a more cost-effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications in National Security Systems*.'

4.3.2 Post-quantum symmetric key cryptography

Symmetric key cryptography means ciphers designed for encryption and message authentication (MAC) where both sender and receiver share a secret key. Typically, the shared secret key is the outcome of a previous key exchange or key transfer protocol, based on public key tools. The most widely used symmetric encryption scheme is AES, which is a block cipher. Symmetric ciphers are used together with a mode of operation to provide appropriate security; the most usual situation is to use a mode of operation that provides Authenticated Encryption with Associated Data (AEAD).

Symmetric cryptosystems have an n-bit key (for AES the typical values for n are 128, 192, and 256). The best classical attacks to determine the secret key used in a given session take essentially 2^n executions of the encryption algorithm.

The impact of quantum computers on symmetric key cryptography is a topic of debate. In theory, Grover's algorithm reduces the cost of computing the key from 2^n operations on a classical computer to $2^{n/2}$ operations on a quantum computer. Such an attack usually assumes the attacker is provided with a number of message-ciphertext pairs $(m,E_K(m))$ where m is a message and $E_K(m)$ denotes the encryption function with secret key K. To prevent such attacks, a natural strategy would be to double the key lengths, for example to use AES with 256-bit keys as a minimum. However, this is an oversimplified analysis since the real-world costs of Grover's algorithm do not achieve the full square-root speedup. For example, Table 13 of [46] states that Grover's algorithm reduces the cost to compute an AES-256 key from 2^{256} executions of AES to 2^{192} executions of quantum gates, which is much greater than $2^{n/2} = 2^{128}$.

There are also several different attack models to be considered. One can consider a quantum attacker who is given a set of message-ciphertext pairs $(m,E_K(m))$. Alternatively, one can consider a quantum attacker in a much stronger model (the superposition model or quantum chosen-plaintext attack) where the attacker is provided with access to a quantum circuit that computes EK(m) and so can execute this circuit on a quantum state that is a superposition of messages. In reality, this latter model seems unnecessarily strong and is not usually considered when evaluating the security of current real-world systems. For more discussion see [47].

The paper [48] gives a quantum security analysis of AES. The paper concludes that '*AES seems a resistant primitive in the post-quantum world as well as in the classical one*.'

The NIST document [49] gives further discussion. It says '*Grover's algorithm requires a long-running serial computation, which is difficult to implement in practice. In a realistic attack, one has to run many smaller instances of the algorithm in parallel, which makes the quantum speedup less* dramatic'. This is modeled by NIST using the 'MAXDEPTH' value. The document claims that a quantum attack on AES 128/192/256 requires, respectively, at least 2^{93}, 2^{157}, 2^{221} operations respectively (this is taking MAXDEPTH = 2^{64}.) In other words, the quantum attacks are not as good as the naive 2^{64}, 2^{96}, 2^{128} that would be expected from a square-root speedup.

4.3.3 NIST security levels

As part of the NIST post-quantum standardization process, submitters were requested to propose specific schemes and parameters to reach certain security levels. The security levels were defined in terms of existing standardized and widely used symmetric encryption and hashing primitives. Specifically, the NIST security levels were defined as follows [50].

1. The cost of key search on a block cipher with a 128-bit key (e.g., AES128)
2. The cost of collision search on a 256-bit hash function (e.g., SHA256/SHA3-256)
3. The cost of key search on a block cipher with a 192-bit key (e.g., AES192)
4. The cost of collision search on a 384-bit hash function (e.g., SHA384/SHA3-384)
5. The cost of key search on a block cipher with a 256-bit key (e.g., AES 256)

In addition, the documents state '*Here, computational resources may be measured using a variety of different metrics (e.g., number of classical elementary operations, quantum circuit size, etc.). In order for a cryptosystem to satisfy one of the above security requirements, any attack must require computational resources comparable to or greater than the stated threshold, with respect to all metrics that NIST deems to be potentially relevant to practical security*.'

There are several challenges in deciding whether a claimed set of parameters for a post-quantum public key scheme meets one of these levels.

The first challenge is actually to understand precisely the quantum costs to perform any of the 5 tasks listed above. For example, with level 1 as we have seen it is a non-trivial problem to estimate precisely the cost to break AES128 on a quantum computer. Indeed, in [46] the authors' assessment of the quantum security of AES showed it was a little easier than originally thought, hence '*making it easier for submitters to claim a certain quantum security* category'.

4.3.4 Timeline and Challenges for PQC Migration

The PQC schemes under standardization provide the same interfaces for cryptographic operations as the current public-key schemes. However, the deployment of new PQC schemes is challenging. Regarding performance, PQC schemes often have larger ciphertext/signature size, key size, processing time, and/or memory usage than ECC [40, 41, 42]. For example, a CRYSTALS-Dilithium signature can be more than one or two thousand bytes, compared with tens of bytes for ECC signatures.

There is also a challenge with the wide variety of PQC schemes being standardized. For example, should one use lattice schemes, or a code-based scheme and a hash-based signature?

As already mentioned, if one has a system that requires data to remain private for a long time then one should consider urgently migrating to post-quantum encryption schemes. This is because the development time to bring new tools to market is long. As an intermediate step one should use hybrid schemes, which combine both pre-quantum and post-quantum crypto.

The situation with authentication systems is a little different. For many (but not all) applications of digital signatures it is acceptable to continue using elliptic curve public key signatures until such time as there is a realistic threat that the ECDLP can be solved using a quantum computer (an exception might be the use of digital signatures for firmware updates).

Government and commercial organizations should be thinking about their security needs and risk management, and planning for when they may need to move to post-quantum crypto. Organizations need to invest in reviewing their systems. As stated in [41] it is '*difficult to determine where and with what priority post-quantum algorithms will need to replace the current public-key systems. Tools are urgently needed to facilitate the discovery of where and how public-key cryptography is being used in existing technology infrastructures*'.

PQC is already supported in several products. In 2023 Chrome announced support for a Hybrid ECClattice encryption scheme, and the Signal end-to-end-encrypted messenger app was upgraded to support PQC. In early 2024, the iMessage app was upgraded to support PQC.

4.4 Recommendations

New cryptanalysis (either using quantum computers or classical computers) can happen at any time. Hence, it is necessary for major nation states to maintain expertise and capability in cybersecurity. They can do this by supporting fundamental research into the mathematics and engineering behind PQC.

It is also necessary to aim to be agile with cryptography deployed in real-world systems, though this is extremely challenging in practice (current systems rely on RSA and ECC and are not very agile).

Post-quantum schemes should be used in a hybrid mode together with ECC, so that as long as at least one cryptosystem is unbroken then the whole scheme remains secure.

The biggest immediate risk is public key encryption and key-agreement schemes. An attacker can harvest internet traffic today and then try to break the systems when a quantum computer is built in the future. Hence, depending on the nature of the information being protected, it may be necessary to migrate to post-quantum cryptography as soon as possible.

It is recommended that companies and government agencies comply with the NIST and/or European standardized systems and to start migrating to post-quantum cryptography for data related to national security, health, and for securing critical infrastructure. While QKD is an active area of research, it is not suitable for securing real-world systems and its use is discouraged for most government and industry systems.

4.5 Conclusion

Post-quantum cryptography is a mature and standardized technology for protecting internet traffic and other online information from an attacker in the future with a quantum computer. NIST has published standards for post-quantum key agreements and digital signatures. Organizations can start migrating to post-quantum cryptography now, using existing hardware and networks, by combining the NIST schemes in hybrid mode with classical schemes such as elliptic curve cryptography.

5 Perspective on the QKD versus PQC debate

Renato Renner Institute for Theoretical Physics, ETH Zurich, Switzerland,
Ramona Wolf Department of Physics, University of Siegen, Germany

5.1 Challenges and opportunities for quantum key distribution

Recent publications have discussed the usability and current technical limitations of quantum cryptography, particularly Quantum Key Distribution (QKD) [51, 52, 53]. These analyses identify several challenges with QKD in its current state and recommend addressing these issues before broader adoption. In this article, we review these challenges identified and explore possible ways to overcome the limitations. Further insights are available in [54], with additional perspectives provided in earlier works (see, for example, [55, 56, 57, 58]).

In the following, we summarize seven frequently cited challenges associated with QKD. Our assessment of whether these limitations are problematic now, in the medium-term and long-term future, is summarized in Table 3. 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 a universal quantum computer, respectively. This approach is favorable because of 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.

Table 5 : Summary of our assessment of whether Challenges 1–7 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.

	Problematic now	Problematic medium-term	Problematic long-term
Challenge 1	not within scope of QKD		
Challenge 2	see Table 4	no	no
Challenge 3	yes	to some extent	to some extent
Challenge 4	yes	no	no
Challenge 5	yes	yes	no
Challenge 6	yes	no	no
Challenge 7	yes	yes	no

Challenge 1: Quantum key distribution does not solve the authentication problem

Authentication, whether in classical or quantum systems, always requires either a pre-shared secret or a trusted third party (TTP), and addressing this need is generally outside the primary scope of QKD.

That said, the need for authentication does not necessarily compromise the information-theoretic security QKD provides. It has been shown that a small initial secret (for example, a password) shared by the two parties is sufficient to establish information-theoretically secure authentication [59, 60]. Alternatively, if the two parties can individually establish authentication to a TTP, then the resulting connection between them will also be information-theoretically secure.

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.

To compare the security of QKD and PQC, one has to distinguish between ‘protocol security’ and ‘implementation security’ (see Table 4). Protocol security describes the theoretical security of the abstract protocol: QKD protocols come with a mathematical proof that they are information-theoretically secure [61]. Conversely, the security of PQC protocols is only as well understood as that of classical computationally secure schemes. It 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. 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).

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.

Table 6 : Comparison of how well protocol security and implementation security of post-quantum cryptography (PQC) and quantum key distribution (QKD) are 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 currently 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

		Now	Medium term	Long term
PQC	Protocol security	Bad	Bad	Bad
	Implementation security	Fair	Fair	Fair
QKD	Protocol security	Good	Good	Good
	Implementation security	Bad	Increasing	Good

The situation is a bit different if one considers the security of the actual implementation of a protocol. 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 a little experience with possible side-channel attacks and countermeasures [62]. 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 [63, 64].

Challenge 3: QKD requires special purpose equipment

The requirement of dedicated and, thus, expensive hardware is indeed one of the main reasons why QKD is not widely usable today. Such hardware is anticipated to become more accessible as optical communication technology continues to advance. However, although the cost of QKD hardware is expected to decrease over time, it is likely to remain higher than that of classical communication infrastructure.

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. However, 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 [65], need to be adapted.

Challenge 4: Trusted nodes are needed to overcome signal loss over long distances

At the current state, QKD protocols indeed require trusted intermediate stations to achieve longer distances. However, the need for trusted relays is not fundamental—quantum repeaters [66, 67, 68] 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, 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 [69, 70, 71]. However, since quantum memories are a crucial part of quantum computers, they are being intensively researched on various technology platforms.

Challenge 5: Securing and validating implementations of QKD protocols

The gap between theoretical and implementation security is a common challenge in cryptography, including classical systems where side-channel attacks remain an active area of research. In the relatively young field of quantum communication, research into these implementation challenges is still developing, with efforts to address such vulnerabilities already underway [62]. One potential approach is (semi-)device-independent QKD, which relies on minimal assumptions about the behavior of quantum devices, making it more resilient to side-channel attacks. While still in its early stages, this technology shows promise as a potential solution to these challenges in the long-term future [63, 64].

Challenge 6: QKD lacks official standards

To ensure a fair comparison between the security proofs of QKD and PQC, it is important to recognize the different types of security guarantees they provide. PQC algorithms typically offer asymptotic guarantees, which describe security within the limits of large computational resources but do not provide precise quantitative measures. This is why parameters such as key sizes in classical cryptography often require periodic adjustment. In contrast, QKD provides a potential quantitative security guarantee, specifying the probability of a scheme being compromised. Additionally, QKD security proofs incorporate finite-size effects, considering the actual number of protocol rounds rather than relying solely on asymptotic assumptions. Both approaches have their strengths and limitations, reflecting the differing nature of their security models.

Given these high security standards set for QKD, it is unsurprising that providing security proofs—especially for practical protocols—is particularly challenging. Developing PQC-level (non-quantitative, asymptotic) security proofs for QKD is easier and can already be found in the literature [72]. However, there is no fundamental obstacle that prevents formulating a quantitative finite-size security proof for practically relevant protocols, and the information-theoretic ingredients to such proofs are already available.

Moreover, the need for standards in QKD has been recognized by standardization authorities, and there are already attempts to lay the groundwork for such a standard, for example by classifying side-channel attacks [62].

Challenge 7: QKD increases the risk of denial-of-service attacks

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.

5.2 Conclusion and Recommendations

The issues highlighted around the use of QKD 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 3). Overcoming the remaining limitations, though, will require a long-term investment in developing quantum communication technology.

This effort, however, may be justified: Quantum cryptography has the potential to offer advantages over classical cryptography. Unlike traditional encryption schemes, which require periodic updates to address evolving technological threats, quantum cryptography provably provides a higher level of protocol security, including resilience against potential future threats such as quantum computers. Not only do quantum cryptographic protocols guarantee 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 QKD and PQC in hybrid schemes currently offers an alternative approach to data encryption (this approach was, for example, explored in [73, 74, 58]). A concrete scheme may look as follows: A message is first encrypted using a PQC scheme, which may rely on public-key infrastructure. 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. This hybrid scheme can be a viable interim solution for the medium-term future, when Challenges 2–4 and 6 are (largely) overcome (see Table 3).

6 Bibliography

[1] Julian Jang-Jaccard et al. Quantum Technologies Trends and Implications for Cyberdefence - Semiannual Report/2. 2024. DOI: 10.5281/zenodo.14546900. URL: https://doi.org/10.5281/zenodo.14546900.

[2] 'Crunchbase, Inc.' Historical Company Data. Crunchbase daily *.csv export, data retrieved on February 2025, from https://data.crunchbase.com/docs/daily-csv-export. 2024.

[3] Wikipedia contributors. Quantum volume — Wikipedia, The Free Encyclopedia. [Online; accessed 17 December 2024]. 2024. URL: https://en.wikipedia.org/w/index.php?title=Quantum_volume&oldid=1263213622.

[4] Jason Priem, Heather Piwowar, and Richard Orr. OpenAlex: A fully-open index of scholarly works, authors, venues, institutions, and concepts. 2022. arXiv: 2205.01833 [cs.DL]. URL: https://arxiv.org/abs/2205.01833.

[5] Quantinuum. Quantum Volume reaches 5 digits for the first time, 5 perspectives on what it means for quantum computing. URL: https://www.quantinuum.com/blog/quantum-volume-reaches-5-digits-for-the-first-time-5-perspectives-on-what-it-means-for-quantum-computing. Retrieved on February 25, 2025.

[6] Reuters. Quantum AI startup SandboxAQ valued at 5.6 bln after 300 mln fundraising. URL: https://www.reuters.com/technology/alphabet-spinoff-sandboxaq-valued-5-6-bln-after-300-mln-fundraising-2024-12-18/ . Retrieved on February 24, 2025.

[7] Alice & Bob. Alice & Bob Closes €100M Series B Led by Future French Champions (FFC), AVP and Bpifrance to Advance Towards a Useful Quantum Computer. URL: https://alice-bob.com/newsroom/alice-bob-100m-series-b-fundraising-press-release/. Retrieved on February 20, 2025.

[8] Quantum Computing, Inc. Quantum Computing, Inc. Announces Private Placement of Common Stock for Proceeds of 100 Million. URL: https://quantumcomputinginc.com/news/press-releases/quantum-computing-inc-announces-private-placement-of-common-stock-for-proceeds-of-100-million. Retrieved on February 26, 2025.

[9] Jon Ander González. 3 Types of Encryption - Detailed Guide with Pros & Cons. en-US. 2024. URL: https://www.sealpath.com/blog/types-of-encryption-guide/ (visited on 17 August 2024).

[10] R. L. Rivest, A. Shamir, and L. Adleman. 'A method for obtaining digital signatures and public-key cryptosystems'. In: Communications of the ACM 21.2 (1978), 120–126. ISSN: 1557-7317. DOI: 10.1145/359340.359342. URL: http://dx.doi.org/10.1145/359340.359342.

[11] Victor S. Miller. 'Use of Elliptic Curves in Cryptography'. In: Advances in Cryptology — CRYPTO '85 Proceedings. Springer Berlin Heidelberg, 1986, 417–426. ISBN: 9783540164630. DOI: 10.1007/3-540-39799-X_31. URL: http://dx.doi.org/10.1007/3-540-39799-X_31.

[12] Neal Koblitz. 'Elliptic curve cryptosystems'. In: Mathematics of Computation 48.177 (1987). ISSN: 1088-6842. DOI: 10.1090/S0025-5718-1987-0866109-5. URL: http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5.

[13] W. Diffie and M. Hellman. 'New directions in cryptography'. In: IEEE Transactions on Information Theory 22.6 (1976), 644–654. ISSN: 1557-9654. DOI: 10.1109/TIT.1976.1055638. URL: http://dx.doi.org/10.1109/TIT.1976.1055638.

[14] C. Monroe et al. 'Demonstration of a Fundamental Quantum Logic Gate'. In: Physical Review Letters 75.25 (1995), 4714–4717. ISSN: 1079-7114. DOI: 10.1103/PhysRevLett.75.4714. URL: http://dx.doi.org/10.1103/PhysRevLett.75.4714.

[15] Isaac L. Chuang et al. 'Experimental realization of a quantum algorithm'. In: Nature 393.6681 (1998), 143–146. ISSN: 1476-4687. DOI: 10.1038/30181. URL: http://dx.doi.org/10.1038/30181.

[16] IBM. IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation. uk.newsroom.ibm.com. 2016.

[17] John Preskill. 'Quantum Computing in the NISQ era and beyond'. In: Quantum 2 (2018), page 79. ISSN: 2521-327X. DOI: 10.22331/q-2018-08-06-79. URL: http://dx.doi.org/10.22331/q-2018-08-06-79.

[18] Peter W. Shor. 'Polynomial-time algorithms for prime factorization and discrete logarithms'. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Vol. 124. 1994, pp. 124–134.

[19] Charles H. Bennett et al. 'Strengths and Weaknesses of Quantum Computing'. In: *SIAM Journal on Computing* 26.5 (1997). ISSN: 1095-7111. DOI: 10.1137/s0097539796300933. URL: https://doi.org/10.1137/S0097539796300933.

[20] Carl Pomerance. 'A tale of two sieves'. In: *Notices of the American Mathematical Society* 43.12 (1996), pp. 1473–1485.

[21] Craig Gidney and Martin Ekerå. 'How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits'. In: *Quantum* 5 (Apr. 2021), p. 433. ISSN: 2521-327X. DOI: 10.22331/q-2021-04-15-433. URL: https://doi.org/10.22331/q-2021-04-15-433.

[22] Oded Regev. *An Efficient Quantum Factoring Algorithm*. 2023. DOI: 10.48550/ARXIV.2308.06572. URL: https://arxiv.org/abs/2308.06572.

[23] Bao Yan et al. *Factoring integers with sublinear resources on a superconducting quantum processor*. 2022. DOI: 10.48550/ARXIV.2212.12372. URL: https://arxiv.org/abs/2212.12372.

[24] Ligang Xiao et al. *Distributed Quantum-Classical Hybrid Shor's Algorithm*. 2023. DOI: 10.48550/ARXIV.2304.12100. URL: https://arxiv.org/abs/2304.12100.

[25] Chao Wang et al. 'Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage'. In: *Chinese Journal of Computers* 47.5 (2024). DOI: 10.11897/SP.J.1016.2024.01030.

[26] Eric R. Anschuetz et al. *Variational Quantum Factoring*. 2018. DOI: 10.48550/ARXIV.1808.08927. URL: https://arxiv.org/abs/1808.08927.

[27] Debjyoti Biswas et al. 'A Modified Order-Finding Algorithm for NISQ Devices'. In: *2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2024. DOI: 10.1109/comsnets59351.2024.10426927. URL: https://doi.org/10.1109/COMSNETS59351.2024.10426927.

[28] NIST. 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards'. In: *NIST* (2024). Last Modified: 2024-08-13T11:20-04:00. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (visited on 17 August 2024).

[29] M. Lucamarini et al. 'Efficient decoy-state quantum key distribution with quantified security'. In: *Opt. Express* 21.21 (2013), pp. 24550–24565. DOI: 10.1364/OE.21.024550. URL: https://opg.optica.org/oe/abstract.cfm?URI=oe-21-21-24550.

[30] V. Martin et al. 'MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities'. In: *npj Quantum Information* 10.1 (2024), page 80. DOI: 10.1038/s41534-024-00873-2.

[31] Taehyun Kim et al. 'Development of quantum communication technologies in SK telecom'. In: *2012 17th Opto-Electronics and Communications Conference*. 2012, pages 105–106. DOI: 10.1109/OECC.2012.6276393.

[32] D. Stucki et al. 'Long-term performance of the SwissQuantum quantum key distribution network in a field environment'. In: *New Journal of Physics* 13.12 (2011), page 123001. DOI: 10.1088/1367-2630/13/12/123001.

[33] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. 'Effects of detector efficiency mismatch on security of quantum cryptosystems'. In: *Phys. Rev. A* 74 (2 2006), page 022313. DOI: 10.1103/PhysRevA.74.022313.

[34] National Security Agency. *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. 2024. Accessed: 2024-12-09. URL: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[35] Fadri Grünenfelder et al. 'Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems'. In: *Nature Photonics* 17.5 (2023), pages 422–426. DOI: 10.1038/s41566-023-01168-2.

[36] Yu-Ao Chen et al. 'An integrated space-to-ground quantum communication network over 4,600 kilometres'. In: *Nature* 589.7841 (2021), pages 214–219. DOI: 10.1038/s41586-020-03093-8.

[37] Koji Azuma et al. 'Quantum repeaters: From quantum networks to the quantum internet'. In: *Rev. Mod. Phys.* 95 (4 2023), page 045006. DOI: 10.1103/RevModPhys.95.045006.

[38] Michele Mosca and Marco Piani. *Quantum Threat Timeline*. 2019. URL: https://globalriskinstitute.org/publications/quantum-threat-timeline/.

[39] Michele Mosca and Marco Piani. *2023 Quantum Threat Timeline Report*. 2023. URL: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/.

[40] Bas Westerbaan. *The state of the post-quantum Internet*. *The Cloudflare Blog*. 2024. URL: https://blog.cloudflare.com/pq-2024/.

[41] William Barker, William Polk, and Murugiah Souppaya. *Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms*. 2020. URL: https://csrc.nist.gov/publications/detail/white-paper/2020/05/26/getting-ready-for-post-quantum-cryptography/draft.

[42] Douglas Stebila. *Standardizing Post-Quantum Cryptography at the IETF*. Talk at *Real World Post-Quantum Cryptography*, 2023-03-26. 2023. URL: https://www.douglas.stebila.ca/research/presentations/.

[43] NIST. *Post-Quantum Cryptography*. 2024. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[44] European Union Agency for Cybersecurity (ENISA). *Post-Quantum Cryptography: Current state and quantum mitigation*. 2021. URL: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[45] ANSSI et al. *Position Paper on Quantum Key Distribution*. 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html.

[46] Samuel Jaques et al. 'Implementing Grover Oracles for Quantum Key Search on AES and LowMC'. In: *EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. *Lecture Notes in Computer Science*, vol. 12106. Springer, 2020, pages 280–310. DOI: 10.1007/978-3-030-45724-2_10.

[47] María Naya-Plasencia. *Post-Quantum Symmetric Cryptography*. In: *Symmetric Cryptography 2*. ISTE Editions, 2022.

[48] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. 'Quantum Security Analysis of AES'. In: *IACR Transactions on Symmetric Cryptology* 2019.2 (2019), pages 55–93. DOI: 10.13154/TOSC.V2019.I2.55-93.

[49] National Institute of Standards and Technology (NIST). *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*. 2022. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-digsig-sept-2022.pdf.

[50] National Institute of Standards and Technology (NIST). *Security (Evaluation Criteria)*. n.d. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/postquantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria).

[51] National Security Agency (NSA). *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. Retrieved on November 6, 2024. URL: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[52] National Cyber Security Center (NCSC). *Quantum Security Technologies*. Retrieved on November 6, 2024. URL: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

[53] Agence nationale de la sécurité des systèmes d'information (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), and Swedish National Communications Security Authority. *Position Paper on Quantum Key Distribution*. Retrieved on November 6, 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html.

[54] Renato Renner and Ramona Wolf. 'The Debate over QKD: A Rebuttal to the NSA's Objections'. In: *arXiv:2307.15116* (2023). DOI: 10.48550/arXiv.2307.15116.

[55] Valerio Scarani and Christian Kurtsiefer. 'The Black Paper of Quantum Cryptography: Real Implementation Problems'. In: *Theoretical Computer Science* 560 (2014), pages 27–32. DOI: 10.1016/j.tcs.2014.09.015.

[56] Eleni Diamanti et al. 'Practical Challenges in Quantum Key Distribution'. In: *npj Quantum Information* 1 (2016), page 2. DOI: 10.1038/npjqi.2016.25.

[57] Quantum Communications Hub. *Community Response to the NCSC 2020 Quantum Security Technologies White Paper*. Retrieved on November 6, 2024. URL: https://www.quantumcommshub.net/news/community-response-to-the-ncsc-2020-quantum-security-technologies-white-paper.

[58] Romain Alléaume. *Quantum Cryptography and Its Application Frontiers*. Habilitation, Sorbonne Université. 2021. URL: https://perso.telecom-paristech.fr/alleaume/HDRMainv10final.pdf.

[59] Renato Renner and Stefan Wolf. 'The Exact Price for Unconditionally Secure Asymmetric Cryptography'. In: *Advances in Cryptology - EUROCRYPT 2004*. Springer Berlin Heidelberg, 2004, pages 109–125. DOI: 10.1007/978-3-540-24676-3_7.

[60] 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. DOI: 10.1145/1536414.1536496.

[61] Christopher Portmann and Renato Renner. 'Security in Quantum Cryptography'. In: *Reviews of Modern Physics* 94 (2 2022), page 025008. DOI: 10.1103/RevModPhys.94.025008.

[62] Federal Office for Information Security (BSI). *Implementation Attacks against QKD Systems*. Retrieved on November 6, 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.html.

[63] Ignatius W. Primaatmaja et al. 'Security of Device-Independent Quantum Key Distribution Protocols: A Review'. In: *Quantum* 7 (2023), page 932. DOI: 10.22331/q-2023-03-02-932.

[64] Víctor Zapatero et al. 'Advances in Device-Independent Quantum Key Distribution'. In: *npj Quantum Information* 9 (2023), page 10. DOI: 10.1038/s41534-023-00684-x.

[65] 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. DOI: 10.6028/nist.sp.800-57pt3r1.

[66] Hans J. Briegel et al. ‘Quantum repeaters: The role of imperfect local operations in quantum communication.’ In: *Physical Review Letters* 81.26 (1998), pp. 5932–5935. DOI: 10.1103/physrevlett.81.5932. eprint: quant-ph/9803056.

[67] Nicolas Sangouard et al. ‘Quantum repeaters based on atomic ensembles and linear optics.’ In: *Reviews of Modern Physics* 83.1 (2011), pp. 33–80. DOI: 10.1103/revmodphys.83.33. eprint: 0906.2699.

[68] Koji Azuma et al. ‘Quantum repeaters: From quantum networks to the quantum internet.’ In: *Reviews of Modern Physics* 95.4 (2023), p. 045006. DOI: 10.1103/RevModPhys.95.045006. arXiv: 2212.10820 [quant-ph].

[69] Xiao Liu et al. ‘Heralded entanglement distribution between two absorptive quantum memories.’ In: *Nature* 594.7861 (2021), pp. 41–45. DOI: 10.1038/s41586-021-03505-3. eprint: 2101.04945.

[70] Dario Lago-Rivera et al. ‘Telecom-heralded entanglement between multimode solid-state quantum memories.’ In: *Nature* 594.7861 (2021), pp. 37–40. DOI: 10.1038/s41586-021-03481-8. eprint: 2101.05097.

[71] Julian Rabbie et al. ‘Designing quantum networks using preexisting infrastructure.’ In: *npj Quantum Information* 8.1 (2022). DOI: 10.1038/s41534-021-00501-3. eprint: 2005.14715.

[72] Valerio Scarani et al. ‘The security of practical quantum key distribution.’ In: *Reviews of Modern Physics* 81.3 (2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[73] 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.* Springer International Publishing, 2020, pp. 483–502. DOI: 10.1007/978-3-030-44223-1_26.

[74] Nilesh Vyas and Romain Alléaume. ‘Everlasting Secure Key Agreement with performance beyond QKD in a Quantum Computational Hybrid security model.’ In: *arXiv:2004.10173* (2020). arXiv: 2004.10173 [quant-ph].

Illustrations