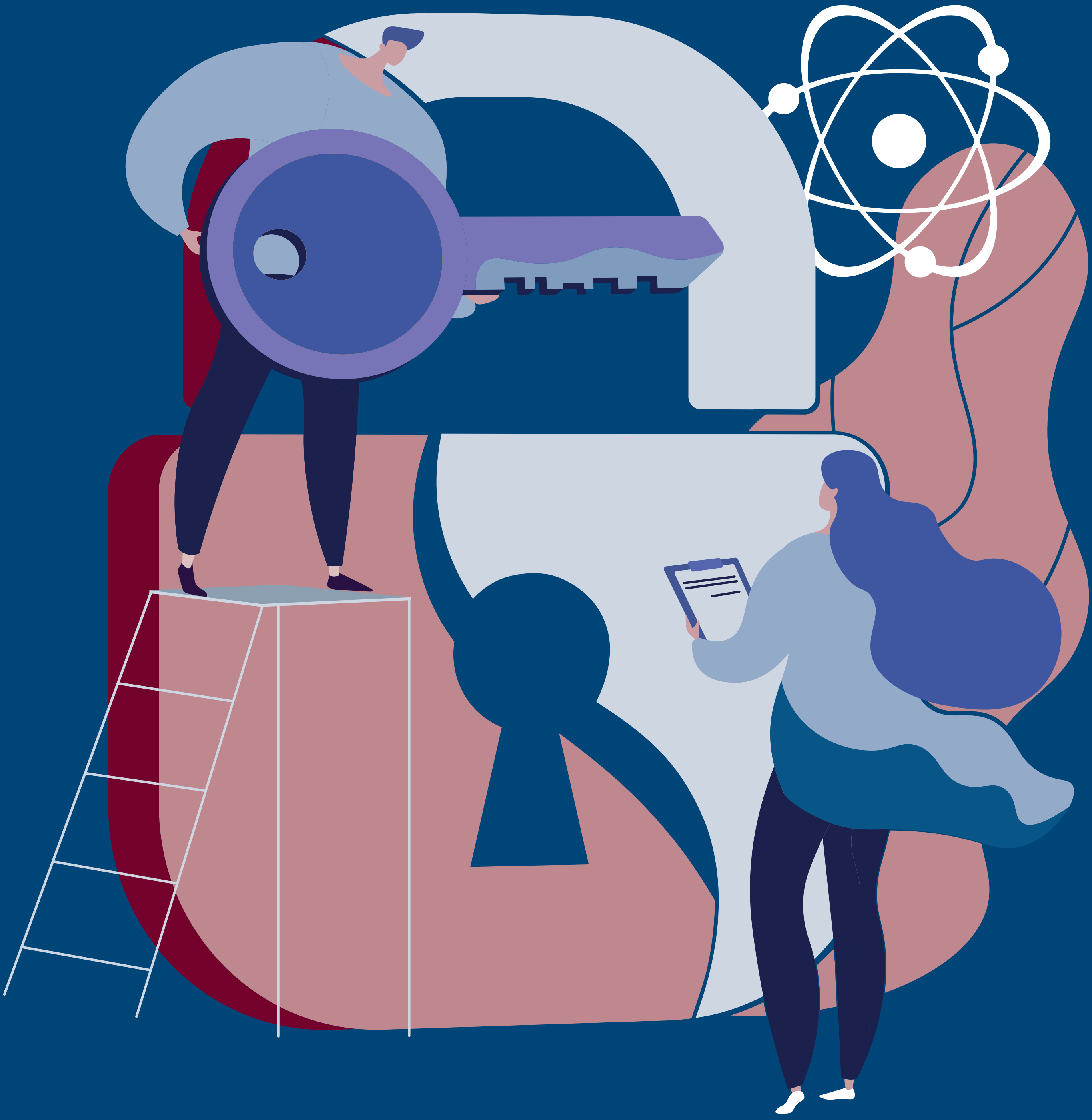
Federal Office
for Information Security



Quantum-safe cryptography –

fundamentals, current developments and recommendations

Foreword

Quantum technologies will change our lives permanently. It has been known since the 1970s that quantum mechanical effects can be exploited for example to accelerate calculations or to measure physical quantities more precisely. Today, there are already first implementations of quantum computers, and the German government is promoting "the development and production of quantum technologies in Germany"[1]. The construction of two quantum computers in Germany is planned as part of the Corona economic stimulus package. In total, two billion euros are being invested in quantum technologies.

Quantum technologies will have a major impact on information security in particular. It has been known since the 1990s that the development of powerful quantum computers threatens the security of public-key cryptography used today. The quantum computers currently available are not yet capable of this, but development is progressing rapidly. Moreover, it is not yet foreseeable what possibilities other quantum technologies will offer. The Federal Office for Information Security (BSI) as the federal government's cybersecurity authority is actively involved in the necessary cryptographic transition.

Since the threat to public-key cryptography posed by quantum computers has been known for a long time, there are also solutions - some of which have existed for a long time - as to how this can be countered. On the one hand, cryptographic schemes which are assumed to be unbreakable by quantum computers - and of course also unbreakable by classical computers - are currently being developed and standardized. These schemes are referred to as post-quantum cryptography.

On the other hand, an alternative proposal, quantum key distribution (QKD), is also attracting strong interest worldwide. Both in the EU and in Germany, intensive work is being done on QKD networks. QKD promises theoretical security based on physical principles, but there are still many open questions about the security of real implementations and their use in communication networks. From BSI's point of view, the focus should therefore currently be on the use of post-quantum cryptography.

With this in mind, BSI has initiated the migration to post-quantum cryptography and published initial recommendations in April 2020. This publication updates and expands them and includes recommendations on QKD. In addition, a detailed exposition of the underlying fundamentals puts the recommendations into context.

Germany.Digital.Secure. BSI - this is our mission in the quantum age also. This publication is intended in particular as a guide for manufacturers and operators of information technology to initiate the migration to quantum-safe cryptography in good time and to make it secure. First of all, it is important to be aware of the problem; and then, as a first step, to take stock of your own systems. This document is intended to support you in this process. Because digitization and information security are inseparable: They are two sides of the same coin and of BSI.

I hope you find it an enlightening read.

Arne Schönbohm

Arne Schönbohm
President of the Federal Office
for Information Security

[1] See https://www.bundesfinanzministerium.de/Web/EN/Issues/Public-Finances/stimulus-package-for-everyone/stimulus-package-for-everyone.html

Summary

Cryptography is in a state of flux. While for a long time it played a role mainly in special applications, such as in the government sector, it is now ubiquitous and its use continues to increase. Cryptography is not only needed to protect sensitive data, but is mandatory in many applications to ensure secure functionality and availability. Just think of the Internet, IoT, long-lived industrial machines or critical infrastructures. At the same time, the so-called "second quantum revolution" has begun: Physical principles discovered about 100 years ago are becoming industrially controllable. Products and applications such as quantum computers, quantum cryptography, quantum sensors and quantum simulators are developing, which will have an impact on the design of secure cryptographic systems.

Today, the security of digital infrastructures is largely based on public-key cryptography (also known as "asymmetric cryptography"). This in turn is essentially based on the assumed difficulty of certain mathematical problems, for example the problem of decomposing a natural number into its prime factors. From these mathematical problems, one-way functions can be derived, i.e., functions that are easy to compute but difficult to reverse. In the example given, the function that is believed to be one-way is the multiplication of two very large primes, which can be done quickly. So far, no efficient classical algorithm is known that can decompose such a large product back into its two prime factors. This observation is the basis for the RSA cryptosystem named after its developers (Rivest, Shamir, Adleman), which is used for encryption as well as for digital signatures. The second mathematical problem, which is the basis for today's public-key cryptography, is the so-called Discrete Logarithm Problem (DLP). On the basis of the DLP, algorithms for key exchange can be constructed, for example.

Usually, cryptographic keys are agreed upon using a public key cryptosystem in order to subsequently encrypt messages with a "symmetric" algorithm (such as AES). According to the current state of knowledge, the common public-key cryptography used today cannot be broken with classical computers. However, the situation will change fundamentally when universal quantum computers of sufficient performance are available. Already in 1994, the mathematician Peter Shor published quantum algorithms, which can efficiently solve the mathematical problems mentioned above. With the development of a quantum computer on which Shor's algorithms can be implemented for sufficiently large input sizes, the basis of today's public-key cryptography would thus be removed. It should be noted that even today an attacker can record communications in order to obtain their contents later ("store now, decrypt later"). For symmetric cryptography, Grover's algorithm would still halve the effective key length. Moreover, quantum computers could also be used to speed up classical cryptographic attacks. It is also conceivable that side-channel attacks on implementations of cryptographic mechanisms could be improved with the help of quantum sensors.

As of now, no quantum computer is available that would be suitable for breaking cryptographic schemes. Nevertheless, the US National Security Agency (NSA) issued an urgent warning in 2015 about the imminent threat to current public key cryptography posed by the development of quantum computers. In order to obtain a well-founded assessment of the current state of development or the potential future availability of a quantum computer, the study "Status of quantum computer development" was conducted on behalf of BSI from 2017 to 2020 [*BSI20*]. Large companies such as Google and IBM have published ambitious roadmaps for the development of quantum computers. For high security systems, BSI acts on the working hypothesis that cryptographically relevant quantum computers will be available in the early 2030s [*BT19/25208*], [*BT19/26340*]. It should be emphasised that this statement is not a forecast of the availability of quantum computers, but rather represents a timeline for risk assessment. BSI has therefore initiated the shift to quantum-safe cryptography in line with the framework programme "Quantum Technologies - from basic research to market" [*BMBF18*].

Also in the recently published Cybersecurity Strategy for Germany 2021 [*BMI21*] of the Federal Ministry of the Interior, Building and Community (BMI), the goal of "Ensuring IT security through quantum technologies" is backed up with a series of metrics. One goal in the cybersecurity strategy, for example, is the migration to quantum-safe cryptography for high-security systems.

But what exactly does the term "quantum-safe cryptography" mean?

In cryptographic research, a new field of work developed parallel to the progress in the development of quantum technologies: post-quantum cryptography. Post-quantum cryptography deals with the development and investigation of cryptographic algorithms that are assumed to be unbreakable even with quantum computers. These algorithms are based on mathematical problems for whose solution neither efficient classical algorithms nor efficient quantum algorithms are known today. Therefore, these solutions are said to be "computationally secure".

Quantum cryptography offers an alternative solution for quantum computer-resistant schemes. It uses quantum mechanical effects to achieve security for cryptographic applications. The protocols of quantum cryptography are supposed to be secure in the sense of information theory, i.e. they cannot be broken even by attackers with unlimited computing power. In real implementations, however, this promise is hard to keep. One example of quantum cryptography is quantum key distribution (QKD), which, however, still leaves many questions unanswered about theoretical and practical security and about embedding it in existing infrastructures. Nevertheless, QKD is attracting more and more interest and a large number of projects for the realization of QKD can be observed. In Germany and the European Union, for example, the QuNET and EuroQCI projects are being carried out, the latter aiming at the establishment of a European quantum communication infrastructure. For the evaluation of QKD devices, BSI is developing a Protection Profile according to Common Criteria in cooperation with ETSI. In addition to research and development, various standardization activities have begun in order to make the schemes available for industrial applications. One of the best known is the standardization process "Post-Quantum Cryptography"[2] of the US National Institute of Standards and Technology (NIST), at the end of which a selection of post-quantum algorithms should be available.

However, the development and standardization of new algorithms is not sufficient. On the one hand, the algorithms do not fit easily into existing cryptographic protocols such as the Transport Layer Security (TLS) protocol. On the other hand, potential vulnerabilities that only arise from the concrete implementation of a new algorithm are not yet as well studied as is the case with algorithms that have been in use for some time. Therefore, quantum computer-resistant methods should not be used alone - at least in a transitional period - but only in hybrid mode, i.e. in combination with a classical method. For this purpose, protocols must be modified or supplemented accordingly. In addition, public key infrastructures, for example, must also be adapted. Here too, the question arises as to whether a signature with a post-quantum procedure is sufficient or whether "hybrid certificates" are required. Many of these questions are (largely) independent of the selection of concrete algorithms and are therefore already being addressed.

Since the security of cryptographic schemes or the suitability of key lengths cannot be guaranteed for a long time, a great need arises for so-called cryptographic agile solutions that allow the secure and easy exchange of cryptographic procedures or even protocols and implementations. To achieve the goal of "cryptographic agility" in the long run, the permanent use of hybrid solutions is also an important building block. Likewise, quantum-safe solutions for software updates should be included where possible. BSI published these and other recommendations for "migration to post-quantum cryptography" in March 2020. This guide supplements and updates the recommendations, explains them and puts them into context.

[2] See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Aim of the document and relation to other documents

This guide is intended to provide an overview of the most important developments in the field of quantum technologies from the point of view of IT security, as well as recommendations for action for migrating to quantum-safe cryptography. The transition to quantum-safe cryptography leads to numerous open questions (for example, the selection of suitable algorithms, necessary adaptations to protocols and standards, and many more), which are discussed in this document. As a basis for this discussion, the possibilities and the state of development of quantum computers are roughly described first. Then, the document discusses post-quantum cryptography and quantum cryptography in detail and distinguishes between these two complementary proposals.

There is now a vast number of projects on quantum technologies and quantum-safe cryptography. This document presents an incomplete selection of projects funded by the Federal Government or in which Germany is involved, as well as activities of BSI on quantum topics. The projects described are primarily those involving BSI. Information on BSI projects aimed at increasing security in the quantum age can be found at:

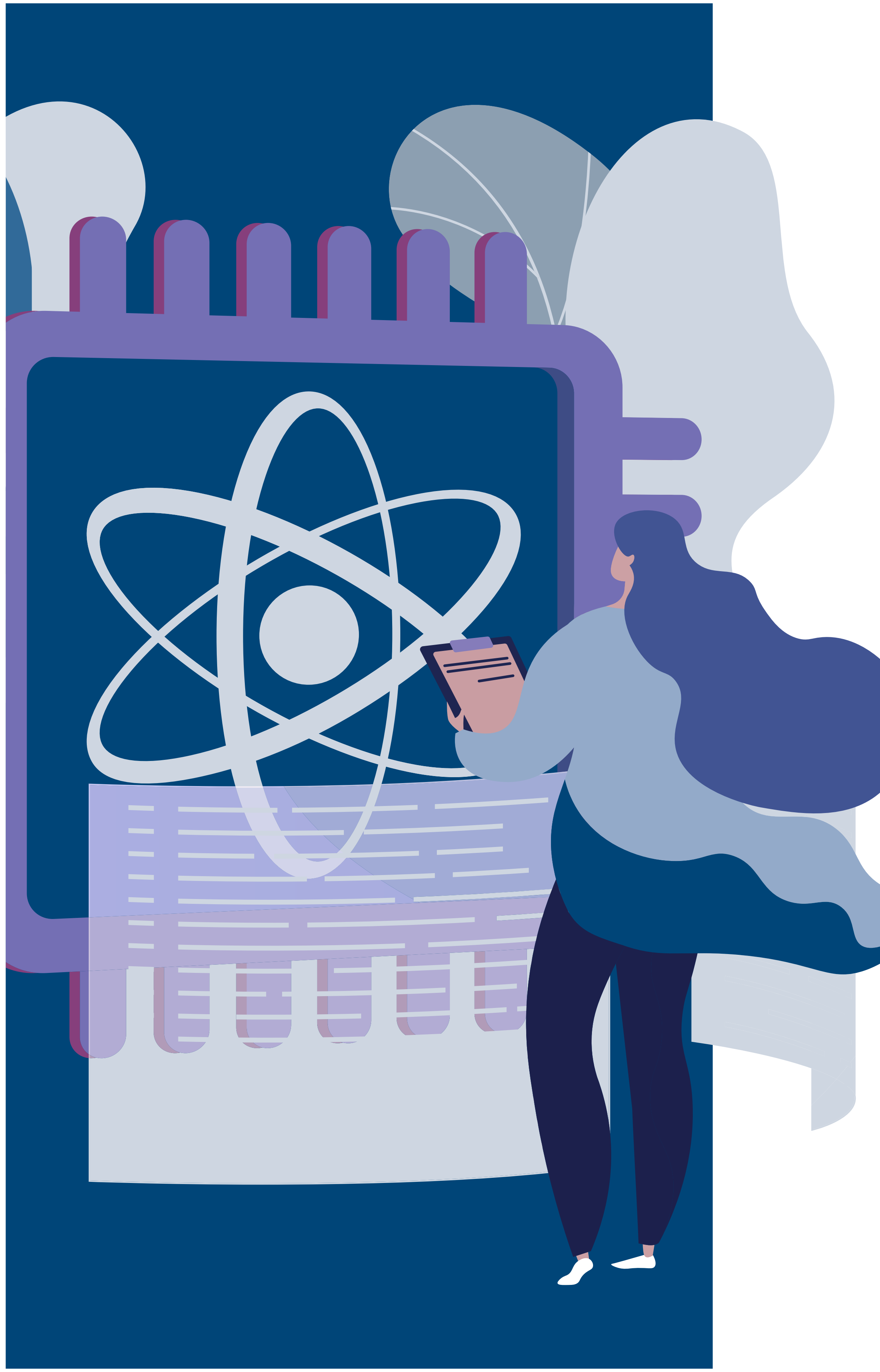
This guide deals with technical topics, but it is neither a scientific treatise nor does it make any statements about patents. Rather, the aim is to familiarise readers with terminology, to provide an overview of current developments and to highlight their interrelationships. The guide endeavours to provide as comprehensive an overview as possible of the current state of knowledge, but does not claim to be exhaustive. The potential absence of an aspect should not automatically lead to its exclusion from further consideration. Likewise, the present document should also be considered in its temporal context in the future, since the technologies described here are developing rapidly and unforeseen leaps in development are entirely possible.

There are already several overview and strategy papers on the topics of quantum technologies and post-quantum cryptography. Examples include the ETSI white paper "Quantum Safe Cryptography and Security" [*ETSI15*] and the German government's framework programme "Quantum technologies - from basic research to market" [*BMBF18*]. In March 2020, BSI published recommendations for action for the "Migration to Post-Quantum Cryptography" [*BSI20b*], which were very positively received and led to many queries and comments. However, these recommendations for action are very concise and are now no longer up to date. Furthermore, they have been limited to recommendations on post-quantum cryptography. However, the rapid developments and great advancement in the field of quantum cryptography make it necessary to assess QKD as a possible solution for quantum computer resistant schemes in more detail and to give more detailed recommendations for the use of QKD. Problems are identified that could in principle stand in the way of a practical use of QKD in large-scale networks. In addition, the use of quantum random number generators is also discussed and put into the context of BSI's assessment methodology. Furthermore, this document not only provides recommendations for action, but also identifies open questions that should be further researched. It thus also pursues the goal of further advancing the discussion on security in the quantum age.

Contents

Foreword

1



1 Quantum computers and their application in cryptography

Our society is increasingly shaped by digitalization and networking. We have become accustomed to digital computers that store and process bits taking values 0 or 1 as the smallest unit of information. As early as the 1980s, however, proposals were made to build computers that compute on so-called qubits instead of bits (see info *"Bits vs. qubits"*), using the quantum mechanical effects of superposition and entanglement (see info *"Superposition"* and *"Entanglement"*). On the one hand, some problems that would classically require a lot of memory can be solved with relatively few qubits. On the other hand, the use of these effects leads to an intrinsic parallelization of some calculations and thus to an acceleration that would not be possible with conventional computers.

A quantum algorithm, i.e., a sequence of manipulations of qubits, exploits precisely this parallelization. Among the best known quantum algorithms are the search algorithm of Lov Grover (1996) and the algorithms of Peter Shor (1994), which can be used to factorize integers and compute discrete logarithms. In particular, the latter algorithms break current public-key cryptography such as RSA, (Elliptic Curve) Diffie-Hellman or ElGamal. Despite the immense impact on current cryptography, the development of quantum computers is mainly motivated by the potential applications in areas such as pharmacy, material science, chemistry or logistics [*ACATECH20*]. In this chapter, we give a brief introduction to quantum computers, report on their state of development, and also describe the main quantum algorithms that are currently known to be cryptographically relevant.

1.1 Quantum computers

Various hardware platforms are being used worldwide for the realization of quantum computers. Leading platforms are currently based on trapped ions and superconductors. The central challenge here is the susceptibility of quantum computers to errors. Quantum systems are very sensitive to disturbances and therefore require an elaborate error correction, which is called quantum error correction (QEC). Its practical implementation is the subject of intense research and although initial successes have been achieved, QEC represents an immense technological challenge. Currently, even with great progress, building a powerful error-tolerant quantum computer is expected to be a scientific and technological challenge.

Currently realized quantum computers that are not fully error corrected are called Noisy Intermediate Scale Quantum (NISQ) computers. These are considered an intermediate stage on the way to fault-tolerant and universally programmable quantum computers. Alternatively, other approaches such as "adiabatic quantum computers" (or "quantum annealers") are already in use today; they require less error correction, but it is debatable whether quantum annealers have already demonstrated advantages over traditional computers.

The first prototypical applications of the currently available NISQ computers focus, among others, on quantum simulation as well as solving certain optimization problems. The former is primarily used to emulate real quantum systems, e.g. in the context of chemical processes or new materials, in order to better predict their behaviour. The latter can be used, for example, in prediction models in the financial sector, in transportation, or in IT security, e.g., anomaly detection in networks. Quantum algorithms are also promising in the context of artificial intelligence (AI) in the sense that they can potentially improve the representational capability and efficiency of purely classical AI methods and enable the design of completely new types of learning methods. In order to be able to set new research directions from the perspective of IT security in the area of Quantum Machine Learning (QML) and to identify targeted further activities, BSI has launched the project "Quantum Machine Learning in the Context of IT Security - Fundamentals (QMLSec)".

In principle, NISQ computers allow the development and evaluation of quantum algorithms, but they have not yet been able to outperform classical computers in concrete applications. For an academic problem with no known direct industrial application, however, such a hardware platform from Google could already achieve the milestone of superiority over classical computers known as Quantum Supremacy [*AAB+19*], [*Wil20*].

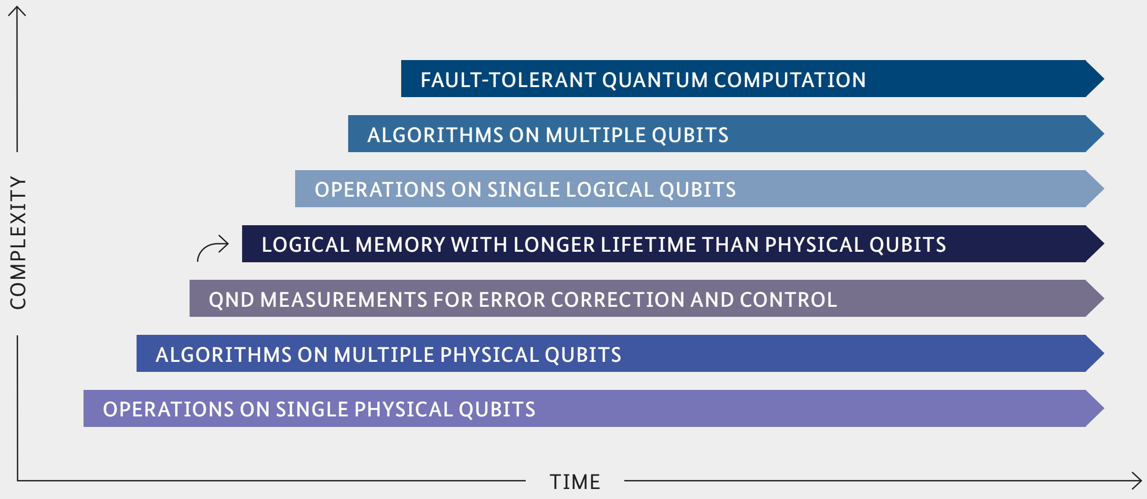

FAULT-TOLERANT QUANTUM COMPUTATION
ALGORITHMS ON MULTIPLE QUBITS
OPERATIONS ON SINGLE LOGICAL QUBITS
LOGICAL MEMORY WITH LONGER LIFETIME THAN PHYSICAL QUBITS
QND MEASUREMENTS FOR ERROR CORRECTION AND CONTROL
ALGORITHMS ON MULTIPLE PHYSICAL QUBITS
OPERATIONS ON SINGLE PHYSICAL QUBITS
COMPLEXITY
TIME

Figure: Development stages for the construction of a fault-tolerant quantum computer.
Source: „Superconducting Circuits for Quantum Information: An Outlook“, https://doi.org/10.1126/science.1231930

In the field of cryptanalysis using quantum algorithms, there are proposals such as factorization on adiabatic quantum computers [*BSI20, §9.1*] and so-called variational factorization [*BSI20, §9.2*], which do not require quantum error correction. For both algorithms, however, a speedup compared to classical factorization algorithms has not been proven. In general, cryptanalytic tasks and algorithms do not seem to be feasible with NISQ computers so far [*BSI20, §4*]. Therefore, taking into account all described approaches to the realization of a quantum computer, fault-tolerant and universally programmable quantum computers currently possess the highest cryptographic relevance.

In the development of a fault-tolerant quantum computer, various technological development stages have to be reached until a quantum algorithm can be executed correctly whilst being scalable to different problem sizes. As already described, the error-proneness or decoherence of quantum mechanical systems represents a central challenge in the construction of a fault-tolerant quantum computer or a scalable qubit technology. In addition to isolating measures such as electromagnetic traps and cryogenic temperatures, a quantum computation must be actively error corrected. In the literature [*DS13*], [*BSI20*], a layer model has been established based on these requirements, which can be used to classify the development stage of a qubit technology. Starting from basic operations on a qubit, i.e. the smallest unit of information of a quantum computer, up to the execution of quantum algorithms such as those of Shor and Grover, it is first necessary to master the structural challenge of the required quantum error correction.

Such a layer model is not fundamentally new. Even on today's commercially available digital computers such as PCs, servers or tablets, algorithms are broken down into elementary operations and executed in processors, i.e. integrated circuits. However, while digital integrated circuits are inherently fault-tolerant, the quantum error correction required to realize a fault-tolerant quantum computer poses significant challenges to science and industry. These challenges are currently being addressed by strong industry players as well as large research programs. IBM has announced ambitious goals in realizing NISQ computing with a "Roadmap for Scaling Quantum Technology"[3]. The two projects funded in the EU Quantum Technology Flagship Programme , AQTION[5] and OPENSUPERQ ,each pursue the goal of realising a European quantum computer.

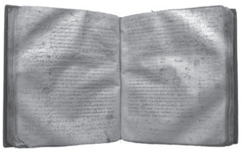
[3] See https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/
[4] See https://www.qt.eu
[5] See https://qt.eu/about-quantum-flagship/projects/aqtion/

In addition to these large-scale projects, the commercialization of quantum computers has begun for example through the availability of Quantum as a Service (QaaS). IBM's QaaS service "IBM Quantum"[6] also offers individuals access to NISQ computers. Similar platforms are offered by Microsoft ("Azure Quantum"[7]) and by Amazon ("Amazon Braket"[8]).

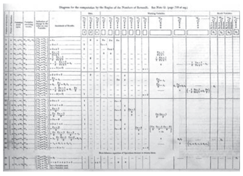
Algorithms

An algorithm is a unique set of instructions for solving a problem. Algorithms are the fundamental starting point for our modern data processing, but they do not represent a technical but a conceptual view of solving a problem and can therefore be written down on paper. The Euclidean algorithm (ca. 300 BC) for computing the greatest common divisor of two integers is considered the oldest known non-trivial algorithm. Charles Babbage took a significant step toward modern computing with the design of the Analytical Engine in the 19th century. For this mechanical calculating machine with memory and arithmetic unit, Ada Lovelace wrote a program to calculate Bernoulli numbers. She is therefore considered to be the person who wrote the first computer program[10]. While the Analytical Engine was never actually built, there were general-purpose computers built in the 20th century with the Zuse Z3, ENIAC and EDVAC in large-scale projects, i.e. computers that could solve many problems based on their range of functions. The Electronic Discrete Variable Automatic Computer (EDVAC), constructed in the 1940s, is the first computer that treated instructions just like the data to be processed by encoding them in binary and keeping them in internal memory [*vN45*], [*Knu70*]. This architecture is ubiquitous in modern digital computers such as PCs, servers, and tablets, and is referred to as the Von Neumann architecture. The universality of today's computers is essentially realized with the basic elementary operation NAND (Not AND). Accordingly, quantum computers also have a set of elementary operations that can be used to efficiently build all quantum operations.

Euclidean Algorithm in Euclid's Elements (Book 7 Proposition 1 and 2)[I]

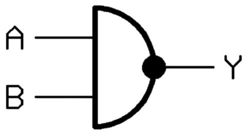


Ada Lovelace's program for calculating Bernoulli numbers on the Analytical Engine[II]



EDVAC[III]

NAND according to DIN 40700[IV]



Source:
I) http://www.claymath.org/euclid/index/b
II) https://de.wikipedia.org/wiki/Datei:Diagram_for_the_computation_of_Bernoulli_numbers.jpg
III) https://de.wikipedia.org/wiki/Datei:Edvac.jpg
IV) https://de.wikipedia.org/wiki/Datei:Logic-gate-nand-de.svg

[6] See https://qt.eu/about-quantum-flagship/projects/opensuperq/
[7] See https://www.ibm.com/quantum-computing/
[8] See https://azure.microsoft.com/de-de/services/quantum/
[9] See https://aws.amazon.com/de/braket/
[10] See https://www.dpma.de/dpma/veroeffentlichungen/aktuelles/patentefrauen/adalovelace/index.html

Bits vs. qubits

The word **bit** is a portmanteau of **binary** digit and refers to a measure of the smallest unit of information in today's digital computers such as PCs, servers, tablets or smartphones. Bits are usually represented by 0 or 1. The word creation and the concept of a bit go back to the work of mathematicians John W. Tukey and Claude Shannon in the 1940s.

Parallel to the development of digital computers, Paul Benioff and Richard Feynman started thinking about quantum computers in the 1980s. One of the first joint milestones was the "Physics of Computation Conference" held in 1981. In the context of quantum computers, the values 0 and 1 act as basic values like the north and south poles of a sphere (noted as |0> and |1> and pronounced "ket-0" and "ket-1") and can be combined in so-called superposition to represent any point on the sphere. This representation is called the Bloch sphere and the elementary storage unit a **qubit**, i.e. quantum **bit**. In contrast to (digital) bits, these additional degrees of freedom, i.e. the possibility of superposition, of a qubit lead to an intrinsic parallelization. A quantum algorithm, i.e. a sequence of manipulations of qubits, exploits exactly this parallelization.

The state of a qubit is thus completely described mathematically by a point on the Bloch sphere. This is the simplest example of a quantum state. Quantum states differ from classical states such as those of a bit, for example, in that they do not behave deterministically when observed, but only assume one of the states |0> or |1> (in the case of the qubit) with a certain probability (see info box "Superposition").

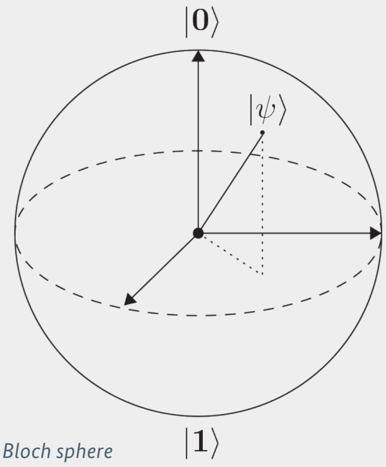


Figure: Bloch sphere

1.2 Quantum algorithms

An algorithm on a classical computer is - roughly speaking - a rule that describes a sequence of manipulations of bits (see info box *"Algorithms"*). In contrast, quantum algorithms, which can be implemented on quantum computers, use qubits as the smallest unit of information. In principle, any quantum algorithm can also be simulated on a classical computer (see info box *"Quantum algorithms vs. classical algorithms"*). However, this requires an exponentially higher effort. On the other hand, quantum effects such as superposition and entanglement open up the possibility of solving some problems much faster on quantum computers than is possible at least with all the classical algorithms known today. It should be borne in mind, however, that quantum computers are far from being able to significantly speed up all problem solutions. For example, it has been shown that for the search problem solved by Grover's algorithm (see Section 1.2.2), asymptotically at most a quadratic speedup is achievable by a quantum algorithm [*BB+97*]. Numerous mathematical problems are assumed not to be solved efficiently even by quantum computers. Details on this can be found, for example, in [*Shor04*]. Post-quantum cryptography is based on such problems (see Chapter 2). In the following, we briefly present the most important cryptographically relevant quantum algorithms that solve certain problems faster than any classical algorithm known so far. This selection does not make any claim of completeness. The “Quantum Algorithm Zoo”[11], which is maintained by Stephen Jordan, is a comprehensive collection of quantum algorithms.

[11] See https://quantumalgorithmzoo.org/

Superposition

A classical bit assumes only the two states 0 or 1. A qubit, on the other hand, can also assume a superposition of two states |0> and |1>. In this case, it exists to some extent in both states simultaneously. If a qubit is in such a superposition state, it only decays with a certain probability into either one or the other state when measured. This destroys the original superposition state and no further information can be obtained about it.

A prominent thought experiment in this context is Schrödinger's cat. Here, a cat is in a specially prepared closed box in which, with a certain probability, a lethal substance is released in a given period of time through radioactive decay. Assuming that the quantum mechanical effects can be applied to the cat, the cat in the closed box is in a superposition state of "dead" and "alive". Different interpretations of quantum mechanics, all consistent with the mathematical formalism, give different answers to the question of when the cat transitions from such a superposition state to one of the two states of "dead" or "alive". As described, this superposition or superposition state of a qubit can be maintained only as long as the information remains unobserved and is not extracted by a measurement.

This property is what makes quantum algorithms so special - one can operate on many pieces of information in superposition simultaneously, but a final measurement provides only severely limited information about the actual outcome of the quantum operation. For a non-trivial quantum algorithm, it is necessary to design a superposition and operations on it in such a way that the "hint" generated by a measurement is still useful.

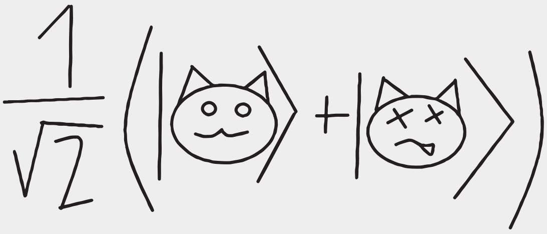


Figure: Schrödinger's cat as "CatKet"

Entanglement

The term entanglement refers to composite physical systems such as two qubits. Two (or more) qubits are said to be entangled if the information represented in them cannot be described solely by the individual information stored in each qubit. For example, two qubits may be entangled such that a measurement of the first qubit assumes the state |0> or |1> with probability 50% in each case, and the second qubit is guaranteed to have assumed the same state as the first after this measurement. This means that a measurement of the first qubit changes the state of the second qubit, even if the two entangled qubits are spatially far apart - a phenomenon Albert Einstein called "spooky action at a distance".

Entanglement plays a central role in quantum computers. Quantum algorithms exploit this inherent property to produce entangled states and thus encode information as densely as possible. A classical digital computer would have to simulate these relationships at great expense. Moreover, the principle of entanglement is fundamental for quantum error correction and thus fault-tolerant computing with quantum computers.

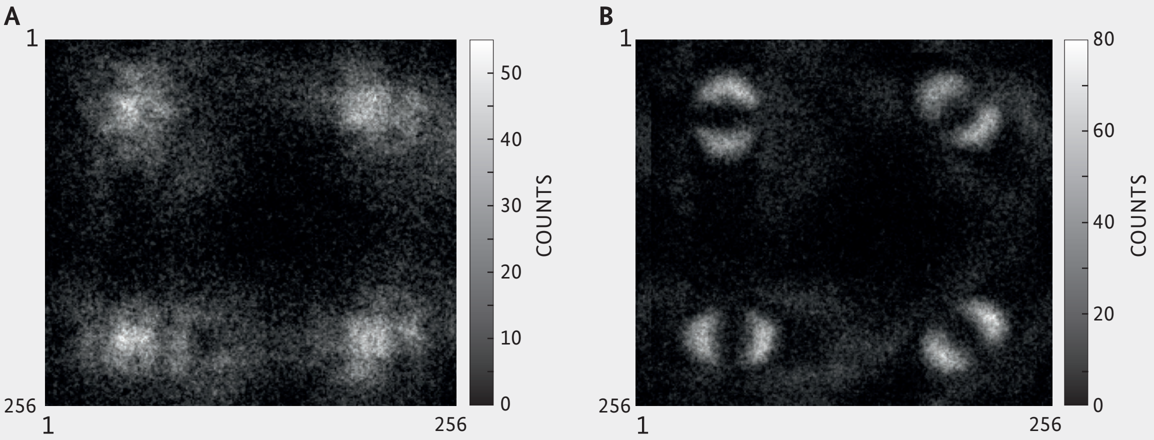


Figure: Experiments with entangled photons
Source: https://advances.sciencemag.org/content/5/7/eaaw2563

Quantum algorithms vs. classical algorithms

The way quantum algorithms and classical algorithms work differs significantly. Classical algorithms, on which our computers are based today, perform calculations by operations on discrete bits. Quantum algorithms, on the other hand, operate on qubits using quantum mechanical effects such as superposition and entanglement.

Nevertheless, every quantum algorithm can in principle be simulated on a classical computer. This is because a quantum mechanical state is completely describable by a complex vector. Furthermore, a quantum algorithm consists essentially of unitary operations on state vectors, which can be described on a classical computer by matrices, and measurements of qubits, which can be expressed by projection mappings and associated probabilities. In this respect, all computations on quantum computers can also be performed on classical computers. However, this can be associated with a significantly higher effort in terms of runtime and memory.

The great potential of quantum algorithms is precisely that they can solve some problems faster than classical algorithms. For example, for searching an unsorted database, Grover's algorithm (see [*Gro96*]) provides a quadratic speedup compared to the best possible classical algorithm. However, it is an open research question whether there are problems that can be solved efficiently, i.e., in polynomial runtime, with quantum algorithms but not with classical algorithms. Factorization of natural numbers into their prime factors is possibly such a problem. However, it has not yet been proved that no classical algorithm with polynomial runtime exists for this.

Of special interest in complexity theory are the problems of the class **NP**. These are problems in which a given solution can be verified in polynomial time. The most difficult problems in NP, to which all others can be reduced with only polynomial overhead, are called **NP-complete**. So far, no algorithms with polynomial runtime are known for NP-complete problems, despite intensive research. However, it has not yet been proved that there are indeed no polynomial algorithms for NP-complete problems. This is one of the most significant open problems in theoretical computer science and is known as the "P vs. NP problem". Moreover, there are also no known quantum algorithms that solve NP-complete problems in polynomial runtime. Assuming that there are no efficient classical algorithms for NP-complete problems, some results suggest that quantum algorithms are not able to do so either (see, for example, [*Shor04*], [*BB+97*]).

1.2.1 Shor‘s algorithms

The security of much of the public-key cryptography used today is essentially based on assumptions about the complexity of certain mathematical problems. For example, an algorithm that efficiently decomposes large natural numbers into their prime factors would break the widely used RSA scheme. To date, no classical algorithm is known to solve the factorization problem efficiently. An algorithm is considered efficient if it solves the problem in a runtime that depends polynomially on the length of the number to be factorized. The fastest known classical factorization algorithm is the number field sieve, which has subexponential but not polynomial runtime. In the mid-1990s, however, Peter Shor published an efficient quantum algorithm for the factorization problem [*Shor94*].

Here we will only roughly sketch how it works. Strictly speaking, Shor's factorization algorithm does not solve the factorization problem directly. Rather, it can first be reduced in a classical way to the problem of determining the period of a certain periodic function. Shor's factorization algorithm starts there and determines this period in polynomial runtime. In doing so, the superposition property of quantum states is exploited in a clever way. Shor's factorization algorithm is a probabilistic algorithm and gives the correct result with high probability. In practice, the correct factorization is obtained with few repetitions. In addition to the factorization problem, a large part of the public key schemes in use today are based on the discrete logarithm problem, for which - similar to the factorization of integers - no efficient classical algorithm is known today. In the same publication in which he describes his factorization algorithm [*Shor94*], Shor also presents a quantum algorithm that computes discrete logarithms in polynomial runtime. His two algorithms use essentially similar ideas and techniques and are known as Shor's algorithms.

1.2.2 Grover‘s algorithm

Shortly after Peter Shor, in 1996 [*Gro96*] Lov Grover published a probabilistic search algorithm for quantum computers that finds an element in an unsorted list of N elements with high probability in $\sqrt{N}$ steps. With classical algorithms, finding an element can only be guaranteed after N steps.

Suppose an unsorted list with N entries is given. This could be, for example, entries of an unstructured database or a list of numbers. This list is to be searched for an entry with a certain property. The checking of the respective property can be modelled quite generally by a black box function that takes a list entry as input and indicates as output whether the property is satisfied or not.

If the list is searched with a classical computer, then in the worst case all N elements must be traversed and the black box function applied to each element. Grover's algorithm, on the other hand, uses a superposition of quantum states in which each list element is contained with equal probability. By repeatedly applying the so-called Grover transformation, which also includes the black box function, the so-called probability amplitude for the searched elements is gradually increased. Thus, with high probability, an entry with the required property can be determined after only about $\sqrt{N}$ steps. Thus, Grover’s algorithm does not provide an exponential speedup, but at least a quadratic one, which can make a significant difference for very large N.

Because of its generality and great flexibility, Grover’s algorithm is applicable in many contexts where problems can be formulated as search problems. Relevant in cryptography is, for example, the search of the key space in symmetric algorithms. For keys of 128 bits in length, the key space can theoretically be searched in about 2^{64} quantum operations using Grover’s algorithm. However, for a key length of 256 bits, an order of magnitude of 2^{128} quantum operations is required, which is not considered feasible today. From a practical point of view, implementing a Grover search on quantum computers places high demands on quantum circuits. For example, a key search for AES would require the AES algorithm for the black box function to be implemented in the circuit. Symmetric cryptographic algorithms, however, can only be implemented in a quantum circuit with great effort due to their nonlinearity.

1.2.3 The HHL algorithm

The HHL algorithm of Harrow, Hassidim and Lloyd [*HHL08*] is a quantum algorithm for solving systems of linear equations. Under some conditions on the linear system of equations (for example, it must be sparse), the HHL algorithm provides an exponential speedup over the known classical algorithms.

Linear systems of equations underlie many mathematical problems. In this respect, numerous applications of the HHL algorithm are conceivable, among others in the field of machine learning. Possible cryptographic applications arise, for example, in the decryption of symmetric encryption algorithms such as AES. This can be traced back to the solution of a system of polynomial equations, to which HHL can be applied when solving a related system of linear equations.

However, the actual practical cryptographic use of HHL is currently unclear. This is partly because the runtime of the algorithm depends on a characteristic of the system of equations under consideration, called the condition, and the condition is difficult to estimate. Second, there is currently little work in the literature on efficient quantum circuits for HHL. Previous work suggests that the practical implementation of HHL for cryptanalysis is very complex and these ideas are currently only theoretically relevant, see for example [*SV+17*] and [*BSI20, §9.6.3*].

1.2.4 Combination of classical algorithms with quantum algorithms

Quantum algorithms can also be combined with classical algorithms and thus accelerate solving certain problems compared to purely classical algorithms. As an example, two cryptographically relevant combinations of Grover's algorithm with a classical algorithm are presented below.

The number field sieve is the fastest known classical factorization algorithm for large numbers, such as RSA numbers. In [*BBM17*], Bernstein, Biasse, and Mosca use the Grover algorithm to speed up an important step of the number field sieve. By doing so, they do not achieve polynomial runtime like Shor's factorization algorithm but at least a speedup over the number field sieve. Moreover, this algorithm requires asymptotically fewer logical qubits (see Section 1.3) than Shor's factorization algorithm. This means that at least for sufficiently large numbers to be factorized, fewer logical qubits are needed. However, an exact analysis for concrete orders of magnitude, such as for the factorization of a 2048-bit RSA modulus, is difficult. Thus, no reliable statement can be made at present to what extent this algorithm offers an advantage over Shor's algorithm for cryptographically relevant orders of magnitude. But it is at least conceivable that this algorithm is less complex to implement and thus becomes cryptographically relevant earlier than Shor's original quantum algorithm.

As shown before, Grover's algorithm can be used to search the key space of a symmetric encryption scheme faster than is possible with classical algorithms. In [MM+18] it is shown how side-channel information about the key space can be included in the search. The result of a side-channel analysis is usually a quantitative statement about the distribution of individual parts of the secret key. From this, a key rank can be calculated, which ranks the possible keys according to their probability, taking into account the given side-channel information. The paper mentioned describes how to efficiently enumerate the keys within a given rank range. Grover's algorithm can then be used to search the most likely key ranges one by one, instead of searching the entire key space immediately. Compared to a classical search with side-channel information, this achieves a quadratic speedup.

1.3 BSI study: Status of quantum computer development

In order to make an independent assessment of the threat, BSI had a study on the development status of quantum computers carried out and published in the period 2017-2020 [*BSI20*], [*CK18*]. The aim of the study was to provide a sound and independent assessment of the current state of development of a cryptographically relevant quantum computer. "Cryptographically relevant" in this context means a sufficiently powerful quantum computer to perform, for example, the Shor algorithms for key lengths used today in realistic runtime. Only publicly available and verified information was to be used. Due to the rapidly progressing developments in the field of quantum technologies and especially quantum computers, BSI intends to continue the study on the development status of quantum computers.

A central challenge for the development of a scalable qubit technology is the error-proneness or decoherence of quantum mechanical systems. In addition to isolating measures such as electromagnetic traps and cryogenic temperatures, a quantum computation must be actively error-corrected. This results in the layered model (A-E) summarized in the study, which can be used to classify a candidate qubit technology. Starting from basic functions (A) up to error-tolerant elementary operations (D) and the assembled implementation of quantum algorithms (E), the path leads via the operational quality of a single qubit (B) and systematic quantum error correction (C) (see info box "*Classical error correction and quantum error correction*").

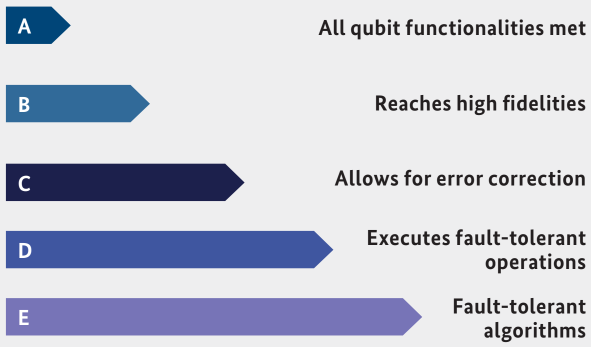

A
All qubit functionalities met
B
Reaches high fidelities
C
Allows for error correction
D
Executes fault-tolerant operations
E
Fault-tolerant algorithms

Figure: *Layer model for the construction of a fault-tolerant quantum computer.*
Source: *BSI study "Status of quantum computer development".*

Classical error correction and quantum error correction

A classical bit is either in state 0 or 1. The only error, and therefore the only unintended change, that can occur in a single bit is the bit flip. This changes 0 to 1 or 1 to 0. Classical error-correcting codes add redundancy to correct for individual bit flips. A simple example is the repetition code, which repeats each bit, for example encoding 0 as 000 and 1 as 111. A single bit flip can be corrected by simple majority voting, for example correcting 010 to 000.

The state of a qubit is described by a point on the Bloch sphere. Thus, in contrast to the classical bit, a qubit can assume an infinite number of different states, which initially results in an infinite number of possible error cases, i.e. unintended changes of the original state. These errors are caused, for example, by the decoherence of a quantum mechanical state, i.e. the interaction with the environment, or by imperfections in the technical realization of quantum gates operating on qubits.

Thus, at first sight, two difficulties arise in the error correction of quantum mechanical states compared to classical bits: Firstly, the state of a qubit cannot simply be redundantly repeated as in classical bits, since according to the no-cloning theorem of quantum mechanics, perfectly copying arbitrary quantum states is impossible. Secondly, there is a continuum of infinitely many possible error cases.

By exploiting specific properties of quantum systems, it is nevertheless possible to develop suitable mechanisms for quantum error correction. The essential idea can be roughly described as follows: The state of a single qubit is mapped onto a system of several entangled qubits in such a way that an error can be detected and subsequently corrected without destroying the essential information about the original state by a measurement. The process of this indirect detection is called syndrome measurement. Syndrome measurement is designed to project the faulty state of the entangled qubits into one of finitely many error cases, thereby reducing the infinitely many error cases to finitely many. For example, the correction of arbitrary errors on a qubit can be reduced to the correction of only bit and phase flips [*KL97*]. The result of the syndrome measurement reveals which of the finitely many error cases occurred, so that the corresponding reversal operation can be performed and the original state restored.

Only a high operation quality allows for efficient quantum error correction. This relationship is precisely described in the Quantum Threshold Theorem by Aharonov and Ben-Or [*AB99*]. 2D transmons (Google) and ion traps (IBM) have been identified as qubit technologies which, with their currently achieved operation quality, allow a functioning quantum error correction in principle, but cannot yet be scaled up to a larger extent.

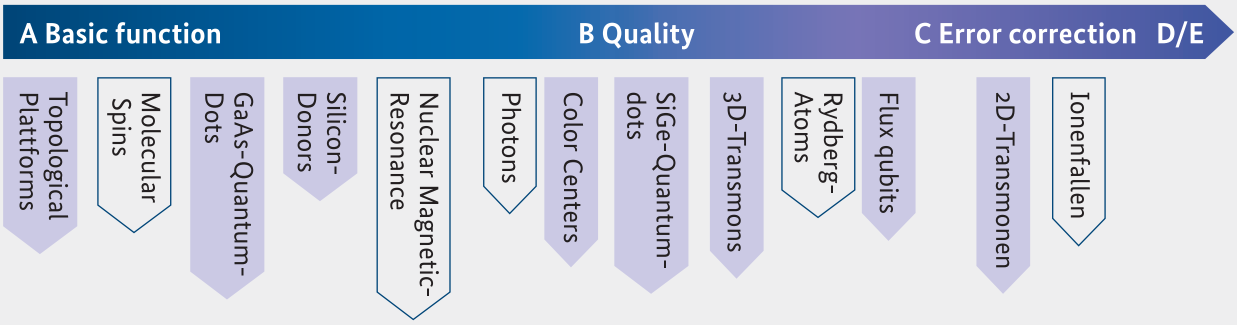


Figure: Classification of different platforms in the layer model.
Source: BSI study "Status of quantum computer development".

For these technologies it is possible to extrapolate a quantum computer based on them, e.g. for the factorization of a 2048-bit RSA module. For this, a single so-called physical qubit must be converted into an error-correcting architecture. Classical error-correction mechanisms encode information redundantly, but are not applicable to quantum states due to the no-cloning theorem. Instead, a quantum error-correcting code transfers the state of a physical qubit to an entangled, i.e. quantum mechanically connected, system of data and syndrome qubits called a logical qubit. Representatives of such codes are the 9-qubit code introduced by Peter Shor (1995) and the currently leading architecture referred to as the surface code. The expansion factor in the transition from physical to logical qubits and thus the overall extrapolation are decisively influenced by the operation quality or error rate and the applied quantum error correction.

The no-cloning theorem

For any given classical bit sequence, such as 11010001, it is easy to describe a procedure to duplicate it: Read the sequence one bit at a time from left to right, and make a copy of each bit after each read. In the example, this yields 11010001 11010001, two perfect copies of the original bit sequence.

Classical states describable by bit sequences can thus be copied arbitrarily. This is in contrast to quantum states - in the simplest case the states of qubits: It follows from the principles of quantum mechanics that there is no quantum mechanical operation that can create an independent identical copy of any given quantum state. This result is known as the no-cloning theorem of quantum mechanics (see [*WZ82*]) and impressively illustrates that classical and quantum mechanical states have very different properties in many respects.

Even if exact copying of arbitrary quantum states is not possible, at least approximate copies of arbitrary quantum states can be created up to a certain degree. Moreover, in many contexts it is sufficient to copy only selected quantum states as accurately as possible. This can lead to copies of these quantum states that have a better quality than if the best possible copies of arbitrary states are aimed for. There are numerous results on the conditions under which a certain quality of copied quantum states can be achieved. An overview of results can be found in [*SIGA05*].

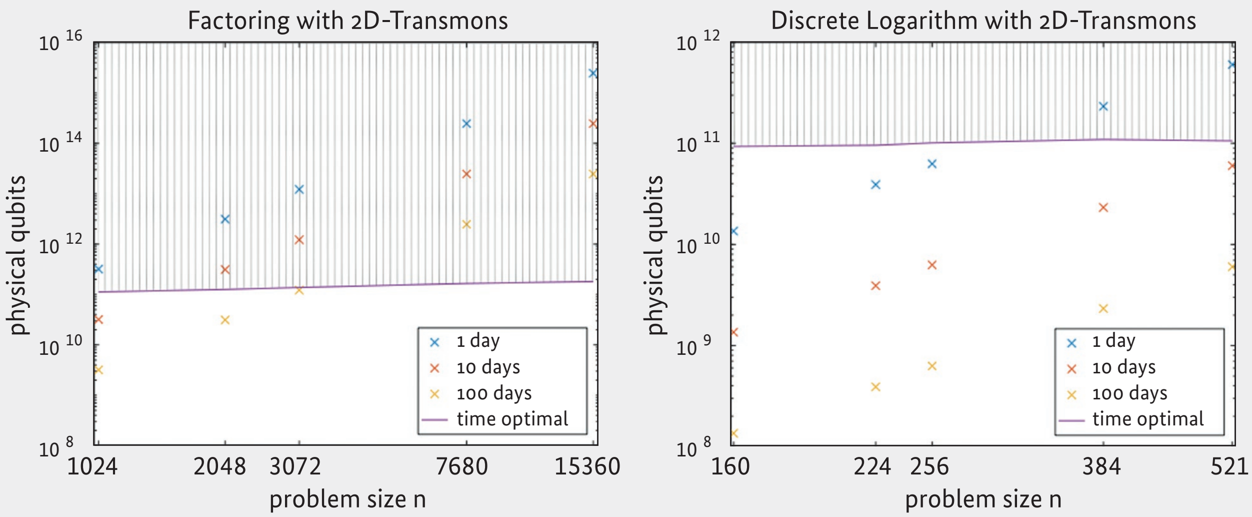


Figure: Size of a 2D transmon quantum computer for factorization and calculation of a discrete logarithm at today's error rate of 1:100.
Source: BSI study "Status of quantum computer development".

From the extrapolation of the study, based on the surface code and an established error rate of 1:100, a 2D transmon quantum computer with a few billion physical qubits would factorize a 2048-bit RSA module in 100 days. At a generally targeted error rate of 1:10000, it would take a few million physical qubits. Due to technological advances, these figures are subject to constant change. In the continuation of the study, the extrapolation will be updated. The addition of "in 100 days" results from a space-time trade-off, because an extrapolation does not result from an isolated consideration of quantum error correction alone. In addition, it is necessary to relate this to elementary operations and cycle times. In the study, first the algorithms of Grover and Shor are decomposed into elementary steps. Here, we make use of the construction of Kitaev [*Kit97*] and Solovay [*Sol00*], which describes a set of elementary operations from which each quantum operation can be efficiently composed.

FACTORING		
n	Qubits	Elementary Operations
1024	2050	$5.81 \cdot 10^{11}$
2048	4098	$5.20 \cdot 10^{12}$
3072	6146	$1.86 \cdot 10^{13}$
7680	15362	$3.30 \cdot 10^{14}$
15360	30722	$2.87 \cdot 10^{15}$

DISCRETE LOGARITHM ON E(F_P)		
m	Qubits	Elementary Operations
160	1466	$2.97 \cdot 10^{10}$
224	2042	$8.43 \cdot 10^{10}$
256	2330	$1.26 \cdot 10^{11}$
384	3484	$4.52 \cdot 10^{11}$
521	4719	$1.14 \cdot 10^{12}$

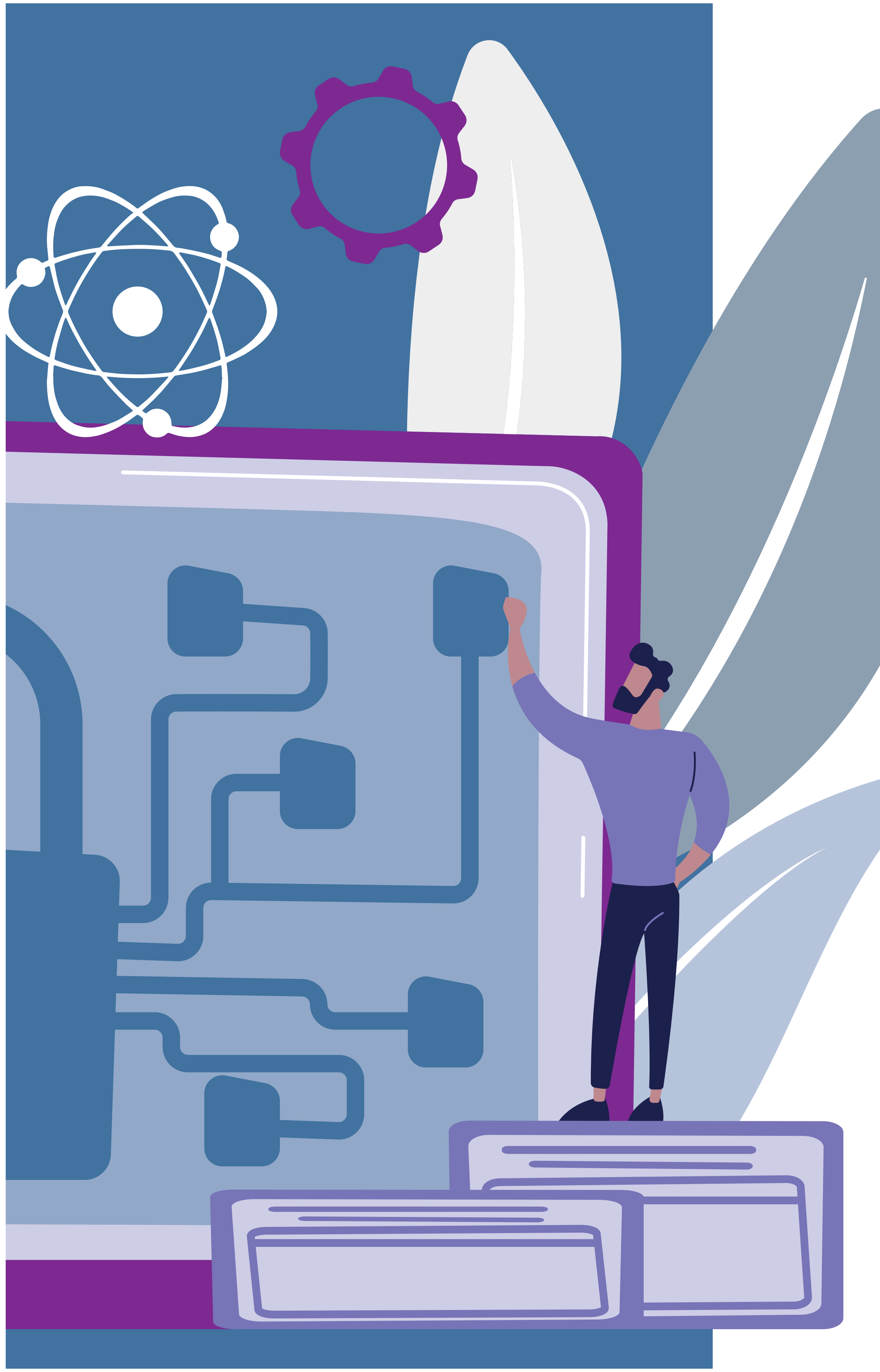
Figure: Elementary operations and (logical) qubits required for a factorization and to compute a discrete logarithm on a generic elliptic curve.
Source: BSI study "Status of quantum computer development".

The study describes and illustrates the interrelationships and concepts outlined here in detail. It provides an overview and classification of current technologies and stakeholders. Algorithmic innovations, such as the optimization of known or the description of new quantum algorithms, leading e.g. to alternative quantum computer realizations or less required quantum error correction or lower number of required qubits, are included. The peripherals for operating a quantum computer are also considered, and residual risks such as potential rapid developments are specifically identified. Overall, the study provides a structured view of the development status of quantum computers. It shows that an enormous effort would currently be required to achieve cryptographically relevant scaling. At the same time, however, it becomes clear that the development has gained momentum due to strong industrial players and large research programmes, and that further commercial applications could accelerate it even more.

1.4 Key points

- Currently used public-key cryptography such as RSA, Diffie-Hellman, ElGamal or ECC is threatened by quantum computing.
- Current cryptographically relevant quantum algorithms essentially require successful quantum error correction (QEC).
- Innovations in quantum algorithms can reduce the technological demands for the realization of quantum computers.
- Cryptanalytical advances based on already available Noisy Intermediate Scale Quantum (NISQ) devices cannot be ruled out.
- The commercialization of quantum computing has already begun, for example with widespread availability of Quantum as a Service (QaaS).

2



2 Post-quantum cryptography

Virtually all asymmetric cryptographic schemes currently in use are threatened by the potential development of powerful quantum computers. Post-quantum cryptography is one way to address this threat. Its security is based on the difficulty of mathematical problems that are currently believed not to be efficiently solvable - even with quantum computers.

2.1 State-of-the-art cryptography and the threat of quantum computers

Symmetric and asymmetric cryptographic schemes differ in the way the cryptographic keys are distributed.

With symmetric cryptographic schemes, the communication partners must be in possession of a shared secret key. This is comparable to a safe that protects contents from access by third parties and can only be opened by those who have the matching key. One advantage of symmetric methods is their efficiency, which is why they are generally used for encryption. A disadvantage, however, is that the keys have to be securely exchanged between the communication partners in advance.

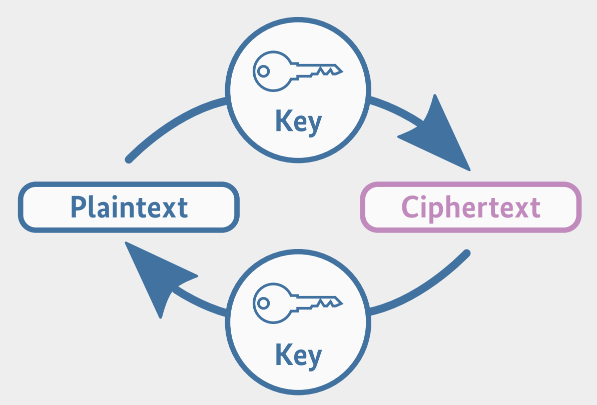


Figure: Schematic illustration of a symmetric encryption or decryption.

Asymmetric cryptographic schemes have the advantage that secret keys do not have to be distributed securely in advance. Each communication party has a pair of keys. One of the keys is public, the second one is secret. For this reason, asymmetric cryptography is also known as public-key cryptography. An appropriate illustration is a mailbox into which anyone can deliver messages, which are then protected from access by third parties because only the owner of a key for the mailbox can retrieve and read the messages. To encrypt a message in public-key cryptography, it is encrypted with the recipient's public key and only the owner of the secret key can decrypt the message. Compared to symmetric cryptography, however, asymmetric algorithms are generally less efficient. Asymmetric methods are used in particular for exchanging keys (see info box “Key agreement”) for symmetric methods via open communication networks such as the Internet and for generating signatures (see info box “Digital signatures”).

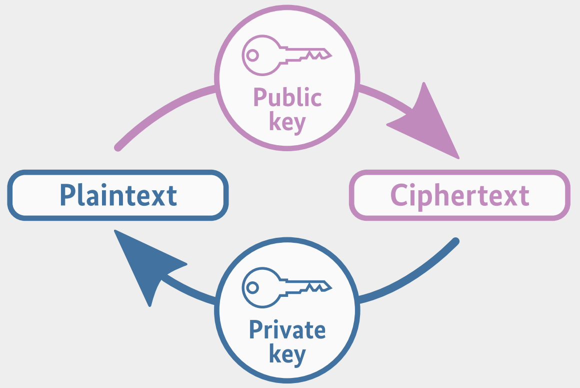


Figure: Schematic representation of asymmetric encryption and decryption

Key agreement

In a key agreement protocol, two[12] parties agree on a common cryptographic key. This key is then usually used to communicate with each other in encrypted form using a symmetric encryption scheme. However, to agree on this symmetric key, an asymmetric algorithm (public-key cryptography) is used to enable secure exchange via a potentially insecure channel.

In key agreement, a distinction is made between two different mechanisms: key exchange ("Key Exchange (KEX)") and key transport ("Key Encapsulation Mechanism (KEM)"). In a key exchange, both parties contribute to the jointly negotiated key. The classic example is the so-called Diffie-Hellman key exchange. In a key transport procedure, in simple terms, one of the two parties generates a symmetric key and sends it to the other party in an asymmetrically encrypted form. However, in some of the currently discussed key transport procedures (see Section 2.3.1), the public key of the second party enters into the generation of the key.

Asymmetric cryptography is based on the construction of so-called one-way functions. These are functions that are relatively easy to calculate, but whose inversion is not considered feasible in practice. An example is the multiplication of two (very large) prime numbers (~ 2000 bits, i.e. a number with about 600 decimal digits). While the multiplication can be computed very quickly, the inversion, i.e. the decomposition of the approximately 4000 bit result into its two prime factors, is not possible in an acceptable amount of time according to the state of the art on classical computers available today. This forms the basis for today's common RSA schemes for encryption and digital signatures, which are intended to guarantee the confidentiality and authenticity of messages. Another mathematical basis for the construction of one-way functions is the so-called Discrete Logarithm Problem (DLP). Methods for key agreement, for example, are based on this problem.

However, with the development of a powerful quantum computer on which Shor's algorithms (see Section 1.2.1) can be used, the security of the public-key cryptography used today will be seriously endangered in the future. This also affects commonly used key agreement schemes (see info box "Key agreement"), which is an essential element for protecting the confidentiality of data. This is especially true for data that must be kept confidential over a long period of time. For example, if a key exchange is recorded by an attacker today, it is possible that in the future, once cryptographically relevant quantum computers become available, the attacker will be able to calculate the shared key and decrypt and read the data encrypted with it. This scenario is also known as "store now, decrypt later".

Digital signatures

In a digital signature scheme, a message is provided with a value that allows the authenticity, integrity and non-repudiable authorship of the message to be verified. Digital signature schemes are asymmetric cryptosystems. The private key is used for signature generation, the public key can be used to verify a signature.

Digital signatures are for instance used to prevent man-in-the-middle (MITM) attacks as part of key agreement. In a MITM attack, an attacker inserts himself into a communication without the original communication partners being aware of this. Mutual authentication using digital signatures effectively prevents this attack.

Authentication by means of a digital signature requires that the originator of the signature can be confirmed. For this purpose, digital certificates are used. A digital certificate binds a public key to the identity of its owner within the framework

[12] There are also more complex variants in which more than two parties agree on a common key. However, these are not considered here.

of a public key infrastructure (PKI). Common certificate formats are PGP [RFC4880] and X.509 [X.509]. As a rule, a public key infrastructure is understood to be a system for validating certificates based on the X.509 standard that is strictly hierarchically structured by means of certification authorities (CAs).

In contrast to key agreement, digital signature schemes are not affected by the "store now, decrypt later" scenario. This is due to the fact that the validity period of the signatures can usually be limited and thus a renewal of the signature or the replacement of the signature procedure can be designed as required. This consideration - considered on its own - is indisputable for the authentication of a key agreement. However, a smooth migration of existing digital infrastructures is costly and takes a certain amount of time. These migration periods must be taken into account, especially in the case of signatures valid for longer periods, e.g. in the context of public key infrastructures.

While asymmetric cryptosystems based on the factorization or discrete logarithm problem can be completely broken by quantum computers using Shor's algorithms, symmetric primitives such as block ciphers (e.g., AES) or hash functions (e.g., SHA-2, SHA-3) are considered fundamentally resistant to quantum computer attacks according to current research, as long as the key lengths are adjusted accordingly. This is because while brute-force attacks or algorithms for finding collisions in hash functions can be accelerated by quantum algorithms such as Grover's search algorithm, they still cannot be carried out efficiently (in polynomial time), cf. Section 1.2. In the case of AES, for example, it is assumed that the use of a key length of 256 bits provides sufficient protection against quantum computer attacks in the long term.

How much time is left for migration?

To estimate when the migration to quantum-safe cryptography is necessary, the following consideration by theoretical physicist M. Mosca from [Mos15] is very illustrative.

Let

- *x* be the number of years that the data to be protected must remain secured,
- *y* be the number of years needed to convert the corresponding system to quantum computer-resistant cryptography, and
- *z* be the number of years it will take for quantum computers to exist that threaten the cryptography currently in use.

Then, if x+y > z, you have a problem!

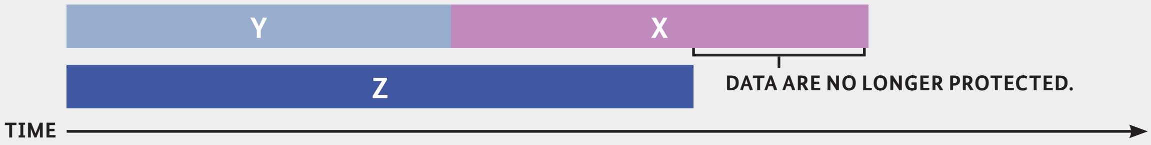


Figure: Illustration of "Mosca's Theorem"

This statement has become known as "Mosca's theorem", even though it is of course a rather obvious statement. In the following, we give a few more details:

If the migration to quantum-safe cryptography is started today, it will be completed after y years. How large y is depends on various factors, such as the extent to which systems are affected and the availability of quantum-safe alternatives. An important first step is therefore to take stock and develop a migration plan, see Section 6.1.

The last data that was still encrypted with the old methods will thus be generated in y years and should then be secured for another x years. In the case of real-time communication, this time period x can be vanishingly small. In contrast, sensitive medical information, for example, should remain secure for several decades.

Assume that x+y>z holds. Then one can intercept the last data that is not yet secured in a quantum-safe manner and decrypt it within the time in which it should be secured. Thus, the migration to quantum-safe cryptography must start early enough that x+y<z still holds for all data to be protected. But how large is z?

For national security systems, BSI works under the hypothesis that cryptographically relevant quantum computers will be available in the early 2030s [BT19/25208], [BT19/26340]. It should be emphasised that this statement is **not to be** understood as a forecast of the availability of quantum computers, but rather represents a benchmark for risk assessment. BSI has therefore initiated the shift to quantum-safe cryptography in line with the federal government's framework programme "Quantum technologies - from basic research to market" [BMBF18].

2.2 Post-quantum cryptography

To counter the threat to today's asymmetric cryptography by quantum computers, a new field of cryptographic research has emerged: **post-quantum cryptography.**

Post-quantum cryptography deals with the development and investigation of asymmetric cryptosystems which, according to current knowledge, cannot be broken even with powerful quantum computers. These methods are based on mathematical problems for whose solution neither efficient classical algorithms nor efficient quantum algorithms are known today. In current research, various approaches are being pursued to realize post-quantum cryptography. These include, among others:

- **Code-based cryptography:** The security of code-based schemes is based on the difficulty of efficiently decoding general error-correcting codes.
- **Lattice-based cryptography:** The security of lattice-based schemes is based on the difficulty of solving certain computational problems in mathematical lattices.
- **Hash-based cryptography:** The security of hash-based signature schemes is based on the security properties of the hash function used.
- **Isogeny-based cryptography:** Isogeny-based schemes base their security on the fact that it is difficult to find an isogeny between two super-singular elliptic curves, if one exists.
- **Multivariate cryptography:** The security of multivariate cryptography is based on the assumption that multivariate polynomial systems of equations over finite fields are hard to solve.

In the following, only the first three classes will be discussed further, since the post-quantum schemes currently recommended by BSI belong to these classes. Multivariate schemes have a long history of attacks and fixes. Currently, BSI does not intend to recommend the use of multivariate schemes. Cryptography based on isogenies (mappings between elliptic curves with special properties) is an interesting research topic that BSI believes should be explored further before a recommendation is considered.

2.2.1 Code-based cryptography

Error-correcting codes

Error-correcting codes make it possible to detect and correct errors in stored or transmitted data. They are used in all storage and communication solutions such as CD/DVD, DVB, WLAN, mobile radio and satellite communication. Their history goes back to the pioneers of modern information theory, Richard Hamming and Claude Shannon.

The simplest example of an error-correcting code is the repetition code, which repeats each piece of information multiple times and corrects errors using majority voting. That is, a bit sequence 1011 is encoded as 111 000 111 111. If one receives a packet 101, this is decoded as 1. In general, error detection and correction depend on the so-called Hamming distance.

Modern error correction methods with special encoding rules allow highly efficient correction mechanisms. A much more general question is posed by the **general decoding problem:** The problem of decoding a received message based on a random or unstructured code. It is well known that this problem is **NP-hard** in general [BMT78], i.e., it is a difficult computational problem as long as P≠NP. Essentially, all approaches focus on solving a linear system of equations **y=zH**, where **y** is the received message and **H** describes the general code, to then find a minimal element $\mathbf{z}_0$ among all solutions.

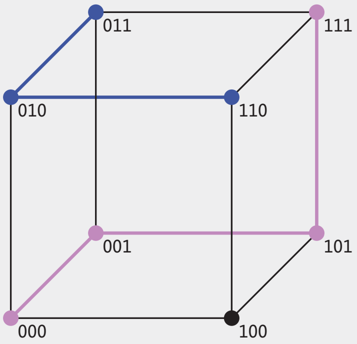


Figure: Hamming Distance in a 3-Bit Example
Source: https://users.cecs.anu.edu.au/~jks/Hamming.html

Code-based cryptography refers to encryption, key agreement, and signature algorithms whose security is based on the General Decoding Problem.

Its most prominent representative is the McEliece cryptosystem, an asymmetric encryption scheme introduced in 1978 by Robert McEliece [McE78]. Its security is based on two assumptions. The first assumption is that the binary Goppa codes used are indistinguishable from random linear codes. The second assumption is that random linear codes can only be decoded with exponential effort due to the General Decoding Problem, both on digital and quantum computers. Apart from an adaptation of the parameters originally proposed by McEliece (these have been attacked in the light of modern computing power in 2008 by Bernstein, Lange and Peters in about 2^{60} operations [BLP08]), after more than 40 years of research it has not been possible to find a structural weakness of the McEliece cryptosystem when binary Goppa codes are used. Thus, the McEliece cryptosystem can be considered to be one of the oldest unbroken quantum-safe proposals.

A major disadvantage is the space requirement of the public key. This can be reduced by a variant of the McEliece cryptosystem described by Harald Niederreiter [Nie86] in 1986, but still remains in the megabyte range for high-security applications. On the other hand, however, the ciphertexts of code-based key agreement schemes are very small (about 200 bytes) and the encryption and decryption is much more efficient than RSA- or EC-based asymmetric encryption schemes. Recent proposals have introduced more structure into the class of codes used to significantly reduce the space required by the public key, e.g., [MB09]. However, these additional structures have led to successful attacks on some of these proposals [FO+16].

Traditional code-based signature schemes, e.g. [CFS01], have so far exhibited significant efficiency problems and are therefore only of theoretical interest. Alternative approaches for more efficient signature schemes [BB+21], which are based on coding theory, are still at a very early stage.

2.2.2 Lattice-based cryptography

Mathematical lattices

A lattice is a discrete subgroup of an n-dimensional real vector space. In simplified terms, subgroup here means that you can add lattice points and thereby get a lattice point again. Discrete essentially means that there is a minimum distance (greater than zero), so that any two different lattice points have at least this distance. Thus, lattice points cannot be arbitrarily close to each other. It is easy to see in the figure why this is called a lattice. There are also special lattices that have additional algebraic structure. This additional structure allows to construct more efficient cryptosystems. However, it may also provide a bigger attack surface.

For example, a difficult computational problem in lattices is the so-called **Shortest Vector Problem (SVP),** the problem of finding a shortest (non-zero) lattice vector (i.e., a nontrivial lattice point that is as close as possible to the origin). While one can still solve the problem relatively easily for low-dimensional lattices (for example using the LLL algorithm ([LLL82]), neither classical algorithms nor quantum algorithms are known which solve the problem efficiently in higher dimensions for general lattices.

However, modern lattice-based cryptosystems are often not based directly on this problem, but on computational problems such as the **Learning With Errors (LWE)** problem. Here, one is given a "noisy" linear system of equations in the form of a matrix **A** and a vector **b=As+e** mod q for an integer modulus q, and is supposed to find the secret vector **s.** The "error vector" **e,** which is also secret, is a "short" vector that can be interpreted as a "perturbation" of the linear system of equations. One can show that the LWE problem is asymptotically at least as hard to solve as a variant of the SVP, given a suitable parametrisation.

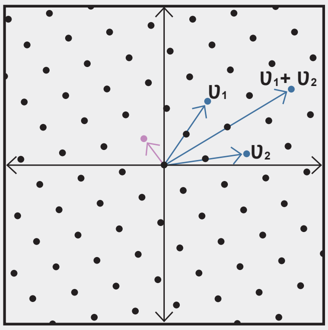


Figure: Example of a 2-dimensional lattice

The security of many cryptographic schemes is based on the assumed hardness of lattice problems - from basic primitives such as encryption, key agreement and digital signatures, to cryptographic schemes with extended functionality such as fully homomorphic encryption.

For cryptographic applications, the work of Ajtai [*Ajt96*] is of fundamental theoretical importance, proving "worst-case to average-case" reductions for certain lattice problems. One of the first lattice-based schemes is by Ajtai and Dwork [*AD97*], which is, however, relatively inefficient.

In search of practical lattice schemes, the NTRU encryption scheme of Hoffstein, Pipher, and Silverman [*HPS98*] and the Ajtai-Dwork inspired cryptosystem of Goldreich, Goldwasser, and Halevi [*GGH97*] were introduced. However, the standard version of the NTRU problem is currently not proven to be at least as hard as "worst-case" lattice problems. Nevertheless, given a suitable choice of parameters, NTRU-based methods have not been broken to date.

Another milestone in the history of lattice-based cryptography was the introduction of the so-called "Learning With Errors" (LWE) problem (see info box Mathematical Lattices) by Regev [*Reg05*] in 2005. Many of today's lattice-based encryption and key agreement schemes are based on the LWE problem or one of its variants.

These variants, such as ring LWE [*LPR10*] or module LWE [*BGV12*], [*LS15*], were introduced to increase efficiency and reduce key sizes. They are based on the assumption that lattice problems are hard to solve even in lattices with additional (algebraic) structure. The NTRU cryptosystem mentioned above is also based on lattice problems in structured lattices. However, besides the increased efficiency, the additional structure in such lattice-based cryptosystems also carries the risk of potentially providing further attack vectors. Whether structured and unstructured lattices provide the same level of security is an important research question that should be investigated further, cf. also Section 2.3.

Lattice-based cryptosystems have received broader attention at the latest since the lattice-based method "New Hope" was experimentally tested in Google's Chrome browser. They have received a lot of attention in cryptographic research and make up a large part of the finalists in the current NIST standardization process (see Section 2.3).

A more detailed insight into the history of lattice-based cryptography can be found in [*Pei16*]. BSI has commissioned a study to evaluate lattice-based schemes [*BSI18*]. This study also describes the basics of lattice-based cryptography.

2.2.3 Hash-based cryptography

Hash functions

Hash functions are compression functions that basically map input data of any length to fixed length values (e.g. 256 bits). Usually, a cryptographic hash function **h** is used, which has the following security properties:

- One-way function (preimage resistance): It is practically impossible to find an input value **x** for a given hash value **y** such that **h(x)=y.**
- Weak collision resistance (second preimage resistance): It is practically impossible to find a second **x'** for a given input value **x,** such that the hash values match **h(x)=h(x').**
- Strong collision resistance: It is practically impossible to find two input values x and x' such that the hash values match h(x)=h(x').

Commonly approved construction principles for hash functions are the Merkle-Damgård and Sponge construction for the SHA-2 and SHA-3 families, respectively.

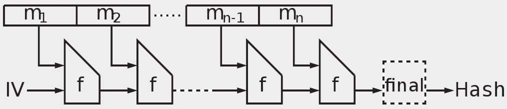


Figure: Merkle-Damgård construction
Source: https://de.wikipedia.org/wiki/Datei:MerkleDamgard.svg

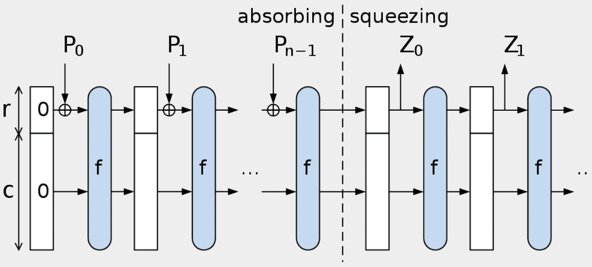


Figure: Sponge construction
Source: https://de.wikipedia.org/wiki/Datei:SpongeConstruction.svg

One-time signatures and hash trees

One-time signature schemes (OTS) allow a private key only to be used once to generate a signature. The Lamport-Diffie or Winternitz OTS are among the best-known such schemes. One-time signature schemes can be illustrated with the following example.

Suppose a person A wants to be able to communicate a yes-no decision to a fixed reference person B on short notice via an untrusted channel. For this purpose, A can make use of a one-way function h (e.g., a cryptographic hash function), compute two values y1= h(x1) (for "yes") and y2= h(x2) (for "no"), and communicate the values y1 and y2 as well as the used one-way function h to his fixed reference person B (e.g., in person) before such a decision occurs. Person A is now able to reliably communicate his decision over an open channel. He either transmits x1 for "yes" or x2 for "no". For example, if person B receives x1, B computes the value h(x1) and determines y1= h(x1), i.e., "Yes". Because of the one-way function, no one is able to manipulate the decision as long as x1 and x2 are kept secret by A.

The example illustrates that a private key (here x1 and x2) may only be used once. If one wants to make many authentic yes-no decisions, e.g., sign a binary-encoded message 010101110100001010 , one potentially needs a large set of private and public keys. Therefore, in a digital and multilateral environment with many communication partners, one-time signature schemes are highly unpractical. This problem was solved by Ralph Merkle in 1979 [Mer79]. He is credited with the invention of the hash tree or Merkle tree, in which the public keys (h(x1) and h(x2) in the example) are compressed in pairs using a cryptographic hash function. This procedure is repeated until one arrives at the so-called root of the resulting binary tree. The value of the root in this Merkle signature procedure is now the public key, which is the same for all individual private keys.

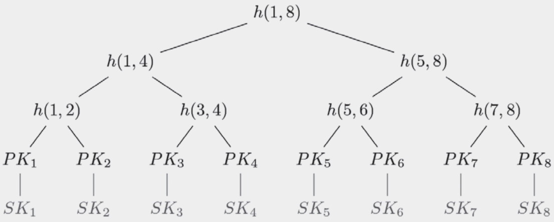


Figure: Merkle tree

Hash-based cryptography is a generic term for cryptographic constructions based on the security of hash functions. Essentially, the terminology refers to digital signatures that are constructed with the help of hash trees and one-time signature schemes. A distinction is made between stateful and stateless hash-based signatures.

The construction of hash-based signatures goes back to Ralph Merkle [*Mer79*], which is why they are also referred to as Merkle signatures. The security properties of Merkle signatures are very well understood, and in their current form (LMS [*LM95*], XMSS [*BDH11*]) they are considered to be mature quantum-safe signature schemes. However, a key drawback is their statefulness: the signer must keep exact track of which one-time signature keys have already been used. Any error in this track keeping procedure results in the loss of security and thus high requirements are imposed on the implementation and usage. In addition, the number of possible signatures is limited. When generating keys, a trade-off must be made between signature size and the number of signatures that can be created. Therefore, Merkle signatures, in addition to symmetric methods, are particularly suitable for future-proof software update concepts, where statefulness can be handled well and the maximum number of required signatures can be estimated. Accordingly, Merkle signatures are recommended in Technical Guideline TR-03140 under the Satellite Data Security Act (SatDSiG) as future-proof digital signature schemes "for update-able crypto module by signature methods" [*TR-03140, 5.5.2.1*]. In general, BSI has long recommended Merkle signatures [*Mer79*] as quantum-safe signatures in its Technical

Guideline TR-02101-1 [*TR-02102-1*]. The stateful hash-based signature schemes LMS and XMSS have already been standardized by the IETF as RFC8554 [*RFC 8554*] and RFC8391 [*RFC 8391*], respectively. NIST has adopted these standards as Special Publication 800-208 [*SP800-208*]. Both standards were also incorporated into TR-02102-1 in 2021. In parallel, hash-based signature schemes in the form of LMS have found their way into Cryptographic Message Syntax (CMS) [*RFC 8708*] and Concise Binary Object Representation (COSE) [*RFC 8778*]. CMS and COSE are basic data formats that are used, for example, in S/MIME and IoT, respectively.

As a stateless variant of a hash-based signature scheme, SPHINCS [*BH+15*] has been developed in recent years. It goes back to a design by Goldreich [*Gol86*]. While it is no longer necessary to keep track of which signature keys have been used, this statelessness entails certain efficiency disadvantages (e.g., signature size) due to its design principles compared to LMS and XMSS. In a concrete application scenario, it must be assessed whether SPHINCS is a suitable solution despite the efficiency disadvantages.

2.3 Standardization of post-quantum cryptography

In recent years, post-quantum cryptography has gained considerable importance: In August 2015, the U.S. National Security Agency (NSA) warned about the impact of quantum computers on the security of cryptographic schemes and initiated a migration to post-quantum cryptosystems. As justification, the NSA has cited advances in physics and technology that could enable the development of a cryptographically relevant quantum computer. The NSA did not name any specific post-quantum algorithms, but referred to the future standards of the National Institute of Standards and Technology (NIST).

In the past, NIST has conducted competitions that have produced the widely recognized algorithms AES and SHA-3. In line with the NSA announcement, NIST started a process in November 2016, at the end of which a selection of post-quantum schemes should be available[13]. This process is conducted in several rounds. By the November 2017 submission deadline, a total of 82 proposals were submitted, of which 69 met the minimum criteria and were accepted by NIST as candidates in the first round. In January 2019, based on public comments from the research community and NIST's internal analysis, NIST selected 26 of these candidates to advance to the second round. These 26 second-round candidates include 17 schemes for asymmetric encryption or key agreement and 9 digital signatures schemes. Then, in July 2020, NIST announced the candidates that will advance to the third round. NIST divided the third round candidates into "finalists" and "alternate candidates". The reasons why some schemes were named alternate candidates vary widely. It is anticipated that a selection of finalists will be standardized at the end of the third round. NIST announced in June 2021 that there will be a fourth round at the end of which additional candidates may be standardized. The finalists of the third round are the four asymmetric encryption or key agreement schemes Classic McEliece [*ABC+20*], CRYSTALS-KYBER [*SAB+20*], NTRU [*CDH+20*] and SABER [*DKR+20*] as well as the three signature schemes CRYSTALS-DILITHIUM [*LDK+20*], FALCON [*PFH+20*] and Rainbow [*DCP+20*]. The eight alternate candidates are BIKE [*ABB+20*], FrodoKEM [*NAB+20*], HQC [*MAB+20*], NTRU Prime [*BB+20*], SIKE [*JAC+20*], GeMSS [*CFM+20*], Picnic [*ZCD+20*], and SPHINCS+ [*HB+20*].

One class of cryptographic schemes that NIST has considered separately are stateful hash-based signature schemes [*SP800-208*]. This is because they were standardized early on by the IETF due to their well-understood security properties (see Section 2.2.3).

According to NIST, the first drafts of standards from the NIST process are not expected until between 2022 and 2023 (and final standards not before 2024). Due to the urgency of the transition to quantum computer-resistant key agreement procedures, BSI has recommended two of these schemes in its technical guideline TR-02102-1 [*TR-02102-1*] already at the beginning of 2020 for the first time. At the same time, this should provide orientation for the German crypto industry and allow it to develop market-ready products at an early stage, and it will help BSI to focus security investigations on relevant algorithms. The two schemes are the lattice-based FrodoKEM [*NAB+20*] and the code-based Classic McEliece [*ABC+20*], both of which were in the second round of the NIST process at the time. While Classic McEliece is now among the finalists for the third round, FrodoKEM was included in the list of alternate candidates, see Section 2.3.1.

[13] See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Parallel to the NIST process and also in the context of post-quantum cryptography, there are other standardization activities. The Chinese Association for Cryptologic Research (CACR) held a national competition from 2018 to 2019[14]. The Russian Technical Committee for Standardization "Cryptography and Security Mechanisms" (TC26) of the national standards organization ROSSTANDART established a working group in February 2020 that aims to finalize draft standards by the end of 2021 [*Fed21*].

BSI welcomes the NIST process as a method of defining standards in a transparent international process that can then be used worldwide. It is particularly opposed to a separate process for standardising German or European algorithms. A "proliferation" of international standards would both hamper interoperability and reduce the market opportunities of crypto producers. In addition, a splitting of personnel and research resources would lead to a lower evaluation quality for those algorithms that are ultimately selected.

2.3.1 Key transport

The NIST process originally sought methods for both key transport and encryption. However, it has become apparent that the submissions essentially focused on key transport and defined asymmetric encryption only as a preliminary stage for such a mechanism. Therefore, the description in this section is limited to key transport procedures. It mainly deals with the FrodoKEM and Classic McEliece methods, which are recommended by BSI. FrodoKEM is a lattice-based key transport scheme whose security is based on the assumption that the so-called Learning With Errors (LWE) problem (see info box "Mathematical lattices") is difficult to solve for classical and quantum computers. Unlike many other lattice-based schemes in the NIST process, FrodoKEM's underlying lattices have no additional algebraic structure. Although it is not known whether such additional structure can be exploited by attackers, FrodoKEM thus eliminates this risk. On the other hand, FrodoKEM is somewhat more inefficient compared to some other lattice-based key transport schemes. Further information on FrodoKEM can also be found in the BSI magazine [*Hag20*]. NIST justifies the decision to include FrodoKEM in the list of alternate candidates by stating that although FrodoKEM has potential security advantages over other lattice-based schemes, it also offers poorer performance. Thus, FrodoKEM's standardization could likely wait until after the end of the third round, and FrodoKEM could also serve as a "conservative backup" if cryptanalytic advances were made regarding lattices with additional algebraic structure. Since the reason FrodoKEM was not included in the list of third-round finalists does not concern the security of the scheme, BSI continues to stand by its recommendation of FrodoKEM.

Classic McEliece is a code-based key transport scheme based on Niederreiter's variant [*Nie86*] of the McEliece encryption scheme [*McE78*], instantiated with binary Goppa codes. The original McEliece cryptosystem was introduced as early as 1978, so it has a long history of not being broken compared to other post-quantum cryptosystems. One drawback of the scheme is that it requires very large public keys compared to other candidates, which could make its use problematic for some scenarios.

The other finalists in the NIST process among the key agreement schemes are the structured lattice-based CRYSTALS Kyber, NTRU, and SABER. The remaining alternate candidates are the code-based methods BIKE and HQC, the structured lattice-based NTRU Prime, and the isogeny-based scheme SIKE.

2.3.2 Signature schemes

The finalist candidates for signature schemes in the third round of the NIST process are the lattice-bases schemes CRYSTALS Dilithium and FALCON and the multivariate scheme Rainbow.

The security of CRYSTALS-Dilithium is based on the lattice problems module-LWE and module-SIS, which are structured variants of the LWE and SIS (Short Integer Solution) problems, respectively. Overall, Dilithium has good performance, moderate key and signature sizes, and is easier to implement than FALCON according to NIST [*MAA+20*].

The security of FALCON is based on the SIS problem instantiated with so-called NTRU lattices, which also have additional structure. One design goal of FALCON is compactness, i.e. minimizing the sum of the sizes of the public key and the signature. Signing and verification with FALCON are also efficient, but key generation is slower compared to Dilithium.

[14] See http://sfis.cacrnet.org.cn

Due to new attacks on multivariate methods in the third round of the NIST process, it is currently not expected that Rainbow will be standardized [*Beu22*]. NIST has announced that it will not standardize both Dilithium and FALCON (at least not at the end of the third round). Furthermore, NIST plans to accept new proposals for signature schemes within 6-12 months after the end of the third round of the standardization process. In this case, especially those schemes will be considered which are not based on structured lattices, see also [*NIST20*].

Among the alternate candidates in the NIST process, SPHINCS+ [*HB+20*] is a conservative choice as a stateless hash-based method. NIST sees SPHINCS+ as a directly available alternative should cryptanalytic advances limit confidence in the security of the finalists. Other alternate candidates include Picnic and GeMSS, where Picnic is based on symmetric primitives and zero-knowledge techniques and GeMSS is a multivariate signature scheme.

2.4 Key points

- The development of powerful quantum computers is a threat to public-key cryptography used today.
- For high-security applications BSI works under the hypothesis that cryptographically relevant quantum computers will be available in the early 2030s.
- Post-quantum cryptography offers a quantum-safe alternative to currently used public-key cryptosystems. These schemes can be implemented on conventional hardware.
- Post-quantum cryptography is currently being standardized in a process by the US National Institute of Standards and Technology. However, final standards will not be available until 2024 at the earliest.
- BSI has already made recommendations for post-quantum key agreement mechanisms in 2020. From a security perspective, the two recommended schemes are conservative choices.
- Hash-based signatures are recommended by BSI, but cannot be used for every application.

3

3 Further development of cryptographic protocols

For the future use of post-quantum cryptography, it is not sufficient to standardize cryptographic algorithms. Rather, it is also necessary to adapt cryptographic protocols to the new algorithms. This is due, for example, to the fact that in many protocols the lengths allowed for the public keys are limited and are no longer sufficient for the new algorithms. The essential point, however, is that post-quantum algorithms should generally not be used alone, but only in hybrid mode, i.e. in combination with a classical procedure. Changes in protocols and standards must be initiated and co-designed by the industry. This work is already in progress for many protocols. This chapter describes what BSI understands by a hybrid approach and reports on the current developments in IKEv2, TLS and X.509.

3.1 Hybrid approaches for key agreement and digital signatures

At present, post-quantum cryptographic schemes are generally not yet trusted to the same extent as established cryptosystems since they have not been equally well studied in terms of side-channel resistance and implementation security, for example. At the same time, however, a switch to quantum-safe schemes must be made in a timely manner. For this reason, the idea of not using post-quantum cryptography in isolation, but only in combination with established algorithms, has generally gained acceptance.

3.1.1 Key agreement

The idea of hybrid key agreement can be described as follows: One performs a "classical" key exchange and another key agreement with a quantum-safe algorithm. The obtained shared secrets are then combined in a suitable way to obtain a secret key for the encryption of the payload data. Difficulties arise if one wants to implement this idea in an existing protocol (for example, the Internet Key Exchange (IKE) protocol). Furthermore, the question arises how the derivation of the secret key from the shared secrets should be done concretely. This will be discussed in the following.

A key derivation function (KDF) is a function that is used to derive cryptographic key material from a shared secret, for example for the encryption of user data. This is used, for example, to bind key material to protocol data or to derive session keys from a master key. Such a KDF may be used in the context of a hybrid key agreement, for example, to derive a common cryptographic key from the resulting shared secrets of the individual key exchanges. If necessary, in addition to the shared secrets, a common pre-distributed key (a so-called pre-shared key) can also be accepted as input. BSI recommends a key derivation function according to [*SP800-56C*], which also takes the hybrid case into account.

BSI does not recommend combining the shared secrets using a pure XOR because it has theoretical weaknesses. For example, this construction only preserves the IND-CPA security of the key agreement algorithms [*GHP18*, Lemma 1 and 2]. The stronger IND-CCA(2) security of corresponding key agreement algorithms is generally lost.

If a QKD key (see chapter 4) is to be used in a hybrid key agreement scheme, this is currently regarded by BSI as an additional optional input; two additional inputs would then still be required.

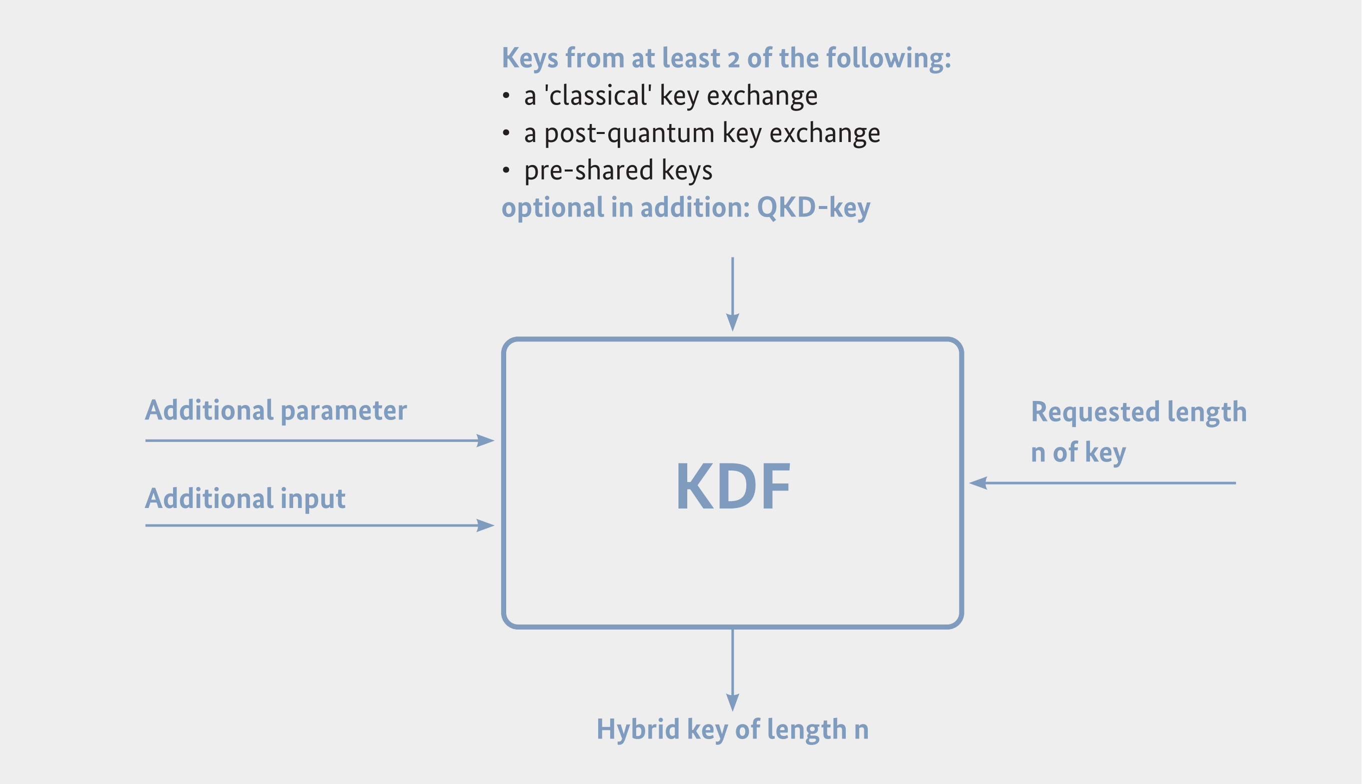

Keys from at least 2 of the following:
• a 'classical' key exchange
• a post-quantum key exchange
• pre-shared keys
optional in addition: QKD-key
Additional parameter
Additional input
KDF
Requested length n of key
Hybrid key of length n

Figure: Schematic representation of the hybrid key agreement by means of a key derivation function (KDF)

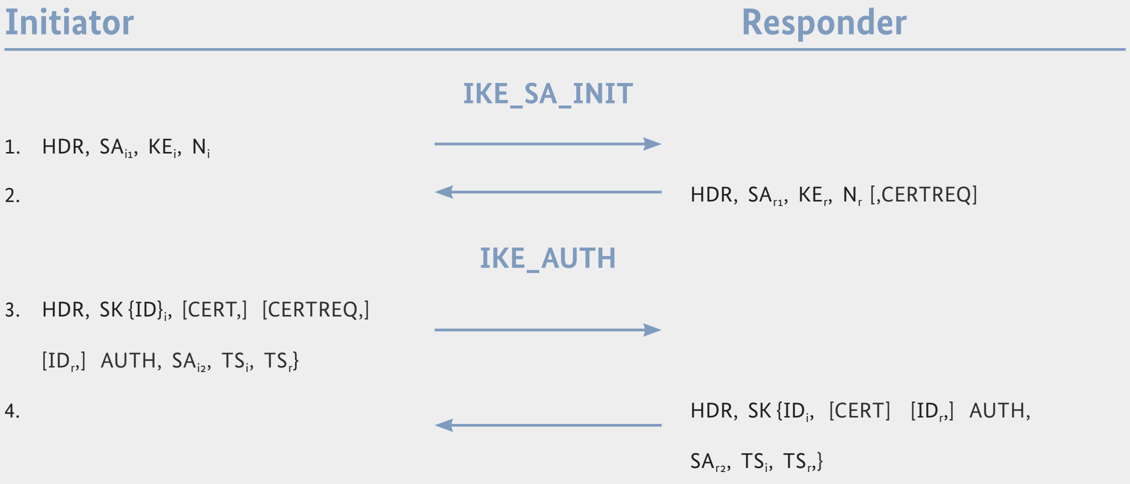
3.1.2 Hybrid signatures and adaptation of public key infrastructures

When using digital signature algorithms for message authentication and the design of public key infrastructures, one faces similar problems as with key agreement in security protocols. Here, too, using a combination of quantum-safe signature algorithms and established classical algorithms such as ECDSA in the form of "hybrid certificates" is an obvious idea. For public key infrastructures, migration paths for the introduction of quantum-safe schemes are currently being worked on as an alternative to migrating in one go at a fixed deadline or using parallel PKIs. These aspects and specifically the X.509 certificate format are discussed in more detail in Section 3.4.

3.2 Internet Key Exchange Protocol Version 2 (IKEv2)

Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) protocol is used to negotiate the key material and to authenticate the communication partners for IPsec connections. The current version is IKEv2 [*RFC 7296*]. The original version (IKEv1) is deprecated but still in use. The figure shows the sequence of a key negotiation with IKEv2.



Initiator
Responder
IKE_SA_INIT
1. HDR, SA_{i1}, KE_i, N_i
2.
HDR, SA_{r1}, KE_r, N_r [,CERTREQ]
IKE_AUTH
3. HDR, SK {ID}$_i$, [CERT,] [CERTREQ,]
[ID_r,] AUTH, SA_{i2}, TS_i, TS_r}
4.
HDR, SK {ID_i, [CERT] [ID_r,] AUTH,
SA_{r2}, TS_i, TS_r,}

In the IKE_SA_INIT messages, the Security Association Payload (SA_i or SA_r) is used to negotiate which algorithms are to be used for encryption, key agreement and authentication. More precisely, the initiator sends proposals and the responder selects one from each of these. The methods are encoded in "transform types". For the key agreement there is currently only the Transform Type "DHGroup", because only a Diffie-Hellman key exchange is provided. In the Key Exchange Payload (KE_i and KE_r) the public keys for this Diffie-Hellman key exchange are transmitted.

During the IKE_AUTH phase, the key agreement performed in the IKE_SA_INIT phase and all data exchanged up to that point are subsequently authenticated.

Key negotiation via the Internet Key Exchange (IKE) protocol is essentially based on a classical Diffie-Hellman key exchange (over finite fields (DH) or elliptic curves (ECDH)) (see info box "Internet Key Exchange"), so quantum-safe alternatives are urgently needed.

The "IP Security Maintenance and Extensions (ipsecme)" working group of the IETF is responsible for adjustments and extensions to IPsec. In the ipsecme charter there are two fields of action related to the resistance of IKEv2 against quantum computers[15]:

- "IKEv1 using shared secret authentication was partially resistant to quantum computers. IKEv2 removed this feature to make the protocol more usable. The working group will add a mode to IKEv2 or otherwise modify the shared-secret mode of IKEv2 to have similar or better quantum resistant properties to those of IKEv1."
- "Postquantum Cryptography brings new key exchange methods. Most of these methods that are known to date have much larger public keys than conventional Diffie-Hellman public keys. Directly using these methods in IKEv2 might lead to a number of problems due to the increased size of initial IKEv2 messages. The working group will analyze the possible problems and develop a solution that will make adding post-quantum key exchange methods more easy. The solution will allow post quantum key exchange to be performed in parallel with (or instead of) the existing Diffie-Hellman key exchange."

The first point refers to the fact that IKEv1 offers the possibility of using a key distributed by other means (preshared key) for authentication, which is additionally included in the derivation of the session keys for IPsec. This provides a quantum-safe mechanism for key negotiation (at least for a limited set of participants), provided that the cryptographic techniques used for key derivation provide an appropriate level of security.

[15] See https://datatracker.ietf.org/group/ipsecme/about/

With IKEv2, there is also the possibility to authenticate via a pre-distributed key, but this key does not enter into the key derivation. Thus, in this case, the session keys for IPsec are only based on the asymmetric (EC)DH secret and are thus not quantum-secure. To change this, an Internet Draft for a Request for Comments (RFC) was published back in September 2015 by Scott Fluhrer et al. to enable the use of pre-distributed keys for key derivation in IKEv2. This Internet Draft was adopted by ipsecme in October 2017 and has since been published as RFC 8784 [*RFC 8784*]. It should be noted that in this solution, the pre-shared key is included in the authentication keys and the key for further key derivation, but not in the keys with which the IKE messages are encrypted and protected against manipulation. This means that authentication and the IPsec connection are quantum-safe, but not the IKE connection as long as it is not renewed by rekeying.

The use of preshared keys is a transitional solution that can only be implemented with a small group of participants due to the complex key management. The Internet draft [*TT+21*] offers a proposal for a more promising solution. It proposes an approach for hybrid key agreement that is very flexible. This uses a so-called intermediate exchange, which is described in the Internet Draft [*Smy21*]. Here, another pair of messages (IKE_INTERMEDIATE) is exchanged between IKE_SA_INIT and IKE_AUTH (see info "Internet Key Exchange (IKE)"). In [*TT+21*], seven new transform types are defined that can be included in the initial message. Each of these transform types contains a list of supported (quantum-safe) key agreement algorithms. Thus, up to seven additional key negotiations can be performed. However, each of these key negotiations requires an additional Intermediate Exchange. In addition, Transform Type 4, which was previously used for negotiating the group used for the Diffie-Hellman key exchange (and is consequently named Diffie_Hellman_Group), is renamed KE_Method (KE = Key Exchange). The list for selecting the possible methods that can be negotiated via Transform Type 4 is the same as the list from which the methods for the other key exchanges are selected. This means that a classical Diffie-Hellman exchange does not necessarily have to be carried out for the initial key agreement, but a quantum-safe method can already be selected.

One potential problem here is that the public keys of some algorithms are considerably larger than those used previously and do not fit into the key exchange payload of the initial IKE message (IKE_SA_INIT). In addition, IKEv2 does not provide a way to fragment these initial messages. This can lead to fragmentation at the IP level during the (usual) transport via UDP and thus to the loss of individual packets at some network nodes and consequently to the failure of the negotiation of the security association. Transmission of large keys is possible via the IKE-intermediate messages, since there is an IKE-specific mechanism for fragmentation of these, see [*RFC 7383*]. Here too, however, the size of the keys is limited by the size of an IKE Encrypted_Payload.

Another potential protocol change that would enable the use of large public keys is the adjustment of the maximum IKEv2 payload size from the current 64 KB. This limitation goes back to the specification to encode the length of a payload in a field of size 2 bytes. Various approaches are currently being discussed as to how large messages can be transported in IKEv2 messages despite this length limitation [*THS21*].

3.3 Transport Layer Security (TLS)

Transport Layer Security (TLS)

The Transport Layer Security (TLS) protocol is used for the secure transmission of data on the Internet, the latest version is 1.3 [*RFC 8446*]. In a so-called TLS handshake, the required keys are negotiated and the communication partners are mutually authenticated.

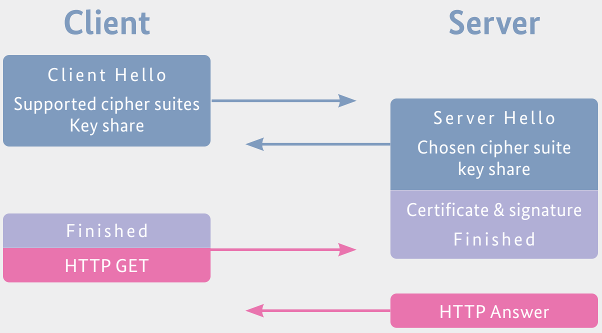


Figure: Rough procedure of a handshake in TLS 1.3

Up to now, "classical" methods such as RSA or (EC)DH have been used for key negotiation in the TLS handshake.

Back in 2016, Google conducted an experiment in which the "New Hope" algorithm was implemented on a test basis in the Chrome browser for key negotiation for TLS 1.2 connections[16]. This experiment has continued over the last few years: In mid-2018, A. Langley and M. Braithwaite of Google investigated the extent to which key negotiation algorithms submitted to NIST can be integrated into a TLS 1.3 handshake[17]. A key point here is that in TLS 1.3 (unlike TLS 1.2), a client Hello includes not only the supported cipher suites, but also public keys matching the cipher suites. This can lead to a huge overhead for some of the post-quantum schemes submitted to NIST, which is why schemes with too large a public key (for example, code-based schemes) were not considered in the project. Experiments based on structured lattices (HRSS-NTRU [*HR+17*]) and isogenies (SIKE, [*JAC+20*]) continued in 2018[18] and were completed in 2019[19]. HRSS-NTRU and SIKE were each used with ECDHE in a hybrid key agreement. The final summary spoke out in favour of structured lattices. The results were presented at a workshop of the NIST Post-Quantum Cryptography standardization process [*KSL+19*].

In April 2020, the IETF TLS Working Group published a draft RFC [*SFG21*] proposing a solution for hybrid key agreement in TLS 1.3, with the intention to submit it for final approval by the Internet Engineering Steering Group (IESG)[20]. The draft is based on earlier drafts by D. Stebila (University of Waterloo), S. Fluhrer (Cisco Systems), and S. Gueron (Amazon Web Services), and essentially proposes to register new Object Identifiers (OIDs) for combinations of one classical and one post-quantum scheme each, and to negotiate them via the "supported_groups" extension in the handshake [*SFG21, 3.1 Negotiation*]. However, for each combination that the client offers, it should also already send the corresponding public keys in its Client Hello message. This approach leads on the one hand to a large number of required new OIDs and on the other hand to very large Client Hello messages.

In the context of TLS and post-quantum cryptography, and in particular of hybrid key agreement, many other considerations and concrete efficiency measurements or benchmarks have been made [*CPS19*], [*PST20*], [*PDT20*], [*SKD20*], so that some experience in this is already available.

[16] See https://www.imperialviolet.org/2016/11/28/cecpq1.html
[17] See Siehe https://www.imperialviolet.org/2018/04/11/pqconftls.html
[18] See e https://www.imperialviolet.org/2018/12/12/cecpq2.html
[19] See https://www.imperialviolet.org/2019/10/30/pqsivssl.html
[20] See https://datatracker.ietf.org/wg/tls/history/

3.4 X.509 certificates

Digital certificates

In digital communication, certificates are used to authenticate and verify public keys. These certificates bind the public key to the identity of its owner within a public key infrastructure. The essential function of a certificate is to make the public key of an owner verifiable as authentic and belonging to the owner. This is achieved by establishing a cryptographic link to a trust anchor via the so-called certification path. To establish this connection, each issued certificate in the path can be verified with the public key of the preceding one by a cryptographic signature. Furthermore, important information is included in each certificate; this can include, for example, references to the owner or information that restricts the intended use or validity of the certificate. Since the associated fields are also included in the calculation of the certificate's cryptographic signature generated by the issuer, these values are also trusted as part of the certificate verification.

The most common standard for the format of certificates is the X.509 standard of the standardization sector (ITU-T) of the International Telecommunication Union (ITU). Since version 3 [*X.509*], this standard provides for the possibility of certificate extensions, which, for example, restrict the intended use of the key. The data formats for certificates and their processing are specified in RFC 5280. There, steps for the validity check of a certificate, the so-called certification path validation, are described in detail.

BSI has developed a Certification Path Validation Test Tool (CPT) to test implementations of certification path validation in libraries and applications.

The tool is available at *https://bsi.bund.de/CPT*. Requirements for certificates and certification path validation have also been compiled in Technical Guideline TR-02103 [*TR-02103*].

In October 2019, ITU-T published an update of the X.509v3 standard [*X.509*]. For the first time, this document addresses the problem that new signature schemes must be introduced into certificates or public key infrastructures without a migration at a fixed deadline. The ITU-T concludes: *"it is unlikely that it is possible to change cryptographic algorithms simultaneously for all entities within a PKI"*. To enable migration from old to new schemes, certificate extensions (*subjectAltPublicKeyInfo, altSignatureAlgorithm* and *altSignatureValue*) are specified so that an X.509 certificate can contain an "alternative" public key [*X.509, §7.22*]. Among the certificate creation and validation rules described in this context, as well as the implications for CRLs and AVLs, three aspects stand out. Firstly, for compatibility reasons, it is recommended to mark the new certificate extensions as "non-critical" [*X.509, §9.8.2., §9.8.3*], so that applications that are not aware of the new extensions can also check the validity of corresponding certificates. Secondly, the described approach does not represent a "hybrid solution". If the alternative values for key, algorithm and signature are available, only these should be used or checked. Thirdly, the adaptations in the certificate structure are only intended as a transitional solution until the migration process to quantum-safe signature schemes is completed. In this regard, the ITU writes: *"After the migration period, it is expected that new public-key certificates be issued without these extensions and with the new set of cryptographic algorithms and the digital signature in the base part of the public-key certificate."* [*X.509, §7.22*].

In addition to the described changes to the certificate structure, there are initial attempts to define quantum-safe signature schemes within the X.509 standard. Especially for the already standardized hash-based signature procedures LMS and XMSS, there was an advance here in the form of an IETF Internet Draft [*vGF19*], which however expired in September 2019. In BSI's view, these signature schemes are most suitable for the design of long-lived root certificates and less suitable for end-user certificates due to them being stateful. This view is also expressed in the aforementioned RFC. Hash-based signature schemes can thus serve to build a *mixed PKI*. A mixed PKI is understood to mean that different signature schemes are used in the end-user certificates than in the root certificates.

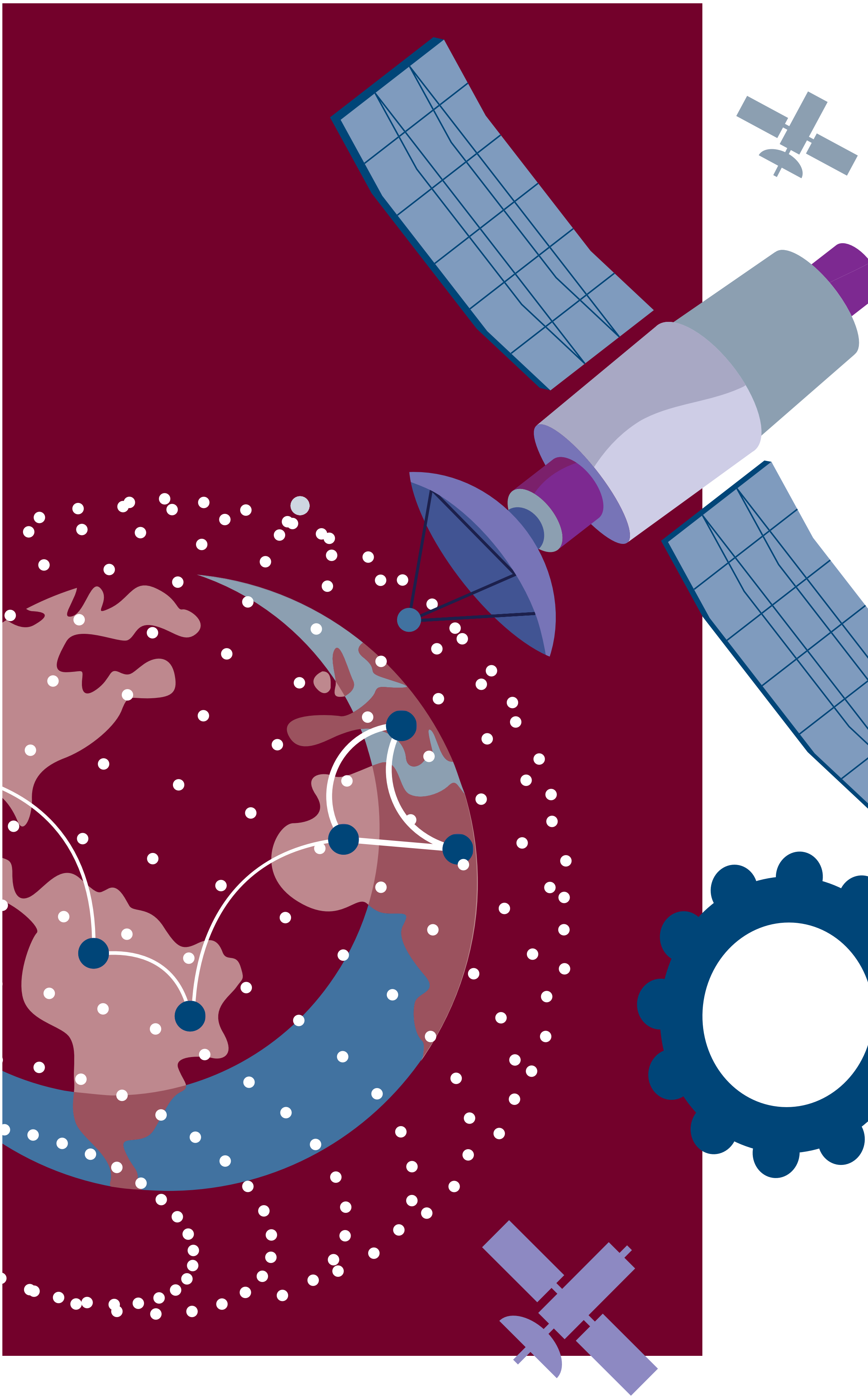
The IETF working group "Limited Additional Mechanisms for PKIX and SMIME (lamps)" has written several aspects into its agenda regarding the migration to post-quantum cryptography[21]. On the one hand, lamps wants to specify the procedures standardised by NIST for use within the Internet profile of X.509 certificates (PKIX) (see [RFC 5280]) and within the Cryptographic Message Syntax (CMS). On the other hand, formats, identifiers, etc. for hybrid solutions for key agreement and for digital signatures ("dual signature") are to be specified. There are already first drafts for RFCs, for example [*OGM21*], [*OP21a*], [*OP21b*]. Further details on the discussions of lamps regarding post-quantum cryptography can be found at *https://datatracker.ietf.org/meeting/111/proceedings* in the meeting minutes of the working group.

3.5 Key points

- Protocols and standard formats must support post-quantum schemes and, in particular, hybrid solutions.
- The changes must be initiated and shaped by the industry. The work on this has already been initiated for many protocols.
- Especially for the migration of public key infrastructures there are still many open questions.
- Hash-based signatures can be a solution for root certificates.

[21] See https://datatracker.ietf.org/group/lamps/about/

4



4 Quantum Key Distribution

Post-quantum cryptography develops classical algorithms for encryption, authentication and key exchange that are intended to be resistant to attacks by quantum computers. In contrast, quantum cryptography uses quantum physical effects to construct quantum-safe cryptographic schemes. In contrast to post-quantum cryptography, this usually requires specialized hardware to generate quantum states for example. Moreover, the security of quantum cryptographic schemes is usually attributed to quantum physical principles and not to assumptions on the complexity of certain mathematical problems.

Currently, the most widespread and practical technology within quantum cryptography is Quantum Key Distribution (QKD). QKD is often discussed as an alternative or complement to post-quantum key agreement schemes. It should be noted that QKD has special security properties and limitations. The race to deploy quantum cryptography was initiated in 2016 with the launch of a Chinese satellite that uses QKD to generate keys for secure communication. A fiber-based QKD network between Beijing and Shanghai has also now been implemented [*Chen+21*]. Numerous other QKD networks - also in Europe - are currently under development. After a brief explanation of how QKD works, in the following we will take a closer look at some important security aspects and limitations of QKD, discuss certification and standardization activities, and conclude with an assessment of the possible use of QKD.

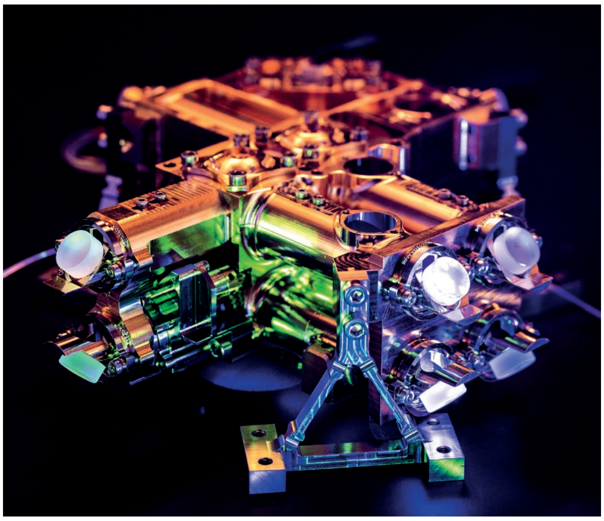


Figure: Photon source developed by Fraunhofer IOF for the generation of entangled photon pairs

Source: ©Fraunhofer IOF

4.1 QKD protocols

In a QKD protocol, two parties, usually called Alice and Bob, want to agree on a secret key over an open channel. An attacker who can listen in on and manipulate the communication between Alice and Bob should not be able to gain knowledge of the agreed key. In contrast to classical key agreement methods, Alice and Bob exchange quantum states in addition to classical information in QKD protocols. Moreover, the security of QKD protocols is not supposed to be based on the complexity of mathematical problems, as is the case with currently used schemes, but ultimately on quantum mechanical principles. In the following, the basic principles of how QKD works will be described.

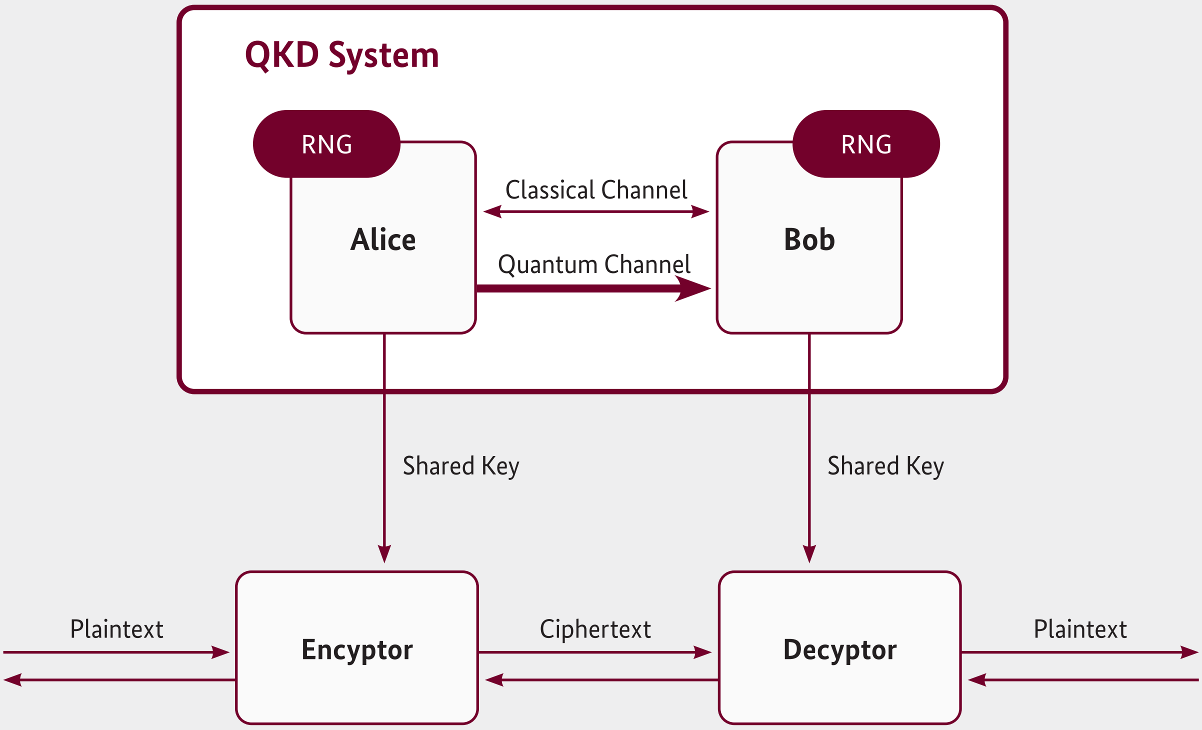


Figure: Systematic representation of a Prepare-and-Measure QKD system.

A QKD system consists of one QKD device with random number generator at Alice's end and one at Bob's end, as well as a classical channel and a quantum channel through which the QKD devices are connected to each other. The QKD devices hand over the shared key to each of the users after the QKD protocol has been successfully executed. It can be used, for example, to encrypt messages.

As a prerequisite for a QKD protocol, Alice and Bob must be connected at least via a classical channel and via a quantum channel. The latter is usually an optical channel over which photons are exchanged. Quantum states can be realized, for example, by the polarization of photons. Moreover, even before performing the QKD protocol, Alice and Bob must be in possession of a shared secret key for authenticating the classical channel, which they exchange beforehand by other means. This is why QKD is sometimes referred to as "quantum key growing", since, strictly speaking, QKD protocols use an existing shared key to agree on a longer key. In addition, many protocols require reliable random number generators.

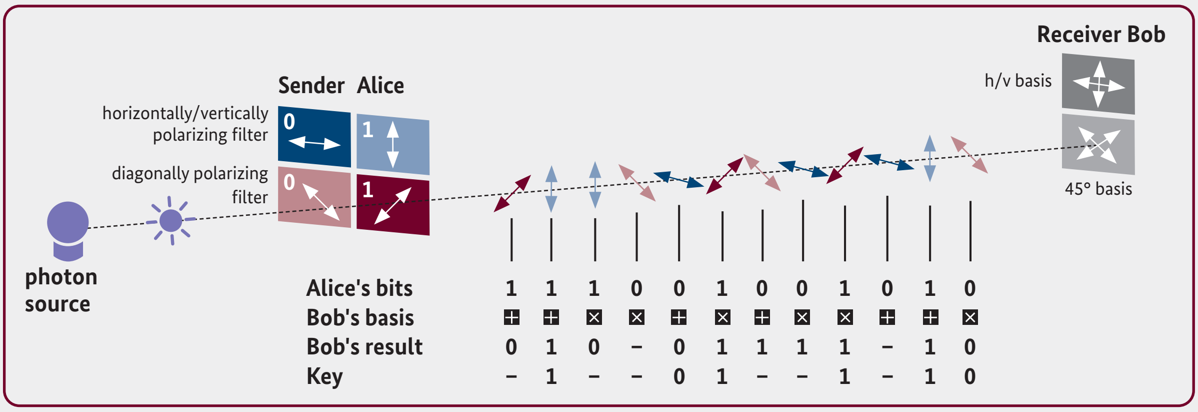
There are a large number of concrete QKD protocols with different theoretical security guarantees and practical requirements, which cannot be presented in detail here. One important class of protocols are the prepare-and-measure protocols. Here, Alice encodes a random sequence of bits in quantum states and sends them to Bob, who makes a measurement on these states. After that, Alice and Bob have correlated bit sequences. Using classical post-processing, which requires authenticated communication over the classical channel, they extract from it a common shorter bit sequence that forms the key. The communication over the classical channel is public, but must be authenticated to prevent a simple man-in-the-middle attack.

BB84

The first QKD protocol was proposed by Bennett and Brassard in 1984 and is now known as BB84 [*BB84*]. It is a prepare-and-measure protocol in which Alice sends polarized photons to Bob to generate a shared key.

The BB84 protocol proceeds as follows: First, Alice generates random bits and encodes them as photons polarized either horizontally, vertically, right diagonally, or left diagonally. These photons are transmitted to Bob via an optical channel, but the information about the polarization is initially kept secret. For each incoming photon, Bob must randomly decide whether to measure it in either the horizontal-vertical basis or the right-diagonal-left-diagonal basis. In practice, this is often accomplished by a beam splitter. For each photon measured by Bob in the same basis in which Alice sent it, Bob learns the correct polarization of the photon by his measurement. If Bob has chosen the other basis, he gets a random measurement result. Now Alice and Bob publish the bases they chose for each photon over the classical communication channel. The information about the photons for which they did not use the same basis is discarded. From the polarizations of the other photons, Alice and Bob derive a bit string b and b' respectively.

Suppose an attacker Eve tries to intercept information about the photons Alice sends to Bob in the optical channel without being noticed. Due to the no-cloning theorem (see info box "The No-Cloning Theorem"), Eve cannot copy the photons because non-orthogonal states are used to encode the bits. It follows from the laws of quantum mechanics that any kind of interaction with quantum states by which information about them can be obtained will, on average, cause a change in the quantum states. In the process, the polarizations of some photons are distorted. Of course, such errors can also occur due to noise in the channel. Due to the errors introduced, probably some of Bob's measurements of the photons are now giving false results. To detect this, Alice and Bob publish a portion of their measurement results and compare the polarizations. If they determine that too many of the photons were corrupted, Eve may have learned too much information about the states of the photons and the protocol is aborted. Otherwise, they begin classical post-processing. In this process, a common bit string is first generated from the two bit strings b and b', for which error correction is used to ensure that it is identical for Alice and Bob with as high of a probability as possible. Then, in the so-called privacy amplification, a shorter bit string is derived from this bit string, about which Eve's information is negligible. This can now be used as a key by Alice and Bob.


Receiver Bob
h/v basis
45° basis
Sender Alice
horizontally/vertically polarizing filter
diagonally polarizing filter
0
1
0
1
photon source

Alice's bits	1	1	1	0	0	1	0	0	1	0	1	0
Bob's basis	⊞	⊞	⊠	⊠	⊞	⊠	⊞	⊠	⊠	⊞	⊞	⊠
Bob's result	0	1	0	–	0	1	1	1	1	–	1	0
Key	–	1	–	–	0	1	–	–	1	–	1	0

Figure: Principle of the BB84 protocol

The best-known prepare-and-measure protocol is the BB84 protocol [*BB84*] (see info box "BB84"). In addition to prepare-and-measure protocols, there are also entanglement-based protocols, in which correlated bit strings are produced by entangled quantum states. Entanglement-based protocols are discussed especially in the context of satellite-based QKD. The best known such protocol is the E91 protocol developed by Ekert [*E91*].

4.2 Security of QKD protocols

There are numerous ways to attack such a QKD protocol. The simplest conceivable attack is a receive-and-resend approach. In a prepare-and-measure protocol, an attacker intercepts the quantum states, makes measurements on them to retrieve information, and then sends the quantum states on to Bob. However, the security of the protocol relies on the fact that, according to the principles of quantum mechanics, quantum states would generally be altered by a measurement, which would be noticed by Alice and Bob in a statistical error estimate. Similarly, according to the no-cloning principle of quantum mechanics, general quantum states cannot be copied perfectly, so an attacker would not be able to simply duplicate the transmitted quantum states in general without changing the original states.

4.2.1 Security definitions and proofs

The security of QKD, at least against a receive-and-resend attack, is thus based on the fact that interaction with the quantum channel results in a change of quantum states and can be detected by Alice and Bob. However, an attacker has many other options. For example, even if perfect cloning of general quantum states is not possible, at least approximate copies can be made (see info box "The No-Cloning Theorem"). In order to consider and exclude all paths of attack and also to make quantitative statements about the security guarantees of the agreed key, it is therefore essential to find a suitable precise security definition and to prove the security of concrete protocols.

Initially, the research community considered "accessible information" as a security criterion. This criterion requires that the probability is very low that Alice and Bob agree on a key about which an attacker can gain more than a negligible amount of information. The first security proofs use this notion of security (for example, [*SP00*]). However, it was later found that the criterion based on accessible information does not provide sufficient security guarantees [*KR+07*]. Therefore, the "trace distance" criterion (see info box "The trace distance criterion") was subsequently proposed as a new security criterion, which has been widely adopted in QKD research. Some operational interpretations of this criterion have been criticized [*Yuen16*]. A useful operational interpretation of the security criterion is important to be able to set an appropriate value of the safety parameter for a desired security level. Current work on security proofs relies mainly on the trace distance criterion. It would be desirable to develop a complete security proof for a practically used protocol that takes into account the most general attack model and real-world circumstances such as finite key lengths.

The trace distance criterion

After the successful execution of a QKD protocol in which an attacker Eve has interacted with the quantum states, there is a shared state consisting of the state ρ_S of the generated key and the state ρ_E of Eve, which are entangled with each other.

In comparison, we consider another fictitious protocol: First, the same QKD protocol as before is performed, and subsequently the generated key is replaced by a new key independent of it and equally distributed described by a quantum state $\rho_{S'}$. This can be considered an 'ideal protocol' since Eve has no more knowledge about the state of the key. The trace distance criterion now roughly requires that for any possible attack strategy, the QKD protocol aborts with high probability or the distance between the shared states of the QKD protocol and the ideal protocol, i.e. ρ_{SE} and $\rho_{S'E}$ in the 'trace norm' is bounded from above by a small security parameter ε. The choice of the size of the security parameter ε depends on the desired level of security. See, for example, [*PR21*] for more details on QKD security criteria.

4.2.2 Information-theoretic security

The advantage of QKD over classical methods and post-quantum cryptography is often cited as the fact that QKD provides information-theoretic security, whereas the security of classical key agreement schemes is based on the fact that certain mathematical problems cannot be solved in realistic time.

Even if satisfactory security proofs for practical protocols are available, however, the intended use of the keys must also be considered. For example, if they are to be used for encryption, an information-theoretically secure algorithm such as the one-time pad would also have to be used to maintain information-theoretic security. However, this is not conceivable for most practical applications as the key rates of practical QKD systems are currently too low. Regardless of practicality, the one-time pad introduces other problems. Since using the same key twice compromises its security completely, it is necessary to ensure that each key is used only once. This makes key management more complicated. Furthermore, the one-time pad alone does not provide integrity protection. However, without using an additional authentication method, it is easy to selectively manipulate individual bits of a message encrypted with One-Time-Pad without needing to know the secret key. Moreover, even little partial knowledge of the key used can be highly problematic with the one-time pad. For example, if individual bits of the key are known, the corresponding bits of the plaintext can be reconstructed from a message encrypted with the one-time pad, which is not as easy to do with AES-encrypted messages, for example.

For these reasons, BSI rejects the sole use of the one-time pad and recommends the use of keys agreed via QKD with a recommended symmetric encryption algorithm (see [*TR-02102-1*]). Hybrid solutions are conceivable, however, in which messages are first encrypted with a recommended symmetric procedure and then additionally with the one-time pad. In any case, symmetric encryption methods that provide computational security must be used. Independently of this, it must be ensured that the components used for encryption are trustworthy. Components from untrusted sources could allow unauthorized information leakage.

4.2.3 Side-channel attacks

Even if a system like QKD is theoretically secure, a secure practical implementation must also be ensured. Side-channel attacks target weaknesses in the implementation of cryptographic systems. Even in practical QKD systems, numerous side-channel attacks have been demonstrated over the years and intensive research is still being conducted in this area [*SM+17*]. In a QKD device, due to its high technical complexity, it is imperative to prevent all known side-channel attacks, to advance research on yet unknown side-channels, and to thoroughly investigate the devices for their resistance to known side-channels.

Photon Number Splitting and Trojan-Horse

If one wants to carry out a prepare-and-measure protocol with so-called discrete variables, such as the BB84 protocol (see info box “BB84”), one actually needs an efficient photon source for this, which only sends individual photons at a time. In practice, however, this is hard to realize. Most practical photon sources therefore always send several photons having the same quantum state at once with a certain probability. Such quantum states can be realized, for example, by the polarization of the photons. In the case of photon sources, a compromise must always be made between the probability that more than one photon is sent and the probability that a photon is sent at all. In the simplest form of the photon number splitting attack, it is precisely this weakness of photon sources that is exploited. If Alice's source sends multiple photons at once, an attacker Eve will split off a photon from it and keep it in quantum storage. After Alice and Bob announce their chosen bases over the classical information channel, Eve can measure her photon in the correct basis and knows the polarization without having disturbed the polarization of the other photons. If the photon source does not send multiple photons, Eve will block the quantum channel. Assuming Eve can store the quantum states, she can thus gain full knowledge of the photons shared between Alice and Bob. This attack can obviously be prevented by using a photon source that actually sends only one photon at a time. However, it can also be detected using improved protocols. In one variant, the photon source sometimes emits so-called decoy states instead of the so-called signal states, in which it is less likely that more than one photon is sent, but even more likely that no photon is sent at all. If an attacker applies the Photon Number Splitting Attack described above to all photons, this can now be determined by statistical methods. For this, it is important that an attacker cannot distinguish the signal states and decoy states from each other.

One attack relevant in current research is the Trojan-Horse Attack [*SM+17*]. Here, an attacker sends a strong light pulse via the quantum channel into a device of the QKD system. Part of the light is reflected back to the attacker. Interaction of the light with the optical components of the QKD device changes the properties of the reflected light. For example, under favourable circumstances, light reflected from a polarizing filter is polarized perpendicular to the filter. Thus, by analysing the reflected light, an attacker can examine the configuration of some components of the QKD system from the quantum channel. As countermeasures against the Trojan-Horse Attack, for example, optical isolators or spectral filters are built into QKD devices. However, privacy amplification (see info box “BB84”) also plays a major role in minimizing the information that an attacker obtains from the Trojan-Horse Attack.

4.2.4 Authentication

The messages sent via the classic channel of the QKD system must be authenticated to prevent a simple man-in-the-middle attack (see info box "Digital Signatures"). A classical authentication mechanism is required for this.

One possible option for this is Wegman-Carter authentication [*WC81*] (see info box "MACs and Wegman-Carter authentication"), which provides information-theoretic security and is therefore often favoured in the context of QKD. In principle, this method is mathematically well understood in its own right. However, there is a lack of suitable standards and a better delimitation of the possible variants of the procedure and the parameters. In addition, the use of Wegman-Carter authentication in QKD systems raises further questions, for example, with regard to how the security of the overall QKD system and the security of the authentication influence each other. For example, in many practical QKD implementations, part of the key agreed upon via a QKD protocol is used for authentication in a later round. Indeed, in the Wegman-Carter protocol, each key may be used to authenticate at most one message. Since a small amount of information about the QKD key always leaks out, the security level of the system decreases with the number of protocol passes performed [*PR14*]. Thus, after a certain period of time, the authentication key must be reinitialized with a random key generated outside the system. For an adequate security analysis, Wegman-Carter authentication or other possible authentication methods can thus not be considered in isolation from the rest of the QKD system.

In addition to the use of Wegman-Carter authentication, other authentication methods such as post-quantum signature schemes using a public key infrastructure are also being discussed. This simplifies the initial key distribution problem considerably, since secret symmetric keys no longer have to be distributed for all communication partners. On the other hand, the security of the overall system against man-in-the-middle attacks is thus ultimately based on the security of post-quantum algorithms. The extent to which key agreement via QKD then offers a security gain compared to pure post-quantum methods for key agreement must always be considered in the specific case.

MACs and Wegman-Carter authentication

Some of the main security objectives of secure communication are authenticity and integrity. This means being able to trace the origin of data and to detect changes to it. In addition to digital signatures (see info box "Digital Signatures"), which are public key schemes and which can also achieve non-repudiation as an objective in addition to authenticity and integrity, there are also symmetric schemes for data authentication with Message Authentication Codes (MACs). For the use of MACs, both communication partners must be in possession of common secret keys in advance. If the sender now wants to send a message, he calculates a key-dependent checksum using the selected scheme, which is sent along with the message.

Wegman-Carter authentication is an example of a MAC that is often considered in the context of QKD and was first described by Wegman and Carter in [*WC81*] in 1981. Here, each key **k** determines a function $\mathbf{h_k}$, which is applied to a message **m** to be authenticated and yields a short checksum $\mathbf{t=h_k (m)}$. In Wegman-Carter authentication, the set of all functions $\mathbf{h_k}$ for all possible keys **k** is a so-called strongly two-universal family of hash functions. Such a family has the property that even if a message-checksum pair **m || t** is known, for every other message **m'**, every checksum is (at least approximately) equally likely as long as the key **k** is not known. It follows that even if a valid key-dependent checksum for a given message is known, an attacker has no better attack option than to randomly guess the checksum for a modified message in order to forge it. It is imperative to note, however, that each key **k** may only be used to authenticate a single message. A new key must be used for each additional message. In practice, slight variations of this procedure are often used, where only a part of the key has to be renewed in each round.

Wegman-Carter authentication is constructed as an information-theoretically secure method, which means that its security does not require any assumptions about the limitation of an attacker's computational power. In exchange, Wegman-Carter authentication is much more inefficient in terms of key consumption compared to MACs widely used today, such as HMAC [*RFC 2104*], CMAC [*SP800-38B*], and GMAC [*SP800-38D*].

4.2.5 Random number generators

An essential part of QKD protocols is that random numbers with high quality must be available. The use of quantum random number generators (QRNGs) is often proposed in this context. BSI, in cooperation with Fraunhofer IOF, has organized two workshops to evaluate QRNGs. QRNGs are a special type of physical random number generators. A priori, QRNGs are not superior to conventional physical random number generators. Certainly false are general statements of the type "QRNGs provide random numbers based on natural laws and are therefore automatically secure". It cannot be assumed that ideal random number generators exist in the real world, i.e. that devices can extract digitized sequences of independent and equally distributed bits from a physical phenomenon in the strict mathematical sense. And even if ideal random number generators did exist, this could not be demonstrated. At best, when evaluating a real random number generator, one can show that it behaves "almost" like an ideal random number generator in some sense. In BSI's methodology for the evaluation and certification of random number generators (AIS 20/31), suitable QRNGs can be assigned to functionality class PTG.2 or (with appropriate cryptographic post-processing) to functionality class PTG.3. To date, there is no certified QRNG with a certificate accepted in Germany.

In principle, BSI recommends the use of hybrid random number generators with cryptographic post-processing which, in addition to the information-theoretic security of the physical entropy source, also provide complexity-theoretic security (computational security). This aspect is of particular importance if the random numbers are used for schemes such as the one-time pad (cf. Section 4.2.2), where even minor statistical defects in the keys have a negative impact on the security properties.

4.3 Limitations and opportunities of quantum cryptography

In addition to security aspects such as theoretical security and side-channel resistance, there are also practical limitations of quantum cryptography that make this technology difficult to use. Some of these are presented in this section, and future opportunities for quantum cryptography are also discussed.

4.3.1 Pre-distributed keys

For the authentication of the classical channel, a secret shared key must already be present at both ends wishing to communicate with each other before the start of a QKD protocol. Consequently, secret keys must be distributed between all pairs of QKD devices that wish to communicate with each other before use. This significantly limits the scalability of QKD networks, or at least makes them more costly. The pre-distributed key is used for the initial authentication of the classical channel, after which a part of the agreed QKD key is to be used for this purpose. Since no QKD key is perfectly equally distributed and a certain amount of information always leaks out (the exact amount is quantified by the security parameter), it becomes necessary after a certain lifetime to distribute a new shared secret key from the outside to both communicating parties if the QKD protocol is to continue to operate securely.

4.3.2 Limited range

Signal losses in optical fibers grow exponentially as a function of distance. Therefore, it is currently not possible to transmit a key over a distance much larger than about 100km using fiber-based QKD. According to the no-cloning theorem of quantum mechanics, there can be no signal amplifiers in the conventional sense where quantum states are copied and retransmitted. Thus, over long distances, "trusted nodes" must be introduced so that a key is agreed between neighbouring nodes at a time. Thus, end-to-end security cannot be achieved over fiber-based QKD and long distances at present. One possible solution is quantum repeaters based on quantum entanglement, which are currently the subject of intensive research. However, it is not foreseeable that market-ready quantum repeaters will be available in the near future. Another approach to guarantee end-to-end security over longer distances is satellite-based QKD, which is, however, relatively costly and raises questions about availability.

4.3.3 Costs and manufacturer

In contrast to classical methods and post-quantum cryptography, QKD also requires specialized hardware. Currently, the acquisition of this equipment represents a cost-intensive investment. Furthermore, no QKD manufacturer from the European Union has yet established itself. In [*ACATECH21*], the importance of digital sovereignty in encryption technologies is pointed out and the development of comprehensive own competences is mentioned as a necessary factor. This applies in particular to quantum communication.

4.3.4 Opportunities of QKD

Despite all the limitations of QKD, it also offers new opportunities. Even though the mathematical problems underlying the security of post-quantum cryptography are well-studied, it is not impossible that these methods can be broken in the future by algorithmic advances. Quantum cryptography presents itself as a possible backup. If QKD is operational, it may thus provide a complement to post-quantum schemes for key agreement.

In addition, the technologies developed for quantum communication can be used to allow quantum computers to interact with each other. These quantum networks can be used, for example, for distributed computing on quantum computers. Due to the increasing relevance of quantum computing alone, it makes sense to continue research into the underlying technologies of quantum cryptography. Quantum communication is an emerging new technology that should lead in several steps to larger quantum networks with the establishment of a global quantum network as a long-term goal (cf. [*VDI21*], page 20).

The idea of a so-called quantum internet is also controversially discussed (cf. [*ACATECH20*], page 58). While this idea seems feasible to optimists as early as 2035 [*QDelta*], other experts criticize the quantum internet as a term that is still undefined (cf. [*ACATECH20, page 58*]). The Quantum Internet will probably only be a supplement to the classical Internet.

4.4 Standardization and certification

The future interoperable use of quantum communication requires the standardization of many basic building blocks. This concerns the protocols used, the authentication methods used, key management, the integration of repeaters and network aspects. The standardization of QKD protocols with associated security proofs is particularly important in the context of certifications and approvals to be able to assess their security. There are activities on these tasks in various standardization bodies such as ISO, ITU, CEN, CENELEC or ETSI. The IETF has already established a working group, the Quantum Internet Research Group[22], to standardize the Quantum Internet. A report on the necessary steps comes from the US Department of Energy [*DoE20*]. Overall, however, this work is still in its infancy.

Ideally, QKD promises "security based on the laws of physics" and suitability for high-security applications. For this, however, it is not enough to know a theoretically secure protocol - with the open questions described in Section 4.3. It must also be implemented securely. An internationally recognised standard for evaluating IT security products is the Common Criteria (CC)[23]. In cooperation with ETSI ISG QKD[24], BSI has started to develop a so-called Protection Profile (PP). A PP is a kind of blueprint for Security Targets (ST) to be created later by manufacturers of QKD devices, which describe concrete products. As a first step, however, the PP only covers prepare-and-measure QKD and is limited to point-to-point connections. Both entanglement-based QKD and network aspects remain open for the time being.

The PP should correspond to the Evaluation Assurance Level EAL4+AVA_VAN.5+ALC_DVS.2, whereby a high attack potential is assumed appropriate to the area of application and the life cycle of the product is taken into account. There are certainly voices that consider a lower assurance level EAL 2 to be appropriate. This assessment is not shared by BSI, but EAL4+ is seen as a minimum requirement, because QKD represents a significant investment that should provide high security. EAL 2 does not meet this requirement.

In addition, a certification ecosystem for QKD products must be established, in which test criteria and evaluation methods - for example for side-channel attacks -are coordinated and further developed.

[22] See https://datatracker.ietf.org/rg/qirg/about/
[23] See https://www.commoncriteriaportal.org
[24] See https://www.etsi.org/committee/qkd

4.5 Assessment and recommendations

The French ANSSI has already commented on the use of QKD in a position paper [*ANSSI20*]. It mentions the limitations that have already been discussed here. Among other things, the complex and cost-intensive acquisition, the large number of demonstrated side-channel attacks against QKD devices, the limited range and the lack of end-to-end security over longer distances are considered problematic. ANSSI concludes that post-quantum cryptography provides an alternative that is simpler and cheaper to implement and is not subject to many of the limitations of QKD. Therefore, the focus should be on advancing post-quantum cryptography as quantum-safe cryptography.

The NSA also points out the technical limitations of QKD[25]. These include the need to distribute keys for authentication, the expensive acquisition of specialized hardware, and the high vulnerability to attacks on the physical implementation and to denial-of-service attacks. For these reasons, NSA is opposed to the use of QKD in National Security Systems until the aforementioned limitations are addressed.

The UK NCSC also opposes the use of QKD in government and military applications [*NCSC20*].

As discussed earlier, QKD is subject to many practical limitations. Some of these may be overcome in the future. Particularly desirable would be the development of quantum repeaters to maintain end-to-end security. However, this is not to be expected in the next few years. Furthermore, no European QKD products are currently available on the market. Even if European products are developed, they must first be evaluated according to criteria that have yet to be developed. It is true that BSI is taking first steps in this direction with the development of a Protection Profile. However, this Protection Profile is limited for the time being to Prepare-and-Measure protocols and point-to-point connections and still requires the subsequent creation of extensive accompanying documentation.

Taking into account the working hypothesis that a cryptographically relevant quantum computer will be available in the early 2030s, BSI believes that it is already urgently necessary to take appropriate measures to switch to quantum-safe schemes. This urgency alone makes the migration to post-quantum cryptography, the standardisation of which is already well advanced in the NIST process, a clear priority from BSI's point of view. Furthermore, post-quantum algorithms are much more flexible, as they can be implemented in existing infrastructure, they are more cost-effective, do not require secret pre-distributed keys and offer end-to-end security.

In contrast to classical and post-quantum schemes, QKD promises information-theoretic security. However, this requires suitable security proofs for practically used protocols and the most general attack model. From BSI's point of view, the theoretical foundations of QKD have not yet been satisfactorily worked out in this respect. In view of this and the susceptibility of implementations to side-channel attacks, assessments of QKD as "ultra-secure" or "super-secure" that are sometimes made appear inappropriate.

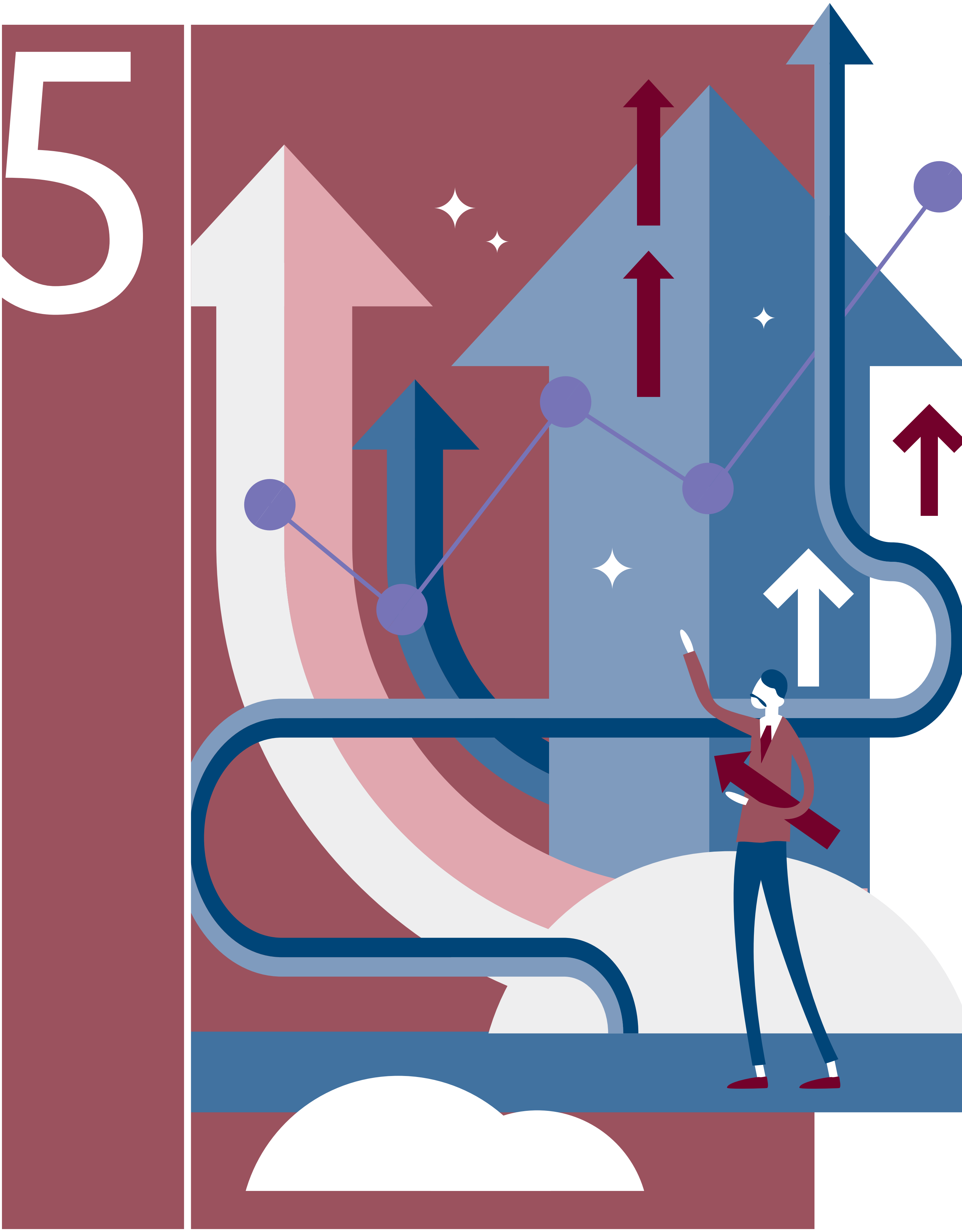
Consequently, from BSI's point of view, there are still numerous issues to be clarified and limitations to be addressed before QKD can be recommended as a security-critical technology for practical applications. However, QKD and post-quantum cryptography have the potential to complement each other, especially since they are based on different principles. The use of QKD is currently conceivable mainly in the context of experiments for restricted use cases where practical limitations are less significant, in hybrid mode as an add-on in conjunction with classical and post-quantum key agreement techniques. In addition, this can also provide end-to-end security over longer distances. Further research in quantum communication is welcome, also because there may be promising applications outside cryptography.

4.6 Key points

- QKD is feasible with technology available today and provides key agreement schemes whose security is based on quantum mechanical principles and which are expected to be information-theoretically secure at the protocol level.
- In addition to theoretical security, implementation security must also be considered.
- QKD is subject to some restrictions and is therefore only suitable for certain application scenarios.

[25] See https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

- Standards, for example on protocols, and certified products are still lacking.
- QKD should only be used in hybrid mode with classical and post-quantum key agreement schemes.
- Using the one-time pad alone for encryption is not recommended.


5

5 Developments in politics, research and industry

Quantum technologies are still in their infancy, but it is now undisputed that they have enormous economic potential and will also influence information security to a great extent. Quantum sensor technology, quantum communication and quantum computers are increasingly becoming the focus of successful long-term economic development in Germany and Europe.

In recent years, major international programmes have been launched to promote quantum technologies. Some German and European initiatives are described here, which go far beyond individual measures and focus on innovative research with a subsequent implementation of these research results in marketable products and services.

5.1 Framework programs of the German Federal Government

The Federal Ministry of Education and Research (BMBF) has declared its intention to promote the development of long-term secure cryptography and its efficient implementation in applications as part of the Federal Government's research framework programme on IT security "Self-determined and secure in the digital world 2015-2020" [*BMBF15*]. To this end, a guideline for funding research projects on the topic of "post-quantum cryptography" was published in August 2018[26]. Within this framework, a total of seven projects is funded in the period 2019-2022 to integrate post-quantum cryptography into applications (Aquorypt), public key infrastructures (FLOQI), the Botan crypto library (KBLS), medical data processing (PQC4MED), embedded systems (Quantum-RISC), networks (QuaSiModO) and critical infrastructures (SIKRIN-KRYPTOV)[27]. The total volume across all these projects is 24.2 million euros, with the BMBF's funding share amounting to approximately 16.1 million euros.

Under the leadership of the BMBF, the Federal Government's Research Framework Programme "Quantum technologies - from basic research to market" [*BMBF18*] will provide federal funding of €650 million for the development of quantum technologies in Germany between 2018 and 2022. The focus here is on funding application-oriented research work with the prospect of commercial exploitation of the research results. The funded projects cover a broad spectrum of quantum technologies and are oriented towards the focus areas of "quantum computers and simulation", "quantum communication", "quantum-based measurement technology", "basic technologies for quantum systems" and "outreach". In the latter priority, the "Quantum Futur Programme" is dedicated to the promotion of young scientists. A detailed overview of the individual funding projects can be found on the Framework Programme website[28]. Since many of these projects are directly or indirectly related to IT security, BSI is assigned a number of tasks in the framework programme [*BMBF18, §5.7*].

In the above-mentioned framework programme "Quantum technologies - from basic research to market", a potential continuation has already been considered [*BMBF18, §4*]. To this end, an agenda process initiated in 2020 took place under the title "Quantum Systems". The aim of this process was to develop an agenda supported by the specialist community, which sets out the BMBF's strategy for the further development of this area in Germany over the next few years and from which concrete measures can subsequently be derived in the form of a new funding programme. To this end, workshops were held on individual topics such as "Quantum Communication" and "Quantum Technologies - Education, Training, Outreach and Cooperation & Networks", in which BSI participated. Other focus points of the agenda process were "Quantum Computing and Simulation", "Quantum Measurement and Sensor Systems" and "Integrated Quantum Systems and Enabling Technologies".

[26] See https://www.bmbf.de/foerderungen/bekanntmachung-1947.html
[27] See https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/pqk
[28] See https://www.quantentechnologien.de

The final "Agenda Quantensysteme 2030" [*VDI21*] was handed over to Federal Minister Anja Karliczek in March 2021[29]. The agenda serves as a basis for the BMBF's upcoming programme on quantum systems, which will start in 2022.

5.2 Economic stimulus and future package of the German Federal Government

The federal government's stimulus and future package[30] provides a total of 2 billion euros for the development of quantum technologies and in particular for quantum computing[31], of which approximately 1.1 billion euros are allocated to the BMBF and approximately 900 million euros to the Federal Ministry for Economic Affairs and Energy (BMWi)[32].

Specifically in connection with the promotion of quantum computing, an advisory committee appointed in October 2020 has drawn up a "Roadmap Quantencomputing" on behalf of the Federal Government[33] [*VDI20*]. Motivated by this, the BMBF has initiated specific funding measures for "Quantum Computer Demonstration Assemblies"[34] and "Application Network for Quantum Computing"[35] within the funding framework of the currently running programme "Quantum technologies - from basic research to market".

The majority of the funding administered by the BMWi is concentrated on the German Aerospace Center (DLR), with the aim of developing a German quantum computer and corresponding software and applications.

5.3 EU flagship programme "Quantum Technologies"

The EU flagship programme on quantum technologies[36] started on 1 October 2018 with a total of 24 research projects. The programme is designed for 10 years and has a total volume of 1 billion euros. In the first phase from October 2018 to September 2021, it will provide a total of 152 million euros for the 24 projects[37].

The projects cover the aspects "Basic Science", "Quantum Simulations", "Quantum Sensing and Metrology", "Quantum Communications" and "Quantum Computing". These and their roadmaps are described in the "Strategic Research Agenda" [*EUQF20*], [*EC20b*]. In particular, the programme on quantum computing contains two projects for the construction of a European quantum computer.

The OpenSuperQ[38] project focuses on superconducting qubits, similar to IBM, Google, and Rigetti Computing. The goal of the project is to eventually provide a quantum computer prototype with 50-100 qubits and good operational quality at the Jülich Supercomputing Center as a platform-as-a-service. To this end, in addition to scaling up and improving the chips, the surrounding technological ecosystem is supposed to be created, including in the areas of cryogenics, electronics, and firmware. The quantum computer is supposed to be designed for applications without error correction, but will also be able to demonstrate initial error correction steps in principle. The project with a volume of approximately 10 million euros is coordinated by the Saarland University.

The project AQTION[39] uses trapped ions. The goal of the project is to realize portable and in principle commercializable hardware for quantum computers at the level of more than 50 qubits. Again, this includes the ecosystem including optics, middleware, compilation and scalable benchmarking. The goal is to try and achieve a true quantum advantage. The project, which also has a volume of about 10 million euros, is coordinated by the University of Innsbruck.

A "Midterm Report of the Quantum Technologies Flagship" [*EC20a*] on the progress of the projects over the first 18 months was published in September 2020.

5.4 EuroHPC JU

The European High Performance Computing Joint Undertaking (EuroHPC JU) pursues the goals of building a European supercomputing infrastructure and promoting research and innovation in this field[40]. Following a reorientation of the programme in September 2020, the budget for the period 2021-2033 is now 8 billion euros and includes the construction of a quantum computing and quantum simulation infrastructure to integrate into the High Performance Computing (HPC) infrastructure[41]. The intention is to construct such a state-of-the-art pilot by 2023[42].

5.5 QuNET

QuNET[43] (cf. also [*BT19/18355*]) is a national research project on quantum key distribution using various technologies with a project volume of 165 million euros until 2026, of which the BMBF is contributing 125 million euros in funding. The core institutes involved in QuNET are the Fraunhofer Institute for Applied Optics and Precision Engineering (IOF), the Fraunhofer Heinrich Hertz Institute (HHI), the Institute of Communication and Navigation of the German Aerospace Center (DLR-IKN) and the Max Planck Institute for the Science of Light (MPL). The project will develop concepts of an overall network and the necessary system architecture as well as new key technologies for quantum communication. Standardization and certification requirements of overall QKD systems will also be taken into account. Part of the QuNET-alpha subproject was the establishment of an encrypted connection between the BMBF and BSI in Bonn in August of 2021. It was designed as a hybrid scheme by combining a post-quantum scheme and QKD for key agreement.

5.6 Q.Link.X and QR.X

The range of QKD is very limited due to signal losses in optical fibers. In order to achieve longer ranges for fiber-based QKD without trusted nodes, as needed to build a national network while maintaining end-to-end security, repeaters are required. However, due to the no-cloning theorem of quantum mechanics, it is not possible to use conventional signal amplifiers. Repeaters in the sense of quantum communication therefore use more complex protocols that exploit quantum mechanical effects and quantum memories.

In the Q.Link.X project[44], which is funded by the BMBF with about 15 million euros until 2021, different approaches for quantum repeaters are being investigated practically and theoretically. They are to be demonstrated in practice in the follow-up project QR.X[45]. Numerous universities and research institutes from Germany are participating in the project.

5.7 EuroQCI

The European Quantum Communication Infrastructure (EuroQCI)[46] is an initiative that shall ultimately lead to a European quantum communication infrastructure. In 2019, Germany was one of the first signatories of the EuroQCI Declaration; in the meantime, it has been signed by all EU member states.

It states, among other things:

„The participating member states [...] [p]lan to work together to establish a cooperation framework - EuroQCI - for exploring within the next 12 months, the possibility of developing and deploying in the Union, within the next 10 years, a certified secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored ultra-securely and capable of linking critical public communication assets all over the Union."

This illustrates that EuroQCI should be designed to meet the highest security requirements and is one of the reasons for the selection of EAL4+ for the Protection Profile which is being developed by BSI in cooperation with ETSI ISG QKD[47]. The mentioned space component is developed within the project SAGA[48].

5.8 Industrial associations

The increased interest in quantum technologies is also reflected in the formation of interest groups. Examples include the German Industry Association for Quantum Security (DiVQSec) (*www.divqsec.de*), the European Quantum Industry Consortium (QUiC) (*https://qt.eu/about-quantum-flagship/the-quantum-flagship-community/quic/*) and the Quantum Technology & Application Consortium (QUTAC) (*https://www.qutac.de/*).

[29] See https://www.bmbf.de/bmbf/shareddocs/kurzmeldungen/de/uebergabe-der-agenda-quantensysteme-2030.html

[30] See https://www.bundesfinanzministerium.de/Web/EN/Issues/Public-Finances/stimulus-package-for-everyone/stimulus-package-for-everyone.html

[31] See https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/karliczek-mit-grossen-schritte-uantencomputer-made-in-germany.html

[32] See https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/05/20210511-BMWi-foerdert-Quantentechnologien-mit-878-Millionen-Euro.html

[33] See https://www.bundesregierung.de/breg-de/suche/quantencomputing-1836542

[34] See https://www.quantentechnologien.de/forschung/foerderung/quantencomputer-demonstrationsaufbauten.html

[35] See https://www.quantentechnologien.de/forschung/foerderung/anwendungsnetzwerk-fuer-das-quantencomputing.html

[36] See https://www.qt.eu

[37] See https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship and https://qt.eu/about-quantum-flagship/projects/

[38] See https://qt.eu/about-quantum-flagship/projects/opensuperq/

[39] See https://qt.eu/about-quantum-flagship/projects/aqtion/

[40] See https://digital-strategy.ec.europa.eu/en/policies/eurohpc-ju

[41] See https://ec.europa.eu/commission/presscorner/detail/de/ip_20_1592

[42] See https://digital-strategy.ec.europa.eu/en/policies/quantum

[43] See https://www.qunet-initiative.de

[44] See https://www.qlinkx.de

[45] See https://quantenrepeater.link/

[46] See https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[47] See https://www.etsi.org/committee/qkd

[48] See http://www.esa.int/Applications/Telecommunications_Integrated_Applications/European_quantum_communications_network_takes_shape

6

6 Recommendations

From BSI's point of view, the question of "if" or "when" there will be quantum computers is no longer in the foreground. Post-quantum cryptography will become the standard in the long term. Depending on the use case, it should be considered at an early stage (and continuously adapted to current developments) within the framework of moderate risk management whether and when a switch to quantum-safe schemes should be made. In the following, some measures are pointed out as to how a migration to post-quantum cryptography can already be initiated today, and general recommendations are given for a future-proof use of cryptography.

6.1 Preparation

The first step before migration is a survey of the existing situation and the development of a migration plan. This should include answering the following questions: What cryptographic algorithms or products are used in my organization? How critical is the data that is being processed and how long is its lifespan? Where is there an immediate need for action? Do the protocols used need to be adapted? Are there already solutions for this? And of course many more... Recommendations for the development of a migration plan have already been published by the European Telecommunications Standards Institute (ETSI) [*ETSI20*]. The US NIST is also currently working on recommendations[49] [*BPS21*].

6.2 Cryptographic agility

Concerning further development of applications, particular attention should be paid to making cryptographic mechanisms as flexible as possible in order to be able to react to developments, implement upcoming recommendations and standards, and possibly replace algorithms in the future that no longer guarantee the desired level of security ("cryptographic agility"). This is particularly important due to the threat posed by quantum computers, though not exclusively: classical attacks can also evolve and make encryption schemes or key lengths once considered secure obsolete. Cryptographic agility should therefore become a design criterion for new products - irrespective of the development of quantum computers.

Even if cryptographic agility is implemented, however, this does not mean that users can rely on it being available for the entire lifetime of a product, or that all the data one wants to protect will also be protected in the long term. For example, quite often software is only maintained by the manufacturer for a limited period of time. In the case of long-lived products, it is not even guaranteed that the manufacturer will still be there at the end of the product's life. With very short-lived products, on the other hand, it can be more economical to replace endangered products quickly instead of implementing cryptographic agility.

Using blockchain applications as an example, [*BSI19, §6*] argues that an exchange of cryptographic mechanisms does not automatically preserve the original security guarantees. This is especially true when encrypted data is stored publicly.

6.3 Short-term protective measures

Typically, asymmetric cryptography is required to exchange a shared secret between the communication partners, from which symmetric session keys are then derived. As a short-term protection measure against attacks with quantum computers, a pre-distributed symmetric long-term key can be used for the key derivation in addition. Similarly, it is possible to symmetrically encrypt an asymmetric key exchange using a pre-distributed secret. Of course, the problem of distributing the symmetric long-term keys must be solved in each case.

For cryptography on elliptic curves, the use of secret curve parameters offers some protection against attacks with quantum computers. It should be noted that the curve parameters can usually be computed given knowledge of three points on the curve. Thus, measures (e.g., point compression) must be taken to protect the curve parameters. In addition, it must be ensured that the curves used are cryptographically suitable. Details on this can be found in [*RFC 5639*].

[49] See https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

6.4 Key lengths for symmetric encryption

As mentioned above, symmetric encryption algorithms are much less threatened by the development of quantum computers than asymmetric methods. However, when using keys with a length of 128 bits (or less), quantum computer attacks with Grover's search algorithm cannot be completely ruled out. Especially if long-term protection of data is important, a key length of 256 bits should therefore be provided for new developments in which a symmetric encryption algorithm is to be implemented.

6.5 Hybrid solutions

The quantum-safe algorithms that are currently being standardized are not yet as well researched as the "classical" methods (for example RSA and ECC). This applies in particular to weaknesses that largely only become apparent in applications, such as typical implementation errors, possible side-channel attacks, etc. BSI therefore recommends that post-quantum cryptography should not be used in isolation if possible, but only in hybrid mode, i.e. in combination with classical algorithms, see Section 3.1. For high-security systems, BSI calls for the use of hybrid solutions. This applies in particular to key agreement procedures, but also to all post-quantum signature schemes. Provided that the limitations of stateful schemes are carefully considered, hash-based signatures can in principle also be used on its own (i.e., not in hybrid mode). In particular, stateful schemes should only be used in systems where the reuse of key material can be excluded [*RFC 8391, §1.1*], [*RFC 8554, §1.1*].

6.6 Post-quantum algorithms for key agreement

As discussed in Chapter 2, for quantum-safe key agreement, the lattice-based scheme FrodoKEM and the code-based scheme Classic McEliece are the most conservative choices among the candidates in the NIST process from BSI's perspective. Since the protection of long-term secrets may require timely action, BSI decided in late 2019 not to wait for NIST's decision and since version 2020-01 of its Technical Guideline TR-02102-1 [*TR-02102-1*] recommends the two schemes mentioned (in a hybrid solution), see Section 2.3.

6.7 Hash-based signature schemes for firmware updates

As described in Section 2.2.3, stateful hash-based signature schemes have certain disadvantages. For example, they can only be used to create a number of signatures that is limited in advance. However, they are particularly suitable for signing firmware updates, since only a small number of signatures are required for this purpose. Thus, they provide an important contribution towards cryptographic agility. As of version 2021-01, the Technical Guideline TR-02102-1 [*TR-02102-1*] of BSI recommends the hash-based signature schemes LMS and XMSS as "a good method for creating long-term secure signatures".

6.8 General signature schemes for authentication

The migration to hybrid solutions using post-quantum signature schemes should also be prepared for digital signatures. Here, the two lattice-based schemes CHRYSTALS Dilithium and FALCON should be considered in particular, one of which is expected to be standardized by NIST. SPHINCS+ can also be considered as a particularly conservative choice, although the size of the signatures and the performance limit the possible areas of application here. In the case of signature schemes in particular, the further standardization process should also be observed, as it is likely to be extended by further schemes in the next few years, see Section 2.3.

6.9 Adaptation of cryptographic protocols

The migration to post-quantum algorithms, in particular the use of hybrid solutions, requires adjustments in the cryptographic protocols and standard formats used today. These can be carried out (or at least started) independently of the concrete selection and standardisation of post-quantum schemes. Depending on the protocol in question, there are also (initial) proposals and some finalised solutions for this, see Chapter 3. Since different technical issues are relevant here, these adaptations cannot be assessed purely from a cryptographic perspective. Manufacturers should keep an eye on current developments here and, if necessary, contribute concrete requirements. In particular it is of course important to check their own (proprietary) protocols for resistance to attacks with quantum computers.

6.10 Migration to quantum-safe public key infrastructures

As described in Section 2.1, although signatures for authentication usually only need to be valid for a short time, the associated signature keys may be long-lived. This applies in particular to the root CA keys of a public key infrastructure (PKI) stored in root certificates. Various solutions are currently being discussed here, such as migration at a fixed deadline, parallel PKIs, mixed PKIs. As described in Section 6.5, BSI also recommends hybrid solutions for signature schemes. Since the change to quantum-safe public key infrastructures will be costly and lengthy, it is advisable to initiate this on time.

6.11 Recommendations for Quantum Key Distribution

QKD as a technology for key agreement is based on completely different principles than post-quantum methods for key agreement and thus represents an interesting addition. With regard to the practical use of QKD, further experience should first be gathered within the framework of suitable test networks. BSI currently recommends the use of QKD only as an add-on in hybrid mode, together with post-quantum key agreement and classical procedures. In this manner, QKD can provide additional protection, for which, however, trusted components are necessary. With a view to possible future approvals, it is therefore important that European manufacturers establish themselves on the market to secure technological sovereignty. Agreed keys can be used for encryption by means of an established and recommended algorithm such as AES; BSI does not recommend the sole use of the one-time pad.

6.12 Migration to post-quantum cryptography has priority over the use of QKD

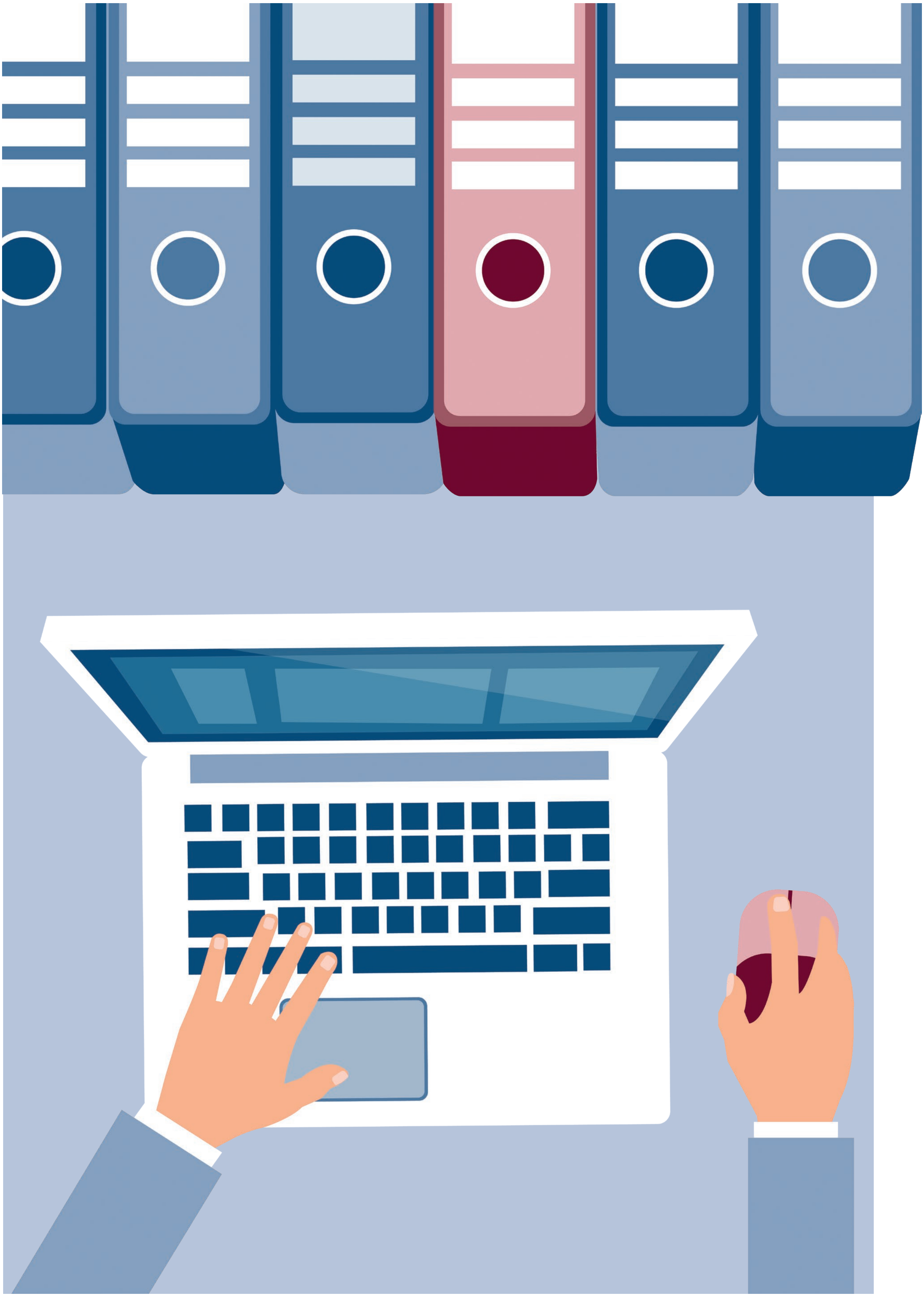
As discussed in Chapter 4, QKD is subject to some practical limitations and there are currently no certified products. Thus, QKD is not yet ready to use in applications with high security needs. Due to the urgency of migrating to quantum-safe solutions, migration to post-quantum cryptography should therefore be a priority.

6.13 Need for further research on quantum-safe cryptography

How well cryptographic algorithms can be attacked with quantum computers depends not only on the progress made in building quantum computers, but also significantly on algorithmic innovations. For example, are there cryptographically relevant quantum algorithms that require fewer qubits? Or that get by with less or no quantum error correction? Or that have a lower circuit depth? Can cryptographic attacks be accelerated using special-purpose quantum computers? These questions show that it is important to combine research on quantum computers and quantum algorithms.

There are also still numerous open questions concerning post-quantum cryptography. On the one hand, the side-channel resistance and implementation security of these cryptosystems have not yet been sufficiently investigated. On the other hand, further research is of course needed on possible cryptanalytic advances, both with classical computers and with quantum computers. In particular, the question of whether structured and unstructured lattices provide the same security is an important research question that should be pursued.

As described in Chapter 4, there are still many questions regarding the theoretical security, secure implementation and use of QKD, which should be investigated further before deployment beyond the necessary field experiments. In the medium term, BSI intends to make further recommendations on the use of the agreed keys and on suitable QKD protocols and authentication mechanisms.



List of abbreviations

Abbreviation	Explanation
ANSSI	Agence nationale de la sécurité des systèmes d'information
BMBF	Federal Ministry of Education and Research
BMF	Federal Ministry of Finance
BMWi	Federal Ministry for Economic Affairs and Energy
CA	certification authority
CACR	Chinese Association for Cryptologic Research
CMS	Cryptographic Message Syntax
COSE	Concise Binary Object Representation
DH	Diffie-Hellman
DLP	Discrete logarithm problem
DLR	German Aerospace Center
ECC	Elliptic Curve Cryptography
ECDH	Diffie-Hellman elliptic curve
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
HPC	high-performance computing
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
AI	Artificial intelligence
LMS	Leighton-Micali Signature
LWE	Learning With Errors
MAC	message authentication code
NCSC	National Cyber Security Centre
NISQ	Noisy Intermediate Scale Quantum
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTRU	N-th Degree Truncated Polynomial Ring
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
QaaS	quantum as a service
QEC	quantum error correction
QKD	Quantum Key Distribution
RFC	Request For Comments
RNG	Random Number Generator
ROSSTANDART	Federal Agency on Technical Regulating and Metrology
RSA	Rivest Shamir Adleman
S/MIME	Secure / Multipurpose Internet Mail Extensions
SIKE	Supersingular Isogeny Key Encapsulation
SPHINCS	Stateless Practical Hash-based Incredibly Nice Cryptographic Signatures
TLS	transport layer security
UDP	User Datagram Protocol
XMSS	eXtended Merkle Signature Scheme

FIND

Bibliography

[AAB+19]
Arute, F., Arya, K., Babbush, R. et al.: “Quantum supremacy using a programmable superconducting processor”, Nature 574, 505–510 (2019).
Available at:
https://doi.org/10.1038/s41586-019-1666-5

[ABB+20]
N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zemor, V. Vasseur, S. Ghosh: „BIKE“, National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[ABC+20]
M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, W. Wang: „Classic McEliece“, National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[AB99]
D. Aharonov, M. Ben-Or: “Fault-Tolerant Quantum Computation With Constant Error Rate”, SIAM Journal on Computing, Vol. 38, Iss. 4

[ACATECH20]
National Academy of Science and Engineering: “The Innovation Potential of Second-generation Quantum Technologies”, March 2020.
Available at:
https://www.acatech.de/publikation/innovationspotenziale-der-quantentechnologien/

[ACATECH21]
National Academy of Science and Engineering: “Digital Sovereignty - Status Quo and Perspectives”, March 2021.
Available at:
https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/

[AD97]
M. Ajtai, C. Dwork: “A public-key cryptosystem with worst-case/average-case equivalence”, STOC 1997, S. 284-293.

[Ajt96]
M. Ajtai: “Generating hard instances of lattice problems”, Quaderni di Matematica, 13:1-32, 2004.

[ANSSI20]
Agence nationale de la sécurité des systèmes d'information (ANSSI): “Should Quantum Key Distribution be Used for Secure Communications?”, Technical Position Paper, May 2020.
Available at:
https://www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf

[BB84]
C. H. Bennett, G. Brassard: “Quantum cryptography: Public key distribution and coin tossing”, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Volume 175, S. 8, 1984.

[BB+97]
C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani: “Strengths and Weaknesses of Quantum Computing”, SIAM Journal on Computing 26(5), S. 1510-1523, 1997.

[BB+20]
D. J. Bernstein, B. B. Brumley, M.-S. Chen, C. Chuengsatiansup, T. Lange, A. Marotzke, B.-Y. Peng, N. Tuveri, C. van Vredendaal, B.-Y. Yang: „NTRU Prime“, National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[BB+21]
M. Baldi, M. Battaglioni, F. Chiaraluce, A. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger: “A New Path to Code-based Signatures via Identification Schemes with Restricted Errors”, August 2020.
Available at:
https://arxiv.org/abs/2008.06403

[BBM17]
D. Bernstein, J.-F. Biasse and M. Mosca: “A low-resource quantum factoring algorithm”, Post-Quantum Cryptography – 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, 26. – 28. Juni, 2017, Proceedings, Lecture Notes in Computer Science vol. 10346 Springer, 2017, S. 330-346.

[BDH11]
J. Buchmann, E. Dahmen, A. Huelsing: “XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions”, Lecture Notes in Computer Science: Post-Quantum Cryptography, 2011.

[Beu22]
W. Buellens: “Breaking Rainbow Takes a Weekend on a Laptop”, February 2022.
Available at:
https://eprint.iacr.org/2022/214.

[BGV12]
Z. Brakerski, C. Gentry, V. Vaikuntanathan: “(Leveled) fully homomorphic encryption without bootstrapping”, ITCS 2012, S. 309-325.

[BH+15]
D. Bernstein, D. Hopwood, A. Huelsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn: “SPHINCS: Practical Stateless Hash-Based Signatures”, Lecture Notes in Computer Science: Advances in Cryptology – EUROCRYPT, 2015.

[BLP08]
D. Bernstein, T. Lange, C. Peters: “Attacking and Defending the McEliece Cryptosystem”, Proceedings of the 2nd International Workshop on Post-Quantum Cryptography, 2008, S. 31-46

[BMBF15]
Federal Ministry of Education and Research: „Self-determined and secure in the digital world 2015-2020“,The German Government's research framework programme on IT security, March 2015.
Available at:
https://www.forschung-it-sicherheit-kommunikationssysteme.de/service/publikationen/self-determined-and-secure-in-the-digital-world-2015-2020

[BMBF18]
Federal Ministry of Education and Research: „Quantum technologies – from basic research to market“, A Federal Government Framework Programme, September 2018.
Available at:
https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Federal-Government-Framework-Programme-Quantum-technologies-2018-bf-C1.pdf

[BMI21]
Federal Ministry of the Interior and Community: „Cyber Security Strategy for Germany 2021", October 2021.
Available at:
https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.html

[BMT78]
E. Berlekamp, R. McEliece, H. Tilborg: "On the Inherent Intractibility of Certain Coding Problems", IEEE Transactions on Information Theory, Vol. IT-24, No. 3, 1978.
Available at:
https://authors.library.caltech.edu/5607/1/BERieeetit78.pdf

[BPS21]
W. Barker, W. Polk, M. Souppaya: "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms", NIST Cybersecurity White Paper, Gaithersburg, Md., April 2021.
Available at:
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[BSI18]
Federal Office for Information Security: Evaluation of Lattice-Based Cryptographic Algorithms, January 2018.
Available at:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Gitterbasierte_Verfahren/Gitterbasierte_Verfahren.html

[BSI19]
Federal Office for Information Security: "Towards Secure Blockchains", March 2019.
Available at:
https://www.bsi.bund.de/EN/Topics/Cryptography/Blockchain/blockchain_node.html

[BSI20]
Federal Office for Information Security: „ Status of quantum computer development ", November 2020.
Available at:
www.bsi.bund.de/qcstudie

[BSI20b]
Federal Office for Information Security: "Migration zu Post-Quanten-Kryptografie", August 2020.
Available at:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html

[BT19/18355]
Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/17500 – Hochsicheres Quantennetzwerk QuNET.
Available at:
https://dserver.bundestag.de/btd/19/183/1918355.pdf

[BT19/25208]
Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Anna Christmann, Kai Gehring, Margit Stumpp, weiterer Abgeordneter und der Fraktion BÜNDNIS 90 / DIE GRÜNEN – Drucksache 19/24762 –,
https://dserver.bundestag.de/btd/19/252/1925208.pdf

[BT19/26340]
Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Dr. Irene Mihalic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90 / DIE GRÜNEN – Drucksache 19/25549 –,
https://dserver.bundestag.de/btd/19/263/1926340.pdf

[CDH+20]
C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijneveld, J. M. Schanck, P. Schwabe, W. Whyte, Z. Zhang, T. Saito, T. Yamakawa, K. Xagawa: "NTRU", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[CFM+20]
A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem: "GeMSS", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[CFS01]
N. Courtois, M. Finiasz, N. Sendrier: "How to Achieve a McEliece-Based Digital Signature Scheme", ASIACRYPT 2001: Advances in Cryptology — ASIACRYPT 2001, pp 157-174

[Chen+21]
Chen et al.: "An integrated space-to-ground quantum communication network over 4,600 kilometres", Nature, Vol. 589, S. 214–219 (2021).

[CK18]
A. Cordel, S. Kousidis: "Quantum Computers – A BSI-Study on the Development Status", BSI-Magazine 2018/02, S. 24-25.
Available at:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2018-02.pdf?__blob=publication-File&v=1

[CPS19]
E. Crockett, C. Paquin, D. Stebila: "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH".
Available at:
https://eprint.iacr.org/2019/858.pdf

[DCP+20]
J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, M. Kannwischer, J. Patarin: "Rainbow", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[DKR+20]
J.-P. D'Anvers, A. Karmakar, S. S. Roy, F. Vercauteren, J. M. Bermudo Mera, M. Van Beirendonck, A. Basso: "SABER", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[DoE20]
U.S. Department of Energy: „From Long-distance Entanglement to Building a Nationwide Quantum Internet", June 2020.
Available at:
https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf

[E91]
A. Ekert: "Quantum cryptography based on Bell's theorem", Physical Review Letters. 67 (6), 1991, S. 661-663.

[EC20a]
European Commission: "Midterm Report of the Quantum Technologies Flagship", September 2020.
Available at:
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70073

[EC20b]
European Commission: "New Strategic Research Agenda on Quantum Technologies", February 2020.
Available at:
https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies

[ETSI15]
European Telecommunications Standards Institute: "Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges", 2015.
Available at:
https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[ETSI20]
European Telecommunications Standards Institute: "Migration strategies and recommendations to Quantum Safe schemes", TR 103 619.
Available at:
https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[EUQF20]
EU Quantum Technologies Flagship: "Strategic Research Agenda", March 2020.
Available at:
https://qt.eu/about-quantum-flagship/resources/

[Fed21]
A. Fedorov: "Quantum-safe cryptography research and development activities in Russia", ETSI Quantum Safe Cryptography Technical Event (02/2021)

[FO+16]
J.-C. Faugère, A. Otmani, L. Perret, F. de Portzamparc, J.-P. Tillich: "Structural cryptanalysis of McEliece schemes with compact keys", Designs, Codes and Cryptography, Vol. 79, Issue 1, 2016, S. 87–112

[GGH97]
O. Goldreich, S. Goldwasser, S. Halevi: "Public-key cryptosystems from lattice reduction problems", CRYPTO 1997, S. 112-131.

[GHP18]
Giacon F., Heuer F., Poettering B.: "KEM Combiners". In: Abdalla M., Dahab R. (eds) Public-Key Cryptography – PKC 2018. PKC 2018. Lecture Notes in Computer Science, vol 10769. Springer, Cham. *https://doi.org/10.1007/978-3-319-76578-5_7*

[Gol86]
O. Goldreich: "Two remarks concerning the Goldwasser-Micali-Rivest signature scheme", Advances in Cryptology CRYPTO '86, Vol. 263, LNCS, S. 104-110, *https://www.wisdom.weizmann.ac.il/~oded/PSX/gmr.pdf*

[Gro96]
L. Grover: "A fast quantum mechanical algorithm for database search", Proceedings, 28th Annual ACM Symposium on the Theory of Computing, S. 212, 1996.

[Hag20]
H. Hagemeier: Frodo is the "New Hope", BSI-Magazine 2020/01, S. 12-14.
Available at:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2020-01.pdf?__blob=publicationFile&v=1

[HB+20]
A. Hülsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, J.-P. Aumasson, B. Westerbaan, W. Beullens: „SPHINCS+", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[HHL08]
A. Harrow, A. Hassidim, S. Lloyd: "Quantum algorithm for solving linear systems of equations", Physical Review Letters 103 (15), 2008.

[HPS98]
J. Hoffstein, J. Pipher, J. H. Silverman: "NTRU: A Ring-Based Public Key Cryptosystem", ANTS 1998: S. 267-288.

[HR+17]
A. Hülsing, J. Rijneveld, J. Schanck, P. Schwabe: "NTRU-HRSS-KEM – Algorithm Specification and Supporting Documentation", 30. November 2017,

[JAC+20]
D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, G. Pereira, K. Karabina, A. Hutchinson: "SIKE", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[KL97]
E. Knill, R. Laflamme: "Theory of quantum error-correcting codes", Phys. Rev. A 55, 900, 1997

[Knu70]
D. Knuth: "Von Neumann's First Computer Program", Computing Surveys, Vol. 2, No. 4, 1970,
https://dl.acm.org/doi/10.1145/356580.356581

[KR+07]
R. König, R. Renner, A. Bariska, U. Maurer: "Small Accessible Information Does Not Imply Security", Physical Review Letters 98 (14), 2007.

[KSL+19]
K. Kwiatkowski, N. Sullivan, A. Langley, D. Levin, A. Mislove: "Measuring TLS key exchange with post-quantum KEM".
Available at:
https://csrc.nist.gov/Presentations/2019/measuring-tls-key-exchange-with-post-quantum-kem

[LDK+20]
V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehle, S. Bai: "CRYSTALS-DILITHIUM", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[LLL82]
A.K. Lenstra, H. W. Lenstra, Jr., L. Lovász: "Factoring polynomials with rational coefficients". Mathematische Annalen, 1982, 261 (4): S. 515–534.

[LM95]
T. Leighton, S. Micali: "Large provably fast and secure digital signature schemes from secure hash functions", U.S. Patent 5,432,852, July 1995.

[LPR10]
V. Lyubashevsky, C. Peikert, O. Regev: "On Ideal Lattices and Learning with Errors over Rings", EUROCRYPT 2010, S. 1-23

[LS15]
A. Langlois, D. Stehlé: "Worst-case to average-case reductions for module lattices", Des. Codes Cryptogr. 75(3), S. 565-599 (2015).

[MAA+20]
D. Moody, G. Alagic, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y. Liu, C. Miller, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, J. Alperin-Sheriff: "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process", 2020, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], *https://doi.org/10.6028/NIST.IR.8309*

[MAB+20]
C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, J. Bos: „HQC", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[MB09]
R. Misoczki, P. Barreto: "Compact McEliece keys from Goppa codes". Selected Areas in Cryptography (SAC 2009), August 2009.

[McE78]
R. J. McEliece: "A public-key cryptosystem based on algebraic coding theory", Technical report, NASA, 1978,
https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF

[Mer79]
R. Merkle: "Secrecy, Authentication, and Public Key Systems", Stanford University Information Systems Laboratory Technical Report 1979-1, 1979.

[MM+18]
D. Martin, A. Montanaro, E. Oswald, D. Shepherd (2018): "Quantum Key Search with Side Channel Advice". In: Selected Areas in Cryptography – SAC 2017. SAC 2017. Lecture Notes in Computer Science, vol 10719. Springer.

[Mos15]
M. Mosca (2015): "Cybersecurity in an era with quantum computers: will we be ready?".
Available at:
https://eprint.iacr.org/2015/1075.pdf

[NAB+20]
M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila: "FrodoKEM", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[NCSC20]
National Cyber Security Center: "Quantum security technologies", Whitepaper, 24. March 2020.
Available at:
https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf

[Nie86]
H. Niederreiter: "Knapsack-type cryptosystems and algebraic coding theory". Problems of Control and Information Theory, 15(2), S. 159–166, 1986.

[NIST20]
National Institute of Standards and Technology: "NIST Status Update on the 3rd Round", July 2020.
Available at:
https://csrc.nist.gov/Presentations/2021/status-update-on-the-3rd-round

[OGM21]
M. Ounsworth, J. Gray, S. Mister: "Composite Encryption For Use In Internet PKI", July 2021, available at https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-encryption/

[OP21a]
M. Ounsworth, M. Pala: "Composite Public and Private Keys For Use In Internet PKI", February 2022.
Available at:
https://www.ietf.org/id/draft-ounsworth-pq-composite-keys-01.html

[OP21b]
M. Ounsworth, M. Pala: "Composite Signatures For Use In Internet PKI", February 2022.
Available at:
https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/

[PDT20]
P. Schwabe, D. Stebila, T. Wiggers: "Post-Quantum TLS Without Handshake Signatures", CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, *https://doi.org/10.1145/3372297.3423350*

[Pei16]
C. Peikert: "A Decade of Lattice Cryptography", Found. Trends Theor. Comput. Sci. 10(4): S. 283-424 (2016).

[PR14]
C. Portmann, R. Renner: "Cryptographic security of quantum key distribution", preprint arXiv:1409.3525 (2014).

[PR21]
C. Portmann, R. Renner: "Security in Quantum Cryptography", Available at:
https://arxiv.org/abs/2102.00021

[PST20]
C. Paquin, D. Stebila, G. Tamvada: "Benchmarking Post-Quantum Cryptography in TLS", PQCrypto 2020, *https://dx.doi.org/10.1007/978-3-030-44223-1_5*

[QDelta]
Quantum Delta Nederland: "Economic impact of Quantum in The Netherlands".
Available at:
https://quantumdelta.nl/pdf/20200518%201400%20QuTech_Economic%20Impact%20of%20Quantum_vFinal2_200728.pdf

[Reg05]
O. Regev: "On lattices, learning with errors, random linear codes, and cryptography", STOC 2005: S. 84-93.

[RFC 2104]
M. Bellare, R. Canetti, H. Krawczyk: "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, 1997.

[RFC 5639]
M. Lochter, J. Merkle: "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

[RFC 7296]
C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 7296, Oktober 2014.

[RFC 7383]
V. Smyslov: "Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation", RFC 7383, November 2014.

[RFC 8391]
A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld, A. Mohaisen: "XMSS: eXtended Merkle Signature Scheme", IETF RFC 8391, May 2018.
Available at:
https://tools.ietf.org/html/rfc8391

[RFC 8446]
E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, August 2018.

[RFC 8554]
D. McGrew, M. Curcio, S. Fluhrer: "Leighton-Micali Hash-Based Signatures", IETF RFC 8554, April 2019.
Available at:
https://tools.ietf.org/html/rfc8554

[RFC 8708]
R. Housley: "Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS)", IETF RFC 8708, February 2020.
Available at:
https://tools.ietf.org/html/rfc8708

[RFC 8778]
R. Housley: "Use of the HSS/LMS Hash-Based Signature Algorithm with CBOR Object Signing and Encryption (COSE)", IETF RFC 8778, April 2020.
Available at:
https://tools.ietf.org/html/rfc8778

[RFC 8784]
S. Fluhrer, P. Kampanakis, D. Mc Grew, V. Smyslov: "Mixing Preshared Keys in IKEv2 for Post-quantum Security", RFC 8784, June 2020.
Available at:
https://datatracker.ietf.org/doc/html/rfc8784

[SAB+20]
P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, D. Stehle: "CRYSTALS-KYBER", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

[SFG21]
D. Stebila, S. Fluhrer, S. Gueron: „Hybrid key exchange in TLS 1.3", July 2021, IETF RFC Draft,
https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design

[Shor04]
P. Shor: "Progress in Quantum Algorithms", Quantum Information Processing 3, S. 5-13, 2004.

[Shor94]
P. Shor: "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press: S. 124-134, 1994.

[SIGA05]
V. Scarani, S. Iblisdir, N. Gisin, A. Acín: "Quantum cloning", Rev. Mod. Phys. 77, 1225 (2005).

[SKD20]
D. Sikeridis, P. Kampanakis, M. Devetsikiotis: "Post-Quantum Authentication in TLS 1.3: A Performance Study", Network and Distributed Systems Security (NDSS) Symposium 2020, *https://dx.doi.org/10.14722/ndss.2020.24203*

[SM+17]
S. Sajeed, C. Minshull, N. Jain, V. Makarov: "Invisible Trojan-horse attack", Scientific Reports, 7, 2017.

[Smy21]
V. Smyslov: "Intermediate Exchange in the IKEv2 Protocol", August 2021, draft-ietf-ipsecme-ikev2-intermediate-07.

[SP00]
P. Shor, J. Preskill: "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters 85 (2), 2000, S. 441-444.

[SP800-38B]
National Institute of Standards and Technology: "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", Special Publication SP 800-38B, 2005.

[SP800-38D]
National Institute of Standards and Technology: "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication", Special Publication SP 800-38D, November 2007.

[SP800-56C]
National Institute of Standards and Technology: "Recommendation for Key-Derivation Methods in Key-Establishment Schemes", Special Publication SP 800-56C Rev. 2, August 2020, *https://doi.org/10.6028/NIST.SP.800-56Cr2*

[SP800-208]
National Institute of Standards and Technology: "Recommendation for Stateful Hash-Based Signature Schemes", Special Publication SP 800-208.
Available at:
https://csrc.nist.gov/publications/detail/sp/800-208/final

[SV+17]
A. Scherer, B. Valiron, S.-C. Mau, S. Alexander, E. van den Berg, T. E. Chapuran: "Concrete resource analysis of the quantum linear system algorithm used to compute the electromagnetic scattering cross section of a 2D target", Quantum Inf. Process. (2017) 16: 60.

[THS21]
Cj. Thai, T. Heider, V. Smyslov: "Beyond 64KB Limit of IKEv2 Payload", July 2021.
Available at:
https://tools.ietf.org/html/draft-tjhai-ikev2-beyond-64k-limit-01

[TR-02102-1]
Federal Office for Information Security: "BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths".
Available at:
https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/tr02102/BSITR02102.html

[TR-02103]
Federal Office for Information Security: „BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung", 2020.

[TR-03140]
Federal Office for Information Security: "TR-03140 Technical Guideline „SatDSiG".
Available at:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03140/TR-03140_node.html

[TT+21]
C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, V. Smyslov: "Multiple Key Exchanges in IKEv2", July 2021, draft-ietf-ipsecme-ikev2-multiple-ke-03.

[VDI20]
VDI Technologiezentrum GmbH: „Roadmap Quantencomputing", October 2020,
https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Roadmap-Quantencomputing-bf-C1.pdf

[VDI21]
VDI Technologiezentrum GmbH: „Agenda Quantensysteme 2030", March 2021,
https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Agenda_Quantensysteme_2030_web_C1.pdf

[vGF19]
D. Van Geest, S. Fluhrer: Algorithm Identifiers for HSS and XMSS for Use in the Internet X.509 Public Key Infrastructure, IETF RFC Draft, March 2019,

[vN45]
J. von Neumann: "First Draft of a Report on the EDVAC", 1945

[Wil20]
F. Wilhelm-Mauch: „Quantum Computers and Quantum Superiority", BSI-Magazin 2020/01, S. 15-17.
Available at:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2020-01.pdf?__blob=publica-tionFile&v=1

[WC81]
C. Wegman, Carter: "New Hash Functions and Their Use in Authentication and Set Equality", Journal of Computer and System Science, 22, 1981.

[WZ82]
W. K. Wootters W. H. Zurek: "A Single Quantum Cannot be Cloned", Nature 299 (5886), 802-803, 1982.

[X.509]
Internationale Fernmeldeunion: "ITU-T Recommendation X.509 10/2019", October 2019.
Available at:
https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509

[Yuen16]
H. Yuen: "Security of Quantum Key Distribution", IEEE Access, vol. 4, pp. 724-749, 2016.

[ZCD+20]
G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, J. Katz, X. Wang, V. Kolesnikov, D. Kales: „Picnic", National Institute of Standards and Technology, 2020.
Available at:
https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions

www.bsi.bund.de

Legal notice

Published by:
Federal Office for Information Security (BSI)

Source:
Federal Office for Information Security (BSI)
Godesberger Allee 185–189
53175 Bonn

E-Mail:
quantum@bsi.bund.de

Phone:
+49 (0) 22899 9582-0

Fax:
+49 (0) 22899 9582-5400

Last updated:
Oktober 2021

Printed by:
Appel & Klinger Druck und Medien GmbH, Schneckenlohe

Design:
Faktor 3 AG

Content and editing:
Federal Office for Information Security (BSI)
Dr. Stephan Ehlen, Dr. Heike Hagemeier, Dr. Tobias Hemmert,
Dr. Stavros Kousidis, Dr. Manfred Lochter, Stephanie Reinhardt and
Dr. Thomas Wunderer

Image credits:
S. 1: AdobeStock© Visual Generation; S. 10: AdobeStock© Visual Generation; S. 24: AdobeStock© Visual Generation; S. 36: AdobeStock© hasan; S. 44: AdobeStock© Visual Generation; S. 56: AdobeStock© VectorMine; S. 60: AdobeStock© Visual Generation; S. 64: AdobeStock© Feodora; S. 66: AdobeStock© Feodora

Diagrams:
Federal Office for Information Security (BSI)

Item number:
BSI-Bro21/01

This brochure is part of the Federal Office for Information Security's public relations work. It is provided free of charge and is not intended for sale.