PQC versus QKD

A Comparison

Authors: Felix Trunk, Martin Seidel, Sascha Schweiger

Content

Introduction

Especially with the continued development of quantum computers, the question arises as to whether cryptographic methods used so far are sufficient to secure computer networks and confidential data. The reason for this is that there are special quantum algorithms for quantum computers that can solve problems that are classically difficult to solve much more easily.

The most well-known of these new algorithms is the *Shor Algorithm*, which would enable a drastic acceleration for the calculation of the prime factorization of natural numbers. Other cryptographically relevant quantum algorithms are a second quantum algorithm from Shor, which would enable a comparatively drastic acceleration for the calculation of the discrete logarithm and the *Grover Algorithm* which promises a strong acceleration for the search of unsorted databases [1], [2].

This is a problem because current asymmetric cryptosystems such as RSA, the *Diffie-Hellmann key exchange* (DH) or the *Digital Signature Algorithm* (DSA) are based on the difficulty of calculating a prime factorization or the discrete logarithm. For example, according to ITU-T X.1811 a quantum computer with just over seven million physical *qubits* would be needed to break RSA1024 encryption with just over half a trillion gate operations in less than 10 hours. The security of symmetric AES encryption is also endangered by the *Grover algorithm*.

It must be noted that such quantum hardware is currently still in uncertain distance. For comparison, the quantum computer which was demonstrated in 2019 by *Google* had only 53 qubits. However, since considerable progress has been made in this field and the (complete) migration to secure procedures will take a long time in any case, it is urgent to deal with this topic early enough [3].

Asymmetric cryptographic methods such as RSA, DH and DSA are widely used. If they were to become insecure, this would also affect many protocols, products and security architectures [4]:

Key Exchange: For secure communication over an insecure (public) channel, two people can exchange a public key in order to agree on a secret key. This is used in major encryption protocols such as SSL/TLS, SSH, and IKE/IPsec.

VPN: Secure communication over insecure IP networks can be realized with IPsec. The IKE protocol is used for key generation.

SSL/TLS: This encryption protocol is particularly known for its use in the HTTPS communication protocol.

Public Key Infrastructures: In these structures *Certificate Authorities* (CA) create certificates that can be used to uniquely assign a public key to a person or institution.

Software validation: Software updates also include a digital signature to verify the authenticity of the software.

S/MIME: To secure emails and their attachments, S/MIME also uses certificates issued by a CA.

This document therefore describes approaches that are able to guarantee encryption and digital signatures despite quantum computers, or that are well researched and are considered resistant to attacks by known quantum algorithms, to create so-called *post-quantum* or *quantum-safe* security. On the one hand there is ***Post Quantum Cryptography***, where new quantum-secure approaches for asymmetric cryptosystems are used instead of the insecure encryption and signature methods utilized so far. On the other hand, there is also the approach of ***quantum key distribution***, in which new hardware uses the properties of quantum mechanics for secure encryption.

PQC

Definition

PQC (short for ***Post Quantum Cryptography***) are new asymmetric cryptographic methods that are supposed to be secure against attacks by quantum computers. These algorithms are developed to ensure the long-term security of digital signatures and encryptions.

Even if current cryptographic methods are currently secure with sufficient key length, there is a risk that encrypted communication will be intercepted and stored until decryption is possible. This danger is less important for digital signatures, as they often have a limited period of validity [5].

According to current knowledge, symmetric encryption methods such as AES and hash functions are less vulnerable to quantum computers and can be secured against new quantum algorithms such as the Grover algorithm by simply increasing the key length. In contrast, the asymmetric methods used for encryption and signatures are based on complexity assumptions that are no longer valid due to Shor's algorithms. PQC is therefore investigating new approaches to enable asymmetric encryption and signatures. [5]

Variants / Algorithms

The following part describes the five types of algorithm families that are being investigated for the realization of asymmetric PQC systems [5], [6]:

Hash-based signatures

In the case of hash-based signatures, systems are considered where security is based on the well-studied difficulty of the computability of symmetric hash functions. These methods often use hash trees, a special procedure that makes it possible to assign a common verification key to several one-time signatures. Such systems are therefore stateful, i.e. the creator of the signature must update his signature key after each operation and the maximum number of signatures is already determined when the keys are created. These procedures include the already standardized *eXtended Merkle Signature Scheme* (**XMSS**) and *Leighton Micali System* (**LMS**). Stateless signature systems based on hash functions are also possible, but more computing time is required to create the signatures and longer signatures have to be used. An example of a stateless signature system is **SPHINCS** [7].

Code-based cryptography

It is also possible to realize encryptions based on the assumption that certain mathematical problems of the coding theory applied to *Error Correcting Codes* are difficult to solve. The best-known representative is the **McEliece** Cryptosystem, which has been studied for more than 40 years and is based on so-called *Goppa Codes*. In addition to the long-term security analysis, it is very efficient in encryption and decryption. However, the public keys are extremely large. The **Niederreiter** cryptosystem can reduce the size of the public keys to about 1 MB, but more structured codes are used, such as *QC-MDPC*, which have not yet been analyzed so deeply. On the 22nd DFN Security Conference, it was demonstrated that the DH algorithm in the IKE protocol can be replaced by the Niederreiter method [8].

Multivariate cryptography

Multivariate cryptography refers to cryptosystems that are based on the difficulty of solving multivariate polynomial systems of equations over finite fields. Many of these systems are signature systems that are very efficient and use short signatures but very long keys. Well-known examples of this type of algorithm are **GeMSS** and **Rainbow**.

Lattice-based cryptography

These cryptographic systems are based on the difficulty of mathematical problems in lattices. Due to their high efficiency in cryptographic applications, they are studied very intensively. Key exchange systems include **NewHope**, **FrodoKEM** and **CRYSTALS-Kyber**, while lattice-based signature systems include **FALCON** and **CRYSTALS-Dilithium**. The lattice-based CRYSTALS-Kyber is already being used in a variety of ways. As an example, *Google Chrome* has been supporting the X2551Kyber768 key exchange method for TLS since the end of 2023 (version 116), which uses a PQC key generated from (*Elliptic Curve*) ECDH and CRYSTALS-Kyber [9]. Similar to this, the messenger *Signal* has been using the PQXDH protocol since the end of 2023 [10] and *Apple* announced at the beginning of 2024 that it would use the PQ3 protocol for its messenger *iMessage* in the future [11]. Both protocols are hybrid key exchange methods based on ECDH and CRYSTALS-Kyber.

Isogen-based cryptography

These types of algorithms are also known as supersingular isogene-based algorithms. As a cryptographic principle, a known isogeny (i.e. a mapping with special properties) between two supersingular elliptic curves is exploited. For attackers, the difficulty is finding this isogenia between the two curves. One example is the so-called *Supersingular Isogeny DH Key Exchange* (**SIKE**) algorithm [12].

Standardizations and recommendations

NIST

In 2016 the *National Institute for Standards and Technology* (NIST) started a multi-step selection process that aims to find and standardize suitable PQC algorithms for digital signatures and key exchange [13]. The first PQC standardization conference to present potential candidates took place in 2018. More than 50 algorithms were presented at this conference. In 2022, the fourth PQC standardization conference took place. Particularly noteworthy was the presentation of a side-channel attack on the FACLON signature. The following algorithms were then selected to meet the criteria of the NIST [14]:

Table 1: NIST PQC Candidates 2022.

Classification	Algorithm	Category
Public-Key Encryption	CRYSTALS-Kyber[1]	lattice-based
Digital Signature	CRYSTALS-Dilithium	lattice-based
	FALCON	lattice-based
	SPHINCS$^+$	hash-based

A fifth PQC standardization conference will be held on April 10-12, 2024 [15]. A complete overview of all PQC algorithms that have participated in the NIST selection process so far is available at [16].

In addition to selecting suitable PQC algorithms, NIST is also actively involved in the standardization of the selected algorithms. Together with the *U.S. Department of Commerce* the *Federal Information Processing Standards* (FIPS) are published. Currently, three PQC methods are in the standardization process: CRYSTALS-Dilithium, CRYSTALS-Kyber and SPHINCS$^+$ [17]. In addition, the standardization of the stateful hash-based signature methods LMS and XMSS was already completed in October 2020. An overview of FIPS publications related to PQC is given in Table 2: Overview of FIPS publications.:

Table 2: Overview of FIPS publications.

Specification	Basic algorithm	Title
FIPS-203	CRYSTALS-Dilithium	Module-Lattice-Based Key-Encapsulation Mechanism (**ML-KEM)** Standard
FIPS-204	CRYSTALS-Kyber	Module-Lattice-Based Digital Signature (**ML-DSA**) Standard
FIPS-205	SPHINCS$^+$	Stateless Hash-Based Digital Signature (**SLH-DSA**) Standard
SP 800-208	LMS	Recommendation for Stateful Hash-Based Signature Schemes -> Extension of FIPS-186 (Digital Signature Standard)
	XMSS	

ETSI

The *European Telecommunications Standards Institute* (ETSI) is a European standardization organization that creates global standards in the field of information and communication technologies. For PQC, ETSI has created the *Quantum Safe Cryptography* (QSC) Working Group [18], which issues recommendations and assessments for PQC protocols and guidelines for the implementation of such protocols. In 2020, the QSC Group published the strategy paper ETSI TR 103 619, which contains recommendations and strategies to facilitate the transition to PQC secure systems. There is also a white paper *Quantum Safe Cryptography and Security* that deals with potential upgrades of certificates such as X.509, TLS, IKE, among others [4].

[1] **Note on CRYSTALS-Kyber**: Swedish scientists were able to show in 2023 that this algorithm has a vulnerability in terms of cryptographic security. With the help of machine learning, it was possible to implement a side-channel attack. This attack will probably be presented at the fifth PQC standardization conference [54].

BSI

The *Federal Office for Information Security* (BSI) also deals with PQC and analyzes potential dangers posed by future quantum computers. In the section "The status of quantum computer development" [19], the BSI provides information on the state of the art and technologies that are likely to be used in quantum computers.

In order to prepare organizations such as companies or public institutions in the best way possible for future threats from quantum computers, the BSI regularly publishes recommendations for action and technical guidelines that contain topics such as PQC algorithms, the quantum-safe design of cryptography and migration to PQC. In addition, the BSI also conducts market surveys on the topic of cryptography and quantum computing in order to increase awareness of this topic among companies. Updated links to the described topics and surveys are published in the section “Quantum Technologies and Quantum-Secure Cryptography” [20].

For key exchange, the BSI currently recommends the code-based method Classic McEliece and the lattice-based method FrodoKEM [5].

In addition to simply providing information on the topic of PQC, the BSI is also actively involved in the implementation of quantum-safe algorithms. To this end, the BSI is cooperating with the company *Rhode & Schwarz Cybersecurity GmbH*. The aim of this cooperation is to create a new version (3.0) of the free cryptography library *Botan*, which is to contain PQC algorithms in addition to conventional ones [21].

BMBF

The *Federal Ministry of Education and Research* (BMBF) has already founded various research projects that investigate the usability and influence of quantum technology on different industries. These projects include [22]:

- *Aquorypt*: Covers embedded systems in the industry and smart card-based security applications.
- *PQC4MED*: Deals with applications in the field of medical technology.
- *QuantumRISC*: Addresses the special requirements that arise from the limited resources of embedded systems.
- *FLOQI* (Full Lifecycle Post Quantum PKI): Aims to develop a quantum computer-resistant PKI.
- *KBLS*: Wants to expand the free cryptography library *Botan* with PQC methods.

CACR

Analogous to NIST, the *Chinese Association for Cryptologic Research* (CACR) launched a call for PQC algorithms in 2018 and 2019. However, only proposals from Chinese developers were accepted. Unfortunately, the 36 algorithms submitted are only available in Chinese so far. Nevertheless, the further development of these PQC proposals should be followed, as CACR could launch another call at the international level and China also plans to align its proposals on PQC with international standards [23].

NCSC

The British *National Cyber Security Center* (NCSC) regularly publishes articles on PQC migration and the preparation for this new technology. In contrast to the CACR and NIST, the NCSC does not develop its own

algorithms for later standardization. So far, two white papers on PQC migration [24] and the preparation for PQC [25] have been published on the NCSC website. These white papers show that the NCSC is also recommending the algorithms and specifications from Table 2. However, the following points should be taken into account:

- The algorithms in the categories ML-KEM (CRYSTALS-Kyber) and ML-DSA (CRYSTALS-Dilithium) have a wide range of applications. In particular, the NCSC recommends the use of ML-KEM-768 and ML-DSA-65 as they are characterized by a high level of safety and efficiency.
- The hash-based signatures SPHINCS$^+$, LMS and XMSS differ from ML-DSA and FALCON in that they are based on different (cryptographic) assumptions. SPHINCS$^+$, LMS and XMSS are significantly slower than ML-DSA and have long signatures and are therefore not intended for general use. They are more suitable for applications in which digital signatures are occasionally used, such as software and firmware updates, where speed and performance are less important.
- When using XMSS and LMS, it is important to ensure that a signature is only used once. Therefore, these two algorithms should only be used in cases where monitoring the status of a key is guaranteed.

Market outlook

Software is mainly used in the implementation of PQC algorithms. As a result, expensive hardware can be largely avoided and PQC integration is much more cost-effective. It also makes it much easier to integrate PQC technology into existing networks, regardless of hardware.

The disadvantage is that despite years of development and testing of these algorithms, there is no 100% guarantee of cryptographic security. In 2023, Swedish scientists were able to demonstrate a side-channel attack on a PQC algorithm classified as safe by NIST, see above in the note on CRYSTALS-Kyber.

Migration

Companies and authorities should now already develop an awareness of the future threat posed by quantum computers for currently employed cryptographic methods. If sensitive encrypted data is intercepted today that cannot currently be decrypted with classical computers, it will (possibly) no longer be secure in the future. For this reason, there is already a strong need for action to secure critical infrastructures and data against quantum computers. Although the standardization of PQC algorithms has not yet been completed, there are already recommendations for a migration to quantum computer-resistant methods.

CISA/NSA/NIST

In August 2023, the American *Cybersecurity and Infrastructure Security Agency* (CISA), in cooperation with the NSA and NIST, has issued recommendations for companies and authorities to switch to PQC [26]. It recommends that a management team should be established within an organization to take care of the planning and preparation of the PQC migration. Another so-called *Quantum Readiness* Team is to identify cryptographic systems used in the organization that are vulnerable to attacks by quantum computers. After identifying critical infrastructures, prioritization for the PQC migration can be carried out, depending on the respective risk. As a further measure, organizations should contact manufacturers or suppliers to evaluate the extent to which they intend to secure their products (software, hardware) against the (future) threat and what roadmaps and measures they plan to take with regard to the PQC migration.

BSI

The BSI has already published some recommendations [5] [27] to make it easier to switch to PQC technology:

- **Cryptoagility**: Cryptoagility is an important design criterion for current and future cryptographic protocols and applications. If possible, these should be designed in such a way that a cryptography method that turns out to be insecure in retrospect can simply be replaced by another without much effort or even reimplementation.
- **Hash-based signature methods**: Stateful signature methods should be used for firmware updates if possible. The reason for this is that these PQC methods only deliver a small number of signatures and are therefore suitable for firmware updates, for example.
- **Key length for symmetric encryption**: As already mentioned, symmetric cryptographic methods are more resistant to quantum computers in contrast to asymmetric ones. However, the key length should be increased to 256 bits in order to reduce the vulnerability to the Grover algorithm.
- **Short-term protective measures**: Symmetrical keys are mostly distributed via PQC-prone asymmetric procedures. Therefore, pre-distributed long-term symmetrical keys can ensure protection against attacks. However, the problem of distributing these keys remains.
- **Hybrid solutions**: Since the development and standardization of quantum-resistant methods has not yet been completed and possible weaknesses may become apparent during implementation or through side-channel attacks, the BSI recommends not using such algorithms in isolation, but only in combination with classical methods.

Adaption of cryptographic protocols

Various security protocols have to be adapted, as they use vulnerable asymmetric algorithms. Possible adaptations of TLS, IKE and X.509 certificates to PQC will be explained in the following [4] [5]:

IKE

The IKEv2 protocol only allows the (EC)DH algorithm, which is vulnerable to attacks by quantum computers, for the generation of the common session key. In contrast, IKEv1 offered the possibility to use a pre-shared key for the process of authentication and the generation of the shared key. In IKEv2, such keys can only be used for authentication. However, RFC 8784 makes it possible again to use pre-shared keys also for the key generation. However, the use of (hybrid) PQC procedures requires a major change in the standard.

TLS

As with IKE, TLS uses an asymmetric method such as RSA or ECDH for key exchange, making TLS vulnerable. In 2018, *Google* investigated to what extent the PQC methods for key exchange presented by NIST can be integrated into TLS 1.3 [28]. The two most important results of this two-stage study were: PQC algorithms based on unstructured lattices lead to a large additional delay in the TLS handshake and are therefore unsuitable for integration into the TLS protocol. Cryptographic methods that use structured lattices or supersingular isogeny are suitable for use in TLS, whereby the former is significantly faster and therefore leads to lower delays. While the addition of a (hybrid) PQC key exchange method is basically only a small change to the standard, it is problematic that in many PQC

procedures the public keys used are very large. This severely limits the possible PQC algorithms, since the public keys are included in the initial TLS handshake as of TLS 1.3.

X.509 Certificates

The X.509 certificate structure can be easily expanded to include new signature procedures. However, these certificates are used in very diverse protocols, which may have problems with very long signatures. For hybrid signature procedures, the first IETF drafts are already available, see e.g. draft-ounsworth-pq-composite-sigs-12.

QKD

Definition

QKD (short for ***Quantum Key Distribution***) describes a group of methods that make it possible to generate secret shared random numbers based on quantum mechanical principles. While encryption is based on (often unproven) mathematical complexity in the classic case, QKD could enable absolute security, as the encryption is based on fundamental physical laws. QKD is particularly suitable as a replacement for asymmetric encryption methods used so far.

As part of the second quantum revolution, QKD is at the transition between research and application and the first commercial systems are already available. At the same time, new methods are being developed and it is not clear which protocols will become established.

What all approaches have in common is that there are currently strong limitations in terms of reach and transmission rates. In addition, new components are needed in parallel to the existing hardware to create so-called quantum channels. Unless otherwise specified, the following sections are based on [29].

Background

In the quantum channels, information transport takes place by means of so-called qubits. Analogous to the classic bits that can appear in different forms, e.g. as a light pulse in an optical fiber or as a magnet in a hard disk, qubits can also be realized in different ways. For the transport of information photons, also known as 'light particles', are used almost exclusively. Often binary information is encoded in the light polarization, the direction of oscillation of the light field. In the following description it is assumed that a photon with a vertical or diagonal polarization (state |↕> or |↗>) is equal to **0**, and a horizontal or antidiagonal polarization (state |↔> or |↖>) corresponds to **1**.

Quantum objects have a number of special properties. Famously, there is no possibility to copy states and measurements modify or destroy the original state. For the polarization states described above, for a given photon it can only be determined if this photon is vertically/horizontally polarized (hereinafter referred to as measurement in the +-basis) or anti-/diagonal (measurement in the x-basis), since after the measurement the photon is no longer in its original state. For example, starting from a photon in a |↕> state, a measurement in the +-base would result in a vertical polarization and then convert the state into |↕>. However, if measurements were to be taken in the x-base, anti-/diagonal polarization would be measured with a 50% probability in each case and the state would then assume the measured polarization. The original information about vertical polarization would be lost.

Another fascinating property of quantum objects is that they can be entangled. For example, if two photons are entangled, they are in a common state and measurements on one of the two photons determine the possible measurement results of the other, no matter how far apart the two photons are.

However, quantum states are very sensitive and are destroyed by interactions with the environment during propagation in optical fibers after a few hundred kilometers at the latest. The generation and detection of individual photons is also technically very demanding and requires specialized hardware.

Protocols

BB84 Protocol

The BB84 protocol was one of the first considerations for QKD. The transmitter Alice prepares the polarization of photons according to random bits with random base selection and then sends them to the receiver Bob. He measures in a random base and thus partially receives Alice's bits as well as random values. In the next step, Alice and Bob use a classic communication channel and publicly agree on the cases in which they happened to have used the same base and thus should now have the same random numbers. Table 3 shows the underlying principle in the ideal case. Finally, some of the common random numbers can be publicly compared to determine the error rate, as any attempt by a third person Eve to access quantum communication would inevitably cause errors. If the error rate is considered small enough, classical error correction algorithms can ensure that Alice and Bob receive the same key from the remaining common random numbers. In 2013, it was demonstrated that the BB84 protocol can achieve transmission rates of at least 1 Mbps over 50 km of fiber [30]. In 2017, a key exchange with a satellite was realized by a Chinese research group [31], and in 2018, a key was successfully generated over more than 400 km of fiber optics [32].

Table 3: Principle of BB84.

Alice Bits	0	1	0	0	1	1	1	1	0
Alice Base	+	+	x	+	x	x	X	+	+
Sent Photon	|↕>	|↔>	|↗>	|↕>	|↖>	|↖>	|↖>	|↔>	|↕ >
Bob's Base	+	x	x	+	x	+	+	+	x
Bob's Bits	0	?	0	0	1	?	?	1	?
Common Key	**0**		**0**	**0**	**1**			**1**	

E91 Protocol

In the E91 protocol, entangled photon pairs are generated from a central source and distributed to the participants. Alice and Bob each measure in a random base. Subsequently, it is publicly clarified via a classic channel whether the same base was used or not. In the case of different bases, the measured values obtained are used to calculate a correlation function that provides information about whether the quantum channel and the measuring devices behave as expected. If this is the case, the measured values for identical bases are processed into a common key.

Other protocols

In addition to the two protocols just presented, there exists a variety of other protocols that can be used to realize QKD. Based on whether entangled states are used (like in the E91 protocol) or unentangled states are prepared and then measured (like in the BB84 protocol), one speaks of ***entanglement-based*** **(EB)** and ***prepare-and-measure*** **(PM)** protocols.

Since the actual implementation of QKD may create vulnerabilities that could be exploited in side-channel attacks, there exists also an approach to develop protocols that ensure the correct behavior of the devices during key generation. As these protocols are independent of the devices used, they are called ***Device Independent*** **(DI).** Very similar to the E91 protocol, entangled states are used and correlation functions are

calculated. However, the increased safety entails additional technical effort, which is reflected in shorter ranges and lower key rates.

A similar strategy is also followed by protocols, in which Alice and Bob only send quantum particles, while the measurements take place at a central public relay. Since the security of these methods is independent of the actual implementation of the measurement, they are referred to as ***Measurement-Device-Independent* (MDI)**.

A promising realization of PM MDI QKD is given by the ***Twin Field* Protocol**. Alice and Bob send specially prepared weak laser pulses to a central relay station where interference takes place and then a measurement with public results is conducted. By revealing certain properties of the used laser pulses, Alice and Bob can obtain a secret key. This method is similar to classic network structures and enables increased ranges and transmission rates, for example the transmission of a secret key over 833 km of optical fiber was demonstrated in China in 2022 [33].

Instead of discrete quantum states such as the polarization described earlier, it is also possible to use continuous properties. In this case, one speaks of ***Continuous Variable* (CV)** QKD and uses special laser pulses in contrast to ***Discrete Variable* (DV)** QKD, where individual photons are used. Often coherent states prepared by Alice via Gaussian modulation and read out by Bob by means of a homodyne measurement are employed. Again, a public comparison of parts of the data allows for an error estimation and, if the error is small enough, error correction together with discretization takes place. One advantage of CV methods is that they are technically closer to established methods and are theoretically more powerful than DV methods. However, they currently have a shorter range. It was not until 2020 that a transmission over 200 km of optical fiber with more than 5 bps was realized [34].

With all methods, keys can only be generated over a few hundred kilometers. Since classical repeaters destroy quantum information, higher ranges can currently only be achieved via *trusted nodes*. However, current research is also investigating so-called *quantum repeaters*, which could make it possible to transport quantum states over long distances by means of entanglement.

Risks and attacks

The QKD protocols presented above would be provable secure if implemented perfectly. However, it is possible that the technical implementation creates vulnerabilities that enable side-channel attacks. The possible attack vectors differ from protocol to protocol and the (M)DI protocols in particular have fewer points of attack.

An important attack vector in PM QKD is the ***photon number splitting*** attack. Since single-photon sources are technically demanding, often strongly attenuated laser pulses are used instead. However, as these often contain more than one photon, this allows some photons to be diverted and measured unnoticed, thus spying on parts of the key without increasing the error rate.

A possible countermeasure to this is the method of ***decoy states***. By occasionally sending a laser pulse with a different intensity, it is possible to detect such an attack during *post-processing* and adjust the key rate accordingly.

Further attack strategies and possible countermeasures are discussed in the ETSI whitepaper *Implementation Security of Quantum Cryptography* [35] or in more detail in the publication *Implementation Attacks against QKD Systems* of the BSI [36].

It is also important to emphasize that classic communication must be authenticated for all protocols, otherwise a ***man-in-the-middle*** attack could be carried out. In such an attack, the attacker pretends to Alice to be Bob (or vice versa) and thus gains access to the entire communication since the encryption would in this case only exist between Alice and the attacker. To prevent this, digital signatures can be used for authentication: If Alice signs her encrypted messages, Bob can use her public verification key to ensure that the message really came from Alice. However, previous authentication methods are usually based on approaches that are not quantum-safe.

As described in [37], it is possible to use *Pre-Shared Secrets* and classic *Message Authentication Codes* such as the *Wegman-Carter* procedures for quantum-safe authentication. Here, a secret exchanged between Alice and Bob before communication is used to determine a checksum for each message, which ensures the authenticity of the messages. Although this approach can achieve such a high level of security that symmetric encryption is the weakest link in the overall system during the entire communication, the logistical effort involved in the *pre-shared secrets* is very disadvantageous. However, it is also possible to use PQC signatures, which work analogously to current approaches for authentication. If the signature is not broken before and during communication, this approach also makes it possible for symmetric encryption to be the weakest link in the overall system, at least regarding long-term security after the communication.

Standardizations and recommendations

Since QKD is used in the field of information security, there are strong efforts in terms of standardization despite the relatively young age of the technology. In particular, ETSI and the International Telecommunication Union (ITU) have already published recommendations and standards.

A fairly up-to-date and detailed overview of standardization efforts that have already taken place, are still ongoing or planned can be found in ITU-T FG QIT4N D2.5 and ITU-T Y.Sup74. The following is an overview of the different directions of standardization efforts:

Architecture, Management and Machine Learning

The currently available QKD hardware is limited to relatively short-ranged *point-to-point* connections. By using a key management system with *trusted nodes*, key transport between participants in a QKD network at any distance can be realized. A large part of the standardization effort is related to this key management system.

ITU-T Y.3800/3801/3802 define a layered model consisting of the quantum layer, the key management layer, the control plane, the management plane, and the application layer. Figure 1 illustrates the functionalities of the different levels and their relationship with each other:

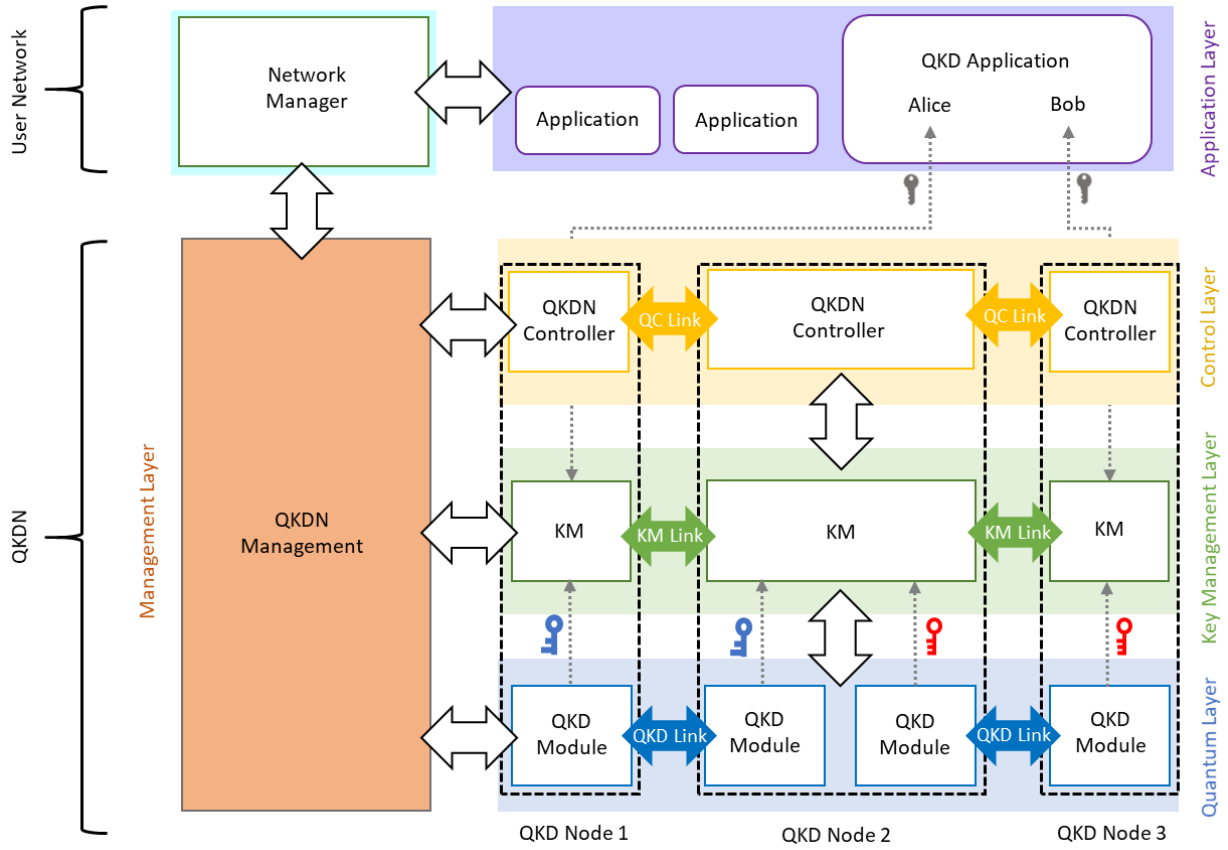

Figure 1: Realization of a QKD application using a QKD network (QKDN) with 3 nodes and a decentralized control plane.

In the quantum layer, the generation of common keys takes place between neighboring nodes of the QKD network. The QKD modules communicate via QKD links and obtain common secret random numbers after the *post-processing*. These are sent to the key management (KM) layer. In addition to managing the keys in the nodes, this layer also realizes the key exchange across the entire network using the KM links and also communicates with the applications in the application layer. The control plane coordinates the key management layer distributed across all nodes and can be implemented by a central QKDN controller as well as by decentralized QKDN controllers in all nodes. The management plane manages the entire network.

Recommendations for the key management layer can be found in ITU-T Y.3803. General recommendations for the control and management plane are given in ITU-T Y.3804, while *Quality of Service* is discussed in ITU-T Y.3806/3807/3811. In addition, ITU-T Y.3805 deals with *Software-Defined Networking,* for which interfaces are defined in ETSI GS QKD 015/018.

How *Machine Learning* can be used is discussed in ITU-T Y.3812/3814/3816/Sup70, in particular with regard to control and management.

ITU-T Y.3808 and ITU-T X.1715 deal with considerations for the integration of QKD networks with *Secure Storage Networks*.

Interoperability

Since there are many different QKD protocols, each with very specific hardware requirements, standardization efforts so far have mainly focused on the layers above the quantum level. However, the soon to be published ETSI GR QKD 019 deals with the interfaces for the authenticated classical communication at the quantum level, among other things. The QKD modules at the nodes are not really interoperable.

However, there is potential for the coexistence with classical traffic in the optical fibers as described in ETSI GS QKD 012 and in particular ITU-T FG QIT4N D2.4. *Wavelength-division multiplexing* with classic data traffic is possible in principle, but classical signals are several orders of magnitude stronger and must therefore be attenuated to reduce interference. CV QKD is less sensitive here. Classical repeaters destroy the quantum information and must not be contained in the channel or bypassed. Even in *multicore fibers* there are restrictions on the wavelengths used by the adjacent channels. Separate quantum channels are particularly important for long ranges, as any interference reduces the range and data rate and specialized hardware such as *hollow core fibers* can be advantageous.

Interoperability between different key management systems is discussed in detail in ITU-T Y.3810/3813/3817/3818. In addition, the soon to be released ETSI GS QKD 020 will define an interface for this.

For the transfer of keys to applications, there are recommendations in ITU-T Q.4160 and the interfaces defined in ETSI GS QKD 004/014 are often used. In addition, there are also proprietary approaches such as the CISCO SKIP (*Secure Key Import Protocol*) for key transfer to CISCO devices.

Safety certifications

With regard to a safety certification according to ISO/IEC 15408 "Common Criteria" for QKD devices, there exists a definition of a protection profile according to ETSI GS QKD 016 for PM QKD based devices and an alternative approach in ISO/IEC 23837, where basic functional safety requirements for QKD systems are defined and investigated.

Beyond that, ITU-T Y.3815 deals with the resilience of QKD networks and security recommendations for the key management layer can be found in ITU-T X.1710/1712/1714. ETSI GS QKD 005/008 and the soon to be published ETSI GS QKD 010/013 deal with implementation security and characterization of QKD modules and critical components, respectively.

Market analysis

QKD is a new technology with a lot of potential. Currently, there are many new start-ups in the field, which are often spin-offs from research institutes. However, there are also already companies that have several years of experience and furthermore some large international companies are active in the field. There is also often very close cooperation with the telecommunications companies. The GÉANT Infoshare of 21.06.2023 [38] provides an instructive insight, on which this section is based unless otherwise stated.

Table 4 shows a selection of currently available commercial QKD systems. Already in 2009, the price for a QKD device pair from *ID Quantique* was just over $80,000 [39]. However, research and development in the field of integrated optics, the optical equivalent of integrated circuits, is expected to reduce the costs in the future.

Table 4: Selected commercial QKD systems.

Manufacturer	**Product (Year)**	**Maximum range**	**Key Rate**	**QKD Protocol**
Standards	**Size**	**Frequency band**	**Notes**	
Toshiba	Multiplexed QKD System MU (2020) [40]	30 dB -> 90 km	300 kbps @ 10 dB	Decoy BB84
ETSI 014	19'', 3U	O		
Toshiba	Long-Distance QKD System LD (2020) [40]	30 dB -> 150 km	300 kbps @ 10 dB	Decoy BB84
ETSI 014	19'', 3U	C		
LuxQuanta	NOVA LQ (2023) [41]	8 dB -> 40 km		CV QKD
ETSI 004+014	19‘‘	C	100% EU	
QTI	Quell-X (2022) [42]	30 dB	2 kbps @ 14 dB	Decoy BB84
ETSI 014+015, CISCO SKIP	19'', 2U	C, O	100% EU	
ID Quantique	Clavis XG (2022) [43]	30 dB -> 150 km	1 kbps @ 24 dB [44]	Decoy BB84
ETSI 014+018	19'', 1U	O	100% EU	
ID Quantique	Cerberis XG (2021) [45]	18 dB -> 90 km	2 kbps @ 12 dB [46]	PM QKD
ETSI 014+018	19'', 1U	O	100% EU	
ThinkQuantum	QuKy (2022) [47]	33 dB -> 165 km	18 kbps @ 13 dB	Decoy BB84
ETSI 004+014, CISCO SKIP	19'', 2D	C, O	100% EU	

Migration

Encryption based on QKD is possible in different layers. Usually, QKD is used for the initial key exchange. An up-to-date overview of compatibility with currently used encryption protocols can be found in ITU-T XSTR-HYB-QKD. As with PQC, standardized integration is still in its infancy, but working solutions are already available.

An example of Layer 1 encryption with QKD via the ETSI 014 interface are the *Apollo TM400ENB – 400G Multiservice Encryption Muxponder* from *Ribbon* [38]. Compatibility between MACsec in Layer 2 and ETSI 014 has been verified by *Juniper* in a white paper [48] and a concrete protocol is proposed in [49]. In Layer 3, IPsec with IKEv2 currently does not use a *post-quantum* protocol, but RFC 8784 for IKEv2 allows the additional use of pre-shared keys which can come from QKD, for example. This approach has already been commercially implemented by *CISCO* with the help of the CISCO SKIP interface [38]. An analogous approach by *Juniper* is based on ETSI 014 and described in [50]. TLS 1.3 in layer 5 also offers possibilities for pre-shared keys which can come from QKD, as has been investigated in [51].

Result

Quantum-secure cryptography is an important topic with immediate need for action. Both PQC and QKD are able to increase the security of cryptosystems against the developments in classical algorithmics, computer technology and their quantum equivalents. In addition, approaches and commercial solutions regarding migration are available.

Comparison

Since PQC and QKD represent very different approaches, they each have their own strengths and weaknesses. Table 5 compares the most important key points.

Table 5: Comparison of PQC and QKD.

Property	**PQC**	**QKD**
Security	security proofs for underlying mathematics subject to current research, security certifications mostly pending	security of underlying physics proofed, side-channel attacks possible, *trusted nodes* needed in the foreseeable future, authenticated classic channels needed, security certifications pending
Implementation	mainly software-based	special hardware required
Costs	low costs as software-based	high costs due to special hardware
Transmission Media	fiber, copper cables, RF transmission	only optical transmission or free space
Reach	-	limited (few hundred km at most)
Key Rate	sometimes high computational effort	limited

Recommendations against QKD

In the course of the comparison, the recent position paper *Position Paper on Quantum Key Distribution* from the cooperation of the BSI and its sister authorities from France, Sweden and the Netherlands must be mentioned [52]. Starting with the problems of QKD in Table 5, it is shown that PQC is recommended over QKD for most applications. It is also emphasized that even for possible applications in special niche markets, the lack of security certifications is a major problem.

The NSA is also currently advocating the use of PQC instead of QKD [53].

In view of the fact that both approaches are comparatively new technologies for which new findings are regularly provided, it remains to be seen how these recommendations will be evaluated in the future. In particular, the advancing safety certification processes for QKD and the PQC procedures should be closely monitored.

Bibliography

[1] Wikipedia, „Shor's algorithm," 29 01 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Shor%27s_algorithm&oldid=1200508621. [Zugriff am 08 02 2024].

[2] Wikipedia, „Grover's algorithm," 02 02 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Grover%27s_algorithm&oldid=1202313743. [Zugriff am 08 02 2024].

[3] F. Arute et al., „Quantum supremacy using a programmable superconducting processor," *Nature,* 23 10 2019.

[4] ETSI, „White Paper: Quantum Safe Cryptography and Security," 06 2015. [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Zugriff am 22 02 2024].

[5] BSI, „Quantum-safe cryptography – fundamentals, current developments and recommendations," 18 05 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626. [Zugriff am 22 02 2024].

[6] T. Pöppelman, J. Haid und P. Schmitz, „Die Zukunft der Kryptographie im Zeitalter der Quanten," Security Insider, 26 09 2017. [Online]. Available: https://www.security-insider.de/die-zukunft-der-kryptographie-im-zeitalter-der-quanten-a-645548/. [Zugriff am 09 02 2024].

[7] D. J. Bernstein et al., „SPHINCS: Practical Stateless Hash-Based Signatures," *Advances in Cryptology,* 2015.

[8] E. Zimmer, „Post-Quantum Kryptographie für IPsec," 2015. [Online]. Available: https://svs.informatik.uni-hamburg.de/publications/2015/2015-02-24-Zimmer-DFN-PQC-fuer-IPsec.pdf. [Zugriff am 22 02 2024].

[9] The Hackers News, „Enhancing TLS Security: Google Adds Quantum-Resistant Encryption in Chrome 116," 11 08 2023. [Online]. Available: https://thehackernews.com/2023/08/enhancing-tls-security-google-adds.html. [Zugriff am 23 02 2024].

[10] ehrenkret, „Quantum Resistance and the Signal Protocol," Signal, 19 09 2023. [Online]. Available: https://signal.org/blog/pqxdh/. [Zugriff am 23 02 2024].

[11] Apple, „iMessage with PQ3: The new state of the art in quantum-secure messaging at scale," 21 02 2024. [Online]. Available: https://security.apple.com/blog/imessage-pq3/. [Zugriff am 23 02 2024].

[12] D. Jao et al., „Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies," *Lecture Notes in Computer Science,* 2011.

[13] NIST, „Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," 20 12 2016. [Online]. Available: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms. [Zugriff am 09 02 2024].

[14] NIST, „Selected Algorithms 2022," [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. [Zugriff am 09 02 2024].

[15] NIST, „Fifth PQC Standardization Conference," 30 08 2023. [Online]. Available: https://csrc.nist.gov/Events/2024/fifth-pqc-standardization-conference. [Zugriff am 09 02 2024].

[16] Fraunfofer AISEC, „qpdb," [Online]. Available: https://www.pqdb.info/. [Zugriff am 09 02 2024].

[17] NIST, „Post-Quantum Cryptography Standardization," 03 01 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. [Zugriff am 09 02 2024].

[18] ETSI, „Quantum-Safe Cryptography," ETSI, [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Zugriff am 09 02 2024].

[19] BSI, „Entwicklungsstand Quantencomputer," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer_node.html. [Zugriff am 09 02 2024].

[20] BSI, „Quantentechnologien und quantensichere Kryptografie," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html. [Zugriff am 09 02 2024].

[21] BSI, „BSI-Projekt: Entwicklung einer sicheren Kryptobibliothek," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html. [Zugriff am 09 02 2024].

[22] BMBF, „Post-Quanten-Kryptografie," [Online]. Available: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/pqk. [Zugriff am 09 02 2024].

[23] QApp, „CACR post-quantum competition," 2022. [Online]. Available: https://en.qapp.tech/help/cacr. [Zugriff am 09 02 2024].

[24] H. John, „Migrating to post-quantum cryptography," NCSC, 03 11 2023. [Online]. Available: https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc. [Zugriff am 09 02 2024].

[25] NCSC, „Next steps in preparing for post-quantum cryptography," 03 11 2023. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography. [Zugriff am 03 11 2024].

[26] CISA, NIST, NSA, „QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY," https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf, 2023.

[27] BSI, „Migration zu Post-Quanten-Kryptografie," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1, 2020.

[28] A. Langley und M. Braithwhite, „Post-quantum confidentiality for TLS," Imperialviolet, 11 04 2018. [Online]. Available: https://www.imperialviolet.org/2018/04/11/pqconftls.html. [Zugriff am 09 02 2024].

[29] S. Pirandola et al., „Advances in quantum cryptography," *Adv. Opt. Photon,* 2020.

[30] M. Lucamarini et al., „Efficient decoy-state quantum key distribution with quantified security," *Opt. Express,* 2023.

[31] J. G. Ren et al., „Ground-to-satellite quantum teleportation," *Nature,* 09 08 2017.

[32] A. Boaron et al., „Secure Quantum Key Distribution over 421 km of Optical Fiber," *Phys. Rev. Lett.,* 11 2018.

[33] S. Wang et al., „Twin-field quantum key distribution over 830-km fibre," *Nat. Photon,* 2022.

[34] Y. Zhang et al., „Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber," *Phys. Rev. Lett.,* 06 2020.

[35] ETSI, „Whitepaper: Implementation Security of Quantum Cryptography," [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Zugriff am 08 02 2024].

[36] BSI, „Implementation Attacks against QKD Systems," 21 12 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.html. [Zugriff am 08 02 2024].

[37] M. Mosca et al., „Quantum Key Distribution in the Classical Authenticated Key Exchange Framework," *arXiv,* 2012.

[38] „GÉANT Infoshare: QKD and Quantum Solutions 21 June 2023," 21 06 2023. [Online]. Available: https://www.youtube.com/watch?v=bjWvw3rmFQs. [Zugriff am 09 02 2024].

[39] D. Graham-Rowe, „Quantum Cryptography for the Masses," MIT Technology Review, 28 08 2009. [Online]. Available: https://www.technologyreview.com/2009/08/28/210221/quantum-cryptography-for-the-masses/. [Zugriff am 08 02 2024].

[40] Toshiba, „Toshiba launches Quantum Key Distribution (QKD) System Business," 19 10 2020. [Online]. Available: https://www.global.toshiba/ww/news/corporate/2020/10/pr1901.html. [Zugriff am 08 02 2024].

[41] J. Dargan, „LuxQuanta Launches its First CV-QKD System, NOVA LQ™," The QUANTUM Insider, 02 05 2023. [Online]. Available: https://thequantuminsider.com/2023/03/02/luxquanta-launches-its-first-cv-qkd-system-nova-lq/. [Zugriff am 08 02 2024].

[42] EasyEngineeringMag, „INTERVIEW WITH QTI," Easy Engineering, [Online]. Available: https://easyengineering.eu/interview-with-qti/. [Zugriff am 08 02 2024].

[43] IDQ, „ID Quantique expands the XG Series with the launch of the Clavis XG," 10 05 2022. [Online]. Available: https://www.idquantique.com/id-quantique-expands-the-xg-series-with-the-launch-of-the-clavis-xg/. [Zugriff am 08 02 2024].

[44] IDQ, „Clavis XG QKD System," [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/. [Zugriff am 08 02 2024].

[45] IDQ, „ID Quantique unveils its 4th generation of Quantum Key Distribution (QKD): the Cerberis XG, the ultimate in quantum-safe security," 17 05 2021. [Online]. Available: https://www.idquantique.com/id-quantique-unveils-its-4th-generation-of-quantum-key-distribution-qkd-the-cerberis-xg-the-ultimate-in-quantum-safe-security/. [Zugriff am 08 02 2024].

[46] IDQ, „Cerberis XG QKD System," [Online]. Available: https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/. [Zugriff am 08 02 2024].

[47] ThinkQuantum, „History," [Online]. Available: https://www.thinkquantum.com/projects/. [Zugriff am 08 02 2024].

[48] JUNIPER, „Integrating Quantum-Safe Security with existing encryption solutions," 2022. [Online]. Available: https://www.idquantique.com/quantum-safe-security/integrated-solutions/. [Zugriff am 09 02 2024].

[49] J. Cho et al., „Using QKD in MACsec for secure Ethernet networks," *IET Quant. Comm.,* 2021.

[50] JUNIPER, „DAY ONE: QUANTUM-SAFE IPSEC VPNS," 2023. [Online]. Available: https://www.juniper.net/documentation/jnbooks/us/en/day-one-books. [Zugriff am 09 02 2024].

[51] C. Garcia et al., „Quantum-resistant Transport Layer Security," *Computer Communications,* 2024.

[52] ANSSI, BSI, NLNCSA und Swedish Armed Forces, „Position Paper on Quantum Key Distribution," 26 01 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html. [Zugriff am 08 02 2024].

[53] NSA, „Quantum Key Distribution (QKD) and Quantum Cryptography (QC),“ [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. [Zugriff am 08 02 2024].

[54] E. Dubrova et al., „Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste,“ in *ASIA CCS '23: ACM ASIA Conference on Computer and Communications Security*, 2022.