Otto-von-Guericke-University
Faculty of Computer Science
Magdeburg, Germany

STRATEGIC APPROACH TO POST-QUANTUM CRYPTOGRAPHY MIGRATION

- Analyzing the impact of quantum computing on the domains of cryptography and cybersecurity, as well as formulating possible paths to overcome the stated challenges

Master's Thesis in Computer Science
by

Jacob Ludwig Schmidt

18. September 2024

1. Examiner
Prof. Dr. rer. pol. habil. Hans-Knud Arndt
Faculty of Computer Science
Otto-von-Guericke-University
Magdeburg, Germany

2. Examiner
M.Sc. Nicklas Körtge
Quantum-safe Cryptography Research Group
IBM Research
Zurich, Switzerland

Schmidt, Jacob Ludwig
Strategic Approach to Post-Quantum Cryptography Migration
Master's Thesis in Computer Science, Otto-von-Guericke-University
Magdeburg, Germany, 2024.

Contents

Abstract

This thesis outlines the effects of quantum computing on the domains of cryptography and software security. Quantum computing poses a significant threat to current public-key encryption algorithms, as it theoretically possesses the ability to solve the underlying mathematical operations in a trivial amount of time. The effects of which are difficult to predict as to the current wide-ranging application of quantum-vulnerable public-key encryption, nonetheless the potential of breach of any information secured through public-key encryption, such as communication over the internet, is grave enough to warrant action. With the estimated time frame of as early as in 10 years time this capability could be achieved and with the danger of harvest-now-decrypt-later type of attacks this prompts an immediate incentive to migrate to quantum-safe cryptography. The current state of governmental policy and legislation regarding cryptography shows an awareness of the danger of quantum computing, but no precedent has been set to change the law for a specific vulnerability. The responsibility to act lies on the private sector to protect itself and dependent actors. Major software and information technology businesses identified the need for quantum-safe cryptography and communicated their efforts to conduct a cryptographic migration of their services. This does not translate to industry-wide knowledge of quantum-safe cryptographic migration. The self reported possible transition timelines on average will miss the estimated breaking point of public-key encryption by several years. The lack of public discussion on general approaches to quantum-safe cryptographic migration reflects such. This thesis aims to engage this research gap by providing an extensive examination of the potential impacts of broken public-key encryption due to quantum computing and proposing a migration strategy to post-quantum cryptography. The strategy is informed by the review of prominent historic migrations, current migration recommendations, and properties of related fields such as software supply chain security and cryptographic agility. The migration strategy is designed to provide guidance in the approach to adopting quantum-safe cryptography and entering a sustainable state of cryptographic security.

1 Introduction

Quantum computing opens new ways of solving complex mathematical operations otherwise deemed practically unsolvable with currently available computing hardware. This development has an extensive impact on the domains of cryptography and software security. Currently, a massive part of digital systems—or to be more precise, their software—use asymmetric-cryptography to communicate in a secure way. One of such is the prominently used RSA-encryption scheme, which uses the mathematical problem of factoring to calculate its keys and in doing so secures, for example, the traffic of communication over the internet. Quantum computing has the ability to completely erase any security granted by these frequently used cryptographic algorithms, as it can solve the mathematical problems they are based on with comparatively low effort. [1, p. 4-5, 25–28]

In theory, this was established as early as the year 1994 when mathematician and computer scientist Peter Shor published a paper on the ability of quantum computers to break known ciphers and cryptographic algorithms [2]. It describes the theoretical ability given a powerful enough quantum computer to solve the underlying mathematical problem of factoring in a short amount of time, rendering encryption schemes based on it insecure. The amount of qubits (used as a general descriptor of the computing power of quantum computers) needed for Shor's algorithm to become reality exceeds the number any quantum computer currently has [1, p. 4-5]. Steady advancements and improvements raised this number considerably and seem to further do so at an ever-increasing pace [1, p. 11-22]. Predictions about the time frame until quantum computers will be powerful enough to break current encryptions are as early as the beginning of the 2030s [1, p. 35]. Although the unpredictability of breakthroughs leading to a greater increase in qubits could shift the breaking point even earlier.

Knowing the inevitability of the breaking point of our current encryption schemes enables other possibilities of attack aside from a direct decryption attempt. Seeing that all pieces required for a decryption of factoring-based cryptographic algorithms are already laid out given Shor's algorithm, one only has to wait for a powerful enough quantum computer to execute with comparatively minimal effort. This gives any attacker a level of certainty that enables planning for a widespread encryption-breaking event. An attacker can store any interesting encrypted information now, with the certainty that he will be able to break the encryption later. Given the widespread use of quantum vulnerable cryptographic algorithms, we are now especially vulnerable to any harvest-now-decrypt-later attack [1, p. 26]. With an ever-accelerating timeline of quantum computer advancements, it seems this breaking point could be reached in just a couple of years—while the vulnerability to harvest-now-decrypt-later is already in place. Concluding, all time even before switching to a quantum-safe encryption method (also called post-quantum cryptography) is potentially unsecured.

A cryptographic vulnerability is resolved by a migration to another, presumably safe, cryptographic algorithm. A process necessary throughout cryptographic history to maintain the security and privacy granted through encryption. The rapid progress of computational power in the last decades has overcome the mathematical complexity of numerous cryptographic algorithms, making migrations to some degree a reoccurring process. Depending on the circumstances, the resource and manpower investment necessary for the migration process can be prohibitively costly. Viewed across the domain, this, in general, led to a years- if not decades-long transition process which sometimes extended past the breaking point of the vulnerable encryption. [3]

Despite this evident pattern, the research field of cryptographic migration is scarce in material, with only infrequent academic contributions. The foundation on which a shared understanding and knowledge of cryptographic migration could be built upon and strategy and procedure be deduced from has yet to be established. This realization is shared in the opinion piece "Where Is the Research on Cryptographic Transition and Agility?" in the prominent *Communications of the ACM* journal, published in April 2023 [4]. In their article the authors David Ott, senior researcher and academic program director at VMware, Kenny Paterson, professor of computer science at ETH Zürich and leader of the university's Applied Cryptography Group at the Institute for Information Security, and Dennis Moreau, senior director of Security Strategy at Intel, describe the lack of research in the field of applied cryptography that would address the gap between high-level discussion on cryptographic policy and low-level cryptographic theory or technical implementation.

This sentiment is reflected in the public discussion or rather lack of discussion of strategies and procedures of quantum-safe cryptography migration, as no leading academic theory has emerged on said topic thus far. A recent study of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) on the topic of quantum computing and its impact on cryptography has concluded with the finding that on average, the time to complete a migration to quantum-safe cryptography will exceed the encryption breaking point by 6 and a half years by its participants [5, p. 19]. With no holistic collection of related information and its evaluation available, the situation remains unclear as to the impact of the quantum vulnerability, the general awareness of its dangers and what actions should be taken to avert negative consequences.

This compels further research to aggregate information on related domains, finding connections and implications between them, mapping out possible solutions, and contribute to providing guidance to achieve a quantum-safe state of software security.

1.1 Hypothesis

The thesis is grounded on assertions relating to the awareness, acknowledgment, and action regarding the stated capabilities and resulting problems of quantum computing as previously described.

(1) Quantum computing will make all currently used asymmetric cryptographic algorithms obsolete and insecure.

(2) Harvest-now-decrypt-later will even make the time before that potentially insecure.

(3) Governments and industry in general are not aware of this or are not acting on this fact.

(4) There is no holistic summary of this topic that provides the necessary information to get a comprehensive overview.

(5) As a consequence thereof, no public discussion of strategic software engineering approaches to cryptographic migration has been taking place.

(6) This results in organizations lacking a plan to transition to quantum-safe cryptography, resulting in potentially insecure communication now or usage of obsolete cryptography later.

(7) A comprehensive strategy for post-quantum cryptographic migration on an organizational level providing guidance on how to proceed with the new quantum-safe developments and encompassing them in their operations would enable a cryptographic transition, accelerate the process and decrease the cost of possible future migrations.

1.2 Goal of this thesis

This thesis aims to provide a comprehensive overview of the topic of quantum-safe cryptography and create a possible strategy to migrate to quantum-safe cryptography in the context of a wider scale adoption.

1.3 Structure of this thesis

This thesis is organized into distinct chapters, with each building upon the previous to research the intersection of cryptography and quantum computing.

In chapter 2 the foundational background information necessary to understand the challenges posed by quantum vulnerability is provided. It covers the basics of cryptography including key concepts, prominent algorithms, and the process of cryptographic migration. Following are the basics of quantum computing, including its differentiating physical properties, application, quantum algorithms of interest, and the current state of development. The intersections of both domains is examined, and the potential impact is put into the context of cybersecurity and real-world applications. Related works to the posed problems are examined and evaluated as to their applicableness.

In chapter 3 the forthcoming agenda of the thesis is established, describing the research approach taken and the matter of which a post-quantum migration strategy should be created.

In chapter 4 the response to the established quantum vulnerability problem is explored and analyzed. It includes both the perspective of public and private institutions. It examines existing laws and policy positions, governmental acknowledgement and actions, as well as industrial acknowledgement and action to the cryptographic threat of quantum computing. Current standardization efforts of post-quantum cryptography and migration recommendations are examined. An analysis of the presented state is performed as to the appropriateness of the given response, and the chapter concludes with an extensive summary of all presented facts in a clear argumentation reinforcing the assertions made in the hypotheses.

In chapter 5 the thesis's development process of a post-quantum cryptography migration strategy is described and performed. The general conduct of cryptographic migrations is formulated and extended with the examination of prominent historic migrations. Properties and approaches of the fields of software supply chain security and cryptographic agility are considered. A four-step migration strategy is presented to facilitate the adoption of quantum-safe cryptography.

In chapter 6 an evaluation and discussion of the research approach and content is performed, reviewing the assertions made in the thesis's hypotheses and highlighting the limitations of the presented work.

In chapter 7 the key findings of the thesis are summarized, emphasizing the need for post-quantum cryptography migration to secure digital communication against the emerging quantum threat.

2 Background

To accurately engage with the subject of this thesis, a foundation of knowledge has to be established. This chapter will provide an overview of the important background information while concentrating the material on the necessary elements for this thesis. To establish the assertions stated in chapter 1.1 information regarding the fields of cryptography, quantum computing, the intersection of both and implications for the domain of cybersecurity will be discussed.

2.1 Cryptography

Modern cryptography is described as "[...] the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks." [6, p. 1] by Katz and Lindell in their encompassing book about the field. It has the objective of encoding information to shield it from any prying eyes and unauthorized access [6, p. 1-6]. Only the intended recipient should be able to access any part of the encrypted information. Through the use of codes and algorithms, cryptography secures information in general, including communication, masking the true content from unknowing actors [6, p. 1-6]. Historically, it grew out of the related fields of mathematics and statistics, computer science as well as information and signal processing [7].

In the digital age, cryptography guarantees the security and privacy of digital data in communication and transaction, as well as in storage. It is integral in the process of ensuring confidentiality of transmitted data, the authenticity of authorship, and the integrity of the communicated message. By safeguarding sensitive information and establishing trust in the actions and agency over a wide range of sectors, cryptography is essential in maintaining a secure and private infrastructure of operations—be it in personal data privacy, commerce and business, financial systems to governmental institutions, military, and intelligence agencies. [8]

2.1.1 Foundation and theory

The process of cryptography is important for the topic discussion of this thesis. The cryptographic terminology is a reoccurring theme, describing concepts and frameworks that are applicable to different cryptographic approaches, algorithms, ideas, and thus they are important to be aware of. In general, to secure a text or message in cryptography, one explores an idea for a cipher or a code to obfuscate the true meaning of said text. This is also called an encryption scheme. An easy illustration of this concept is the cipher used by the infamous roman dictator Gaius Julius Caesar in which each letter will be shifted a set number of places in the alphabet, with the message now resulting in a gibberish collection of seemingly random letters. The original message is also called the plaintext, the encrypted message is called ciphertext. The figure 2.1 illustrate the encryption procedure. To recover the original text, one has to reverse the encryption scheme—a process called decryption. In the example given, this would mean shifting each letter in the ciphertext back to its original place. The obvious solution to solving this encryption scheme is knowing the number of places in the alphabet letters get shifted—this is the key to encrypting a message but also decrypting it later on. In this case, the message can be secure if only the sender and the receiver are in possession of the specific key used. The category of cryptographic encryptions where a single key is used for both processes is called private-key or symmetric-key encryptions. [6, p. 2-4, 6–8]

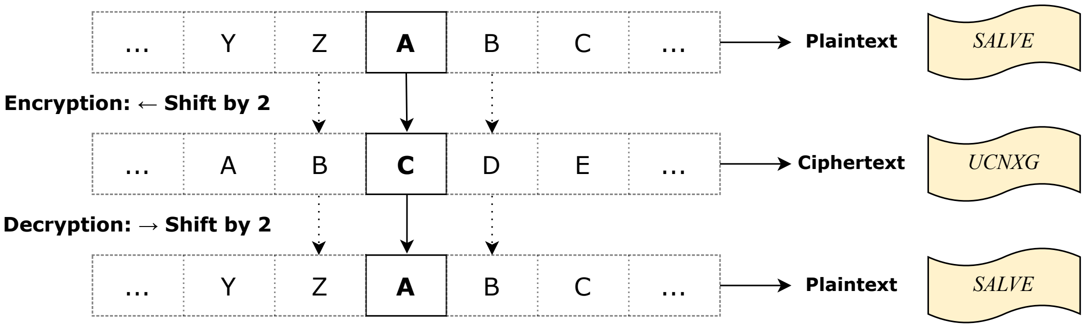


Figure 2.1: Illustration of Caesar's cipher as described by Katz and Lindell [6, p. 6-8]

In contrast to this and important in the context of quantum computing is asymmetric-encryption, also known as public-key encryption. Encryption and decryption do not share the same key in this instance. This does enable the secure communication between two individuals without any collaboration in setting up a secure environment with a private key known to both. A party, who wants to receive a message, needs to have two keys: a private key—also called the secret key—and a public key. The public-key will be, as the name implies, public and in the open for anyone to see. The public-key itself will be used to encrypt a message to the party the public-key belongs to. The public-key can not be used to decrypt a message encrypted by this key. To decrypt the message, the receiver will use its secret-key. This way, everybody is able to send encrypted messages to a party without having to exchange any key beforehand. The figure 2.2 shows the described difference in the cryptographic concept between symmetric and asymmetric cryptography. [6, p. 401-404]

There are many different ideas and theorized encryption schemes about how a key can be used to obfuscate a message, be it in mathematical operations, the shifting of bits or other ways of manufacturing a complex sequence of undecipherable letters to the unknowing eye. The need for different algorithms becomes clear after establishing the qualities each encryption scheme inhibits, which influence how and why they are used. The reason the ancient Romans do not dictate our cybersecurity policy anymore is grounded in the fact that the security of their chosen encryption becomes superficial once you figure out the underlying information encryption idea. Then you can simply take at guess at the key to unlocking the message. The possibility of a random guess is not unique to this cipher, but the number of guesses needed to find the correct key is. The alphabet consists of 26 letters, leaving 25 possible letters to shift to, assuming the ciphertext is not legible. This would be forcing the solution through sheer force of trying every possible key, also called brute-force. A downfall which shares its name with the man and his cipher. The makeup of the key correlates with

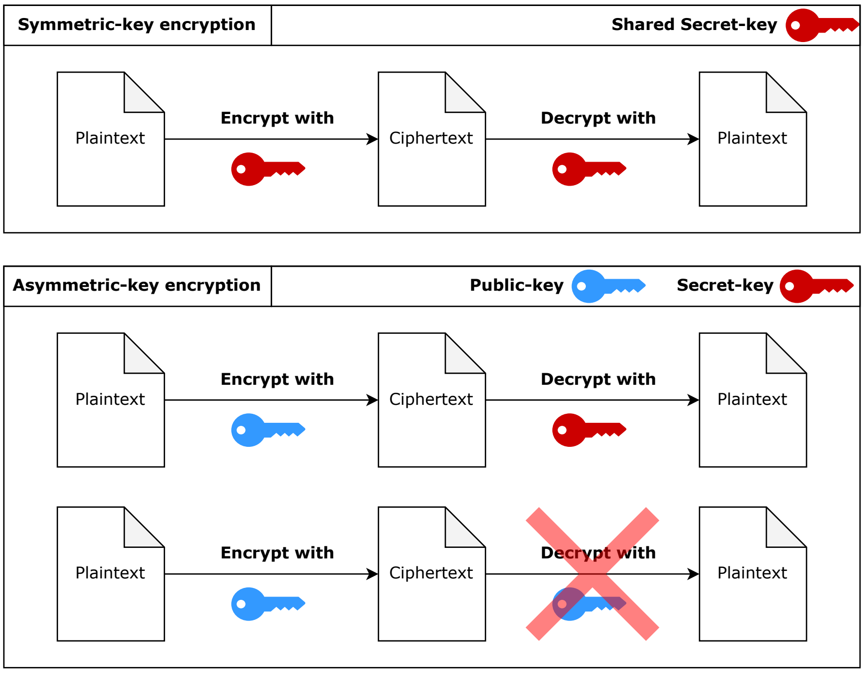


Figure 2.2: Illustration of the cryptographic mechanisms of symmetric and asymmetric-encryption as described by Katz and Lindell [6, p. 401-403]

the security of the scheme, but also the principle behind the encryption and decryption is important. Rather than wasting time with every possible key combination, effort can be saved if one can utilize additional information about the process. In the case of communication with a substitution cipher, you can use the fact that every letter is shifted by the same number of places, meaning finding the solution for one word solves the whole encrypted message. One can look for instances of repeated and often used words or phrases that would be contained in a message, like a roman greeting at the beginning of every message. Shifting the first letters of the ciphertext to a simple ‘salve’ will take even less time than just going through the alphabet. Both aspects inform our judgment on the value of security we attribute to a given cryptographic algorithm. Something that can also adjust with time and technology, as the process of thinking and guessing was augmented with machines and computers. In the discussion of cryptography and a related algorithm, the magnitude should now be in the realm of years and decades or even centuries of processing effort that should statistically have to be invested to break its encryption. [6, p. 2-21]

2.1.2 Application

The described theoretical foundation informs and ensures a constant change of cryptography throughout our history. Starting with the early well-documented use in sensitive diplomatic and military correspondence with the famous Caesar cipher, the aforementioned substitution method from ancient Rome, or the transposition ciphers from ancient Greece [6, p. 6-11]. Both methods show the intent behind the use of cryptography—to conceal the message’s true content. The simplicity necessitated change once its methods and how to solve them were known, leading to another famous example of a more complex cryptographic scheme from the renaissance period. The Vigenère cipher, part of the category of polyalphabetic ciphers, uses multiple substitution alphabets as to increase the complexity and, in turn, the time to brute-force all possible combinations one has to try to find the right key [6, p. 11-14]. The great wars of the 20th century brought more developments with the shift to mechanical and electronic devices like the German Enigma machine used for encrypting and decrypting highly sensitive radio messages [9] [10]. In the effort to break the complex German cryptography, the mathematician Alan Turing played a crucial role and devised a machine capable of executing a great number of mathematical operations used to find the key. This Turing machine was also the foundation of what is today to be understood as the field of computing and computing machines, making cryptography (or the will to break it) the catalyst for this development [9] [10]. Going forward to the digital time period of today, cryptography is integral to securing the communication of data. With the transition to digital systems and the internet, new cryptographic algorithms have been created, matching the need for complex security. Modern cryptography maintains the data protection and confidentiality and thus enables privacy [8]. The obfuscation of information in essence offers the capability to safeguard any and all information deemed worth protecting. This includes information from and intended to oneself and information from oneself intended to another party, regardless of which ways and intermediaries it is communicated through.

Given the described abilities of cryptography, the following set of general applications have arisen:

Data encryption

Cryptography can be used to secure information. This directly translates out of the ability to generate ciphertexts with an encryption algorithm, preventing access to the information from anyone, who is not in possession of the corresponding key. In concept, this is applicable to all data and thus enables the secure and private storage of information. [8]

Secure communication

With the ability to encrypt data, it is also possible to transfer this encrypted data and let it be decrypted by a recipient party. Intermediaries and malicious actors intercepting any traffic of the encrypted communication are not able to read the ciphertext, and therefore privacy and security of communicated information is preserved through the use of cryptography. The most prominent application of the protection of communication is done on the global network of the internet. [8]

Data integrity

Through the use of cryptographic hash-functions, the integrity of a data element can be verified. An error through, for example, faulty transmission or malicious tempering can be detected if the corresponding checksums of the original data element and the data element in question are compared. [8]

Data authenticity

Through the use of cryptography, it is possible to verify the authenticity of data and their authorship. The sender of information can digitally sign a message with his private-key, and any receiver can verify the authenticity through the use of the corresponding public-key (see chapter 2.1.4). [8]

2.1.3 Current prominent algorithms

Two of the most prominent cryptographic algorithms in use today are *RSA (Rivest-Shamir-Adleman)* and *AES (Advanced Encryption Standard)*, which also represent the two categories discussed prior of public-key and private-key, respectively.

RSA is the first published asymmetric-cryptographic algorithm, meaning the communicating parties do not share a key for encryption and decryption. It was developed in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman who also gave the algorithm its name. It derives its mathematical complexity by the factoring of large prime numbers in the creation of the two keys. Because one of the keys is only used to encrypt information, it can be shared publicly to anyone who wants to communicate with the entity holding the corresponding private key which can decrypt the information and, as the name suggests, should remain private as to maintain secrecy. Now, as two prime numbers were used to construct both keys and one of them being public knowledge, one could try to guess which two prime numbers could make up the public-key and in turn the secret private-key. This is also known as the RSA-problem and is predicated on the problem of factoring large numbers. Traditional computing hardware would take millennia trying to find the original prime factors of this encryption-scheme, making any attempt futile. [6, p. 331-336] [11, p. 640-644] [12]

AES or Advanced Encryption Standard is an in the year 2000 standardized and widely used symmetric encryption algorithm. In this cryptographic scheme, the same key is used for encryption and decryption, as described earlier. It is based on a substitution-permutation network, where any plaintext is subjected to multiple rounds of substitutions and permutations based on the private-key. So far, they are no known cryptographic attacks on AES that would perform better than brute-force. [6, p. 238-240]

2.1.4 Digital signatures

Continuing with the development of public-key encryption and the ability to communicate securely with another party—be it only one way in the beginning—is the addition of a method to verify the integrity and authenticity of a message. Digital signature schemes allow the verification of the original sender of a message by anyone with the public-key associated with the sender. This reverses the flow of communication previously explained for public-key encryption. The party, who is in possession of its very own private-key, can receive messages encrypted with its associated public-key—the original key-pair that is created together in the public-key encryption scheme. If this party wants to send a message back to anyone in possession of their public-key, the same encryption and decryption procedure is not possible. But, with a digital signature, it is possible to have this exchange with the public-key holder, knowing that a message is coming from the original party in possession of the private-key. The sender can use their private-key on the message with a signature algorithm to create a digital signature. This signature will be sent alongside the message. The receiver in possession of the public-key can use the message, the signature algorithm and said public-key to verify the signature. If the signature is valid, the receiver knows that this message could have only come from a sender in possession of the associated private-key, and thus the message is authenticated. If a malicious actor interjects in this process and changes either the message or the signature, the receiver can now reject this tampering by verifying the signature with the public-key. [6, p. 463-464]

2.1.5 Cryptographic migration

The process of migration describes the transition from one cryptographic scheme or architecture to a different one [13, p. 22]. In modern cryptography, this means an exchange of cryptographic algorithms used in digital systems. Migration and transition are both used in this context and both describe the same process and thus can be used interchangeable.

As described in this chapter, the evolution of cryptography has been guided by a constant fight of concealing information and a resulting desire to reveal it. A historic precedence has been set that despite the best intentions a perfectly secure scheme has not been found so far, as evident in the progression of cryptographic approaches [6, p. 6-21]. With the gift of hindsight the limitations of a Caesar cipher (the shifting of each letter a number of places in the alphabet) might be obvious but with the development of modern cryptography the ability to manually execute a brute-force attack does not seem to be possible anymore with human brains alone. Consequently, the line between a secure cryptographic scheme and an insecure one can become fuzzy as the knowledge to confirm either one is built upon an exploration of mathematical and logical proofs [6, p. 14-21]. Despite being created with the purpose of providing security through the use of the most up-to-date cryptographic knowledge, a historical pattern of eventual insecurity of every cryptographic scheme has emerged [6, p. 6-21] [14]. If this state of vulnerability is reached by exploring procedural steps of the algorithm, new mathematical proofs unknown at the time of creation or by gaining new computational resources making the underlying complexity obsolete is not relevant as either compromise the security of the cryptographic algorithms. In every instance of a broken encryption scheme, a transition to a different scheme had to take place to remain in the state of cryptographic security.

2.2 Quantum Computing

Quantum mechanics form the basis of a new field of computing theory known as quantum computing. Taking advantage of the physical properties exhibited in quantum mechanics expressing the state of matter as particles and waves, quantum computing takes a different approach to calculation as current computers. This represents a fundamental shift in the approach to processing digital information and differs structurally from current computing methodology. With the exploration of new physical properties described through quantum mechanics, it became possible to predict the subatomic behavior and thus challenge or rather expand the principles of classical computing used so far. [11, p. 1-16] [15, p. 3-8]

2.2.1 Foundation and theory

The current digital infrastructure and processing hardware of classical computing has been built on a binary system of information representation. Digital systems use a primary data unit called a bit. Any information element of the real world is translated to the digital world through the use of only two symbols or states—1 or 0. A bit can adopt one of these two distinct states. Like the letters of the alphabet are used in our language, bits and their binary states are used to convey information in digital systems. The binary system forms the basis of current computational technology, encompassing anything from simple calculators to complex supercomputers. This clear but narrow framework enables the digital representation of information and every following processing operation. [15, p. 3-8] [16, p. 1-28]

Quantum computing utilizes several properties of physics expressed in the field of quantum mechanics, differentiating itself from classical computing. Prominently, the quantum phenomena of superposition and entanglement form the basis of quantum computing. The concept of superposition introduces a new way of representing information in the computational system called quantum bits, abbreviated to qubits. The quantum data units of information differ fundamentally from classical bits. Quantum superposition allows a qubit to simultaneously assume more than one state. While a normal bit is restricted to a single state of either 1 or 0 at any point in time, the physical properties of superposition of a qubit allow the adoption of the state of 1 or 0 or any linear combination of the two. The ability of qubits to inhibit multiple states simultaneously is fundamentally different from classic computing. This exceptional element of simultaneous occupation of both binary states allows quantum computing to process a multitude of operational outcomes simultaneously. The parallelization exponentially increases the processing speed at which suitable problems can be solved, and thus significantly enhances computational efficiency compared to classical computing. [11, p. 12-16]

The second influential property described through quantum mechanics is the entanglement of qubits. The entanglement is the description of a connection of physical particles which prescribes shared properties and behavior between the linked particles. This allows the prediction of the state of one particle if its entangled counterpart is observed. In this manner, the entanglement of a qubit ties the state of one qubit directly to the state of another. This relationship persists regardless of physical distance between the two. Any effect on the state of one qubit is shared instantaneously with its entangled counterpart. Entanglement has foundational implications for data processing. Entangled qubits have the capability to perform operations in a coordinated manner, which is not possible to replicate with normal bits and their independent states. Leveraging entanglement allows the parallel processing of multiple possible solutions to a posed problem statement, offering a potential speedup in computation. [11, p. 111-118] [15, p. 21-23]

In opposition to the new applications and benefits quantum mechanics offers for computing, they also introduce new challenges that impede the implementation of quantum computing. Denoted as quantum decoherence is the process by which qubits lose their superposition state, primarily due to interaction with their external environment. This phenomenon effectively erases the quantum information stored in the qubits and thus nullifies the advantage granted over classical computing. A major point of interest in the research and development of quantum computing and driver of progress in computational power is the limitation of quantum decoherence. [11, p. 277-283] [15, p. 567-573] [17, p. 1-4]

2.2.2 Quantum algorithms of interest

With the new theoretical foundation of quantum computing, algorithms have to be developed or adapted to utilize the described advantages of quantum bits. The computational approach to solving problems has to be adjusted to take the superposition property into account to gain the potential processing speedup compared to classical computing. Two prominent quantum computing algorithms are important in the context of this thesis—Peter Shor's algorithm and Lov Grover's algorithm.

In 1994, mathematician and computer scientist Peter Shor presented an algorithm that could find the prime factors of large numbers in polynomial time and thus faster than any other algorithm on classical hardware. Shor's proposed algorithm would theoretically outperform any algorithm or brute-force search on a timescale magnitudes smaller than previously thought possible. Through the use of quantum phenomena like superposition and entanglement, Shor implicates a revolutionary step in the execution of computational power. With the capabilities of parallelization of operations and simultaneous exploration of possible solutions, a solution to the mathematical problem of factoring could be found in a practical time frame with a feasible expenditure of computational effort, unachievable by classical computers. This theoretical concept had a major impact on the perceived utility of quantum computers, presenting a case for the usefulness of the field of quantum computing and driving research and development efforts in the field. [2] [6, p. 502-503] [18]

To this date, the largest number Shor's factoring algorithm could be executed on, was $N = 21$. This was demonstrated in 2021 on a 5 qubit quantum processor, serving as a proof-of-concept for the viability and correctness of Peter Shor's work. [19]

The second important quantum algorithm was developed by Lov Grover in 1996. Grover's quantum search algorithm for unstructured search problems obtains a quadratic speedup in comparison to classical algorithms. The unstructured search problem describes the process of finding a solution in the range of a solution space. In comparison to a simple linear search which would try every possible solution in the process, Grover's algorithm only requires the square root number of operations. This, although significantly smaller speedup than Shor's algorithm offers, is applicable to solve a wider range of problems, illustrating the ability for quantum computing to optimize general search problems. [11, p. 38-39, 248] [20]

2.2.3 Current quantum computing capabilities

Extending the foundation of quantum algorithms laid out by Shor and Grover, further research has changed the assessment of the feasibility of computationally hard problems. The continued research and development in quantum computing has brought additional quantum algorithms and applications, illustrating the increasing viability and potency of quantum computing. Demonstrating this progress is the work by Farhi and colleagues in the domain of general optimization problems with their *Quantum Approximation Algorithm (QAOA)* [21] [22, p. 68-75] and various publications on the application of quantum computing in the field of machine learning [22, p. 130].

The advancements of quantum computing have not been constraint to just theoretical research. Shifting focus to the practical implementation of quantum computing theory, an equally rapid—if not greater—scale of progression can be observed. An important showcase of the viability and prowess of quantum computing was achieved in 2019 by the software and information technology company Google. Unveiling its *Sycamore* quantum processor and accompanying statements of computational ability, Google claimed to have reached a significant milestone in the 'quantum advantage' (formerly referred to 'quantum supremacy') over classical computing. This was demonstrated in the execution of the computational task of the random sampling problem, with their quantum computer completing the task in 200 seconds. A task which would be claimed to have taken approximately 10,000 years to complete on the most powerful classical supercomputer available at the time. [23]
A claim that subsequently has been subject to controversy. Critics, including researchers from the software and information technology company IBM and competitor in the field of quantum computing, claimed an overexaggeration of the advantage Google achieved. They suggested that the time this task might be accomplished by a classical computer would be much shorter than Google estimated, cutting the time from millennia to potentially a couple

of days. A difference in asserted advantage to the scale of magnitudes less, however, still representing a stark contrast of computational power between quantum and classical computing. [24]

To further ascertain the current possibilities and practical implementations of the theorized algorithms, the available hardware of quantum computers should be discussed. The number of advancements and improvements over the last years show a trend of progression that should be considered in the evaluation of future quantum computing power. To get an understanding of the current level of quantum computing power, the hardware of two already named actors in the field will be discussed: Google and IBM. This does not diminish the importance of other projects and research initiatives contributing to the field but serves as a benchmark of the current landscape of quantum computing hardware.

An important contributor to the field of quantum computing hardware is the information technology and web service provider Google. Interested in amplifying their own computing power and capabilities as well as providing quantum computing as a service to outside customers, Google has dedicated resources to researching quantum computing and developing its own quantum hardware [25]. As mentioned before, in 2019 they demonstrated their quantum processor Sycamore with 53 qubits [23]. In 2023, they announced an improved 70 qubit version with additional improvements in noise reduction, resulting in a monumental improvement of 241 million times compared to Sycamore-53, in the specific task of random circuit sampling [26]. As described in chapter 2.2.1, quantum decoherence is a major point of hindrance in the practical implementation of quantum computing hardware and thus not just the addition of qubits, but also the reduction of quantum noise contributes to the computational power of a quantum processor.

The quantum computing branch of the information technology company IBM continuously contributes to the progress in quantum computing in research and development of quantum computing hardware. One of its last released products is the *Condor* processor formerly showcased in December 2023 sporting a number of 1,121 qubits in its integrated circuit [27]. This is following a sharp developmental timeline of ever more powerful quantum processors, with Condor succeeding the 433 qubit processor *Osprey* from November 2022, the 127 qubit processor *Eagle* from November 2021, the 65 qubit processor *Hummingbird* from 2020 and the 27 qubit processor *Falcon* from 2019 [28] [29]. This already evidently shown trend of increasing quantum computing power is reinforced by the companies own statements regarding future products in their development roadmap, showing plans to integrate multiple quantum processors in one system [27] [30].

Looking at the presented developments, one can reasonably infer an increase in quantum computing power in the future. The multiples of power expansion have been shown in only a few years of time and statements from manufacturers seem to indicate a continuation of this trend, although an inherent bias needs to be taken into account. The chaotic nature of rapid advancement makes in difficult to give an exact prediction on what level of computational power and importantly computational power in which specific task or problem will be reached.

The current advancements signify a shift in the quantum computing discussion from theoretical possibilities to practical applications. The ongoing developments of quantum algorithms and their applications in areas such as optimization problems and machine learning illustrate the growing maturity of quantum computing technology and its potential to innovate various aspects of computation and data analysis. In the realm of computer science and technology, quantum computing marks a pivotal new computational ability that challenges previous assumptions on computational limits. It opens the possibilities of solving traditionally computationally hard problems with an advantage of often orders of magnitude compared to classical computing. Limited through the complexity of hardware and software the specialized quantum computing hardware will not serve as replacement of our general classical computing hardware but augments computation as an additional separate resource, that—when applicable—can produce an extreme amount of computational power. With regard to the topic of this thesis, the new resource of quantum computing has grave implications for the field of cryptography, which will be discussed in the following chapters.

2.3 Intersection of cryptography and quantum computing

Central to the discussion of this thesis is the intersection of the two previously described fields of cryptography and quantum computing. The resource of quantum computing enables a new processing capability of previously thought hard-to-solve computational problems—a factor that grants modern cryptography its security and thus the there are immense implications for current cryptographic standards and practices.

To evaluate the implications, three distinct but dependent points of interest can be identified. Starting with the direct impact of quantum computing on so far identified properties of cryptography first. Having identified this point, its downstream dependencies are affected by necessity and thus follows second the question of impact on the field of cybersecurity as build upon the qualities of cryptography. Third, followed to its logical conclusion, the impact on real-world elements that are depended on the field of cybersecurity.

2.3.1 Impact of quantum computing on cryptography

As described in chapter 2.1, modern cryptography is built upon the complexity of calculations or mathematical problems and an order of specific operations. To encrypt or more importantly decrypt information, a specific key is necessary as said cryptographic schemes take a key as the basis for their mathematical operations. The security of the cryptographic scheme is derived from the difficulty of obtaining said key through the deconstruction of the encryption process. Cryptography locks information for anybody who is not in possession of the specific key that fits in the lock. Continuing the physical analogy, the reversal of the key-generation process is the breaking of a cryptographic encryption scheme as it takes the lock and calculates the size and shape of the corresponding key without any additional information about it.

In the RSA public-key encryption scheme, as described in chapter 2.1.3, two secret prime numbers are used to generate the private and public-key. To illustrate the general operating principle, it suffices to say that the public-key is generated by multiplying these two prime numbers. Given only the public-key, one would have to find the factors that make up the public-key to find the original prime numbers and regenerate the corresponding private-key. The difficulty of factoring a number depends on its size, with larger numbers being harder to factor. The computational effort needed to break the RSA encryption in this manner is for all intends and purposes deemed unsolvable by all current classical computers. [6, p. 331-336] [11, p. 640-644] [12]

The in chapter 2.2.2 described quantum algorithms challenge this assumption of computational unfeasibility. Shor's algorithm greatly accelerates the computational speed at which the mathematical problem of factoring for any number can be solved. The shift in the order of magnitudes of computational effort necessary to solve this mathematical problem changes the status of cryptographic security, as it nullifies the underlying complexity of the encryption scheme. As all widespread public-key encryption schemes in use today rely on this category of factoring and computing discrete logarithms mathematical problems, it follows that all public-key encryption schemes, i.e., RSA, *DH (Diffie-Hellman), ECC (elliptic-curve cryptography)*, are vulnerable to quantum computing. [6, p. 502-503]

In contrast to the stated inherent vulnerability of asymmetric-key encryption, the impact on symmetric-key encryption appears to be negligible based on current assumptions. The quantum algorithm by Grover, described in chapter 2.2.2 offers a quadratic speedup over classical algorithms in finding the private-key. Grover's algorithm is rated to be optimal in this circumstance, and no better quantum algorithm is possible. The speedup granted by Grover's algorithm translates to an effective halving of encryption key length if one compares the execution time of exhaustive search on classical and quantum computers. Logically, it follows that doubling the key length will grant the same level of cryptographic security between the threat classical computers pose now and a quantum computer able to execute Grover's algorithm. [6, p. 500-502]

2.3.2 Impact of quantum computing on cybersecurity

To elaborate on the previous point of impact discussion, the next logical step has to be considered in the evaluation of quantum vulnerability. Given the fact presented in chapter 2.3.1 regarding the vulnerability of public-key encryption to quantum computing, the downstream effects on the more macroscopic scale of cybersecurity need to be analyzed.

In general, cryptographic schemes are not invincible and do get broken as time goes on. Be it through assumptions about the process reducing the number of guesses needed to solve the encryption or the available computing hardware reducing the time for trying different keys from unfeasible to feasible. A combination of both factors is usually the case. Any time this happens, a change of cryptographic algorithm used is needed, to maintain the privacy of information, resulting in a migration to a different cryptographic standard. [14, p. 4-5, 12–17, 36–42, 80–82, 94]

Public-key encryption schemes are used as the standard that governs the secrecy of data exchange over an open channel [6, p. 385-386, 396–399] [14, p. 87-96]. Self-evidently, this would encompass any and all data passed through said channels, as the data-messages are encrypted with a shared cryptographic scheme. Further illustrating the possible implications this includes, for example, personal information and communication, personal data uploaded to the online cloud but also business communication, customer information, trade secrets, research and development data, financial data and transactions, as well as governmental services and information, tax information, sensitive diplomatic data, military data and communication—anything and everything that is exposed to an open network infrastructure like the internet where public-key encryption is used to secure the privacy of data exchange [14, p. 87-96] [31]. As public-key encryption is the foundation on which a secure channel is established, it also represents a single point of failure in the event of a cryptographic breach—even if it is only used to set up a different cryptographic encryption method. As described before in chapter 2.1.3 the RSA encryption currently does have no major vulnerabilities exploitable with classical computing capabilities despite its ongoing decades long service life and thus represents a sensible option to use as a cryptographic foundation securing the exchange of all types of sensitive data stated above.

Peter Shor introduced a theoretical concept of an algorithm capable of breaking factoring-based encryption schemes in a very short amount of time through the use of quantum computing. The mathematical concept of factoring is the underlying problem, resulting in a complexity that classical computer can not feasibly solve. Although it proved the underlying security assumption of the scheme wrong, a practical implementation was not possible at that time, as it hinged on the execution on a powerful enough quantum computer. Certainly at the time of publishing in 1994, the timeline of quantum computing and also the development of the internet were uncertain. With the advancement of quantum computers not only in theoretical concepts but also in practical developments, the procedure laid out in Shor's paper is no longer just is theoretical nature. So far, no quantum computer exists powerful enough to execute Shor's algorithm on a practical application scale, but the multiplication of processing power of quantum computers in recent years, as described previously, points to a breaking point in the nearer future. Estimations reach from the end of the 2020s up to the 2040s, with a cautious consensus around the early 2030s [1, p. 4-5, 17, 35].

Following this logic, in the past and currently, quantum computing has no immediate and direct impact on cryptography and therefore cybersecurity. But with the pace of advancement in the field of quantum computing, reaching the quantum computing capability needed to execute Shor's algorithm and breaking known public-key encryption algorithms is considered an inevitability. In the last years, the progression in quantum computing development is consistent and rapid, closing the computational difference to a possible execution. As Shor's algorithm has already been executed on a very small number, it has been proven to work in practical implementation.

The internet and every organization, service, and data point connected to it is relying on the secure nature of communication and transmission of this data. The described presumed security of RSA and its already long service life has led it to be one of the prominent standards for any public-key encryption usage, such as in the *SSL/TLS* protocols securing internet communication in the *HTTPS* protocol [31]. Emergent from that, the scale of effect on every part of this system, all connected systems and thus on every part of our lives would be considerably. Not only is the number of systems using the internet and this kind of cryptography immense, but given the described associated information and operations, the function is critical for our society. Consequently, the implications of a broken RSA encryption are considerably severe.

Reaching the breaking point of the current public-key encryption scheme by no means is just a black and white event. The danger of a broken cryptographic algorithm used, presents itself as the unauthorized access of data from malicious actors. So far, the number of actors in the field of quantum computing is manageable, and any involvement is only possible with the access to highly specialized knowledge and engineering capabilities. The breaking point signifies that at least one actor and one quantum computer exist that are capable of execution Shor's algorithm to the intended capability. This would inherently mean that the security of the cryptographic scheme is no longer ensured.

In practical terms, this does not necessarily mean the encryption scheme is worthless in its entirety, since presumably only one actor has the ability to decrypt data not addressed to him. But it is a signal that the capability of decryption is achievable and could spread to different actors in the following time, although be it restricted by the complex nature of engineering necessary in building quantum computers. Once this point is reached, there are no certainties of who and when any malicious actor gains this capability, meaning that going forward one has to regard any use of the encryption scheme in question as insecure and negligent. Cybersecurity is severely impacted by quantum computing through the described breach of public-key encryption cryptography. Public-key encryption algorithms are essential to the concept of cybersecurity and its purpose to secure the privacy of data and especially data exchange.

Harvest-now-decrypt-later attack

An additional element to the already stated danger of outright breaking the currently widespread public-key encryption, when a powerful enough quantum computer will be developed and constructed, is a harvest-now-decrypt-latter type of attack [1, p. 4, 26]. As the name implies, an attacker would harvest any data of interest to him now in the current time, even if he presently has no possibility of gaining any information of this encrypted data. But because he is certain that the encryption used will be broken later, he can wait until said time and then decrypt the data he has stored. This type of attack—while simple in concept and execution—may not an attractive way of trying to gain sensitive information. Depending on how broad or narrow his interest is, he has to store the intercepted communication for a maybe unknown amount of time and take up storage resources for the duration. Adding to this, it is usually not known if or when any cryptographic algorithm will be broken, making this kind of endeavor very uncertain in terms of results. [32]

In the case of factoring-based public-key encrypted data, this still applies. What is changing and increasing the likelihood and thus the danger from this attack is the certainty of breaking this type of cryptographic algorithm in the near(er) future. The timeline of development of quantum computers becomes clearer with each iteration and new release of more powerful quantum hardware. Any attacker can infer a general timeline of a probable breaking point from these developments and public estimates of quantum computing associated institutions—but that this point will be reached seems inevitable. Given the circumstances and the more open academic discussion on the quantum vulnerability of current asymmetric cryptography, a level of public certainty is granted to the breaking point of current public-key encryption which in turn reduces any stated negatives of this type of attack, leaving only the binding of storage resources. [32] [33, p. 3-4]

This point considerably enhances the danger associated with the quantum vulnerability of public-key encryption. With the prominence the encryption scheme is used now and the relative certainty that a powerful quantum computer will probably exist in the next 10 to 20 years there is an absolute incentive for malicious actors to store anything and everything that could be of interest even if the information can only be accessed in a decade's time. [32] [33, p. 3-4]

Current and future capabilities for big data storage and computation

In connection with the previously discussed harvest-now-decrypt-later attack and associated with the feasible assumption of such attack is the assessment of current and future big data storage and computation capabilities. Given the public-key encryption protected domain of the internet, a potential target for malicious actors could be the traffic over said network. For an attacker, a potentially interesting textual data point could only be a few kilobytes in size, but without having previous knowledge isolating this data in the communication, all surrounding traffic would have to be saved as well. The exact way of obtaining the networking traffic is not relevant for the discussion of this thesis, and we will therein assume an attacker having this capability. A significant number of factors contribute to the difficulty and effort of executing such an undertaking, depending on the target and their behavior. Once the capability to wiretap is established by an attacker, the main limitation is the storage capacity for intercepted traffic.

To evaluate the possibilities related to the harvesting of data, it is important to understand the orders of magnitude of data and the logistics they imply. The table 2.1 shows the units of measurement of data in relation to the foundational element of data representation of classical computing: the bit.

Bit	1 Bit
Byte	8 Bits
Kilobyte	1,024 Bytes
Megabyte	1,024 Kilobyte
Gigabyte	1,024 Megabyte
Terabyte	1,024 Gigabyte
Petabyte	1,024 Terabyte
Exabyte	1,024 Petabyte
Zettabyte	1,024 Exabyte
Yottabyte	1,024 Zettabyte

Table 2.1: Units of measurements for data. [34]

Quantifying the data exchanged through the internet network is not straightforward as the global network involves distinct countries, organizations, businesses, and network providers. The information technology and communication company Cisco aggregated available sources and tried to compile an estimation of the global internet traffic in their annual *Visual Networking Index (VNI)*. Their last estimate of global internet traffic for the year of 2022 quantifies it at 396 EB (Exabyte) per month or 4.8 ZB (Zettabyte) annually—equal to one trillion gigabytes [35, p. 1]. This would represent a threefold increase in a 5 year timespan from 2017. This translates to a monthly internet traffic of 50 GB per capita [35, p. 1].

Putting this in context, the market research company IDC has quantified the global installed base of storage capacity in 2020 at 6.7 ZB with a forecasted growth to 14 ZB in 2025 [36]. This includes all possible storage capacity in any device—from data centers to small IoT devices. There is no differentiation between used and unused storage. Assuming that all in 2025 predicted storage capacity could be utilized in a harvest-now-decrypt-later style of attack, it would only be possible to store roughly three years of global internet traffic, assuming no growth in global internet traffic has taken place since the 2022 estimate. The self-evident impossibility of the stated scenario narrows the upper end of the possible scale down considerable. Even for more differentiated geographic regions the numbers seem improbable: Cisco's VNI estimates, that the North American region's internet traffic to have reached 108.4 EB monthly or $\sim$ 1,300 EB/ 1.3 ZB annually [35, p. 3] and the Western European region's internet traffic to have reached 49.9 EB monthly or 598.8 EB annually by 2022 [35, p. 3]. Keeping the same incoherence between the time frame of the estimations, it would still predicate that an attacker would have control over a significant portion of the global storage capability.

Nonetheless, between the indiscriminate total collection of traffic and a single human target exist a probable case of opportunity and feasibility. As of April 2024, the starting price of hard drives in Germany is around €16 per TB/ €0.016 per GB (on 16/18 TB hard drive models) on consumer storefronts [37]. Taking the 2022 estimate of 50 GB of traffic per month, per capita, this translates to a price of €0.80 (80 cents) for the storage of an average amount of traffic of any individual per month or €9.60 per year. Relating to this number is the question if an attacker, in a months time, could extract information worth 80 cents from any individual to make this endeavor economically viable. This simple calculation by no means encompasses all associated factors, like accommodating physical space for the storage hardware, electricity costs, logistical scale limitations, hard drive lifespans, etc., which would contribute to the economic evaluation of this type of attack but gives a baseline of understanding to the economics of scale involved. Any major advancements in data storage technology in the following years could also further decrease costs and increase the viability of this attack as long as the cryptographic quantum vulnerability persists.

Going forward with the established general magnitude of cost, it follows that all the personal interaction through the internet from a single person could be the subject of interest and would certainly be economically viable even for a small-scale operation. The extrapolation of this to a longer time frame would just be a question of economic and organizational ability of the attacker. On the individual scale, the mentioned use-case is feasible and trivially easy given all the stated assumptions. The lower boundary for this type of attack is therefore established and together with the established upper boundary informs potential threat scenarios. The danger for any entity, be it a private individual or an organization, depends on one's estimate of its most capable possible attacker and from there derive the possibility if their own data may be subject to such an attack. In this analysis one should factor in all possible actors from self-interested private individual attackers, hacking groups, commercial organizations, infrastructure operators, data-oriented IT businesses to state actors and agencies.

Illustrating the last point were the revelations of former USA National Security Agency (NSA) employee Edward Snowden. Snowden shared rare insights in the conduct and capabilities of such a state-sanctioned agency with the mandate and funding to carry out wide-ranging surveillance operations. Under the top-secret program called Prism, the NSA organized its capability to access systems, servers, and traffic of major software and information technology companies like Microsoft, Google, Meta (formerly known as Facebook), Apple and others. With the alleged cooperation of the listed U.S. firms, any communication-data of users would be subject to access and surveillance by the state agency if requested. Different from the in this thesis discussed vulnerability to quantum computing, the cryptographic security did not have to be broken, as the described ability to compel one side of the cryptographic relationship to provide access was sufficient. [38]

With the overall information on tools and programs that were leaked, one can infer the scale of this institution and the execution of its mandate. To calculate if an individual, a business, an organization, a state is subject to this level of potential scrutiny, one has to know the intentions of the attacker and the value of information the target possesses. In light of the revelations provided by Snowden dating back to 2013, it seems highly unlikely that there would not be a powerful enough malicious (from the viewpoint of a cryptographic attack) actor that would pass on the ability to gain uninhibited access to data communication even if delayed by years or decades.

Disregarding any possible knowledge an attacker might have to pinpoint valuable information from the heap of collected traffic, one could assume to be protected by the amount of assumingly uninteresting data hiding anything of importance, thus making any attacker search for the proverbial needle in a data-haystack.
The field of Big Data engages with the subject of data processing and analysis for (relatively) large amounts of data. It aggregates and provides tools and techniques to organize and extract information from large amounts of unsighted and unorganized data, and therefore would have equal applicability to the described circumstances of a harvest-now-decrypt-later attack. Interactions through the internet often have a pattern of communication style and content that is shared across the network. Any information regarding the types of traffic is thus directly transferable to a different set of traffic, reducing the number of unidentified categories of data. This process of data mining would also be applicable to sort through still unknown traffic types to identify patterns and relationships. Although providing an obstacle related to the computational effort and some unpredictability, any obfuscation through quantity of data can not be considered a reliable measure of information protection. [39] [40]

Another challenge to the assumption of quantity obfuscation are new emerging technologies of Large Language Models (LLMs), also currently colloquially described under the umbrella of artificial intelligence (AI) [41]. LLMs posses the ability to understand natural language at an unprecedented level, gaining attention as a breakthrough in computational and AI research [41] [42]. Prominent LLMs are the AI company OpenAI's *GPT* models as well as its *ChatGPT* service [43], Google's *Gemini* (formerly known as *Bard*) [44], Meta's *Llama* [45] and Anthropic's *Claude* [46]. These models are regarded to have a better ability to process large amounts of data than traditional big data methods, as they possess more innate knowledge through the LLM's training and thus are able to understand and in turn organize data more efficiently [41] [42]. The same capability of LLMs can also be used to extract information from data, as they possess the ability to synthesize natural language, making communication with the LLMs possible [41] [42].

In the context of the previously described timeline of quantum computing, it is important to recognize that this only represents the current state of AI capabilities. As the analysis of data from harvest-now-decrypt-later would only take place after the encryption would be broken with a powerful enough quantum computer, there still is time for further development and improvement of LLM or other AI capabilities.

2.3.3 Real-world implications

The next important factor in the evaluation of the danger of the quantum vulnerability are the downstream effects based on the previously described impacts on the cryptography and consequently cybersecurity. With two degrees of separation, the evaluation of impacts on real-world elements, downstream from cybersecurity, is a predominantly theoretical analysis that relies on logical cause-and-effect relationships. As there are no direct comparisons available of cryptographic vulnerabilities of this scale and widespread in any modern environment, definitive claims about probable effects are difficult to make. The evaluation thus has to rely on assumptions made based on current implementations of public-key cryptography and resulting foreseeable consequences if said encryption would become insecure. As this discussion predicates any call to action for a potential cryptographic migration, it has a degree of inaction to the stated danger built-in to simulate the effects if no recourse is taken.

The following domains will be discussed separately: governmental institutions, critical infrastructure and industry.

Governments and governmental agencies

One major potential target is governments and its institutions as the governing power of any nation and therefore in charge of its society. As established in chapters 2.1 and 2.3.2, public-key cryptography is ubiquitously used in nearly all points of communication on a network-like infrastructure, which of course includes the internet. All communication would be subject to potential decryption in the event of a breaking point being reached, which would have far-reaching consequences for any administration and the national security it guarantees. A complete analysis of all possible effects and resulting chain-reactions is not possible in the scope of this thesis. Only the major points of interest in connection with governmental danger will be discussed to illustrate the magnitude of scale of potential effects of quantum computing.

Secrecy of information is used to avert potential bad effects from adversarial actors gaining said information and having the ability to act on it or gain an advantage over the other party. To govern the information space, governments usually have systems in place for the categorization of information and knowledge as to remain in control of access and secrecy over them. A prominent categorization of information to ‘classified’, ‘secret’ or ‘top-secret’, etc. is used to describe information that is restricted to certain actors. With the gradual transition to digital systems, so did classified information transition to data that in turn also gets communicated over network infrastructure like the internet. As described in chapter 2.1, cryptography is the tool to conceal information and data from unwanted access. The direct inherent consequence of the public-key quantum vulnerability is the compromise of communication, which includes any sensitive information. Cryptography ensures security of communications pertaining to diplomatic matters, military operations, and national intelligence. Privileged communication between members of governing bodies like a parliament or ministries, leaders and decision makers in the administration, but also between governments, can contain highly sensitive information that once exposed could influence the sovereignty of the state. The decryption of these types of communication could lead to geopolitical instability and even conflict. [47] [48] [49]

Confidential data that is routed through systems connected to publicly accessible networks is at risk. This would contain data from ministries and governmental services, implicating personal information of citizens and their affairs with the government, which could be subject to exposure. Intelligence agencies and their operations rely on a high level of secrecy, which in the instance of public-key encryption could not be enforced anymore as this encryption methods is potentially insecure to outside attackers. This would extend to the collection of intelligence and sharing of information, disrupting the nation’s capability in intelligence operations and compromising the threat awareness. The origin or identity of intelligence sources would be at risk of exposure if any trace could be found in the compromised data. A fundamental building block of a nation’s ability to enact secrecy in governance, law enforcement and intelligence operations would be broken. [48] [49] [50, p. 1-8]

This problem also extends to the nation's military forces. The management and collection of information has equal application as described before, as the operation of military forces is influenced by the protection and secrecy of information to gain an advantage over potential enemy forces or foreign adversaries [51]. The political and military alliance North Atlantic Treaty Organization (NATO) has identified data exploitation as the fundamental element of every operation in the alliance and sets the importance of "information superiority and data-driven decision making" [52] as a key resource. The stated goal is to move NATO to a "data-centric organisation" [52] further highlighting the priority of digitization of military operations. The process of digitization of military hardware is increasing the interconnectivity of systems and the exchange of data [53]. While these combat-related systems usually do not rely on the same communication networks as civilian applications, the same cryptographic circumstances of quantum vulnerability still apply if an attacker can intercept any communication [54]. They still present a potential target, depending on the attacker's ability and the specific cryptographic foundation of communication. The advantage gained over an enemy through cryptographic compromise was showcased in the break of the German Enigma encryption in the second world war, which gave the Allied powers the ability to gain information on future orders and military operations, especially in the context of (preventing) German U-boat attacks in the Atlantic [10]. Although not comparable to modern times in scale and integration of digital system, any compromise of military secrecy implies similar results. The ability of a nation to defend its state and sovereignty could become compromised, which poses a danger to the existence of the state itself.

An example of this kind of incident, that could occur in a compromised environment, was the public release of a recording of a digital meeting between high ranking military officials of the German Bundeswehr at the beginning of March 2024 [55] [56]. In this call, a discussion was held over the availability of 'Taurus' cruise missiles and potential associated logistical challenges of transferring said weapon system to the country of Ukraine as military assistance in the ongoing conflict with Russia. The content of the call contained not publicly known properties of the weapon system, its capabilities and the capabilities of the German military. In addition, the previously unknown presence of military personnel of fellow NATO alliance members in Ukraine was acknowledged. Next to the disclosure of military secrets, it also impacted the domestic and international political landscape, as the potential delivery of this specific weapons system ran contrary to the publicly stated position of the German government at the time [56] [57]. To be explicitly clear, the cause of this leak, as publicly known so far, does not seem to be because of a direct decryption event in the manner described in this thesis but a failure of configuration and negligence [58]. It does provide a recent real-world example of possible consequences of compromised government secrecy that could potentially occur with cryptographic quantum vulnerability. Just this one specific instance of compromised security influenced national politics, challenged the public's trust in government, stifled diplomacy efforts, and exposed concrete military capabilities. Extending this scenario to the described unrestrictive nature of a complete decryption of all quantum-vulnerable data and communication would accordingly lead to more extensive repercussions.

Critical infrastructure

The umbrella term of critical infrastructure unites aspects of function and utility that are regarded as fundamental and essential to the functioning of society [59] [60]. This includes public utilities like water, electricity and natural gas as indispensable resources but also the provision of healthcare and public safety. Regardless of public or private ownership, the disruption of any of these services would have devastating effects on the economy, public health and national security [61]. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has identified 55 critical functions in their "National Critical Functions Set" [60], which include the following:

- ***Connect***
  - *Operate Core Network*
  - *Provide Internet Based Content, Information, and Communication Services*
  - *Provide Internet Routing, Access, and Connection Services*
  - *Provide Positioning, Navigation, and Timing Services*
- ***Distribute***
  - *Distribute Electricity*
  - *Transmit Electricity*
  - *Maintain Supply Chains*
  - *Transport Passengers by Mass Transit*
- ***Manage***
  - *Develop and Maintain Public Works and Services*
  - *Enforce Law*
  - *Provide Medical Care*
  - *Provide Public Safety*
  - *Operate Government*
  - *Perform Cyber Incident Management Capabilities*
  - *Protect Sensitive Information*
  - *Provide and Maintain Infrastructure*
- ***Supply***
  - *Generate Electricity*
  - *Supply Water*
  - *Produce and Provide Agricultural Products and Services*
  - *Produce and Provide Human and Animal Food Products and Services*
  - *Provide Metals and Materials*
  - *Produce Chemicals*

The energy infrastructure is in a sensitive spot that almost every part of the identified critical infrastructure relies on, and thus is of utmost importance. These energy related services rely on secure communication for the control, maintenance, and data transmission for critical parts of their operation. As described before, the danger of cryptographic quantum vulnerability could compromise digital communication channels to outside attacks. The exposure to adversarial actors could lead to exposure of information regarding the structure and condition of a nation's energy infrastructure. A loss of control over the operations of any of these services could lead to limitations, or worse, a complete termination of energy supply with potentially catastrophic downstream effects. [59] [62]

Industry

The industry as part of this thesis is categorized as all business and commerce activity taking place, which are contributing to a country's economy. Businesses and organizations part of the industry provide goods and services but also jobs and salaries, giving momentum to the economic exchange cycle [63]. All while the stimulated economic activity provides tax money going to the state to be spent on governmental services and projects. This capitalistic system of economic organization is practiced in some form in most country worldwide, where demand and supply dictate the price and flow of goods, while the capital is allocated freely by independent actors [63]. In this context, the susceptibility to disruption is important to consider. Once a significant disturbance is caused, a chain reaction could cause an economic downturn with fewer goods produced and sold, less spending power gained by employees to unemployed with less tax income for the state and possibly an increase in social security spending [64].

As well as the government, the industry can also be affected by quantum computers breaking currently used encryption schemes indirectly, by means of the prior mentioned situations like the supply of materials and energy, but also directly as the sole target of an attack. As an individual business, all of this is dependent on the use of public-key cryptography in their operations. With any kind of network or internet activity, be it with suppliers, customers or just employees needing to use the internet for their work, one becomes vulnerable to attacks on their cryptographic algorithms as described in previous chapters 2.3.1 and 2.3.2. In every case forward it is important to remember that two types of attacks are possible: using quantum-vulnerable cryptography after a breaking point has been reached, making it possible, that anybody with a powerful enough quantum computer can decrypt your communication—and the harvest-now-decrypt-later attack which will save your data and communication from any point before the breaking point in anticipation of decrypting it later on, which would make even all the time before reaching a breaking point potentially dangerous.

As well as in all other scenarios mentioned, the communication with all business relationships would be at risk of exposure. That includes customer information and what dealings they have with a business and all other businesses as well as suppliers a business is working together with. Breaching internal communication not directed at the customers, e.g., prototyping or testing data showing unfavorably result for a product (even if the product would not be released in that form), market research and concepts on marketing and pricing, could be devastating in trust and goodwill build up by a business. The same change in perception, as well as legal challenges, could arise from breached customer information, e.g., identifying information like addresses and phone numbers. Losing payment information would also be a case in which the image of a business could be damaged. In domains like healthcare, this could lead to breaches of individual privacy on the most sensitive level. [65] [66]

Not just the customer-facing side of a company would be at risk. Internal processes and institutional knowledge are often factors that differentiate businesses and give them the ability to deliver unique selling points. Research, development, and engineering operations are driving the product development forward, all of which are part of the business secret. In the domain of information technology, often the product itself is the software built from the business's institutional knowledge. Just as before, if any of these steps involve the communication over the internet, an attack would be possible. With a harvest-now-decrypt-later attack, the same economics around recording and storing traffic data apply as they would with an individual person. The feasibility depends on the size of business operation and the capabilities of the attacker, but are to some degree always possible, even if just in partial. Corporate espionage would be driven by rivaling companies or even governmental actors from adversarial countries. [65] [66] [67]

2.4 Related work

The discussion of approaches to alleviate the threat posed by quantum computing is built upon the concept of cryptographic migration as described in chapter 2.1.5 in connection with quantum-safe cryptographic alternatives. Despite the at this point decades old publications of Shor and Grover, the practical implementation of their theoretical work has only been potentially made possible with the more recent developments in quantum computing described in chapter 2.2.3. The academic research and discussion around the topic of the impact of quantum computing on cryptography is resultingly lagging behind in the exploration and research of the implications this would pose. Especially the domain of migration to quantum-safe cryptographic alternatives is currently left relatively unexplored with only few publications having relevance to the strategic approach of the application of new quantum-safe cryptographic algorithms to the current environment or even cryptographic migration in general. With the focus of this thesis on the handling of a cryptographic transition to preempt the breaking of current public-key cryptography, this leaves almost no related academic work that further research could be founded upon.

This thesis identified two publications that are directly or tangentially relevant to the posed topic of discussion. One of the first academic contributions to the general field of cryptographic transition strategy is the 2006 paper "Cryptographic transitions" by Stapleton and Poore as part of the IEEE Region 5 Annul Technical Conference proceedings [13]. They describe a general approach to cryptographic transitions on an organizational level above the technical implementation details and thus provide a first basis of discussion on how any cryptographic migration could be planned and organized despite not being adapted to the current problem of quantum vulnerability. The second and directly applicable publication is the article "Transitioning organizations to post-quantum cryptography" by David Joseph and colleagues, published in May 2022 in the prominent *Nature* journal [68]. It similarly describes the danger of new quantum computing resources to current cryptography, as done in this chapter, and it prescribes some general actions or concepts that can be adopted to make a cryptographic transition process possible.

2.4.1 Stapleton and Poore: Cryptographic transitions (2006)

An early contribution to the organizational aspect of the domain of cryptographic migration was done by Stapleton and Poore in a paper published as part of the IEEE Region 5 Annul Technical Conference proceedings in 2006 [13]. Their observations and consequent recommendations can serve as a confirmation of observations regarding the general inevitability of cryptographic scheme compromise, as described earlier, and guide the development of a strategic approach to quantum-safe cryptographic migration.

The authors start by grouping the emergent cryptographic vulnerabilities into three categories: "Key Life Cycle", "Algorithm Life Cycle", and "Product Life Cycle" [13, p. 22]. These distinctions were built on the historic observation of continued developments of computational power diminishing the security through complexity aspects of cryptographic algorithms as well as additional cryptanalysis through new techniques in computer science and mathematics making cryptographic algorithms and products obsolete, which they express in life cycles [13, p. 22-24].

Stapleton and Poore make several assertions about guiding principles that would lead to a successful planning and execution of a cryptographic transition. The following list extracted from their paper shows the leading points they discuss as part of their approach to cryptographic migration [13]:

- ***Transition Principles***
    - *Business Requirements*
    - *Cryptographic Hardware*
        - *Tamper Resistant Security Module*
        - *Interoperability*
        - *Reliability*
        - *Certification*
    - *Application Management*
        - *Algorithm Independence*
        - *Security Architecture*
        - *Enterprise Management*
        - *Security Guidelines*
- ***Transition Process***
    - *Vulnerability Assessment*
    - *Impact Analysis*
    - *Implementation*
    - *Reconciliation*

First, they assert the necessity to for every project to take note of technical and operational goals and state the underlying business goals [13, p. 24]. The second principle the authors discuss is the necessity for dedicated cryptographic hardware, as opposed to executing cryptographic algorithms on general purpose computers [13, p. 24-25]. While in theory a legitimate technique to shield the cryptographic implementation from tampering and unauthorized access it neglects the current prevalent setting of software implemented cryptography, which also in general is not applicable to the software resources this thesis discusses in connection with public-key encryption. Under this second principle of cryptographic hardware they also list additional related concepts such as the use of “Tamper Resistant Security Module”, “Interoperability”, “Reliability” and “Certification” [13, p. 25]. The Tamper Resistant Security Module is described as “[...] a high degree of assurance that the product is free from defects or malicious attributes such that its security features and mechanisms resist accidental and malicious attacks, both physical and logical attacks, throughout the product’s life cycle.” [13, p. 25]. The resistance of hardware to tampering in the context of cryptography and security is certainly an important requirement that is always applicable regardless of context. With the Interoperability concept, the authors prescribe that products should share the cryptographic standard with other products to assure compatibility [13, p. 25]. Reliability prescribes that manufacturers have to “[...] employ quality assurance standards, trusted engineering techniques and verifiable project management controls across the development life cycle." [13, p. 25], which the authors closely link with tamper resistance of cryptographic hardware. The fourth and last concept of Certification prescribes the need for certification of products by cryptographic institutions like the U.S. National Institute of Standards and Technology (NIST) or the U.S. National Security Agency (NSA) for the compliance to industry standards [13, p. 25]. The authors do not explain how or why the certification concept fits into the wider strategic approach to cryptographic migration, but in general, it can be presumed that the adherence to cryptographic standards and the accreditation of the implementation of said standards ensures the correct application. While all concepts prescribe principally sound recommendations covering important aspects of cryptographic hardware, it does only tangentially address the 'how' question of cryptographic migration. In connection with outdated assertions about the usage of dedicated cryptographic hardware instead of general-use computers, the second Transition principle does not address the current problem of cryptographic quantum vulnerability.

The third Transition principle Stapleton and Poore assert is the "Application Management" and its additional four sub-concepts of "Algorithm Independence", "Security Architecture", "Enterprise Management" and "security Guidelines" [13, p. 26] under which the authors group operational issues of cryptographic migration [13, p. 26]. Algorithm Independence prescribes a flexibility in the implementation of any cryptographic algorithm [13, p. 26]. Any cryptographic architecture should make an effort to facilitate the exchange of algorithms. This concept is directly applicable to the focus of this thesis on post-quantum cryptography (PQC) migration, as well as any additional future migration. With the concepts of Security Architecture, Enterprise Management and Security Guidelines the authors drift from a directly migration related guideline to more general cybersecurity and business related guidelines, prescribing an enterprise wide security framework that must be consistent with the laws of a given country, an enterprise wide device management strategy as well as adopting appropriate security policies and guidelines for the organization. While all important points in the context of cybersecurity, they similarly to the Cryptographic Hardware principle do not directly address the approaches and practices for a cryptographic migration.

The next point discussed is the "Transition Process" which in turn is divided into the four phases of "Vulnerability Assessment", "Impact Analysis", "Implementation", "Reconciliation" [13, p. 26]. In the Vulnerability Assessment, information regarding the current systems and their incorporation into the wider security strategy should be gathered first with a following determination of requirements for a new cryptographic system as well as a determination of infrastructure requirements [13, p. 27]. Concluded is the concept of Vulnerability assessment with "[...] a formal risk assessment of systems and infrastructures to ascertain the potential threats, realistic vulnerabilities, business and technical risks and derive the appropriate security requirements." [13, p. 27]. The assessment of danger and risk arising from cryptographic vulnerabilities is an important part of recognizing a need for action, and thus foundational in forming the intent to perform a cryptographic migration. It is equally important in the case of quantum-safe cryptographic migration and should be part of a migration strategy.

In the second proposed phase is the Impact Analysis, which should entail the current and future impact of cryptography on business systems [13, p. 27]. It first consists of an assessment of how and where cryptography is used, which is expanded to an analysis of the dependencies to other systems or infrastructure [13, p. 27]. The authors then prescribe a need to handle the potential legislative requirements of different countries [13, p. 27]. The last step of the Impact Analysis is the determination of suitable cryptographic replacements [13, p. 27]. The phase of Impact Analysis by Stapleton and Poore describes a more direct handling of cryptographic migration in comparison to their earlier recommendations, and thus is more applicable to the current case of post-quantum cryptographic migration. While that being the case, the authors do not venture further in explanation or recommendation of how the task of inventory assessment of cryptography could take place, making it difficult to gain more information about cryptographic migration.

In the next phase of Implementation the authors insert the normal project management life cycle, which they consolidate into the planning tasks of development, testing, quality assurance and deployment [13, p. 27]. All of which cover the technical implementation of any cryptographic algorithm including manpower and other resources, test cases and unit tests, documentation and code review, and deployment schedules, which all fall outside the organizational level of strategic approach to a cryptographic migration this thesis aims to explore. In the final phase of Reconciliation, the authors prescribe a review of the transition process, monitoring the success of the project and analyze potential mistakes made. Stapleton and Poore conclude their strategic approach by providing practical recommendations for the project planning of implementation and its review, which on its own is certainly valuable information but, same as some of the points made before, it ventures from the core exploration of the cryptographic migration progress.

In the context of the cryptographic vulnerability of public-key encryption, not all aspects of Stapleton's and Poore's work find a direct application to the challenges presented in this thesis. It also does not convincingly close the gap between the high-level security policy discussion and the low-level technical and mathematical discussion of cryptographic algorithms explaining the process of execution from one to another could be achieved. But this can and should also not be the expectation of a single entry in the academic discussion as, in light of the nonexistence of alternatives, this paper is upon the first exploration of viable approaches on any organizational level. In this context, no remarks or criticisms levied against this paper could diminish the value it has provided.

2.4.2 Joseph et al.: Transitioning organizations to post-quantum cryptography (2022)

David Joseph and colleagues published the detailed article “Transitioning organizations to post-quantum cryptography” in May 2022 in the Nature journal about the quantum vulnerability problem to cryptography as well as providing information on the cryptographic background, progress on quantum-safe encryption algorithms and recommendations to plan and prepare a transition to quantum-safe cryptography. The authors start by providing a brief cryptography background, as well as explaining Peter Shor's impact on public-key encryption as described by this thesis at length earlier in this chapter. The information at hand regarding the current state of quantum computing hardware is representative of the state in 2022, but the authors assert the same general pace of development in the field as done earlier in this chapter. [68, p. 237-238]

The article describes current and future events relating to post-quantum cryptography in three simultaneous segments. The first segment shows the timeline of threats posed by cryptographic quantum vulnerability being currently harvest-now-decrypt-later type of attacks up until powerful enough quantum computers exist that are able to outright break the encryption. Then the threat would shift to the break of RSA and digital signatures, endangering the security of all system relying on current public-key encryption algorithms. The second segment shows the authors' prescribed timeframe of cryptographic transition to quantum-safe cryptography. It is divided into three phases, with the first "Planning" phase currently ongoing, followed by a "Transition" phase in the near future. The Transition phase should be in the "Done" phase before the threat shift shown in the first segment is coming to pass. The third segment underpins both timelines with an ever ongoing standardization effort of post-quantum cryptography. The associated figure from the article is shown in figure 2.3. Given these timelines and information on quantum vulnerability before, Joseph and colleagues urge any organization potentially effected to start the planning of transition and integration of post-quantum cryptography into their systems. [68, p. 238-239]

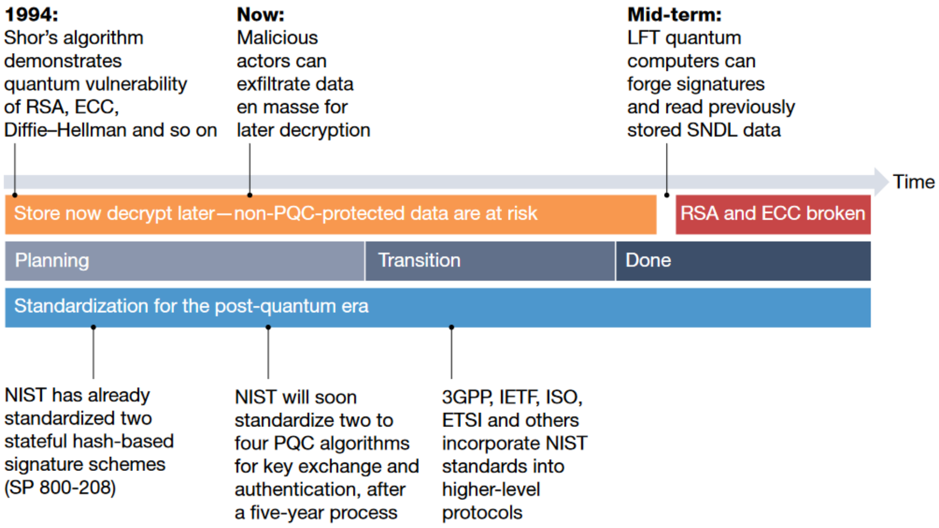

1994:
Shor's algorithm demonstrates quantum vulnerability of RSA, ECC, Diffie–Hellman and so on
Now:
Malicious actors can exfiltrate data en masse for later decryption
Mid-term:
LFT quantum computers can forge signatures and read previously stored SNDL data
Time
Store now decrypt later—non-PQC-protected data are at risk
RSA and ECC broken
Planning
Transition
Done
Standardization for the post-quantum era
NIST has already standardized two stateful hash-based signature schemes (SP 800-208)
NIST will soon standardize two to four PQC algorithms for key exchange and authentication, after a five-year process
3GPP, IETF, ISO, ETSI and others incorporate NIST standards into higher-level protocols

Figure 2.3: Post-quantum cryptography timeline from the Joseph et al. Nature article "Transitioning organizations to post-quantum cryptography". [68, p. 238]

Reinforcing this general recommendation of cryptographic transition, the authors list several reasons to start the process of post-quantum cryptography migration, highlighting the time sensitivity of this task. The first reason being the threat of harvest-now-decrypt-later type of attacks, which we already explained in this chapter. The possibility of future decryption of any data stored now negates the presumed secure that public-key encryption provides, even before a powerful enough quantum computer exists to execute such decryption. The authors name this the most import reason to start the process of transition as early as possible. The second reason named is the use of post-quantum cryptography in long lifespan projects such as vehicles or critical infrastructure. Objects that are in use for years and decades would—given the presumed timeline of quantum development—be cryptographically insecure within their lifetime, with cryptographic updates being difficult to perform and costs being immense. Post-quantum cryptography should therefore be considered immediately for any such projects. The third reason brought forward is the long lead time cryptographic transitions typically take. The authors point to historic examples of changes in perception and adoption of new cryptographic algorithms taking multiple years or even decades, and use this to emphasize the point of time sensitivity of post-quantum cryptography transition. The fourth reason named is the already ongoing effort of standardization of several new post-quantum cryptography algorithms giving indications on, which encryption algorithms it will be possible to transition to in the future, allowing the preparation of the migration process.

The authors close by again stating the immediate need for any organization affected by quantum vulnerability to start or at least plan their cryptographic migration strategy. [68, p. 239]

Joseph and colleagues continue by describing the current state of effort regarding the standardization of post-quantum cryptography algorithms by NIST, the Internet Engineering Task Force (IETF) as well as others. The standardization organizations provide a level of scientific and legal certainty in the security of cryptographic algorithms they research and codify. So far, only one digital signature algorithm has been standardized by IETF and NIST for post-quantum cryptography use. NIST is currently heading the standardization effort of asymmetric quantum-safe cryptography, with a public competition started in late 2016. In following rounds of testing and evaluation, NIST has identified several candidates for standardization at the point of release of the article. The authors recommend that organizations should start gathering information regarding all finalist candidates to reduce any transition time. [68, p. 239-241]

In the preparation of a cryptographic migration strategy to post-quantum cryptography, Joseph and colleagues state several general recommendations. The first recommendation is "Crypto-agility" [68, p. 241]. With new cryptographic algorithms come changes in associated encrypted file sizes and signature lengths. Different key sizes may also impact the digital operations, making it necessary to be adaptable to new cryptographic circumstances in software and hardware. Cryptographic-agility prescribes a layer of abstraction for the implementation of cryptographic algorithms. This allows the referencing of a cryptographic function or library where the implementation of specific cryptographic algorithms can be centralized. Any adjustment or change in parameters of an algorithm, or even the complete transition to a different cryptographic scheme, can then be executed at much reduced time and effort. [68, p. 241]

The second recommendation is the incorporation of a "Prioritization strategy" [68, p. 241]. To successfully implement a cryptographic transition, the order of change should be carefully planned to prevent unnecessary system downtime and compromises in security. The prioritization should be based on the amount of risk for any cryptographic scheme. The authors identify key exchange algorithms, i.e., public-key cryptography, at the highest risk with the currently discussed problem of quantum vulnerability as well as the associated possibility of harvest-now-decrypt-later type of attacks. In contrast, digital signatures, while equally affected by quantum vulnerability, would require a real-time forging of signatures to hijack an online interaction and thus should be at a lesser level of risk. [68, p. 241]

The article's third recommendation is the use of "Hybrid algorithms" [68, p. 241]. Joseph and colleagues propose rather than to replace the current proven cryptographic algorithms—apart from the quantum vulnerability—with relatively unproven quantum-safe ones, both should be combined to get a base level of security. In the case of vulnerabilities in new post-quantum cryptography algorithms, security would still be provided by the non-post-quantum algorithm through the use of a combination of the algorithms. Both algorithms would be used for a key exchange and establish separate shared private-keys, which in turn could be combined into a single shared private-key. In the process of transition, the security would therefore not fall beyond previous levels. [68, p. 241-242]

The authors conclude their recommendations by emphasizing the need for organizations to make themselves familiar with the software implementations of potential post-quantum cryptography candidates to make plans for the integrating into their systems. [68, p. 242]

Joseph and colleagues provide information regarding the topics of quantum computing and the quantum vulnerability of cryptography, affirming the information established in this chapter. While delivered in an abbreviated form comparatively, it confirms the main points stated about the impact quantum computing could have on cryptography and describes the same potential threats from harvest-now-decrypt-latter type of attacks to outright decryption. According to the authors, to remain secure, a cryptographic migration to a quantum-safe encryption algorithm will be necessary [68, p. 237]. Given the wide-ranging current use of public-key encryption algorithms, the scale of transition would be unprecedented compared to historic examples. With the experiences of past migrations taking years or decades to complete, the timeline for a post-quantum cryptography migration would have to start immanently even before any quantum-safe public-key cryptography standards exist [68, p. 238-242]. To make this transition possible, any organization affected by quantum vulnerability should therefore prepare a migration strategy [68, p.241-242]. The article did not provide such a strategy but made several general recommendations which in their view should be incorporated to make the transition process easier. As being one of the few works in the academic discussion related to cryptographic migration strategy and post-quantum cryptography, Joseph and colleagues provide a first basis on which further research on the topic can be built upon.

2.5 Summary

Modern cryptography provides a way of securing information so that only the intended owner is able to read the original information. An encryption algorithm transposes a text into gibberish, unreadable to anybody without the right key. Unlocking this text can only be done with the right key and decryption algorithm. The setup of the cryptographic algorithms and the key is what grants the scheme its security, as it usually needs an unfeasible amount of computing power in the realm of millennia to break the cryptographic algorithm and guess the correct key of an encrypted text. This process allows private and secure communication and data exchange to take place, which enables such a widespread interconnected network like the internet.

Quantum computing has the ability to substantially change the status quo, as it can provide a new dimension of computational capability and power that thoroughly changes the calculation of feasibility of execution of certain mathematical algorithms. As it happens, a class of cryptographic algorithms' complexity is based on an assumption of unfeasibility of factoring large numbers, a problem quantum computer should be able to solve in seconds compared to the thousands of years a traditional computer would take due to a quantum algorithm developed by mathematician Peter Shor. One of the cryptographic algorithms in question is the RSA public-key encryption scheme, with is currently responsible for securing a wide range of communication applications, which includes numerous activities on the internet.

So far, no quantum computer powerful enough exists that is capable of executing Shor's algorithm. The development and engineering of new quantum computers is progressing at a steady pace, generally doubling performance every year. Estimates of when the computational level will be reached, range from as low as 5 years up to as high as 20 and beyond. A consensus seems to be building around the 10-year mark—early to mid-2030s. The danger of quantum computing to cryptography is not just represented in this breaking point but also the possibilities of harvest-now-decrypt-later attacks. While not having access to quantum computers today, the certainty of reaching a breaking point on a roughly predictable timeline gives an attacker confidence in the viability of this type of attack.

Both attacks—the outright breaking of encryption and harvest-now-decrypt-later—could have devastating impacts on almost every aspect of government, society, and economy. The potential for damage is correlated with the widespread usage of affected cryptographic algorithms in every sector, as public-key encryption is common in networking activities. With digital communication and data transfer being ingrained heavily in a lot of elemental processes, by definition all these processes are in danger of being intercepted, spied upon and disrupted. To preserve the security granted by current encryption algorithms, a cryptographic migration has to take place to a different cryptographic scheme that is not based on mathematical problems feasible solvable by quantum computers.

Academic research or public discussion regarding cryptographic migration to quantum-safe algorithms or migration in general is sparse and difficult to identify. How a cryptographic transition should or can be achieved remains a largely unexplored topic, leaving affected individuals or organizations little guidance on how to proceed with the given threat of quantum vulnerability.

3 Methodology

The previous chapter provided a foundation of knowledge in the fields of cryptography and quantum computing. As discussed, this new computational resources could lead to a compromise of encryption, presumed a continued development of quantum hardware based on current trends. A cryptographic migration to new quantum-safe cryptography would be needed to preserve the security and privacy provided by public-key encryption. The establishment of currently known facts attest to the first two premises set forth at the beginning of this thesis. To answer and affirm the remaining sequence of hypotheses, a qualitative analysis of the response to the presented quantum vulnerability problem and an exploration of mitigating steps has to take place.

To contribute to the public discussion about cryptographic transition, this thesis will explore a strategic approach to post-quantum cryptography migration. This strategy, in line with the presented information so far, aims to formulate a generalized and sustainable way of preparation and approach to any individual or organization for the cryptographic migration of their codebase to quantum-safe cryptography. The description of 'strategic approach' is a deliberate choice and stands in contrast to a technical implementation, which would define a specific and direct programming and integration approach. The strategy would stand above the direct implementation details and recommend possible migration steps. To formulate such a migration strategy, it is necessary to explore and analyze the response to cryptographic quantum vulnerability as the current academic research on said topic, for all intents and purposes, is almost nonexistent. To alleviate the deficiency in quantum-safe cryptography migration described in the previous chapters, the lack of publicly available information regarding the migration process needs to be addressed.

Given the lack of publicly available information, the intention of the thesis is to provide a holistic collection and summary of cryptography and quantum computing related information and possible actions covering the whole domain of both fields, including a quantum computing impact analysis, evaluation the general level of acknowledgment and action, as well as possible mitigation approaches. As such work appears to not have been conducted to this extent thus far, the thesis can not be based on or rely on any specific prior related work in the domain of post-quantum cryptography migration.

The research follows a qualitative and exploratory approach with a focus on compiling and analyzing information from the domains of cryptography, quantum computing, cybersecurity, as well as related data and current trends. The exploratory approach is necessary due to the scarcity of contemporary research covering the process of cryptographic migration in the given quantum vulnerability background. In this manner, the state of publicly available information is to be revealed, set in context, and used to establish a migration strategy.

The data and information is collected through a review of academic literature, industry white papers and publicly available technical information, news reports, government reports and case studies. All sources will be selected based on their relevancy and representative value, their credibility, and their informational value in contributing to a comprehensive understanding of post-quantum cryptography and cryptographic migration. Key sources are the governing bodies and associated institutions, current recommendations from standardization organizations like the U.S. National Institute of Standards and Technology (NIST), industrial publications from prominent information technology businesses like Amazon, Google, IBM, Microsoft, as well as reports on general readiness for post-quantum cryptography by other industry participants.

To accurately represent the current response to the quantum vulnerability and its effect on cryptography and cybersecurity, several aspects are to be considered. With the broad range of affected organizations and individuals, the amount of data points is nearly limitless, making a consolidation of the most important conditions necessary. The aspects to cover include both public and private institutions and their reaction to quantum vulnerability. Governments, policy, and laws need to be examined and their role in the space of cryptographic security determined. The acknowledgment and actions of private businesses and organizations need to be ascertained and the sufficiency of current behavior evaluated. Next to the already examined related work of academia, other sources of potential supporting information or recommended conduct should be explored. The range and depth of information to be covered extends beyond the scope of a single research project but nonetheless should be attempted to explore as to build a first basis on which more work can be continued from.

The collected data is subject to analysis to identify important aspects, reoccurring themes, challenges, and missing links in the broader context of cryptographic migration. Parts of this review have already been done in the previous chapter on cryptography and quantum computing, as well as the analysis of potential impacts. The analysis ties in all threats of covered information into their logical conclusion, validating the argumentation of the hypotheses.

The limitation of this methodology is the reliance on numerous single data points of varying quality and depth from different sources, such as government reports, legislative texts, publications from public institutions, news reports, and statements from private companies. While the compilation of these sources contributes to a comprehensive understanding of the collective response to the quantum vulnerability problem, it can introduce potential inaccuracies. Since the domain of post-quantum cryptography migration is relatively unexplored, many of these data points can not be validated against other sources. Conclusions and further prescribed mitigation actions thus must rely on the current limited foundation.

The to be conducted consolidation of relevant information from the domains of cryptography, quantum computing, and cybersecurity leads to the formulation of a strategy for post-quantum cryptography migration. This strategy will focus on the distinct replacement of the application of cryptography in software. The business policy or other bureaucratic aspects pertaining to the organization's economic planning and management fall outside the focus of this migration strategy and are only considered in scope if they directly tie into the transition process. To prescribe possible steps of conduct in a cryptographic migration, an evaluation of past and present information takes place, in which suitable actions for migration are identified. This includes an analysis of prominent past migrations and the exploration and evaluation of possible new approaches compatible with cryptographic transitions. This approach ensures that the proposed migration strategy has an extensive foundation in both historical context and current recommendations. On this basis, a comprehensive strategy for quantum-safe cryptographic migration is to be developed that remains relevant for contemporary and future applications.

The strategy entails possible steps and approaches for a post-quantum cryptographic migration directed at any individual or organization. The level of proximity to actual code implementation should be akin to the level of proximity from an architectural blueprint to the building of a house. The proposed strategy provides guidance on how to construct a quantum-safe software security blueprint for one's own codebase. In the development of said strategy, the general steps of cryptographic migration and potential problems and challenges are explored. This includes an exploration and evaluation of historic migrations and techniques and approaches from related fields of study. The strategy aims to prevent or reduce risks described in the previous chapters, reduce costs related to cybersecurity failures, reduce implementation time compared to a manual migration, as well as provide cryptographic flexibility for future developments.

4 Exploration and analysis of response

In the previous chapters, the theoretical background of the stated problem of cryptographic vulnerability to quantum computing has been examined and followed to its logical consequences. In this chapter, the reaction of affected actors—be it political or economical—will be explored and reviewed to further ascertain if they are able to counteract the arisen developments. To this end, this thesis will try to get a representative sample of the overall responses and activities, summarizing the different actions taken to form a holistic view of the cryptographic environment. The scale of the stated cryptographic problem necessitates a global effect, which results in a near limitless amount of affected parties.

To understand what is currently happening, this chapter will take a look at the actors who arguably have the most power to impact any movement of cryptographic migration activity. In the political realm, this responsibility falls to governments of countries and political unions leading the world economy. On the other side, the major players in the IT-sector individually contribute to the cryptographic environment with the products and services they provide, which can be looked at as a guideline for technological progress for other organizations and individuals. In both cases, first the acknowledgment and then any accompanying actions are of importance to ascertain the recognition of the stated problem of quantum vulnerability. Depending on the circumstances, statistical analysis and studies on these aspects do not exist, as many of the practices are part of ongoing operations and thus potentially sensitive information. In this case, only individual approaches can be evaluated and have to stand in as a general consensus if applicable.

4.1 Governmental responses

Governments and political institutions like ministries and agencies provide guidelines of conduct and, more importantly, boundaries to actions [69]. They have the ability to enforce the rule of law under the threat of penalty, shaping societal behavior in the law's intended direction. In the same way they can also force change in their jurisdiction, which includes the realms of information technology, cryptography, and software security. This does bear them with the responsibility to supervise the stated domains and react to new developments, threatening the government's imperatives. To indicate the awareness of governing bodies, this thesis will analyze the behavior of the governing bodies of two of the largest economies in the world—the United States of America and the European Union [70].

4.1.1 Current laws and policy positions

Born out of the stated governmental responsibility, several institutions and laws have been created to service the cybersecurity domain and related activities. To gain a general understanding of the current responsibility assumed by governments in the scope of this thesis, important legislative initiatives specifically regarding cryptography and encryption are discussed.

From a historical perspective, the government of the United States of America has often taken an adversarial role to the establishment of cryptography outside of military and government use [71, p. 107] [72]. Rules and regulations often pertain to the restriction of cryptography, especially in the commercial sense, under the pretext of export restrictions. The universal nature of cryptographic use described in chapter 2 includes military and governmental applications, which now makes any cryptographic algorithm a potential state secret worthy of protection from outside actors [72]. Cryptographic source code and encryption algorithms are thus defined as 'dual-use' technology by many nations and subject to special consideration [71, p. 103-105] [72]. 'Dual-use' is a concept which has no universal definition but in spirit refers to things which can have both civilian and military application, or non-military things that can be used to produce things for any military application [71, p. 103-105] [72]. This leads to an evaluation on a case-by-case basis and a gray area depending on argumentation in either direction if a specific item applies to this specification and in turn would be subject to stricter laws [71, p. 107]. The US government has classified cryptography as a dual-use technology and restricted its export [71, p. 106-107]. With the proliferation of digital technology and more commercial applications, exemptions have been made to allow the export of specific cryptographic algorithms with restrictions on the cryptographic complexity—expressed through the allowed key-length [71, p. 107-108]. This stance changed with more liberal EU regulations regarding the export of cryptography, granting a general exception to export regulation of any cryptography to the EU. In 2011 followed the complete removal of cryptography from any export regulations regardless of key-length if the cryptographic algorithm is "publicly available" [73, p. 1059].

The U.S. does not have a general law prescribing the protection or encryption of personal data [74]. Only in some specific domains, important legislation regarding the information privacy of citizens has been passed that requires the secure handling of data. Prominently, the *Health Insurance Portability and Accountability Act (HIPAA)* has enshrined the right to privacy and data protection of one's individual healthcare information, mandating that covered entities protect said information adequately from involuntary disclosure [75]. Financial institutions are the second domain that is covered by the *Gramm-Leach-Bliley Act* [76]. It requires customer data to be safeguarded and kept private to preserve the confidentiality of this sensitive information. Specific encryption schemes or algorithms are not prescribed in either legislation, but rather a general adherence to current best data security practices is demanded. Additional less prominent privacy and data protection legislation has been passed in individual states [74].

The European Union has established a similar general outline of policy regarding the export of cryptography. They also categorize cryptography under the umbrella of dual-use, with their definition following the one provided earlier in spirit [71, p. 109-110]. As the US, they also exclude "information and software within the public domain" [71, p. 111] from any special export regulations. The EU members states have differing implementations of the EU framework, which can lead to some inhomogeneity in the execution and control of regulations and laws [71, p. 112]. While both appear to rely on the same foundation of law, with the intention of prohibiting military use (or development) and nuclear weapon proliferation, the US set up another pillar in its dual-use definition under the anti-terrorism label [71, p. 109, 116]. Under which they retain the right to deny export of cryptography even if no prior established restriction is applicable. In contrast, the EU has a special consideration of human rights or the possibility of undermining them under a dual-use definition [71, p. 111-112, 116]. While both retain special dual-use conditions which leaves them with extensive freedom of prohibiting the export of cryptography the underlying intention of national security on the US side and human rights violations on the EU side stand in stark contrast to each other [71, p. 112]—a symbolic difference of spirit which also is represented in other policies.

The EU does have general law prescribing the safekeeping of personal data by those in possession of it. The *General Data Protection Regulation (GDPR)* is a comprehensive umbrella legislation on data privacy and protection of the EU passed in 2018 [77]. It addresses the questions and concerns about the handling of personal data that inevitable arise when one participates in a digitized world of goods and services. In *Art. 32 GDPR - Security of processing* [78, p. 51-52] it is discussed what measures can be taken to secure data appropriately. The regulation does not prescribe a specific set of actions that has to be taken but rather a collection of general appropriate procedures to ensure data protection, like the use of pseudonymisation or encryption on relevant data [78, p. 51]. It does not prescribe a specific encryption scheme or algorithm that should be used. The assessment of the appropriateness of measures taken is dependent on "[...] the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons [...]" [78, p. 51].

4.1.2 Acknowledgment and action

The United States government and the European Union are both aware of the developments and dangers of quantum computing for software security. In an executive order and accompanying national security memorandum from May 4, 2022, United States President Joseph Biden recognizes the importance of research and development of quantum computing platforms, their strategic and economic benefits, and the dangers they pose to public-key encryption algorithms [48] [79]. He acknowledges the need to establish a knowledge base in the domain of quantum computing in the country and prompts schools and academia to incorporate and promote this field of study. It is proposed that the United States should mitigate "[...] as much of the quantum risk as is feasible by 2035." [48]. While the European Union has established an initiative to further develop quantum computing and related infrastructure projects between several member states under the *EuroQCI* initiative [80], they have not adopted a definitive comprehensive cryptographic strategy on quantum computing other than overall statements of will to improve the cybersecurity of the EU [81, p. 3] [82]. The European Union Agency for Cybersecurity (ENISA) has proposed similar foundations as the US White House memorandum established, but it, so far, has not been adopted as a governing policy of the EU [81, p. 3, 6] [83, p. iii-iv].

4.2 Industrial responses

The industry is an encompassing term as described in chapter 2.3.3 referring to all businesses and organizations interacting with a nation's economy. As the provider of goods and services, they are responsible for the generation of economic wealth and thus existential in the current structure of society. What and how the industry is using software and which cybersecurity principles they adhere to is important in regard to the effects of the stated problems of quantum vulnerable cryptography on the industry itself.

To this end, this thesis will try to assess the general acknowledgment of the quantum vulnerability and any potential action to mitigate any associated danger in the industrial domain. As any strategies or solutions to this cryptographic problem are part of a business's institutional knowledge and therefore can be part of their service or product, it is difficult to get public access to concrete solutions. As an alternative, the general statements and declarations have to suffice as a general representation of the current industrial response.

4.2.1 Current use of cryptography

As modern cryptography in general is the field of study of securing digital information, it has a general application in any digital system today where data has to be authenticated, checked for integrity or protected from unauthorized access. With the use of computer hardware and digital technology developed and used by the industry, the field of cryptography has become an integral part of business operations. Businesses have a variety of data they want to keep private as it could potentially compromise the commercial operation or personal information. Every digital data point has the potential for an attack vector of a malicious actor trying to gain access to said information. This danger is especially present when data is communicated over a broadly shared network like the internet, and potential consequences were described in chapter 2.3.3.

Encryption can provide control over the access and ownership of information, which in a digital and interconnected environment can be subject to unauthorized access. The efforts of protection and obfuscation are by definition the use of encryption. As described in previous chapter 4.1.1 the use of encryption is not strictly mandatory and only a result of a general right to privacy of specific data. Under this legislation, the businesses themselves determine the method of guardianship, which leaves room for consideration of operational circumstances (is data exposed to outside traffic e.g., the internet), risk and costs.

To this end, the most important categories of data to protect and to use encryption on are the intellectual property and commercial secrets of the business, the customer information and associated business interaction, employee information, financial information, to gain compliance with privacy and data security regulation and avert liability of data breaches [84] [85, p. 13-14]. As of 2022, the usage of enterprise-wide encryption by industry branch ranges from 72% in “Technology & software”, 71% in “Manufacturing”, 71% in “Energy & utilities”, 69% in “Public sector”, 65% in “Financial services”, 59% in “Consumer products”, 58% in “Entertainment & media”, 57% in “Health & pharma” to 46% in “Transportation” [86, p. 11].

4.2.2 Acknowledgment and plans to migrate

Major businesses in the field of software and information technology show awareness of the quantum vulnerability of current public-key encryption algorithms. In company publications like white papers and blog posts they describe the general problem in the same manner as described in the chapter 2. Microsoft stated in a company blog post in May 2023 that they are working on transitioning their products, infrastructure, and services to quantum-safe cryptography, as well as helping their customers do so on a case-by-case basis [87]. A strategy or procedure on how this migration will take place has not been published. Amazon and its web service provider AWS are working on upgrading their cryptographic security and want to provide a hybrid key exchange as a first step to enable quantum-safe cryptography while retaining compliance and industrial compatibility starting in 2024 [88] [89, p. 1-2]. The specific steps on a strategic or procedural level have not been published. Google has shown the same understanding of the danger of cryptographic quantum vulnerability. In late 2022 they stated that they have started to use the quantum-safe *NTRU-HRSS* cryptographic algorithm in their internal infrastructure communication protocols [90]. In August 2023 Google added support for quantum-safe key exchange algorithms to their web browser *Chrome* (through the open-source project of *Chromium*) in preparation of a cryptographic migration [91]—a change on the client which only takes effect if the server side also supports their implemented algorithm. A wider strategic approach on how to transition to quantum-safe cryptography has also not been published.

In light of the sparse public information landscape regarding any macroscopic approach to the cryptographic migration, the mentioned publications will suffice as a general temperature reading regarding the current state of quantum vulnerability in major IT-companies. An acknowledgment of the in thesis stated problem appears to be there, and the institutional knowledge on migration to quantum-safe cryptography seems to present—as far as it is publicly visible. But this does not seem to trigger an industry-wide momentum in cryptography migration efforts.

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) published in September 2023 a joint study with the accounting and consulting firm KPMG regarding the topic of cryptography and quantum computing and its impact on the respective surveyed organizations [5]. This study provides a rare topical analysis on the state of acknowledgment and action regarding quantum vulnerability that is directly applicable to the topic of this thesis. The study's participants cover a wide range of industrial sectors and company sizes, as shown in figure 4.1, making it a reasonable representation of the general attitude towards quantum computing and cryptography and thus is a key piece of evidence on the question of potential danger.

The participants display an acknowledgment of the impact of quantum computing on cryptography in general as 21% describe the impact as “Today's cryptographic schemes are becoming almost entirely obsolete.” and 71% as “Specific cryptographic schemes are broken, but these are widely used” [5, p. 11]. The same sentiment is echoed in 68% of participants answering, that they are “familiar” or “rather familiar” with post-quantum cryptography [5, p. 12]. The awareness of the topic seems to be there in the majority of participants, but already showing a decrease in knowledge from the initial impact of quantum computing on cryptography to the solution of said impact with post-quantum cryptography.

The in chapter 2.3.3 described potential impact on the industry is mirrored in the participants answers to the current use of cryptography in their organization, as shown in figure 4.2. This translates to a perceived risk in the “security of data transit” as “High” or “Fairly high” in 71% of participants, in the “security of cloud data” as 89% and in the “security of long-term confidential data” as 78% [5, p. 16].

The estimates of when quantum computers will be able to break currently used encryptions are more pessimistic (in the sense of cryptographic security) than most, as described in chapter 2.3.2. 4% believe quantum decryption will happen in under 2 years, 18% believe in 5 years, 57% believe in 10 years, 14% believe in 15 years and 7% believe in over 15 years [5, p. 18].

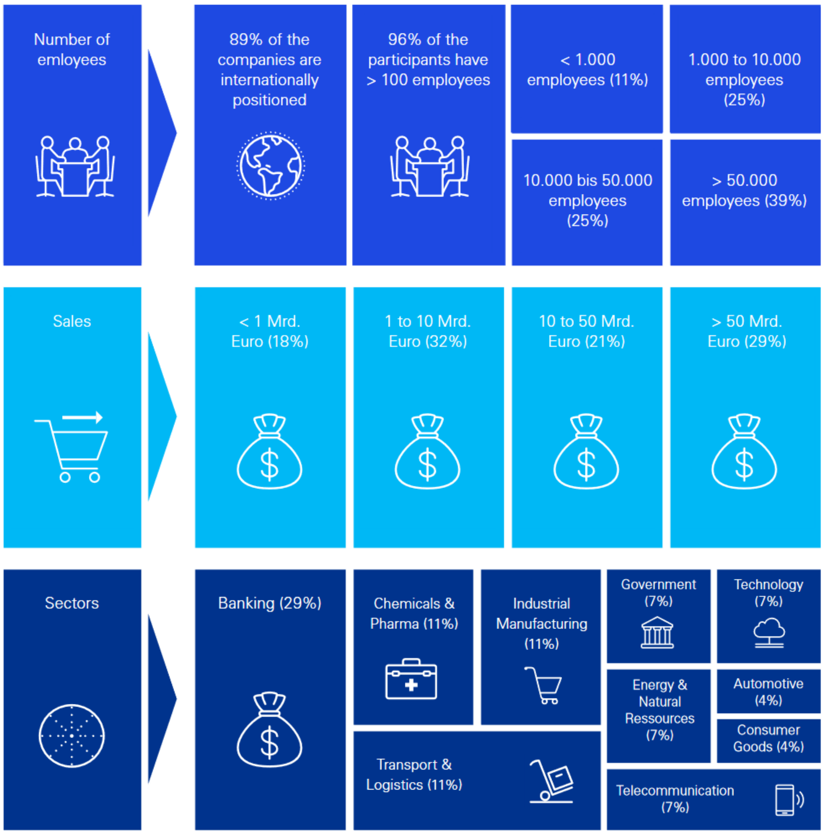


Figure 4.1: Infographic on the participants from the joint BSI and KPMG market study on cryptography and quantum computing. [5, p. 5.]

To the key point of cryptographic migration, three data points were analyzed: the length of time data is retained at the company, when a migration to quantum-safe cryptography will start and how long said transition would take. To the question of data retention length, the participants answered that they 82% must keep data confidential for more than 5 years, 7% for 5 years and 7% for 3 years [5, p. 18]. The transition plans show some immediate movement as 29% report at start-date of 1 year or earlier, 11% within 3 years and 29% with 5 years or longer [5, p. 18]. 32% could not give a start-date [5, p. 18]. The length of time the migration would take, was estimated to take 1 year by 4%, 3 years by 7% and 5 years or longer by an overwhelming majority of 75% [5, p. 18]. 14% could not give a migration time [5, p. 18]. In the assessment of the surveyors, this results in an average miss of in-time migration to quantum-safe cryptography by 6.5 years [5, p. 19]. Participating firms are overwhelmingly not prepared to migrate to quantum-safe cryptography before an estimated breach of security [5, p. 27-28].

To advance in the cryptographic migration, different resources or types of support were mentioned as needed by the participants. 89% reported the need for “Government proposals” or “recommended actions” [5, p. 24]. 75% use or plan to use publicly available information and rely on the support of “Other working groups/interest groups” [5, p. 24]. 64% expected support from “Manufacturing companies (software/hardware)” [5, p. 24].

Differing from the major IT-businesses like Microsoft, Amazon, or Google, the broader industrial base does not seem to be prepared for the transition to quantum-safe cryptog-

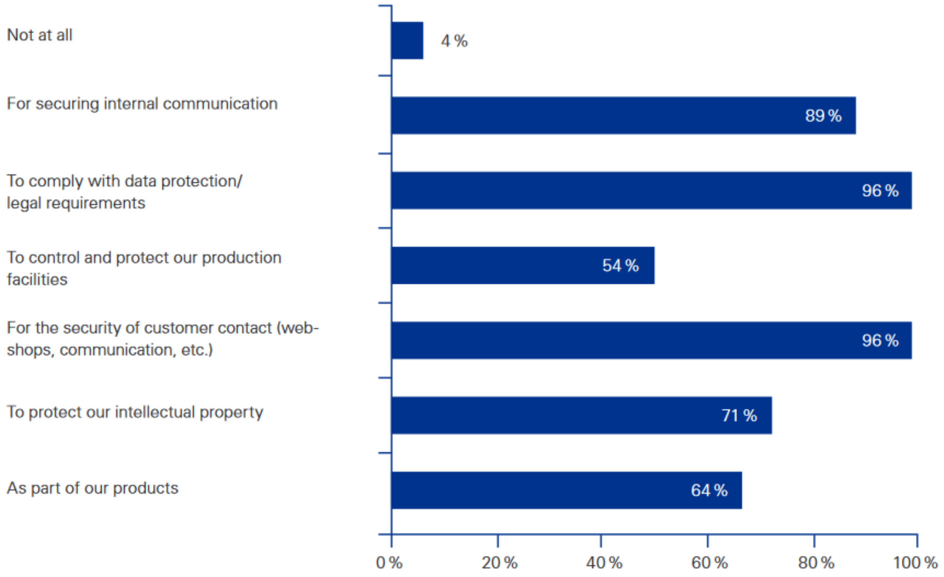


Figure 4.2: Participants answers in percent to the question: “To which end are cryptographic techniques used in your organization?” from the joint BSI and KPMG market study on cryptography and quantum computing. [5, p. 14.]

raphy. They express a clear need for outside knowledge of cryptographic migration from publicly available information from governmental institutions, academia or other sources. The institutional knowledge of major IT-companies does not disseminate publicly to other organizations and seems to only be available in a customer relationship. This results in a timeline for quantum-safe migration that exceeds the average estimates for the breaking point of currently used public-key encryption algorithms. A holistic collection of general knowledge regarding the topic of quantum computing, cryptography and the strategic approach to transition to quantum-safe cryptography does not seem to be available.

4.3 Post-quantum cryptography

Counteracting the stated development of cryptographic vulnerability, the field of quantum-safe cryptography is working on cryptographic algorithms that are not feasibly solvable even with the computational power of quantum computers. The underlying complexity of cryptographic algorithms is built on mathematical problems, as described in chapter 2.1. These for quantum computer easily solvable problems of current cryptographic algorithms, like public-key encryption, are to be replaced by problems that are not feasibly solvable by either classical or quantum computers. The research and development in this field aims to enable a transition to quantum-safe cryptographic algorithms on currently used, non-quantum hardware with reasonably performance characteristics. [1, p. 25-35]

The most prominent effort in the quantum-safe cryptography field is being undertaken at the American National Institute of Standards and Technology (NIST). The NIST is a U.S. governmental institution tasked with developing standards and measurements promoting industrial interoperability [92]. In the field of cryptography NIST has been contributing and coordinating cryptographic research and advanced major encryption standards including the *Data Encryption Standard (DES)* in 1977 [93] and the already in chapter 2.1 mentioned prominent current private-key Advanced Encryption Standard (AES) in 2001 [94]. In late

2016 NIST started an open competition for new encryption algorithms to introduce the next generation of cryptographic standards, replacing quantum-vulnerable ones with new quantum-safe ones [95].

4.3.1 Process of standardization

Under the organization of NIST, suitable submissions of algorithms were evaluated under the competition's requirements and criteria, as well as solicited public feedback [96, p. ii, 1–2]. The 82 submissions in the first round of the competition were evaluated based on the criteria of "Security", "Cost and Performance" and "Algorithm and Implementation Characteristics" [96, p. 4-5]. 26 candidates were selected and moved on to the second round of competition. The following round, while still broadly following the same three criteria, conducted a more in-depth analysis on the theoretical cryptographic assumptions behind each algorithm and more comprehensive benchmarks on different hardware platforms were performed [97, p. ii]. This second round of the competition resulted in four candidates for public-key encryption *Classic McEliece, CRYSTALS-KYBER, NTRU,* and *SABER* and three candidates for digital signatures *CRYSTALS-DILITHIUM, FALCON,* and *Rainbow* declared as finalists for standardization with eight candidates remaining as alternates [97, p. ii]. The third round applied the same general criteria as the first and second round in a stricter fashion. In July 2022 four winning candidates algorithms were announced: CRYSTALS-KYBER as the public-key encryption and CRYSTALS-DILITHIUM, FALCON, and *SPHINCS+* (one of the alternates selected in the second round) as three distinct digital signature standards [98, p. i] [99]. These selected winners moved forward in the process of standardization. While only one public-key encryption algorithm has been chosen, three different digital signature algorithms will be standardized with the intent of diversifying this new cryptographic space.

While declaring the standardization candidates after the third round of the competition, NIST announced a fourth round of competition to further evaluate alternate public-key encryption candidates, indicating the intent to diversify the quantum-safe public-key encryption space. The chosen candidates for the fourth round are *BIKE*, Classic McEliece, *HQC* and *SIKE*. [98, p. i, 52]

The algorithms themselves as well as their evaluation were done with the explicit wish of public input and comment. Every step of this competition was documented and released to the public [96] [97] [98]. Each round ended with a comprehensive status report detailing the structure, procedure, and results of the evaluation. The reputation and credibility of the NIST and the transparent nature of the process instills trust in the results and the institution. This years-long evaluation in a competitive academic environment does yield a high degree of confidence in the cryptographic abilities and correctness of any to be introduced new standard.

4.3.2 Standards

In August 2023, three initial drafts for the new quantum-safe cryptographic standards were released by NIST [100] [101] [102]. The finalization of the proposed standards followed in August 2024 [103] [104] [105]. The three standards are now "[...] ready for immediate use." [106].

Module-Lattice-based Key-Encapsulation Mechanism Standard (ML-KEM)

The key-encapsulation mechanism describes the use of a public-key encryption scheme to establish a secret-key (or private-key) both parties have access to for further communication. For this mechanism, one party generates a decapsulation-key (the private-key) and an encapsulation-key (the public-key). The public-key will be shared with a second party, which in turn generates a to-be shared private-key and encrypts it with the given public-key. The first party can receive this encrypted key and decrypt it using the decapsulation-key. This is the same public-key encryption mechanism as described in chapter 2.1 with the encrypted communication consisting of a shared private-key. Both parties now have the same private-key and can use private-key encryption to communicate. [103, p. i-iii, 1]

This cryptographic standard is based on the submission algorithm CRYSTALS-KYBER in the NIST post-quantum cryptography competition. It is slated to supersede the currently approved by NIST schemes based on the mathematical foundation of discrete logarithms (NIST SP-800-56A) and integer factorization (NIST SP-800-56B), which, as discussed in chapter 2.3.1, are vulnerable to quantum computing. ML-KEM is based on the mathematical problem of Module Learning With Errors (MLWE) with the current assumption of not being feasible solvable with classical or quantum computers. [103, p. i-iii, 1]

Module-Lattice-Based Digital Signature Standard (ML-DSA)

This cryptographic standard is based on the submission algorithm CRYSTALS-DILITHIUM in the NIST post-quantum cryptography competition. It shall be applicable in any case where digital signature schemes are used. The digital signature scheme does function as described in chapter 2.1. It uses properties of a public-key encryption scheme and uses the private-key and a hash function to generate a unique digital signature that anybody with the public-key of the key-pair can validate as being sent from the rightful private-key owner. ML-DSA includes the key generation process, the signature process and the signature verification process. As ML-DSA it is based on the mathematical problem of Module Learning With Errors and thus equally qualifies as quantum-safe. [104, p. i-iii, 1]

Stateless Hash-Based Digital Signature Standard (SHL-DSA)

This cryptographic standard is based on the submission algorithm SPHINCS+ in the NIST post-quantum cryptography competition. As described in chapter 4.3.1 NIST has selected multiple candidates for digital signature standardization to gain cryptographic variety. SHL-DSA shall be applicable in any case where digital signature schemes are used. This digital signature scheme shares the same general functionality as described in chapter 2.1. It includes the key-generation process, the signature process and the verification process. SHL-DSA is based on the mathematical difficulty of finding preimages for the hash-functions used, and thus is presumed quantum-safe. [105, p. i-iii, 1]

4.4 Current post-quantum cryptography migration recommendations and trends

Despite the scarcity of holistic post-quantum cryptography migration strategies governmental and industrial organization have published recommendations or provided insight into their practices for a quantum-safe cryptographic transition, making them valuable observations which can be incorporated into a comprehensive migration strategy. Behaviors or recommendations may be repeated if the practices of different organizations overlap but will be mentioned nonetheless to accurate emphasize their prevalence. The same applies to behaviors or recommendations, which have already been discussed in related work as part of chapter 2.4. As stated before in this chapter, the following list of recommendations can not encompass any and all mentions of post-quantum cryptography migration but aims to describe a representative state of topically available information.

BSI

The German BSI has published several recommendations as part of a general quantum-safe cryptography guide from May 2022 [1]. These recommendations range from general strategic concepts to specific actions. The, in the view of this thesis, most important recommendations include the following points with no deliberate order of significance or importance:

- *Preparation*

  The BSI prescribes a first phase of migration preparation, in which the current situation shall be accessed. This includes an assessment of what cryptography is used and where, which systems or data are critical, and if there already exist solutions for this. [1, p. 61]

- *Cryptographic agility*

  The implementation of cryptography should be made as flexible as possible to have the ability to adapt to changing circumstances. This is not just recommended for the threat of quantum vulnerability, but all future cryptographic vulnerabilities. [1, p. 61]

- *Short-term protective measures*

  For critical operations, the BSI recommends the pre-distribution of symmetric encryption keys for long-term use in a key-derivation function. They acknowledge that this pre-distribution of keys introduces new difficulties and logistical issues. [1, p. 61]

- *Key lengths for symmetric encryption*

  For currently used symmetric key encryption algorithms, BSI recommends increasing the key length from 128 bits to 256 bits. [1, p. 62]

- *Hybrid solutions*

  Since new post-quantum cryptography algorithms are untested on a scale comparable to current algorithms, unknown vulnerabilities could compromise the security of these new algorithms. Therefore, the BSI recommends the use of hybrid algorithms that combine the use of classical algorithms and quantum-safe algorithms in the same way as described in chapter 2.4. [1, p. 62]

- *Post-quantum algorithms for key agreement*

  As replacement algorithms for current public-key cryptography key exchange algorithms, the BSI recommends the use of *FrodoKEM* and Classic McEliece since 2020 and purposefully preempted the completion of the NIST competition for quantum-safe cryptography [1, p. 62]. The 2024-01 version of the BSI Technical Guideline for cryptographic mechanisms includes a brief description of ML-KEM, and the BSI states it intends to add ML-KEM as a recommended algorithm after the completion of NIST's standardization process [107, p. 36].

- *Further Post-quantum cryptography recommendations*

  The BSI states multiple recommendations for different cryptographic applications and infrastructure. They recommend a hash-based signature scheme for signing firmware updates and the algorithms CRYSTALS-DILITHIUM, FALCON, SPHINCS+ for digital signatures. [1, p. 62-63]

The BSI ends their recommendations by emphasizing the untested nature of post-quantum cryptography in real-world application scenarios and the need for further research in quantum algorithms as well as post-quantum cryptography [1, p. 62-63].

NIST

The American NIST has published general points on the challenges of post-quantum cryptography migration and migration planning as part of cybersecurity white paper “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms” from April 2021, which can inform a strategic approach to post-quantum cryptography migration [108]. The authors Barker and colleagues state that the lack of cryptographic agility in many current cryptographic systems discourages the fast adoption of new cryptographic algorithms [108, p. 1]. The severity of impact from the quantum vulnerability problem is linked to the lack of flexibility, which in turn makes any change or transition a manual and labor-intensive effort. Additionally, they state the general rule, that a transition to a new scheme or algorithm can only take place if all related and connected systems are prepared to interact with any new system [108, p. 2]. They identify this as a reason for long transition times of up to decades. Regarding quantum vulnerability, they view key-establishment (also refereed to as key-agreement or key-exchange) algorithms such as RSA and digital signature applications as effected [108, p. 2].

NIST then identifies several aspects of importance in planning or managing a cryptographic transition process:

- *Adaptation of implementation, practices and documentation*

  A change in algorithm usually requires changes in associated cryptographic libraries and their implementation in soft- and hardware. The operating system and other connected systems have to be considered. All changes need to be documented and if necessary translated to updated security procedures. [108, p. 3-4]

- *Current use of cryptography*

  To ascertain which instances of cryptography should be replaced, an understanding of where and what cryptography is used needs to established. NIST identifies an urgent need to develop tools to assist in this task of cryptographic identification. [108, p. 4]

- *Cryptographic discovery*

  Before any cryptographic migration can take place, the need for a migration needs to be discovered first. Information on which cryptographic standards, schemes, or algorithms and corresponding applications are affected by vulnerabilities needs to be communicated by public institutions like NIST and also requested by potentially affected parties. [108, p. 4-5]

- *Implementation details*

  After identifying which and where cryptography is used, several details of the implementations of new cryptographic algorithms need to be considered to ensure compatibility with all associated applications and systems. This includes aspects such as new key length and encrypted message sizes as well as resulting network traffic, latency, adherence to cryptographic protocols, how a cryptographic function is called and whether the quality of cryptographic agility is incorporated. [108, p. 5]

IBM

As a leading company in the domain of quantum computing development, IBM also aims to provide quantum-safe software solutions to customers as part of their distribution of software services. Analyzing their publicly available information on their quantum-safe services can provide insight into their approach to the cryptographic migration process, and therefore be valuable information for public migration strategy discussion. Available information includes marketing material and information published in IBM media, which presumably does not include any information regarded as institutional knowledge and therefore part of IBM's operation as a commercial business.

IBM classifies three areas of operation as part of their approach to quantum-safe cryptography:

- *Discover*

  As a first step, IBM identifies where cryptography is used, as well as which dependencies are called upon. Any instances of cryptographic use shall be listed and summarized under a common framework of inventory. IBM built the proprietary software *IBM Quantum Safe Explorer*, which can scan the source code of any application and automatically find and process instances of cryptography. [109] [110]

- *Observe*

  Next follows an analysis of the cryptographic inventory for potential vulnerabilities or other compliance related issues. The *IBM Quantum Safe Advisor* software will perform this cryptographic analysis and identify the which cryptographic algorithms are used, as well as assigning priority values to potential security vulnerabilities. [109]

- *Transform*

  Under the *IBM Quantum Safe Remediator* software the identified vulnerabilities will be corrected using "quantum-safe best practices" [109]. It will introduce crypto-agility as part of a quantum-safe cryptography implementation [109].

While only superficial in explanation, the provided information does show a general strategic approach to post-quantum cryptography migration.

4.5 Analysis

To make a definitive assessment regarding the impact quantum computing brings to cryptography, this chapter brings the facts established in chapter 2 and the prior discussed response to their logical conclusion. It will analyze the cryptographic realities that would arise from quantum computing and the dangers that entails.

Cryptography in its definitory role provides authenticity, integrity, and confidentiality to the representation of information, be it in storage or communication. The ability to securely transfer information is a cornerstone of our modern society, with a deep interconnection in many parts of the daily life. With the transition to computers and digital systems, an abstraction of language took place to a binary alphabet. Digital communication relies on automated systems to receive, process and answer these bit-messages. Cryptography uses any means by with to obfuscate the original information, relying on the difficulty and time it takes to reverse this process. With digital computers the capabilities to decrypt became greater than any protection analogue encryption method could provide. Leading to the advent of modern cryptography based on mathematical problems that are even too difficult to solve for advanced processors.

The current way of life is enabled through the massive use of digital systems and computational automation. Quantum computers threaten this current order by offering a new way of digital computation. Previously thought hard to solve mathematical problems are solved with little effort by quantum computers. The theory behind it established this as early as 1994. The breaking point of cryptography by quantum computers has not been reached yet, but rapid development of quantum computers in recent years shows an ever clearer timeline. Current estimates by researchers and leading quantum computing companies are pointing to a time-period starting in the early 2030s, where the probability of a powerful enough quantum computer existing will shift to the realm of possible and moving to a certainty as time goes on.

The consequences of broken encryption on a scale like this are grave. Any potential of intercepting, observing, manipulating or destroying any information that is secured through any of the affected cryptographic algorithms is dangerous to personal privacy, business operations and governmental proceedings. The question that arises is, whether this danger to cryptography and its potential consequences will take place and, if it will, is there is an acknowledgment of this and actions taken to prevent it.

Chapters 4.1 and 4.2 describe the current state of awareness of this topic in government and industry in general through a selection of data points. Exact holistic fact of the matter-based statements on a far-reaching, global problem like cryptographic vulnerabilities, are difficult to find, as to the distinctness of all affected domains. A near limitless number of data points and opinions of related organizations have been released so far, which at this point can not be considered in their entirety. To get a general overview of the response, this thesis looked at the overall trends and movements of the most influential governing bodies and industrial organizations to extrapolate the current level of awareness and engagement with the presented quantum-safe problem.

Both the U.S. and the EU government assess cryptography as an area of interest and governmental responsibility. They assert a claim on regulating and legislating the utilization, application, and potency of cryptography. The features cryptography enables described in chapter 2 are invaluable in the process of digitization and interconnection, and, as a consequence thereof, in the growth of productivity in general. The U.S. as well as the EU governments see it in their governmental mandate to protect this asset and direct its use and transfer to other nations—while the main motivation lies more in favor of national security with the former and more in favor of humanitarian concerns with the latter. Both internally are balancing the protection of the privacy of private citizens and organizations with the enforcement of law on malicious actors.

If one is looking for the government to pass legislation to 'solve' the cryptographic quantum vulnerability problem, the question arises of authority and responsibility. As stated, both governments have legislated in the domain of cryptography and established their authority to do so. Laws and policy in general have had a restrictive approach to cryptography, limiting its application under the discretion of the government. Contrary stands the GDPR law passed in the EU, which comprehensively demands the protection of private data of the individual and thus encouraging or rather demanding the use of encryption. In the U.S. no equivalent legislation has been passed, but specific domains like healthcare and financial services are committed to protecting private information. All these approaches formulate the spirit of law as the use of best practices of data protection. The GDPR mentions the use of encryption in general as an example of how this could be achieved. No specific cryptographic approach or method is stated in these laws.

Not writing down a specific cryptographic algorithm does give the stated laws a longevity that logically is not tied to the lifetime of any cryptographic scheme. It shifts the responsibility on the enacting entities to infer the appropriateness of their actions. This certainly provides the benefit of not relying on the bureaucratic process to constantly address the state of security of any by-law demanded algorithm. The associated liability does also get shifted in the direction of private rather than public.

Following this precedence that is set by so far only individual cases of legislation, both the U.S. and the EU government would not put forth any changes to law or policy if any specific cryptographic algorithm is deemed insecure. Although of course possible, it would be an improbable expectation that the discussed governments would change this behavior for any cryptographic vulnerability discovered, as they have shifted this responsibility away by their general laws. The state of best practices, with no specific algorithms attached to it by law, would be determined in the same fashion as it is determined in this thesis: It is the collective consensus of current theory and research and real-world implementation by private individuals and businesses and other organizations. As discussed, this provides a certain level of cryptographic freedom and flexibility, but in the same vein it also could enable inactivity without a strong incentive to adapt to new circumstances.

Out of this behavior two possible, macro-level paths of action can be deduced, to address the stated quantum vulnerability problem from a governmental perspective, under the assumption the current laws do not adequately urge cryptographic change. First would be the assumption of more direct responsibility on the government's part and demanding the implementation of a specific quantum-safe cryptographic algorithm. Secondly would be an additional law more general in scope akin to the current privacy laws of the U.S. and EU, that would demand the use of quantum-safe cryptography but would not prescribe a specific algorithm or method. A possible implementation of this could face even less bureaucratic hurdles if proposed as an amendment to existing laws. In both cases an additional factor would be the extension of domains the legislation covers—while privacy laws lay a good foundation for its implementation, a general demand in any use-case of public-key encryption should be targeted.

This thesis will not make any further legislative or policy recommendations, as it departs from the scope of studies. Nonetheless, the discussed points are important to a comprehensive understanding of actors and actions influencing the quantum vulnerability problem.

The propagation of cryptography throughout every industrial sector has enabled private and secure data handling and interconnection. As stated before, this technological development has solidified digital communication as a foundation of society and commerce, which is held up by the trust in privacy and the reliance on security of information. A disruption of this system has a range of potential damages described in chapter 2.3.3, threatening the current status of our digital environment. Accepting current law and policy, the responsibility falls to private organizations and businesses to secure the private data of citizens by law and their own data willingly.

The study by the German BSI ministry described in chapter 4.2 fits perfectly in the discussion on the current state of response to the posed danger of quantum vulnerability. It showcases the inability of a majority of businesses to address the cryptographic challenge presented to them. There does not exist a clear path for transition from awareness to a new cryptographic solution. It concludes that businesses on average will overshoot the breaking point of current public-key encryption by 6.5 years.

As individual organizations and businesses there exist no obligation to share any operations related information. This is the competitiveness of the free-market economy, but it does hinder the spread of knowledge on how to deal with this quantum vulnerability problem. Big software and information technology businesses have the institutional knowledge to develop and implement new cryptographic solutions for their products and services, which in turn would pass down to their associated customer relationships. This does not lead to a sufficient number of quantum-safe operations, as described in the BSI survey. The current disconnect from software developing and distributing businesses leads to a substantial lead time on the migration to new cryptography for businesses not specialized in cybersecurity. Currently, no widely recognized blueprint for quantum-safe cryptographic migration exists that would address this deficiency.

The vulnerability to cryptographic breaches, outside macroscopic consequences, can also be weight in cost for just individual businesses. The 'Cost of a Data Breach Report 2023' by IBM quantifies the global average cost of a data breach at 4.45M USD and an average 9.48M USD in the USA [111, p. 10-11]. In the '2022 Global Encryption Trends Study' by Entrust, 49% of the participants answered that they experienced a data breach within the last 12 months [86, p. 12]. The cause of the current number of data breaches is currently predominately not related to cryptographic algorithms itself, but rather the implementation, misconfigurations, or soft factors like employee mistakes [111, p. 20]. The quantum vulnerability problem would not alleviate any of these causes but add a new vector of attack that is independent of any previous causes and thus exasperating the situation. Breaches will not be dependent on malpractice, but only on the mathematical limitation of currently used public-key encryption schemes.

The vulnerability of currently widespread cryptography to quantum computers could have potentially devastating effects on private citizens and any organization which in any way is using public-key cryptography, as it enables malicious actors to exploit this situation. If one regards the protection from harm described in this specific instance in the purview of the governmental institutions, the question is posed, if the current actions taken are proportional to the level of danger. Equally important would be the likelihood of each step in the spectrum of potential damage being inflicted.

The facts stated in chapter 2 are in congruence with the estimations of other related businesses and institutions that quantum computing will break the currently established public-key encryption algorithms. With the theoretical mechanism already established in 1994 without any contrary research published in the following 30 years, this thesis assumes the correctness of Shor's theory. Following this, the current limiting factor is only the processing power of quantum computers. The last years have shown rapid developments in processing power, general viability and commercialization of quantum computing related services and products. Estimations range from the late 2020s to late 2030s, with a consensus forming around the first part of the 2030s as a starting point for viability of decryption. This thesis adopts this consensus as a probable date at which any measures to escape the stated consequence have to be taken and come into effect. There a no credible estimations of the extent and amount of potential damages should the breaking point be reached without any change in cryptography. As the amount of damage and disruption is as far-reaching as the use of public-key encryption itself, this thesis assumes a substantial level of disruption and following chain reactions are possible and credible depending on the actor.

Combining both assumptions results in the following working theory of cryptographic quantum vulnerability: given the current speed of development at around the early 2030s a powerful quantum computer could exist at the earliest that can execute on Shor's algorithm and break currently used public-key encryption. Given the potential damages and disruptions this could cause in almost every aspect of society, it is in urgent need of addressing. Even if the scenarios of malicious actors possessing the capabilities needed for such an attack are relatively unpredictable, the amount of possible damage necessitate a concerted effort to eliminate any possibility of such an attack. This assumption is reinforced with the possibility of harvest-now-decrypt-later type of attacks that, given the discussed logistic of data storage, are (probably) not feasible on a global or even country specific scale but could certainly be viable vectors of attack on private individuals, organizations, businesses, and governments. Given the described nature of this attack, all time before the decryption event has become potentially unsecure. It follows that a migration to post-quantum cryptography should take place as fast and immediate as possible.

As described in chapter 2.4 the public discussion on cryptographic migration does currently not provide a sufficiently large base of exploration and research. As mentioned before, experts in the field have described a lack of funding and effort in the field of applied cryptography, which creates as disconnect between the high-level security policy discussions and the low-level algorithmic foundation of cryptography. The road from policy to implementation with the planning of a transition as a first step is considered a necessary progression towards a securer and quantum-safe state of security. With so few related works in cryptographic migration approaches to build upon and the findings of the BSI survey of up to decades long migration lead times, this thesis concludes a lack of public knowledge on cryptographic migration being available. While different pieces of information or recommendations can be found in topical media and select publications, as described in chapter 4.4, they seemingly do not address the apparent challenges to cryptographic competency present in the large scale of quantum-vulnerable individuals or organizations. Since the application of said recommendations is made in the absence of a larger public academic discussion on the merits and interactions of each recommendation, it adds more obscurity to the process. An evaluation of different approaches and processes related to cryptographic migration could provide guidance in the planning and execution of cryptographic migrations, and thus facilitate the transition to quantum-safe cryptography.

4.6 Summary

To establish the forthcoming content of this thesis, the previous chapters will be summarized in a condensed form, highlighting the logical path taken and the foundation of assumptions and assessments. The argumentative direction laid out is the support of the following discussion on countermeasures and action on the issue of quantum vulnerability in cryptography and cybersecurity.

The assessment of the problem quantum computing poses to cryptography is built upon currently known facts and assumptions about future developments:

- Cryptography and the field of cybersecurity enables safekeeping and communication of digital information. It does this with mathematical operations designed to be practically unbreakable with any resources available, creating a complexity barrier to the information it protects. Only entities with the right key can access the secured information.

- Digitization has driven progress in every facet of our society as well as the economy to the point of digital system being present in at least one step of every operation in the majority of industries. The ubiquity of digital systems has enabled an automation of data processing. Networking has enhanced this capability by allowing digital communication. This communication is secured through cryptographic means.

- Currently widespread public-key encryption algorithms securing many aspects of digital communication are based on mathematical problems that are not feasible solvable with the currently available hardware capabilities. Mathematician and computer scientist Peter Shor has published a theoretical concept of how these public-key encryption algorithms can be broken, given a powerful enough quantum computer.

- Quantum computing fundamentally differs from current classical computing, and thus can perform specific operations exponentially faster. This does not translate to a replacement of classical computing but rather a separate computing capability that augments current processing power.

- Current quantum computers are not powerful enough to execute Shor's algorithm.

The implications of these facts have to be discussed and analyzed to evaluate their importance. The assumptions are addressing future developments and thus logically improvable by nature. Expressions on probability are general and meant as an approximation of scale, as exact values are undefinable on a foundation as far-reaching as the domain of cybersecurity.

- A cryptographic vulnerability has the potential to open up any and all data of an affected cryptographic scheme.
- *If* a breach takes place in the manner described, a range of outcomes is possible in any or all domains of government and industry that are in contact with public-key encryption.
- Range of damages and disruption of operations in almost every sector of industry *could* be possible, as it follows from the digital control of connected systems and communication of sensitive information.
- At the current speed of development, it is assumed that quantum computing power could reach the necessary level to execute Shor's algorithm and break current public-key encryption algorithms as early as the beginning of the 2030s.
- Harvest-now-decrypt-later type of attacks make use of the historical precedent of cryptographic schemes being broken given enough time—either though vulnerabilities or advancements in computational power making the underlying complexity obsolete. Given this cryptographic track record, one can store any encrypted data in the anticipation of a future possibility of decryption. Depending on the economic abilities in connection with the in chapter 2.3.2 discussed logistics of data storage, it would be possible to intercept and store the internet traffic of individual people, organizations, businesses, governmental institutions and agencies. The stated circumstances of cryptographic quantum vulnerability make this a credible type of potential attack implicating an additional already ongoing vulnerability.
- The complexity of quantum computing limits the number of possible malicious actors, as their development and manufacturing require a high degree of specialized knowledge. Nonetheless, there already exists a proliferation of quantum computing hardware and quantum computing processing capability as a service to outside customers. State-sponsored agencies like the military and intelligence services would also be likely candidates to utilize such capabilities. Both imply a more limited danger to the privacy of individual citizens if the resource of quantum computing is limited as such and more high-value targets exist—but the strength of this hypothetical is unknowable and still contingent on the willingness to take the risk of exposure.

Following the statements on potential implications is the assessment of the current state of awareness and action. This analysis informs whether a real danger can be expected or averted through adequate counter-developments.

- Governmental institutions provide a legal framework for the operating principle of society. Rules are crafted to assign responsibility and limit unwanted behavior. In the domains of cryptography and cybersecurity, legislation has traditionally been more restrictive than encouraging with a contest between law enforcement, national security and personal privacy. The EU's GDPR law does grant a general right to data privacy for individual citizens. The U.S. does not have an equivalent broad data privacy law but does protect individual financial and healthcare data. All described legislation does not demand the use of specific cryptographic encryption but rather a generalized call for data protection with the implementation left up to current best practices.

- Individual businesses decide on which cryptographic practices they adopt, to comply with the data privacy laws and independently of legislation for their own data. They carry the responsibility and liability for safekeeping this data.
- 46% to 72% of members of different industrial sectors report that they have an encryption strategy for their digital operations (see chapter 4.2.1), showing a general engagement in data security. To the new development of quantum computing, 93% expressed an awareness of the danger of quantum computing to current cryptography (see chapter 4.2.2). Additionally, any action to migrate away from currently used quantum-vulnerable cryptography to a quantum-safe one will on average be completed 6.5 years after an expected breaking point of public-key encryption is reached (see chapter 4.2.2).
- Major software and information technology businesses like Google, Microsoft and Amazon are pushing their on operations to quantum-safe cryptography and by their on estimations seem to be able to migrate before a breaking point is reached. The strategy and procedure for this kind of quantum-safe cryptographic migration is not shared to outside parties.
- The U.S. NIST has started the process of standardization of quantum-safe cryptographic encryption algorithms. The ML-KEM standard has been finalized and is set to replace the current quantum-vulnerable public-key encryption algorithms.

This chapter discussed the emerging consequences when all discussed points are brought together and followed to their conclusion. The progression of further digitalization and interconnection of every aspect of societal way of function is done with the foundational understanding of being in control of the access to information. Under a societally shared agreement on individual privacy, open access to data runs contrary to the norms.

It is the assumption of this thesis that currently used public-key encryption algorithms could be broken in an estimated time frame of as short as 10 years. This estimation is supported by the theoretical foundation of the encryption schemes and Shor's theory on breaking the underlying mathematical problem with quantum computing. In light of this, a migration to new quantum-safe cryptographic algorithms is necessary. Inaction could lead to an unprecedented situation of unprotected communication from quantum-capable malicious actors on a scale that impacts every element, where the said public-key encryption schemes are used. This includes the initialization of communication over the internet, and thus enables a major data interception potential.

The assessment of the probability of such an event is difficult to make. The path of quantum development and the theoretical design of breaking algorithms enforce the view of an inevitable point of decryption. To the point of impact, the complexity of quantum computing manufacturing is majorly decreasing the number of possible actors gaining the capability to execute this vision. The number of current actors and organizations involved would point to a select number of entities having total control over a quantum computing unit, while being able to share said capability through economic activity on a wider scale. A more credible actor would be intelligence agencies, the military or governmental institutions in general. It would present a unique opportunity to gain access to foreign secrets—be it from friendly or adversarial nations—while only having to rely on the communicated data over the networks, themselves invulnerable to outside influences. With a tense geopolitical climate, this alone presents a danger to national security difficult to ignore.

The described data privacy laws governing over the use of encryption (instead of the prevention of it) are general in nature and do not prescribe the use of specific cryptographic methods or algorithms. Both the U.S. and EU legislation protect the security of the information itself—leaving the implementation of said protection open to the responsible parties. The precedence set is one of shifting responsibility to the private sector. Under normal circumstances this will suffice to handle ordinarily occurring cryptographic vulnerabilities limited in scale. Based on this, a change to this behavior should not be expected to mandate the adoption of quantum-safe cryptography.

Major software and information technology seem to be aware of the importance of quantum-safe cryptography and claim to migrate to new cryptographic solutions. Without the specific cryptographic knowledge base, businesses in general seem to lack the foresight or ability to change their operational security before the estimated breaking point would be reached. An open discussion on the strategic approach to address this problem is not taken place at the scale that would encourage the adoption of quantum-safe cryptography.

In view of this thesis, the current situation is untenable. Current developments do not address the stated problem adequately. On an industry-wide scale, the cryptographic vulnerability will probably not be fixed before the expected arrival of quantum computing. In addition, the threat of harvest-now-decrypt-later attacks could compromise data privacy even before any decryption event takes place. Therefore, the need to establish a strategy to facilitate the quantum-safe cryptographic migration is identified. The strategy should address the migration on a macro level, describing the needed procedures and cryptographic concepts that in turn would be applicable and implementable on a micro level for individual businesses. This effort should aim to enable or accelerate the transition rate to quantum-safe cryptography on a wide scale to avert the described possible negative implications.

5 Development of post-quantum migration strategy

In this chapter the process of development of a cryptographic migration strategy is discussed. Based on the knowledge background established in chapter 2, the related works of Stapleton and Poore as well as Joseph et al. in chapter 2.4, the exploration of response in chapter 4 and its analysis in chapter 4.5, a comprehensive strategic approach will be aimed for that can provide guidance on how to proceed with the transition to quantum-safe cryptography. The proposed strategy relies on the past and present approaches to cryptography and cryptographic migration and the incorporation of different recommendations to address the challenges described in the previous chapters.

To complete the collection of related information to be considered for a strategic approach to quantum-safe migration, prominent past cryptographic migrations will be explored as to provide further information on the nature of cryptographic migrations. The process of development will proceed by identifying core challenges in cryptographic migration and use all gathered knowledge and information to formulate steps to address the stated challenge. The formulated steps will be amended by additional concepts from other fields to enhance the migration process.

5.1 Historic cryptographic migrations

This thesis will discuss two prominent examples of historic cryptographic migrations to potentially gain insight into the general procedure or strategy used in these past examples. The prominence of these examples should attest to the fact that the level of public discussion in academia or industry available regarding the chosen examples should far exceed any other historic event and thus provide a more comprehensive volume of information on cryptographic migration.

DES to AES

Cryptographic migration has taken place in connection with modern cryptography, as seen with the private-key encryption algorithm DES, already mentioned in chapter 4.3 as one of the first standardized cryptographic algorithms. Released in 1977 [93] the symmetric encryption standard was deemed insecure as to the limited key length of 56 bit being feasible broken in a brute-force attack with today's computational resources [6, p. 228]. In a timespan from 1997 to 1999 different projects demonstrated the feasibility of breaking DES with ever decreasing costs and time spend, with the last showing a time of only 22 hours [6, p. 234]. In response to the shown fallibility of DES, the U.S. NIST introduced the already in chapter 2.1.3 mentioned AES encryption standard as a replacement in 2001 [6, p. 238] [94]. This promoted a transition—a cryptographic migration—from the DES to the AES encryption algorithm. In 2005 NIST published a notice that the DES standard has officially been withdrawn as a Federal Information Processing Standard (FIPS) and the use of AES encryption is encouraged [112].

In a review of the development process of the AES standard by NIST itself, released in 2021, they describe AES as meeting the demand for a replacement of DES [113, p. 14]. They base this on their validation program of AES implementations, which recorded as many as 5770 AES validations in the 20 years since its release compared to 700 DES validations over the past 30 years [113, p. 14]. Furthermore, they state that the inclusion of AES in a range of IT-related standards from institutions like ISO/IEC and IEEE, as well as the implementation in prominent programming languages and applications, does prove the success of AES. Despite these claimed successes, an earlier analysis on the economic impacts of AES also conducted by NIST itself describes challenges hindering the transition process. In an associated survey, they queried several reasons as to the perceived challenges with the transition process, which included the following: 39% affirmed the perception of "Significant switching costs", over 50% affirmed the perception of "Significant hardware or software upgrades", 31% affirmed the perception "Internal or external 'push-back' ", only 20% affirmed the perception of "Significant training required" [114, p. 59].

Additionally, the review states the average timespan for the adoption of AES, giving further insight into the scale and momentum of prominent historical cryptographic migrations. For private sector consumers, the average "First year of AES adoption" is set to 2010 and the average "Last year of AES adoption" to 2014 [114, p. 57]. This means it took an average of 8 years after the introduction of the AES standard to start a migration and on average 12 years to complete a migration. For public sector consumers, the average year of first adoption shifts to 2009 with the same average completion date of 2014 [114, p. 57].

While taking place in a different environment and a less digitized time period, the DES to AES cryptographic migration does show some resemblance in scale and importance to the in this thesis mainly discussed quantum-safe cryptographic migration. The lengths of time shown in this historic migration do show a similarity with the estimated timespans for a quantum-safe cryptographic migration discussed in chapter 4.2. Subsequently, strategies and solutions from this prior cryptographic migration could inform a strategic approach to quantum-safe migration, which this thesis aims to formulate.

The thesis was not able to identify any sufficiently substantiated information in either academic or industrial discussion regarding the DES to AES transition process, in particular from an organizational or strategic viewpoint. To further clarify this point, any mentions of cryptographic migration or transition regarding DES to AES do discuss the theoretic background of each algorithm, i.e., how they work, the mathematical foundation, their distinct characteristics as well as their strengths, weaknesses, and fallibility [94] [113] [115]. But importantly, no or only superficial mentions of how any such transitions should be organized, which steps should be taken or which practices are beneficial as to planning and the procedural conduct of cryptographic migration, were made. The low number of 20% of participants in the NIST survey mentioned previously reporting the requirement of significant training for the transition process might explain the absence of this information as it indicates that the knowledge about cryptographic migration was deemed trivial in nature which would in turn not warrant further public discussion. This does not prove the nonexistence of such information but indicates the difficulty of obtaining any historical guidance.

MD5 to SHA-1 to SHA-2/SHA-3

Showing a more volatile development is the migration of cryptographic hash functions. In 1992, Ronald Rivest published the prominent *Message-Digest Algorithm 5 (MD5)* hash function [116], which quickly grew in popularity in software implementations for its speed over the DES algorithm [117, p. 5-6]. Potential weaknesses were identified as early as the same year of its release, diminishing its perceived security [117, p. 6]. The complete break of MD5 was achieved in 2004 by Wang et al. [118] demonstrating a feasibly executable way of finding collisions in the hash function [6, p. 249] [117, p. 6]. Since then, the MD5 has been evaluated as not secure for cryptographic use [6, p. 249].

Unsatisfied with MD5, NIST published its own cryptographic hash algorithm *Secure Hash Algorithm (SHA or later known as SHA-0)* in 1993 [119]. A technical flaw discovered after the release led to a revision of SHA as the *SHA-1* standard in 1995 [117, p. 6]. In 2005, analysis of the algorithm uncovered theoretical weaknesses to attacks and finding collisions, lowering the number of operations required in an exhaustive search [6, p. 249-250]. While possible, the brute-force of SHA-1 was at the time still deemed unfeasible, but nonetheless showed the fallibility of the algorithm. This promoted the following recommendation of NIST in 2006 for a rapid transition to the *SHA-2* collection of hash functions [120]. SHA-1 is not recommenced for use anymore and in December 2022 NIST announced plans to deprecate the standard by the end of 2030, while restating the recommendation of transitioning to SHA-2 or *SHA-3* [6, p. 249-250] [121].

In 2002, NIST released three additional cryptographic hash functions *SHA-256, SHA-384* and *SHA-512*, commonly referred to as the SHA-2 family of hash algorithms [117, p. 6] [122]. The 256,384 and 512 numbers indicate the bit size of the message digest of the hash function and an increasing level of security compared to the 160 bit size of SHA-1 [122]. Currently, no known attacks are evaluated as severe enough to compromise the security of SHA-2 and thus the algorithm is still actively recommended [6, p. 250].

Following the discovery of weaknesses in MD5 and SHA-1, NIST started a public competition for a new cryptographic hash function standard in 2007 [6, p. 250]. Similar to the prior AES competition and the future PQC competition, NIST invited public submissions and evaluations of candidate algorithms. The competition resulted in the SHA-3 standard released in 2015 with similar options in bit size as SHA-2 [6, p. 250]. Differing from the general structure of all previously mentioned hash functions, SHA-3 offers an increased security margin at the cost of performance in comparison with SHA-2 [123]. Despite the development timeline and naming scheme, both algorithms are considered as valid and secure at the current time.

The overlapping timelines of release, cryptographic analysis and discovery of weaknesses between all mentioned cryptographic hash functions show the fast pace of change and unpredictability of developments, which can happen in cryptography. As mentioned before in this chapter and explained in the previous chapter 2.1, the historical precedence is set on the inevitable break of any and all cryptographic schemes at some point in time. From inception, to standardization, to compromise of algorithm, to transition to a successor, decades could pass as evident in the prior DES example, or just a few years between the different SHA algorithms. To be prepared and protected from those rapid developments, it seems advisable to not just plan and execute a single cryptography migration, but introduce practices that enable multiple possible cryptographic transitions.

Similar to the previously discussed DES to AES migration, it was not possible to identify distinct information regarding the general strategy or approaches to planning and executing the process of cryptographic migration from the different cryptographic hash algorithms discussed. This claim is exclusively made about the strategic approach to the historical migration of MD5 and SHA cryptographic hash functions. Information about the mathematical foundation, comparisons of algorithms in security or performance and their implementation is publicly accessible [119] [122] [124] [125] but the concrete discussion about organizing a transition process is not found. This does not prove the nonexistence of such information but indicates the difficulty of obtaining any historical guidance.

In concurrence with the previous assertions about the availability of information regarding the transition process, the information space regarding historic cryptographic transition seems almost equally lacking in public discourse. To the question as to why such information is not openly available and easily accessible, this thesis can not provide a substantiated reason. Engaging in cautious speculation several confounding aspects may result in the lack of any substantial corroborated and peer reviewed information regarding cryptographic migration: The transition process itself may be regarded as the simple process of replacing one algorithm with another as described at the beginning of this chapter and thus self-explanatory. The transition process could be viewed as a distinct technical implementation or programming exercise inherent to the tasks of software engineers, without the need for any strategic approach to plan any such transition. In addition to this point the scale and urgency of prior cryptographic transitions could have been assessed as smaller and less severe and thus not receiving priority or resources to elevate the transition process to such an organizational level, despite the in hindsight long average transition times. In any case, on the side of the industry, any information regarding a cryptographic transition process could also be deemed as part of the institutional knowledge and therefore part of the marketable assets a business can provide. This would directly disincentivize any disclosure of information from any business capable of cryptographic migrations, which would coincide with the lack of information from IT and software development companies regarding the specific instance of quantum-safe cryptographic migration discussed in chapter 4.2. The lack of any actionable advice stemming from the exploration of migration is disappointing as despite evident migration challenges being present in the discussed examples, seemingly no academic or otherwise public review of the transition process has taken place so far.

5.2 Requirements analysis

To formulate a possible path to overcome the stated challenges of the previous chapters, it is necessary to identify and consolidate the general requirements such a proposition should fulfill. The requirements this thesis drafts originate from the collected facts and information, as well as their analysis and evaluation. The described disjointed and sparse information space around the topic of cryptographic migration and the quantum-vulnerability problem makes this process difficult as the varied nature of challenges organizations are currently facing leads to more generalized actions as to incorporate all associated parties in a proposed solution. Nonetheless should these requirements capture the essential features necessary to tackle the presented quantum-threat to cryptographic security. The presented requirements target the cryptographic migration process itself as the root of mitigating action, with post-quantum cryptography considered as an application of such proposed attributes. The order of stated requirements does not represent a definitive assignment of importance to each point.

R1 **Cryptographic security**

At the core of a proposed strategy should the intent stand to preserve and maintain the cryptographic security threatened by quantum computing capabilities. As described in chapter 2 currently used public-key encryption algorithms are vulnerable to attacks on their mathematical foundation with Shor's proposed quantum algorithm. Therefore, a mitigation strategy should prioritize and encourage the migration to quantum-safe cryptography.

R2 **Compliance**

The current framework of cryptographic legislation and data protection rights should be considered. The strategy should allow the pursuit of different cryptographic actions compliant with the various regulatory guidelines. The strategy should be able to adapt to changing laws and regulations to maintain compliance for the migrating party. This requirement is derived from the exploration of current governmental policy in chapter 4.1.

R3 **Scalability**

As the described number of individuals and organizations affected by the quantum-vulnerability is near universal, resulting from the wide-ranging utilization of public-key cryptography, a strategic approach to cryptographic migration should take the varied nature of actors and cryptographic applications into account. The strategy should both be applicable to individual operations, but also be able to scale to large businesses with a high degree of complexity to address the quantum-vulnerability problem as comprehensively as possible. The actors and operations associated with quantum-vulnerability were discussed as part of the intersection of cryptography and quantum computing in chapter 2.3.

R4 **Feasibility**

A proposed strategy should be aware of economic circumstances and limit itself to actions and behaviors that are deemed practical and implementable. Therefore, a strategy should offer a range of options to engage in while still achieving the objective of cryptographic migration. A strategy should consist of incremental steps or phases to allow different approaches to prescribed actions and simplify associated management and planning tasks. This requirement is derived from the same set of associated actors as discussed in the previous R3 requirement and chapter 2.3. The discussion of the current industrial response in chapter 4.2 confirmed the need for a realistic and feasible migration approach.

R5 **Flexibility and continuity of operations**

A proposed strategy should be aware of the environment of uncertainty of future developments in cryptography. The mitigation of the quantum-threat to current algorithms should therefore not just propose corrective actions to the threat as it is currently perceived but try to provide for contingencies. A disruption of operations by changing cryptographic algorithms should be avoided as much as possible. The preceding discussion about historic cryptographic migrations in chapter 5.1 described the scenario of rapidly changing cryptographic standards and showed a resulting need for algorithmic flexibility to stay secure.

R6 **Preparation for future cryptographic migration**

A migration strategy should propose actions that simplify the cryptographic migration process. This should translate to possible actions that reduce the time or effort required for additional cryptographic migrations to be conducted in the future. In addition to the proposed cryptographic flexibility, a broader set of behavior should be prescribed to prepare future migrations that would eventually have to take place if the progress of cryptography follows the historic pattern of eventual insecurity as described in chapter 2.1.

5.3 Practical problems and solutions

To enable or accelerate the post-quantum cryptography migration, the strategy development will proceed in outlining the practical problems hindering the transition process as identified in the course of this thesis. This list represents the culmination of problems and actionable steps regarding the general transition process itself, expresses in a simplified and compressed form. The framing of problem statements describes the thought process of identifying challenges associated with cryptography and cybersecurity, which then can be used to develop solutions to said challenges and in turn inform possible migration steps. In the discussion about resolving the stated problems, the prescribed order of conduct of a comprehensive strategic approach will arise.

#1 **Problem or challenge**

Affected parties are not aware of cryptographic vulnerabilities that currently are or in the future will compromise their privacy and security.

Proposed solution

To actively engage with a presumed problem or challenge the problem needs to be perceived first. This would mean that organizations need to have an engagement with the domain of cryptography at all times to monitor the current state of cybersecurity. This does also include the underlying theory to gain an accurate understanding of vulnerabilities and their consequences.

#2 **Problem or challenge**

Parties are unaware of the effect that a cryptographic vulnerability will have on them, their organization and their operations specifically.

Proposed solution

If a sufficient knowledge base of cryptography and perception of vulnerabilities is present, then an analysis of the impact of said vulnerability needs to be performed. This is necessary to make an evaluation if the organization itself is effected and action needs to be taken.

#3 **Problem or challenge**

What action is to be taken? What is to be replaced?

Proposed solution

The organization needs to have an understanding of what action is to be taken to remedy the vulnerability. In the case of quantum vulnerability, the effected cryptographic algorithms and their implementations need to be replaced. To know which algorithms need to be replaced and where they are located, an extensive cryptographic search needs to take place to identify every instance of vulnerable cryptography.

#4 **Problem or challenge**

How to replace?

Proposed solution

The replacement of an algorithm needs to be analyzed in terms of security and performance characteristics. To ensure compatibility within the organization and with external systems, the interoperability of the replacement algorithm needs to be considered.

5.4 Related fields to consider

In connection with the stated problems, other fields can inform the prescribed actions. Two fields of relevance could be identified that could provide guidance on how to solve challenges that are not unique to post-quantum cryptography migration.

5.4.1 Software supply chain security

A supply chain describes the movement and development of goods from the stage of raw materials to a finished product. Taking the perspective of the product, a number of suppliers were needed to supply their services, products or processed materials to assemble the end product. The suppliers in turn can also have a number of suppliers, which supply them with their services, products or processed materials. This succession of suppliers can be followed to some original service or natural resource. The collective of suppliers can be referred to as a supply chain for a single product, but can also be extrapolated to the supply chain of a class of products. [126] [127, p. 2-5]

The relationship of all participants of the chain signifies the reliance of everybody on their suppliers up the chain. Any disruption of the chain means all following steps of production can not take place and the end product can not be produced. The management of material provision and supply chains has therefore been an increasingly important task in a globalized economy with products of high complexity. [126] [127, p. 2-5]

To keep track of all the materials and components of a product, a 'bill of materials' (BOM) is used. This document lists all parts that are necessary for the assembly of a given product and in general represents a central knowledge point for all supplies for manufacturing said product. The BOM can be used in planning and organization of the manufacturing process and in the development of a supply chain providing the materials needed. In the case of material errors or other disruptions in supply, the BOM can be used to identify the point of failure and the associated supplier. [128]

The concept of supply chains and BOMs can also be applied to software. Complex software products can be assembled with externally supplied components, such as functions or libraries from open or closed sources. With these libraries often making calls to other software libraries or functions, the same chain of code supply emerges as described in traditional manufacturing. Analogous follows the concept of 'software bill of materials' (SBOM), which contains all the software's components and external software dependencies. In case of malfunctions, bugs, discontinuation, or updates, the SBOM can identify the source of failed or out-of-date components and thus secure the function or continued function of a software product. [127, p. 2-5] [129] [130, p. 3-6]

The quantum vulnerability of current public-key encryption algorithms could be viewed as a disruption of the function of an important software component responsible for the privacy and security of communication, for example. To identify if this type of affected cryptography is used, in which part of the software and where it was supplied from, an SBOM-type of list of cryptographic algorithms used would give a substantial information advantage in the awareness of quantum vulnerability in one's own specific software and also give indications as to where these instances can be found. In fact, the whole concept can be expanded to not just correspond to the current quantum vulnerability, but to all cryptographic vulnerabilities that could arise.

The expansion of SBOM to the domain of cryptography is currently referred to as the 'cryptographic bill of materials' (CBOM) [131] [132]. The use of CBOMs could drastically reduce the effort necessary for the cryptographic migration process to quantum-safe cryptography as it provides two key indicators: first it stores which type of cryptographic algorithms are used and thus shows if a given vulnerability is impacting the software at all and second when an impact is identified where in the code the use of cryptography is located [131] [132]. Both are integral to any transition to quantum-safe cryptography, and therefore the concept of CBOMs should be incorporated in a strategic approach to cryptographic migration.

5.4.2 Cryptographic agility

The concept of cryptographic agility refers to the ability of digital systems to react to differing cryptographic environments or change their cryptographic scheme [68, p. 241]. This concept was already mentioned several times in this thesis as part of the related work and the general recommendations for post-quantum cryptography migration and thus should be explored and analyzed as to its theoretic functionality and the possible use-case for an incorporation in a strategic approach to cryptographic migration.

As described in chapter 2.1.5, cryptographic migration describes the process of changing the cryptographic scheme of any system to a different one. This becomes necessary to preserve the security and privacy granted if the current cryptography is compromised. As described throughout this thesis and earlier in this chapter, a cryptographic migration is often connected with an extensive amount of effort and resources, resulting in slow and delayed responses to cryptographic vulnerabilities [3]. The introduction of new cryptographic algorithms does imply the rewrite of software and its source code and the updating of systems, making the replacement prohibitively complicated and costly.

Instead of implementing one specific cryptographic scheme, as it is the implied standard in the history of normal product development behavior, a concept of flexibility and adaptability is implemented. This agility in turn would reduce the amount of effort and resources required for any cryptographic migration [68, p. 241]. How big the reduction is and what cases of change are supported is dependent on which agile properties were prioritized. As part of the proceedings of the German BSI organized 18th German IT-Security Conference in 2022 Alnahawi and colleagues made the following four categorical distinctions of how crypto-agility could be achieved as part of their paper describing the current state of crypto-agility [133]:

- *Algorithm and Protocol Agility*

  While cryptographic algorithms themselves can have agile properties, in general, they are not considered crypto-agile. The recombination of different algorithms into a hybrid encryption scheme can introduce agile properties and eliminate the reliance on one specific encryption algorithm, as in the case of compromise, the other algorithms making up the hybrid set still provide security. The use of hybrid scheme can be incorporated into cryptographic protocols and extend the agile properties to them as well. The authors describe the use of hybrid schemes as a reduction of reliance on single algorithms and thus introducing flexibility in regard to vulnerabilities. [133, p. 4]

- *Design Agility*

  Agile properties can be achieved through design considerations in the process of product development. This can be achieved through the variability of algorithm parameters such as adjustable key-lengths, with the peak flexibility at complete algorithm independence being implemented. This concept also includes the capability of enabling updateability of cryptographic software components. [133, p. 5]

- *Hardware Agility*

  The operations of encryption algorithms are often accelerated with purpose-built hardware components that speed up the execution time and reduce resource usage. To introduce cryptographic agility in this domain, new ways of repurposing this proprietary hardware for other algorithms or incorporating accelerators for new cryptographic algorithms need to explored and implemented. [133, p. 5]

- *API Agility*

  This concept describes the use of agile cryptographic libraries and APIs to achieve crypto-agility. Instead of hard-coding specific cryptographic algorithms, an abstraction layer is created that, rather than directly executing a cryptographic algorithm, references a cryptographic library or other API, at which the encryption algorithm is implemented. This leads to a centralization of cryptography implementations and makes the exchange of one algorithm for another considerably easier, as only the dedicated library or API needs to be adapted without having to update any cryptographic reference. [133, p. 5]

As the slow historic adoption patterns of new cryptographic algorithms show, crypto-agility so far has not been adopted on a wide scale as to enable rapid adaptation as to the discovery of new cryptographic vulnerabilities. For crypto-agility as a concept to effect and facilitate cryptographic migrations, it needs to incorporated into new software being created. Existing software would likely need an extensive rewrite to implement any of the agile methods described, and could therefore be interpreted as equally expensive in resources and effort as any other cryptographic migration. But the lack of direct cost reduction can be offset by any future cryptographic migration, as even one more migration of otherwise equal cost could be drastically reduced by a centralized cryptography implementation, minimizing the number of algorithm changes to potentially just one. Additionally, it would allow the preparation of a cryptographic migration even before any new standard would be released. Both of these points extensively are applicable to the current quantum vulnerability: The somewhat unpredictable nature of scientific progress makes it unclear when exactly quantum-vulnerable algorithms will get broken. But in general, the predictions of a breaking point being reached already predate the majority of efforts of post-quantum cryptography introductions, as described in the BSI survey in chapter 4.2.2. The intensifying chance of harvest-now-decrypt-later type of attack as well points to transitioning to quantum-safe algorithms as fast as possible. But with only few or unproven quantum-safe cryptographic standards available, the decision to transition is made difficult. With the concept of crypto-agility, a migration could be prepared at any time, even before any regulatory or standardization effort is completed. With final consensus on a new algorithm, it can be implemented with less time and effort investment, as the brunt of transition work has already taken place before. Additionally, any introduction of further new cryptography in the future will benefit from this style of implementation.

5.5 Result

Based on the discussion in this chapter, an approach to the post-quantum cryptography migration is to be formulated. The approach is to cover a wide range of applicable cases and combine all the information presented in this thesis, as well as incorporate past and present recommendations on cryptographic transitions extracted from publicly accessible information or related work.

5.5.1 Step 1: Cryptographic background and discovery

The starting point to any considerations about actions and changes is to have a solid foundation of knowledge of the related topic and have an awareness of the current environment it exists in. The first step of the approach to post-quantum cryptography migration starts with the imperative of developing a base level of knowledge on the theoretical foundation of cryptography in general, what purpose it serves and how this purpose is achieved. This includes concepts such as public and private-key cryptography and their uses, such as digital signatures. The complete mathematical and logical breakdown of every cryptographic scheme is not directly required to understand if any action in the domain of cybersecurity has to be taken. The level of knowledge deemed acceptable to start the next steps of the migration process is equivalent to the information conveyed in chapter 2.1 of this thesis. This base-level understanding should be sufficient to engage in the current information space around cybersecurity and cryptography from public and private publications, academic institutions, governmental agencies, business operations and important bodies like standardization organizations.

The consumption of publications from all these organizations is necessary to be informed and stay informed on current developments and trends pertaining to the field of cryptography. Sources of news need to be weighed as to their value of information, with organizations with a high degree of authority and trust, such as governmental agencies, providing the highest level of value. To maintain a feasible continuous operation of this first step, a scale of effort is introduced. Not every piece of information is of importance, at all points in time. Depending on the available resources, a prioritization of information and sources needs to take place that will take advantage of the collective intelligence of the domain as a whole to act as a filter for important news. This spectrum of engagement starts with the engagement of every piece of news by individual journalists or private individuals as well as unvetted academic discussion and stretches to the other end with the consumption of information only if the sources of highest value cover and agree in unison on some form of informational content. The certainty of engaging with important information that needs to be considered further is given if a piece of information wandered through all levels of sources and was deemed credible or correct by all participating organizations. Despite the inherent imperfect nature of having to rely on several third parties to supply this kind of reporting and analysis, in the view of this thesis, this behavior is the most practical approach to gain relevant current information on the topic. In the context of this thesis trusted sources include the United States government and its institutions, the European Union government and its institutions as well as the EU member states' government and their institutions, publications having gone through the academic review process, standardization institutions and major businesses associated with software, software security and cryptography.

Having a continuous engagement with the current state of cryptography and a basic level of theoretical background will provide the necessary possibility of receiving critical information regarding cryptographic vulnerabilities and the ability to view these vulnerabilities in the broader context of the domain. This is essential to establishing a strong conviction for any kind of action imperative being formed. Engaging in the described behavior will equip any person in a related position from developer to management to make an informed decision as to the need to take further steps in the process of cryptographic migration—before any kind of more in-depth analysis will take place. If this kind of decision is not made with the appropriate level of background knowledge, no classification of importance or general implications can be made, which in turn leaves any planning without guidance on the necessary appropriation of needed resources.

The execution of this step can be assigned to every level of a related corporate or organizational structure, depending on the specific designation of responsibility of cryptographic security. The deliberate decision made in this migration strategy to prescribe the establishment of knowledge only on a level sufficient to understand the general landscape of cryptography but staying above mathematical or technical details opens this process for all stakeholders. This allows both a bottom-up or top-down approach to the organization of a cryptographic migration. The intention is to supply the necessary topical information to decision makers and policymakers of cryptographic security wherever they may be located in an organization's hierarchy to force an acknowledgment of the presented information. The engagement of managerial positions secures the capability to enact and enforce the change that is inherent to a cryptographic migration and is essential to gain the allocation of an organization's resources. The implementation of this workflow could thus be located at the low organizational level of the developers themselves who now would establish the prescribed knowledge base and continuous discovery of cryptographic vulnerabilities, compile this information and inform a higher up position in the organization's structure until an acknowledgement and resulting action is achieved. The reached decision then presumably follows the structure down again to positions responsible for subsequent steps of the migration strategy. It becomes evident that the higher this process starts on a managerial level the less recompiling and reprocessing of information has to take place from the source of information to the decision maker, making a top-down approach at least equally viable if not beneficial in the right circumstances of organizational structure. The investiture of responsibility for this first step can in this way also be settled outside the organization itself. Holding organizations or a domain-overarching board could assume the task of building the required cryptographic knowledge and informing its members of vulnerabilities and consequent actions. This concept could even be extended to cover a broader jurisdiction as part of a governing body providing and regulating cryptographic policy. The similarity of what is described to the currently presumed tasks of related government institutions is recognized, but as demonstrated throughout this thesis is that the extent of prescribed actions reaches beyond current responsibilities.

The application of this procedure to the quantum vulnerability makes this process straightforward. Instead of a continuous exploration of cryptographic vulnerabilities, the engagement can be focused on a specific instance of importance and the behavior can be adjusted accordingly. Still, the case for cryptographic migration has to be built diligently to establish the background with a convincing argumentation. That means that the prescribed foundation of cryptographic theory is still necessary to develop an accurate understanding of what is described and alleged in the context of the quantum computing. Nonetheless should the compilation of related information in this instance require far less effort as the threat profile of quantum computing has already reached all previously mentioned levels of sources. Throughout the chapters, this thesis has engaged in the prescribed procedures and established a foundation of cryptographic theory, as well as discovering the quantum vulnerability problem this migration approach is founded upon. The results of this behavior is the content of the chapters 2, 4 and 4.5. These chapters stand in as one example of the cryptographic background and vulnerability discovery step of the proposed migration strategy.

5.5.2 Step 2: Cryptographic operational impact analysis

After having established a solid knowledge foundation on cryptographic and software security matters and having discovered a general cryptographic vulnerability of importance, it has to be analyzed and evaluated if and to what expend said vulnerability will have a direct impact on the operation of one's own organization. Several questions should be asked and answered to gain an accurate picture of the potential impact or damage a particular vulnerability could have on one's specific system in use.

(1) Do you use any system, software or cryptographic algorithm that is affected by said vulnerability?

(2) Are you reliant on any external system or software that is affected by said vulnerability?

(3) Which operations of your organization are linked to the instances of use identified in the previous question?

(4) Who is responsible for the software security or cryptographic implementation of potentially affected systems or software?

The answers to the posed question directly influence the type of mitigation proceeding, potential timetable of action and resource allocation depended on the level of prioritization. Questions (1) and (2) mark the first waypoint, deciding if any action has to be taken. Only a clear and direct negation of these question allows the return to the continuous state of step 1 of the migration strategy. If questions (1) or (2) are affirmed, the migration proceeds as prescribed. If the question (1) can not be answered due to the lack of knowledge or uncertainty to any use of said affected cryptography, one has to proceed directly to step 3 of the migration strategy to identify all cryptography used in one's own software.

An impact analysis is necessary to plan and prioritize the next actions to be taken. The nature of this analysis is not set and can vary in the level of extensiveness and depth depending on the available resources for this process. The intent of this analysis is to gain an accurate representation of consequences and coherence of affected systems or software should a vulnerability disrupt the security granted through cryptography. The depth of this analysis should extend as to comprehensively describe the state of affairs resulting from the vulnerability's effect on the answer given to question (3) but nevertheless should not overextend as to cover needless details. It is far more important to identify if any impact is possible, as opposed to conducting a lengthy calculation of the estimated dollar amount of damage accurate to the second decimal place. It is of interest to conduct this analysis as fast as reasonably possible and restrain the content to core operations. This allows for a rapid localization of impact, making subsequent evaluations of potential damages for the organization far easier. The judgment derived from this process should suffice to make claims of potential impacts and damages in the order of magnitudes to accurately describe the severity of the cryptographic vulnerability. This in essence mirrors the process of a traditional risk assessment and can be understood as such. While not as formulaic or extensive as warranted in normal financial or economic circumstances, similar objectives are to be reached—to identify, analyze and evaluate risks associated with a cryptographic vulnerability to justify a cryptographic migration.

The impact analysis is directly used to allocate the organization's resources in an effort to mitigate the found cryptographic vulnerability. Depending on the criticality of the potentially affected area and the nature of vulnerability discovered in step 1 of the migration strategy, a comparative amount of urgency and effort is to be expended. The evaluation of danger and damage in general has to be considered on an individual basis, and therefore a clear threshold for action or inaction can not be prescribed in this strategy. In any case of total loss of security, the highest efforts should be applied to restore the security state.

In the case of the quantum vulnerability of current public-key encryption algorithms, an almost universal applicableness of the vulnerability can be assumed as to the wide-ranging use of the encryption as discussed in this thesis. But this should only be understood as an expression of probability of if one is impacted—the confirmation, however likely, still has to be made regardless to justify any further actions. Should the development of quantum computing progress in the same manner as it has in the last years, a point of executability of quantum algorithms will be reached that allow the decryption of current public-key cryptography and thus the complete loss of cryptographic protection granted by these algorithms. The analysis on this kind of total cryptographic failure can therefore be conducted under binary assumptions of security. The consequences of this assumption need to be estimated for the one's specific organizational environment and circumstances.

Any impact analysis on this vulnerability should also be aware of the harvest-now-decrypt-later type of attacks described in chapter 2.3.2. In addition to the complete decryption at some point in the future, there also exists the possibility of interception of encrypted data at the present which could be decrypted at a later point in time. The likelihood of this type of attack, when it could be expected, what kind of data could be intercepted, and how severe a data leak of this kind would be, are all aspects that need to be evaluated for the specific organization's operations and the results contribute to the prioritization of resources and effort for a potential migration.

The question (4) is important to the assigning of responsibility of action for the mitigation of the impacts identified in the impact analysis. If systems, software, or parts of software are outside the organization's control, the need for actions needs to be communicated to external parties and the expected mitigation of identified issues should be discussed. If no satisfying resolution can be found that adequately addresses the vulnerability in an acceptable timeframe then a decision has to be made on how to proceed in the use of said systems or software, with the organizations itself taking on the responsibility to create the functionality or contract a new supplier of equivalent functionality not compromised by the vulnerability. If the organization itself is responsible for the affected parts, the next steps of the cryptographic migration have to take place.

5.5.3 Step 3: Cryptographic inventory

The first and second step of the migration strategy develop an informed decision-making process that builds the basis for a strong intention for an action and the conviction of all involved stakeholders to execute on said intention. With a shared understanding of the underlying facts of the matter and a formalized reasoning on mitigation, the next step of the migration can take place. As this thesis focuses on the quantum vulnerability of software encryption algorithms, the following discussion will exclude the handling of cryptographic hardware. Nonetheless could the general steps of conduct be extrapolated and applied to the exchange of vulnerable cryptographic hardware components.

In the simplest of terms, the third step of the migration strategy involves the identification of source code that contains the implementation of cryptographic algorithms compromised by the discovered vulnerability in the first step of the migration strategy. The exact location of every instance of vulnerable algorithms needs to be established, as to conduct a comprehensive transition to an uncompromised encryption algorithm. Failing to address all instance of the affected cryptography leaves points of entry for potential attackers taking advantage of the known vulnerability.

In the case of the quantum vulnerability this means the migration of all instances of prominent public-key encryption algorithms like the RSA algorithm, key-exchange algorithms and digital signature algorithms as described in chapter 2.1.3, 2.1.4 and 2.3.1. The identification of the cryptography instances in the source code is the primary task of this third step of the migration strategy. Depending on the size and complexity of the software and available resources, a range of possible options of conduct present itself for this task. The evident requirement is the availability of personnel capable of implementing security related algorithms in code.

The most basic approach would be to manually go through each line of code to find all cryptography instances. This manual approach has to be evaluated for each software repository by its holders as to the feasibility with regard to time and resources this would require. Alternatively, automation tools could be introduced to take advantage of computational resources to scale the search for cryptographic instances for large codebases. While the automated detection will decrease the human input required, the implementation of the scanner infrastructure may exceed the gained savings and may require changes to the software itself [134]. The immense benefits in scaling are also only achievable in the specific types of vulnerability detection currently available [134]. Many scanning products offer additional functionality in vulnerability detection and general code pattern recommendations as to make the implementation worth it if other benefits are factored in [134]. If no automated tools or products for cryptography or vulnerability detection are in use, an analysis should be done as to the feasibility of a manual search—if automated scanning software can be used which automated scanners are available and what functionality they offer, and if the implementation of said scanning software is feasible. Both approaches build the knowledge necessary to proceed with the next step of cryptographic migration.

Substantially facilitating the described task is the concept of cryptographic agility, as described in chapter 5.4.2. Crypto-agility defines the concept of making the transition of cryptography as easy as possible by increasing compatibility with different algorithms and systems and, more importantly in this case, introducing design principles that make the transition of code implementations easier. The concept of API agility prescribes the use of an abstraction layer for the use of encryption algorithms, centralizing the implementation of cryptographic algorithms as much as possible with subsequent code referencing this central point. The deliberate and conscious reduction of cryptographic implementation can in this way make the task of cryptographic detection redundant if—taken to the maximum—only one central instance of cryptography has to be found and identified. The implementation of the API agility concept would reduce the effort and resources needed to perform a search and in turn can change the viability analysis of manual and automated cryptography detection, making further detection tools superfluous and saving additional detection infrastructure.

In the process of cryptographic migration, a replacement of all found vulnerable cryptographic instance would have to take place. If no cryptography agility has been implemented so far, an analysis should be made as to the feasibility of specifically taking the concept of API agility and integrating an abstraction layer of calls to a minimized number of cryptographic implementations in the software. Depending on the circumstances of the individual software product the addition of a central cryptography implementation to the replacement of vulnerable algorithms, which would take place either way, might add comparatively little effort and cost compared to future benefits granted through cryptographic agility.

An additional recommendation of this strategic approach to post-quantum cryptographic migration with the future in mind is the establishment of a persistent cryptographic inventory. This concept intersects in its intent with the just discussed crypto-agility but also covers additional properties of continuous vulnerability discovery. A cryptographic inventory would entail the type and specific code location of any cryptographic algorithm implemented and can contain additional information such as the origin of algorithm, the maintaining party and associated liability. A permanent up-to-date cryptographic inventory would eliminate the whole identification-of-cryptography process as all the needed information to proceed with the migration is already established and thus not just applicable to one cryptographic migration but all future cryptographic migrations. As with the concept of crypto-agility, the establishment of a cryptographic inventory does represent an additional cost factor that requires constant maintenance to not lose its reliability. But also, like with the introduction of crypto-agility, it can be argued that in a simple one-time migration the process of identification of cryptographic instances would have to take place either way and thus elevating the results with an emphasis on permanence should be possible with comparatively little additional effort and cost compared to future benefits granted through a cryptographic inventory.

The knowledge contained in a persistent cryptographic inventory does also inform the second step of the proposed migration strategy as it directly enables the connection of a discovered vulnerability in the first step with any cryptography used and thus providing certainty as to the extent of any effect on the organization. In a standardized format, the cryptographic inventory could also be integrated into automated vulnerability discovery tools, which would alleviate the effort spent on actively seeking out the discovery of cryptographic vulnerabilities. The standardized cryptographic inventory would serve as a comparable template of cryptographic information in use, making the discovery process simpler in identifying affected parties. Therefore, it should be analyzed if the introduction of CBOM-like cryptographic inventory templates, as described in chapter 5.4.1, is feasible.

Both discussed concepts of crypto-agility and CBOMs would offer benefits for the process of migration. Both can work in tandem, but also independent of each other if available resources or other circumstances do not present the possibility for the pair. The additional effort and cost of integrating these concepts in comparison to a simple one-time migration should be offset in resources and time saved from even just one additional cryptographic migration as the steps of discovery, impact analysis and inventory all can be simplified and streamlined.

In the case of external software products, libraries, or any other kind of code in use with origin outside the organization, the same conduct can and should be requested to gain the benefits described. In the context of a such a software supply chain relationship, the use of a cryptographic inventory could inform the supplied party with all necessary information to perform the important second step of the migration strategy without the need to have accessed or analyzed the underlying code. A CBOM-like framework of organized cryptographic content in software allows the independent confirmation of cryptographic security as described throughout the vulnerability discovery process and the operational impact analysis, eliminating reliance on external partners for this activity. It also inadvertently forces the supplier to prepare himself for cryptographic migration in the process of providing such information. Passing this requirement along a chain of suppliers does thus not just provide extensive information about cryptographic instances but equip all participants with the ability to react to demanded cryptographic changes in their supplied software and apply the described benefits to their own vulnerability discovery process. With a CBOM-like framework at hand, the migration process can proceed even without direct control of the underlying asset, but still allows a directive to the supplier which specific algorithms needed to be exchanged to maintain the secure use of their software.

All in this step discussed concepts and behaviors are applicable to cryptographic migrations in general and therefore also to the current problem of quantum vulnerability of public-key cryptography. All stated recommendations stay the same, with all instances of public-key cryptography needing to be identified for potential replacement with quantum-safe algorithms. Crypto-agility and the centralization of cryptographic algorithm implementation would simplify the replacement of current public-key algorithms with any new algorithm with the additional benefit that this step of centralization could be conducted even before any new quantum-safe algorithm is standardized or deemed acceptable. The work of finding and replacing all instances of public-key cryptography could be front-loaded while academic discussions, testing, and standardization processes for post-quantum algorithms take place, cutting the time of inaction and accelerating the migration process. In light of the discussed timeline problems of many organizations facing the problem of quantum vulnerability, it would provide an essential tool for preparing the final migration step without already committing to any cryptographic algorithm. The introduction of CBOMs would equally prepare the final step of migration, as its implementation is equally independent of any new development or standardization of cryptography and can therefore be pursued immediately. In addition, a CBOM would provide a continuous template of comparison between newly discovered vulnerabilities and their effect on one's specific organization. Both concepts should be pursued to their fullest extent possible.

5.5.4 Step 4: Cryptographic correction

Having identified all instances of cryptographic vulnerability, the fourth and final step is the replacement of these algorithm implementations with secure alternatives. The identification of secure and compatible cryptographic algorithms is vital for the sustained privacy, security, and overall function of the organization's operations. The wrong choice of algorithm can lead to the breakdown of software or systems, as its functionality could be compromised or diminished by unsuited cryptographic algorithms.

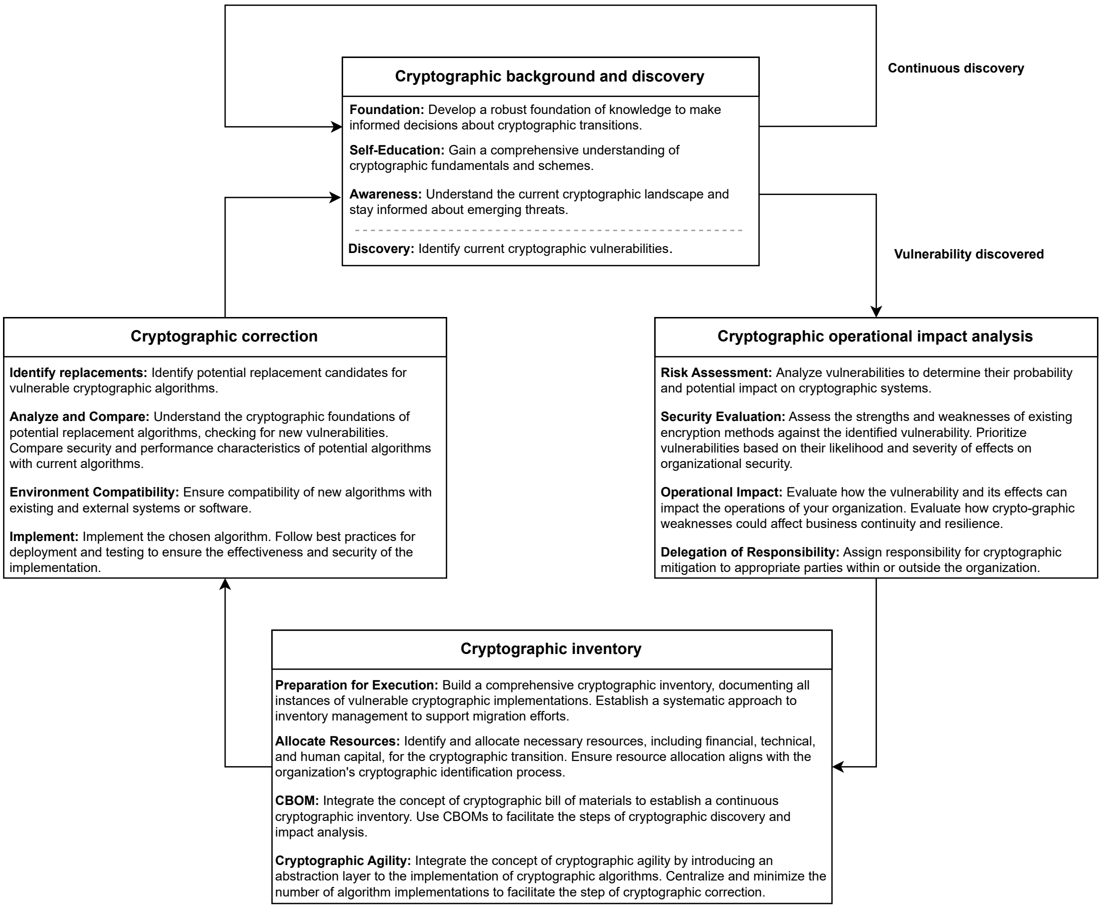
An analysis has to take place as to the characteristics of the currently used algorithm in comparison to any replacement candidate. Therefore, information regarding any new algorithm needs to be gathered and evaluated. This includes establishing a general understanding of the underlying theoretical architecture providing the cryptographic security, with a following analysis if the new cryptographic mechanism has any known vulnerabilities. If deemed architecturally sound, the properties of the algorithm need to be evaluated for the specific use case, which includes characteristics like the proposed key-length and the level of proposed computational complexity. Depending on the circumstances, an appropriate level of cryptographic security through complexity should be chosen as in general, higher cryptographic security implies higher computational complexity, which in turn often correlates with higher performance requirements. Depending on the operational environment these performance characteristics such as an increased encryption process duration or larger message digest can have a large impact on data-driven operations which could lead to further investments being necessary such as increased storage infrastructure, larger networking capabilities or faster cryptographic processing power. In addition to these properties, the operational environment needs to be kept in mind. If cryptography is used in the cooperation with other user or systems outside the direct organization's control, a migration to a new cryptographic algorithm will disrupt the shared operations if the partner does not support said algorithm. For software or systems where this is the case, an analysis needs to take place to ensure the compatibility with outside systems.

If a suitable candidate is found and the described analysis is concluded with satisfactory results, the implementation of the algorithm can begin. All available open-source resources should be used to simplify the implementation process, including code samples or cryptographic libraries. Code implementations of popular encryption algorithms are often publicly available for a variety of different programming languages [135] [136] [137]. If no prior work is available as reference, the implementation has to be conducted thoroughly and precisely as the chosen cryptographic algorithm is described in its documentation. Errors in the correct code translation can lead to the compromise of software security or function and introduce new vulnerabilities specific to only this implementation.

The search for a suitable new algorithm follows the same procedure as laid out in the first vulnerability discovery step of the migration strategy. Depending on available resources, a spectrum of sources should be considered, with weight given to more trusted sources such as governmental institutions, academic institutions or standardization organizations if available resource for this process are a constraint. This information is often already being discussed as part of the publications of vulnerabilities, and thus a superficial outline of information could already be established within the first step. A further simplification of the search and evaluation process can be achieved when one relies upon the work of standardization organizations such as NIST, ISO, etc. These organizations publish standards for cryptographic algorithms covering a wide range of use-cases and scenarios, aiming for an adequate level of cryptographic security and performance for public adoption. The popularity of cryptographic standards leads to a wide range of use, and therefore also a high degree of support, ensuring compatibility with a wide range of software and systems.

If the implementation of the algorithm in question lies with external sources, this process of algorithm selection could be assigned to said party after a vulnerability was discovered. To retain and preserve the cryptographic awareness built throughout the prescribed migration steps, it is in the interest of the instigating party to stay connected with such a replacement process. The corroboration could remain as a passive observer but extend to actively engaging and prescribed cryptographic changes to be made. In either case, the concepts of cryptographic agility and the cryptographic inventory have to be maintained if implemented and an updated CBOM should be required. If the current supplier or source is not able to adequately replace vulnerable algorithms, a new supplier or source should be engaged. For any new external software in use, the requirement should be set that a CBOM-like cryptographic inventory has to be provided and maintained to proactively build the capability to easily evaluate newly discovered cryptographic vulnerabilities as well as transition to safe cryptography rapidly.

For post-quantum cryptography, the search for a new algorithm becomes difficult, as many new algorithms are not yet adopted and proven in the real world and therefore have not established a level of trust in their functionality. As described in chapter 4.3.1, standardization of post-quantum cryptography algorithms is currently in the process with the ML-KEM algorithm as the sole finalized candidate for quantum-safe public-key encryption, with more algorithms to be standardized in the future. The transition to this new post-quantum cryptography algorithm should only be executed if the risk of using a tested but still relatively unproven algorithm is known and in case of errors or new-found vulnerabilities a rapid migration to a different algorithm can be attested to. Additionally, the migration should only take place if the compatibility with other external systems and software can be ensured. Otherwise, the migration to post-quantum cryptography should be prepared as much as possible, as soon as possible, with the final implementation of a new algorithm in standby until all external factors can be accounted for. With the introduction of a cryptographic inventory and cryptographic agility in the previous step, the final implementation of a new cryptographic algorithm should be possible at an instant, giving the organization the ability to finish the migration at any point in time they feel comfortable. The figure 5.1 illustrates and describes the proposed steps of the migration approach in a simplified form.



Cryptographic background and discovery

Foundation: Develop a robust foundation of knowledge to make informed decisions about cryptographic transitions.

Self-Education: Gain a comprehensive understanding of cryptographic fundamentals and schemes.

Awareness: Understand the current cryptographic landscape and stay informed about emerging threats.

Discovery: Identify current cryptographic vulnerabilities.

Cryptographic correction

Identify replacements: Identify potential replacement candidates for vulnerable cryptographic algorithms.

Analyze and Compare: Understand the cryptographic foundations of potential replacement algorithms, checking for new vulnerabilities. Compare security and performance characteristics of potential algorithms with current algorithms.

Environment Compatibility: Ensure compatibility of new algorithms with existing and external systems or software.

Implement: Implement the chosen algorithm. Follow best practices for deployment and testing to ensure the effectiveness and security of the implementation.

Cryptographic operational impact analysis

Risk Assessment: Analyze vulnerabilities to determine their probability and potential impact on cryptographic systems.

Security Evaluation: Assess the strengths and weaknesses of existing encryption methods against the identified vulnerability. Prioritize vulnerabilities based on their likelihood and severity of effects on organizational security.

Operational Impact: Evaluate how the vulnerability and its effects can impact the operations of your organization. Evaluate how crypto-graphic weaknesses could affect business continuity and resilience.

Delegation of Responsibility: Assign responsibility for cryptographic mitigation to appropriate parties within or outside the organization.

Cryptographic inventory

Preparation for Execution: Build a comprehensive cryptographic inventory, documenting all instances of vulnerable cryptographic implementations. Establish a systematic approach to inventory management to support migration efforts.

Allocate Resources: Identify and allocate necessary resources, including financial, technical, and human capital, for the cryptographic transition. Ensure resource allocation aligns with the organization's cryptographic identification process.

CBOM: Integrate the concept of cryptographic bill of materials to establish a continuous cryptographic inventory. Use CBOMs to facilitate the steps of cryptographic discovery and impact analysis.

Cryptographic Agility: Integrate the concept of cryptographic agility by introducing an abstraction layer to the implementation of cryptographic algorithms. Centralize and minimize the number of algorithm implementations to facilitate the step of cryptographic correction.

Figure 5.1: Representation of the proposed strategic approach to cryptographic migration.

6 Evaluation and discussion

This thesis set the point of discussion on the unclear path forward as to the response to the problem resulting from the new capability of quantum computing and its impact on cryptography. With the quantum vulnerability compromising current public-key encryption algorithms at some point in the future in addition to the potential harvest-now-decrypt-later-vulnerability in the present, the apparent limited acknowledgment and action to this, leads to the thesis's hypothesis of the lack of discussion and research in the cryptographic migration process being responsible for insufficient progress. To research this theory, an extensive compilation of information from different domains had to take place, analyzing the intersection of all and ascertaining the current response.

As stated in chapter 1.1, a series of seven consecutive hypotheses were made, describing the reason for a perceived lack of attention and action in response to the quantum vulnerability of public-key cryptography. The general correctness of the ascribed logical progression was affirmed in the course of this thesis, and no hypothesis is outright proven false. Nonetheless, amendments need to be made as varying degrees of accuracy can be assigned to some of the statements made, decreasing the veracity of the overall claim made. The hypothesis (1) and (2) are based on prior established facts described in the background chapter 2 and remain true. The broad statement of hypothesis (3) does leave room for argumentation as to its extensive range of institutions and organizations covered, but its meaning is aimed to describe a currently observable trend. The exploration and discussion of the response in chapter 4 and 4.5 affirms this claim in its general nature, but describes several specific instances of exception. The same chapters as well as the related work chapter 2.4 provide the affirmation of hypothesis (4).

The foundation of these first four hypotheses led to the main logical deduction of hypothesis (5). The matter of fact claim being made in its more hyperbolic fashion certainly has to be scaled back to a more reserved claim of only very little public discussion taking place, resulting from the description and discussions in the related works chapter 2.4 and in chapter 4. The prescription of sole consequence of hypothesis (4) for hypothesis (5) does also lack in its accuracy after taking the contents of the same stated chapters as well as chapter 5.1 into account. Rather than just a missing discussion around the quantum vulnerability of public-key encryption being responsible for a lack of acknowledgment and action, it became apparent that the current research effort on applied cryptography and cryptographic migration in general is the more foundational problem. While a lack of public information and discussion on post-quantum cryptography certainly contributes to the current migration problem, the under-representation of the field of cryptographic migration in public institutions has failed to establish a general competency to deal with cryptographic vulnerabilities as already seen in lengthy, unorganized historical migrations.

Given both the original claim of hypothesis (5) and the amended version, the hypothesis (6) is affirmed by the chapters 2 and 4 with the BSI survey on post-quantum cryptography serving as the key piece of evidence. The last hypothesis (7) can not be confirmed in its entirety in the scope of this thesis. It was established that the lack of research and public discussion around cryptographic migration failed to establish a solid base of knowledge and recommended behavior, which contributed to the difficulties of past cryptographic migration as well as the current transition to quantum-safe cryptography. The development of a migration strategy counteracts this observation and contributes to the field of cryptographic migration and applied post-quantum cryptography, while the extent and impact of this contribution is left to further research and analysis.

The nature and scope of recommended actions in the proposed strategic approach to cryptographic migration directly results from the current landscape of applied cryptography and cryptographic migration as a field of research. In the course of this thesis, it has become evident how unexplored this area of cybersecurity is in relation to the impacts cryptographic security failures can inflict, as discussed in chapter 2.3. A majority of effort in this thesis was therefore spent on establishing a solid foundation of theoretical knowledge and new contemporary information in light of the scarcity of any similar holistic collection and contextualization work on the topic of post-quantum cryptography migration.

The start of the exploration of quantum vulnerability was done by explaining foundational theory of cryptography, quantum computing and its application. The impact the quantum computing capability will have on public-key encryption was discussed, and the quantum vulnerability problem was established from the previous domains. The unique part of the collection of information of this thesis was the attempt to express and quantify the abstract danger of the quantum vulnerability to digital systems and thus many aspects of governmental and industrial operations. The application of this information to the scenario of quantum vulnerability is to this extent not found in other discussions about cryptographic transition, missing the establishment of danger and severity this poses. The decision-making process for alleviating action to this can only be informed if these facts are part of the discussion and taken into account.

The range of consequences of the security failure of digital communication is too broad to be covered in whole in this thesis, but it was attempted to demonstrate the magnitude of possible danger, as discussed in chapter 2.3. The evaluation of danger is by no means complete, with still many unknowns, leaving room for more extensive research. The assigning of probability to these types of possible events was equally difficult and no objective certainty of any event can be established. Nonetheless is the discussion of these exact implications of quantum vulnerability of the utmost importance to the manifestation of clear and concise imperatives for any further conduct and yet scarce in other publications on this topic.

The comprehensive review of current acknowledgment and actions to this danger can only be found in part in other publications. The collection of different reactions is important in the development of an image of response and in the evaluation of the extent of said response. Similar to the evaluation of potential danger, the evaluation of response informs all further actions to be taken or even if any actions need to be taken at all. The collection relies heavily on the work of public studies and surveys such as the BSI market survey on cryptography and quantum computing to build a representative image of the acknowledgment and action of affected organizations. In combination with the analysis of the current laws and policy in regard to the role of governments in software security, a realistic view on who is deemed responsible to take corrective action is formed—the affected organizations themselves. A discussion also absent from other publications on this topic, failing to incentivize the private parties to act on their own behalf.

The thesis itself emphasizes all prior aspects in a collective manner in chapter 4.5 and contextualizes the established facts to their importance in the overall effort to establish a shared understanding of the quantum vulnerability of public-key cryptography. The combination of implication assessment, danger probability assessment and current response assessment led to the recognition of the need for further research and exploration of all aspects relating to migration to post-quantum cryptography. The statement of the need to act on the given vulnerability, found in contemporary media and publications without extensive discussion, is convincingly argued for by this thesis in a comprehensive manner so far rare in the field of cryptographic migration.

The decision to approach the research effort in this exploratory manner remains the reasonable choice of conduct in review of the state of research in the field of cryptographic migration. Given the described lack of substantiated information and empirical data, it was necessary to engage in a collection of varied but isolated points of data to cover the largely unknown space of post-quantum cryptography migration. Each entity and institution provided a unique perspective and informed the broader understanding of the problem, its cause, and its effects. This broad and albeit arguably superficial procedure allowed the identification of gaps and imbalances in the shared knowledge, crucial for any intentional research initiative succeeding the established foundation. As stated before embarking on the examination of the response to the quantum vulnerability, the variety of sources or lack thereof does present a validity problem in the quality and reliability of information presented. The challenge of correctly weighing and interpreting each given response can only be confirmed with additional data points and analyses, arriving at the same conclusions as this thesis did.

Given all explored and analyzed circumstances of cryptographic quantum vulnerability, the evident need for further action is identified to mitigate the current problematic situation. The exploration of related works to cryptographic migration in chapter 2.4 as well as the examination of past prominent cryptographic migrations uncovers a clear lack of public discussion and academic analysis on the preparation and execution of cryptographic migration. To this end, no prescribed actions could be identified to handle the given migration task beyond dispute, as none conclusively underwent the scrutiny of science. As an initial contribution to this stated requirement, this thesis aimed to provide an initial framework for the planning and execution of a cryptographic migration on an organizational level, using all the information collected and analyzed so far.

The proposed strategic approach to the migration to post-quantum cryptography was built on the culmination of the prior established facts and tried to address the identified problems and dangers related to cryptographic quantum vulnerability while conforming to the formulated requirements. For the development of this approach, related works and past cryptographic migrations were analyzed as to their prescribed actions which may be applicable to post-quantum cryptography migration. While the consideration of historic migrations did not result in any actionable advice, the work of Stapleton et al. as well as recommendations by public and private institutions published in contemporary media could be compiled and applied to a comprehensive guide to cryptographic migration. In addition, the concepts of cryptographic agility and CBOMs were incorporated, further enhancing the approach's capability to deal with current and future cryptographic migrations. The resulting strategy addresses all identified problems and dangers in a manner that should be feasible for a wide range of potential users.

Six general requirements were formulated out of the preceding content and discussion of the thesis. The evaluation of the proposed cryptographic migration strategy for post-quantum cryptography in regard to the stated requirements can, in the given scope of this thesis, only be done as a theoretical analysis. The R1 requirement is fulfilled with the strategies overall pursuit of conduct resulting in a cryptographic migration to post-quantum cryptography, with the significant caveat that currently only one such algorithm standard exists that replaces public-key cryptography. The final completion of the migration is also only possible if all externalities as described throughout the steps are taken into account and continued operation can be attested to. The migration step of operational impact analysis identifies and prioritizes vulnerable instances of cryptography and contributes as such to the preserving of cryptographic security. The R2 requirement is fulfilled by the algorithm-agnostic structure of the migration strategy, allowing the implementation of different cryptographic schemes or algorithms depending on the specific legislative requirements. The responsibility for achieving regulatory compliance lies on the migrating party, with the proposed strategy enabling different cryptographic possibilities.

The R3 requirement is fulfilled by the proposed phased approach to the migration, allowing for different courses of actions depending on the available resources, enabling every actor to participate in the migration as to their abilities. The introduction of cryptographic agility and CBOMs allows for immediate preliminary actions, which speed up any eventual migration completion. The R4 requirement is fulfilled by the same general points as is the R3 requirement. The prescribed conduct and behaviors are formulated as to allow a selection of actions to be taken depending on available resources. The second step of the migration strategy assures that a migration will only be conducted if an operational impact is determined and prescribes a forecast on potentially needed resources, making an extensive evaluation of the cryptographic prospects possible. Even with stringent resources available, a minimal and manual approach to the migration is stated, relying on as much outside collection and analysis of cryptographic information as possible to reduce time and effort spent. The different steps of the migration strategy allow the adaption of the strategy to the needs and realities of the migrating party.

The R5 requirement is fulfilled by the algorithm flexibility achieved through the introduction of the concept of cryptographic agility. The described implementation of cryptographic agility as well as CBOMs allows the preparation of the final migration step without changing the cryptographic scheme currently in use, making it possible to engage in the migration process without compromising ongoing operations. The R6 requirement is fulfilled by sustainable behaviors and actions prescribed throughout the migration strategy. The continuous step of cryptographic discovery prescribes a proactive engagement in the cryptographic information space, mandating an active examination of new vulnerabilities. The proposed implementation of a persistent cryptographic inventory simplifies and streamlines both the operational impact analysis and the identification of cryptographic instances, making any subsequent migrations as effortless as possible. Conclusively, the proposed strategy closely aligns with all general requirements as they were established.

The most apparent limitation of this strategy is the extent to which each related aspect of quantum vulnerability and post-quantum cryptography migration can be covered in an encompassing manner. The pervasiveness of digital systems and cryptography to many elements of our way of life complicates the attempt to consider every facet of potential relevance. The effort put forth by this thesis presents a representative compilation of relevant information, but nonetheless is not definitive. Every further expansion of the covered information is outside the possible scope that can be covered as part of this thesis. Building on this extensive foundation, the designed migration strategy remains theoretical in nature and has yet to be tested in any academic or real-world setting, making its claims and recommendations to an extent uncertain as to their realizability and proposed functionality. This constitutes a large limitation resulting from the inherent scope of this topic and the lack of academic work to be relied upon.

However, the research presented in this thesis still carries significance in its implication for academia and industry, as well as any policymaker or political authority. The examined intersection of cryptography and quantum computing formulated the case for the need for cryptographic migration with the associated potential ramifications, assigning the urgency needed to highlight the importance of this finding. The challenges described need to be taken seriously by academia and represented more in the mitigation discussions so far focus on post-quantum cryptography algorithms. On the industrial side, the proactive approach to cryptographic security is a major important virtue needing to be engaged in, seeing the increased reliance on digital systems, digital communication, and digital representation of information. The digital shift of information changes the reality in which one operates in, with old assumptions and rules about possibilities and capabilities quickly being overtaken by new developments in science and computation. The presented problems, discussion and proposed solutions require a more sustainable and continuous engagement with the topic of cryptography to retain the digital initiative in cybersecurity.

To further progress in the understanding of post-quantum cryptography migration, nearly all aspects discussed in the course of this thesis present opportunities for future research work. The exploration of implications and consequences of cryptographic failure stands as the root justification of any following action, and thus should be as accurate as possible. While the function of Shor's quantum algorithm and its mathematical effect on cryptography is known, the subsequent implications are rarely identified and even more rarely quantified. This thesis tried to express this important aspect in its own exploration in chapter 2.3, but the granularity of which each implication is examined can be expanded greatly. A more accurate picture of the ramifications of the quantum vulnerability of public-key cryptography could facilitate the ability to communicate the importance of the subject to public and private parties, raising the general awareness. Whereas this thesis has excluded the possibility of direct political intervention, this could potentially be changed with more research showing the severity of inaction, forcing legislators to adjust current cryptographic policy. Of course, the result of such research—albeit unlikely in the view of this thesis—could also swing in the other direction and prove far less destructive as previously assumed, which would in turn save resources spent on unneeded cryptographic migrations. Both cases incentivize the need for further exploration and analysis.

The same argument can be applied to the exploration of response to the quantum vulnerability. In the interest of driving the adoption of quantum-safe cryptography, it would be useful to identify which demographics of public or private organizations are dealing with the described crisis in what capacity. Increasing the granularity of such information could make the provision of resources and recommended action more precise to the needs of affected organizations.

Another field which should be researched further is the application of cryptography and cryptographic migration. This includes all possible related aspects of the field such as application principles, testing, surveys, historical analysis, etc. as all are currently underexplored relative to their importance in current events. The current body of science on cryptographic migration does not lend itself as a solid basis due to the few numbers of contributions so far, making the research of specific aspects of migration prohibitively difficult. The process of cryptographic migration has to be established in the academic discussion as to its function or procedure, implementation, and peer reviewed status. To this end, the provided migration strategy of this thesis leaves room for further analysis and scrutiny as to its recommended actions and their effectiveness. The holistic approach to encompass the complete migration cycle could only be established in theory, and a real-world integration of the prescribed concepts needs to tested and evaluated.

7
Conclusion

The developments in the field of quantum computing challenge the cryptographic security of current public-key encryption algorithms, making an opposing cryptographic response necessary to preserve and maintain the security of digital communication and data. This thesis has examined the threat of quantum computing, identified deficiencies in the current response, and suggested a strategic approach to migration to post-quantum cryptography. The following sections summarize the key findings made in the course of this thesis:

Quantum vulnerability

Quantum computing enables fundamentally new ways of computation. Mathematician Peter Shor developed a quantum algorithm that can solve the mathematical problem of factoring orders of magnitude faster than traditional hardware, voiding the cryptographic complexity that these public-key encryption algorithms are based on. Current quantum computers are not powerful enough to execute Shor's algorithm outside limited tests, but predictions suggest a timeframe of as early as the beginning of the 2030s where a powerful enough quantum computer could exist.

The computational potential of quantum computers as well as Shor's and other quantum algorithms effectively depreciate the integrity of RSA and other public-key encryption schemes that rely on similar mathematical problems. The shift in computational power means a danger of decryption at some point in the future, making a cryptographic transition to quantum-safe algorithms necessary to preserve the privacy and integrity properties.

Intersection of cryptography and quantum computing

Fundamental assumptions about current cryptographic schemes are voided with the computational ability of quantum computers. The efficiency at which quantum computers can solve the mathematical problems on which public-key cryptography is based, negates the security through complexity which secures many modern communications. The effect is on widely used algorithms like RSA, endangering through such schemes encrypted data at risk of decryption once a powerful enough quantum computer exists.

The cascading effects of such a vulnerability would lead to extensive and far-reaching consequences on the broader field of cybersecurity. As public-key cryptography is used to secure digital communication in global networks such as the internet, it is responsible for the integrity and privacy of all data messages sent. A compromise would threaten this digital infrastructure enabling data breaches exposing personal data, business data, financial information, trade secrets, research and development data but also governmental communications and data, intelligence information and military data. The universal reliance on digital communications networks secured through public-key cryptography thus also means equally extensive exposure potential.

This threat of future decryption is extended by the possibility of harvest-now-decrypt-later attacks. Given the early publishing of Peter Shor's quantum algorithms and the apparent timeline of quantum computing development, it can be presumed with a reasonable degree of certainty that the breaking point of public-key encryption will be reached in the 2030s. A malicious attacker can collect encrypted data and store it with the intention of decrypting it in the future. In addition to the future danger of decryption, this creates a danger for even presently public-key encrypted data to be intercepted and decrypted at a later point in time.

The feasibility of such an attack is dependent on available storage capacity and associated economic factors, but future advancements in the field should be considered in the evaluation of such a threat. With both harvest-now-decrypt-later and general decryption, the amounts of data involved should not be treated as a sufficient protection from discovery and analysis. Big data analysis and new developments of LLMs offer advanced, automated data exploration and categorization abilities that also appear to advance at a rapid pace.

The quantum vulnerability in software and systems can have severe real-world consequences. Governments, governmental agencies, intelligence agencies, militaries, critical infrastructure, private organizations such as businesses could all be affected by the loss of data confidentiality. The extent of possible damage and the probability of these scenarios is difficult to quantify but given the proliferation of interconnected digital systems, the exposure of sensitive communication, personal data, public and private operational information can not be excluded with any certainty. The level of potentially possible economic disruption and geopolitical instability forms a strong imperative for a cryptographic migration to post-quantum cryptography.

Exploration of response

Despite the significant implications, the public and academic discussion of post-quantum cryptography migration is not representative to the relevance it poses to averting the quantum vulnerability problem, leaving a knowledge gap between high-level business and policy and low-level technical and mathematical cryptographic research. The exploration and analysis of the current response revealed that while the awareness of the quantum vulnerability is present at governmental bodies and a majority of industrial organizations, but corresponding actions do not adequately address the vulnerability. The self-reported average timeline of transition extends past a projected breaking point of current public-key cryptography, suggesting a lack of actionable recommendations and strategy for the process of cryptographic migration.

Strategic approach to post-quantum cryptography migration

Following the extensive collection of information, this thesis engaged in the development of a strategic approach to post-quantum cryptography migration to contribute to the identified knowledge and research gap. With the given limited availability of topical related works, the collective strategy was founded on the knowledge established in this thesis while incorporating key insights from academic papers, standardizations organizations such as the BSI and NIST and public business operations material. Techniques and solutions of the related fields of software supply chain security and cryptographic agility were explored and incorporated.

The resulting migration strategy consists of four steps with the goal of providing an actionable framework to plan and execute a cryptographic migration.

The proposed strategy begins with developing an educational foundation in cryptographic theory and a continuous discovery of cryptographic vulnerabilities. An impact analysis and risk assessment in the context of the specific environment of the organization decides if a migration is necessary. To execute a migration, a cryptographic inventory needs to be established that includes every instance of vulnerable cryptography. With the use of a cryptographic bill of materials and the implementation of cryptographic agility, the time and effort of future migrations can be reduced as they simplify the discovery and inventory process greatly. The identified instances of cryptography are finally replaced with a suitable secure algorithm.

Even in the current uncertainty of yet unproven post-quantum encryption algorithms, the migration process needs to be conducted as far as possible and as fast possible. The implementation of cryptographic agility will reduce the final number of implementations of post-quantum algorithms to a minimum, making the preparation of transition complete with an immediate option to insert a suitable replacement candidate.

Outlook and future research directions

The limitations of the theoretical work of this thesis leave several opportunities for future exploration and research. The implementation of the proposed steps of the migration strategy needs to be tested and analyzed extensively to evaluate its validity. Equally important is the further research into the areas of impact of quantum vulnerability and cryptographic vulnerability in general. To propose corrective actions, it is necessary to have an accurate understanding of the underlying circumstances of risks, damages, and the quantification of probabilities.

This thesis explored the challenges posed by quantum computing to cryptography and proposed a strategic approach for a migration to post-quantum cryptography. The research highlights the urgency to address the vulnerability and sets the basis for further research into a cryptographic migration framework. As the domains of cryptography and quantum computing progress, the steps and strategies outlined in this thesis need to be evolved, adapted and supported by accompanying research and testing. Ultimately, the successful migration to quantum-safe cryptography will be the key to securing digital communication against the emerging quantum threat.

A
List of figures

B
Bibliography

[1] Federal Office for Information Security. *Quantum-safe cryptography - fundamentals, current developments and recommendations.* May 2021. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626.

[2] P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science.* 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[3] Jeff Stapleton, Ralph Poore, and Peter Bordow. “Cryptographic Transitions: Historical Considerations.” In: *ISSA Journal* 20.9 (Sept. 2022).

[4] David Ott, Kenny Paterson, and Dennis Moreau. “Where Is the Research on Cryptographic Transition and Agility?” In: *Commun. ACM* 66.4 (Mar. 2023), pp. 29–32. ISSN: 0001-0782. DOI: 10.1145/3567825. URL: https://doi.org/10.1145/3567825.

[5] KPMG and Federal Office for Information Security. *Market Survey on Cryptography and Quantum Computing.* Sept. 2023. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.html.

[6] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* eng. Third edition. Chapman & Hall/CRC Cryptography and Network Security Series. Boca Raton London New York: CRC Press Taylor & Francis Group, 2021. ISBN: 978-1-351-13303-6.

[7] Sattar B. Sadkhan. “Key note lecture multidisciplinary in cryptology and information security”. In: *2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE).* Dec. 2013. DOI: 10.1109/ICECCPCE.2013.6998773. URL: https://ieeexplore.ieee.org/document/6998773.

[8] Josh Schneider. *Cryptography use cases: From secure communication to data security.* IBM Blog. Jan. 17, 2024. URL: https://www.ibm.com/blog/cryptography-use-cases/ (visited on Mar. 13, 2024).

[9] Joanne Baker. “Forgotten heroes of the Enigma story”. In: *Nature* 561.7723 (2018), pp. 307–308. DOI: https://doi.org/10.1038/d41586-018-06149-y.

[10] *How Alan Turing Cracked The Enigma Code.* Imperial War Museum. URL: https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code (visited on Mar. 13, 2024).

[11] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010. ISBN: 978-1-107-00217-3.

[12] Ronald Linn Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342.

[13] Jeff Stapleton and Ralph Poore. "Cryptographic transitions". In: *2006 IEEE Region 5 Conference*. 2006, pp. 22–30. DOI: 10.1109/TPSD.2006.5507465.

[14] John F. Dooley. *A Brief History of Cryptology and Cryptographic Algorithms*. Cham: Springer International Publishing, 2013. DOI: 10.1007/978-3-319-01628-3. URL: https://doi.org/10.1007/978-3-319-01628-3.

[15] Colin P. Williams. *Explorations in Quantum Computing*. Texts in Computer Science. Springer London, 2010. ISBN: 9781846288876. DOI: https://doi.org/10.1007/978-1-84628-887-6. URL: https://books.google.de/books?id=QE8S--WjIFwC.

[16] Andrew S. Tanenbaum and Todd Austin. *Structured Computer Organization*. 6th. USA: Pearson, 2013. ISBN: 978-0-13-291652-3.

[17] Maximilian Schlosshauer. "Quantum decoherence". In: *Physics Reports* 831 (2019). Quantum decoherence, pp. 1–57. ISSN: 0370-1573. DOI: https://doi.org/10.1016/j.physrep.2019.10.001. URL: https://www.sciencedirect.com/science/article/pii/S0370157319303084.

[18] *Quantum Cryptography - Shor's Algorithm Explained*. Classiq. July 19, 2022. URL: https://www.classiq.io/insights/shors-algorithm-explained (visited on Mar. 18, 2024).

[19] Unathi Skosana and Mark Tame. "Demonstration of Shor's factoring algorithm for N=21 on IBM quantum processors". In: *Nature Scientific Reports* 16599.11 (2021). URL: https://www.nature.com/articles/s41598-021-95973-w.

[20] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866. URL: https://doi.org/10.1145/237814.237866.

[21] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. *A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem*. 2015. arXiv: 1412.6062 [quant-ph]. URL: https://arxiv.org/abs/1412.6062.

[22] Alexander M. Dalzell et al. *Quantum algorithms: A survey of applications and end-to-end complexities*. Oct. 2023. arXiv: 2310.03011 [quant-ph]. URL: https://arxiv.org/abs/2310.03011.

[23] Frank Arute et al. "Quantum Supremacy using a Programmable Superconducting Processor". In: *Nature* 574 (2019), pp. 505–510. URL: https://www.nature.com/articles/s41586-019-1666-5.

[24] "The bumpy road to application". In: *Nature Electronics* 489 (2019). URL: https://www.nature.com/articles/s41928-019-0339-6.

[25] *Quantum Computer - Our full stack approach to quantum computing*. Google Quantum AI. URL: https://quantumai.google/quantumcomputer (visited on Sept. 9, 2024).

[26] A. Morvan et al. *Phase transition in Random Circuit Sampling*. en. arXiv:2304.11119 [quant-ph]. Apr. 2023. URL: http://arxiv.org/abs/2304.11119.

[27] Jay Gambetta. *The hardware and software for the era of quantum utility is here.* IBM Blog. URL: https://www.ibm.com/quantum/blog/quantum-roadmap-2033 (visited on Apr. 19, 2024).

[28] *IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two.* IBM Newsroom. en-us. URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (visited on Apr. 21, 2024).

[29] *IBM Unveils Breakthrough 127-Qubit Quantum Processor.* IBM Newsroom. en-us. URL: https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor (visited on Apr. 21, 2024).

[30] *IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility.* IBM Newsroom. URL: https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility (visited on Apr. 19, 2024).

[31] DigiCert. *What is SSL?* FAQ - Public Trust and Certificates. URL: https://www.digicert.com/faq/public-trust-and-certificates/what-is-ssl (visited on Aug. 26, 2024).

[32] Iain Beveridge and Dave Butcher. *Harvest Now, Decrypt Later – Fact or Fiction?* Entrust Blog. Nov. 15, 2023. URL: https://www.entrust.com/blog/2023/11/harvest-now-decrypt-later-fact-or-fiction/ (visited on Mar. 25, 2024).

[33] Ray Harishankar et al. *Security in the quantum computing era.* IBM Institute for Business Value. URL: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption (visited on Mar. 25, 2024).

[34] *Understanding file sizes — Bytes, KB, MB, GB, TB, PB, EB, ZB, YB.* GeeksforGeeks. Feb. 28, 2024. URL: https://www.geeksforgeeks.org/understanding-file-sizes-bytes-kb-mb-gb-tb-pb-eb-zb-yb (visited on Apr. 5, 2024).

[35] *Cisco Visual Networking Index: Forecast and Trends, 2017–2022.* Cisco Systems. Tech. rep. 2018. URL: https://cloud.report/Resources/Whitepapers/eea79d9b-9fe3-4018-86c6-3d1df813d3b8_white-paper-c11-741490.pdf.

[36] Ulrike Hack. *What's the real story behind the explosive growth of data?* Redgate Blog. Sept. 8, 2021. URL: https://www.red-gate.com/blog/database-development/whats-the-real-story-behind-the-explosive-growth-of-data (visited on Apr. 27, 2024).

[37] *Hard Disk Drives (HDD).* Geizhals Preis- und Produktvergleichsportal. URL: https://geizhals.de/?cat=hde7s&sort=r#productlist (visited on Apr. 27, 2024).

[38] Glenn Greenwald and Ewen MacAskill. *NSA Prism program taps in to user data of Apple, Google and others.* The Guardian. June 7, 2013. URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (visited on Apr. 27, 2024).

[39] *What is Big Data?* Google Cloud. URL: https://cloud.google.com/learn/what-is-big-data (visited on Apr. 27, 2024).

[40] *Big Data Analytics: What It Is, How It Works, Benefits, And Challenges.* Salesforce. URL: https://www.tableau.com/learn/articles/big-data-analytics (visited on Apr. 27, 2024).

[41] *What are Large Language Models (LLM)?* Amazon AWS. URL: https://aws.amazon.com/what-is/large-language-model/ (visited on Sept. 6, 2024).

[42] Raul Castro Fernandez et al. "How Large Language Models Will Disrupt Data Management". In: *Proc. VLDB Endow.* 16.11 (July 2023), pp. 3302–3309. ISSN: 2150-8097. DOI: 10.14778/3611479.3611527. URL: https://doi.org/10.14778/3611479.3611527.

[43] *GPT Models.* OpenAI Platform. URL: https://platform.openai.com/docs/models (visited on Sept. 6, 2024).

[44] *Gemini Models.* Google Deepmind. URL: https://deepmind.google/technologies/gemini/ (visited on Sept. 6, 2024).

[45] *Llama Models.* Meta. URL: https://llama.meta.com/docs/overview (visited on Sept. 6, 2024).

[46] *Claude Models.* Anthropic. URL: https://docs.anthropic.com/en/docs/about-claude/models (visited on Sept. 6, 2024).

[47] Exec. Order No. 13526, Daily Comp. Pres. Docs., 2009 DCPD No. 200901022 (December 29, 2009). URL: https://www.govinfo.gov/app/details/DCPD-200901022.

[48] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, Daily Comp. Pres. Docs., 2022 DCPD No. 202200355 (May 4, 2022). URL: https://www.govinfo.gov/app/details/DCPD-202200355.

[49] Dovydas Vitkauskas. *The Role of Security Intelligence Service in a Democracy.* Tech. rep. North Atlantic Treaty Organization, June 1999. URL: https://www.nato.int/acad/fellow/97-99/vitkauskas.pdf (visited on Aug. 5, 2024).

[50] Florina Cristiana Matei and Carolyn Halladay. "The Role and Purpose of Intelligence in a Democracy". In: *Processes, Practices, Cultures.* Ed. by Florina Cristina Matei and Carolyn Halladay. Boulder, USA: Lynne Rienner Publishers, 2019, pp. 1–24. ISBN: 9781626378216. DOI: doi:10.1515/9781626378216-003. URL: https://doi.org/10.1515/9781626378216-003.

[51] *Signals Intelligence (SIGINT) Overview.* U.S. National Security Agency (NSA). URL: https://www.nsa.gov/Signals-Intelligence/Overview/ (visited on Apr. 29, 2024).

[52] *Summary of NATO's Data Exploitation Framework Strategic Plan.* NATO Newsroom. Dec. 9, 2022. URL: https://www.nato.int/cps/en/natohq/official_texts_209999.htm (visited on Mar. 29, 2024).

[53] *Digitalisation in the Army.* German Bundeswehr. URL: https://www.bundeswehr.de/en/organization/army/organization/capabilities/digitalisation (visited on Apr. 29, 2024).

[54] *Data Transfer - What are military data links?* German Bundeswehr. Sept. 18, 2023. URL: https://www.bundeswehr.de/en/military-data-links-5676750 (visited on Apr. 29, 2024).

[55] *Russland veröffentlicht angebliche Abhöraufnahmen.* Tagesschau Online. Mar. 1, 2024. URL: https://www.tagesschau.de/inland/regional/russland-bundeswehr-abhoeren-100.html (visited on Apr. 30, 2024).

[56] *Wurde die Bundeswehr von Russland belauscht?* Tagesschau Online. Mar. 2, 2024. URL: https://www.tagesschau.de/inland/russland-bundeswehr-abhoeren-102.html (visited on Apr. 30, 2024).

[57] *Scholz begründet Nein zu "Taurus"-Lieferung.* Tagesschau Online. Feb. 26, 2024. URL: https://www.tagesschau.de/inland/scholz-taurus-ukraine-102.html (visited on Apr. 30, 2024).

[58] Hauke Friederichs. *Geheimwaffe Zettelkasten.* Zeit Online. Mar. 4, 2024. URL: https://www.zeit.de/politik/deutschland/2024-03/bundeswehr-spionage-sicherheit-kommunikation-digitalisierung (visited on Apr. 30, 2024).

[59] *Cyber attacks on critical infrastructure.* Allianz. June 2016. URL: https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html (visited on Apr. 30, 2024).

[60] *National Critical Functions Set.* U.S. Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov/national-critical-functions-set (visited on Apr. 30, 2024).

[61] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, Daily Comp. Pres. Docs., 2021 DCPD No. 202100622 (July 28, 2021). URL: https://www.govinfo.gov/app/details/DCPD-202100622.

[62] *Preparing Critical Infrastructure for Post-Quantum Cryptography.* Tech. rep. U.S. Cybersecurity and Infrastructure Security Agency (CISA), Aug. 24, 2022. URL: https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf.

[63] Sarwat Jahan and Ahmed Sabe Mahmud. *What Is Capitalism?* International Monetary Fund (IMF). URL: https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Capitalism (visited on Apr. 1, 2024).

[64] Maria Grazia Attinasi et al. *Supply chain disruptions and the effects on the global economy.* European Central Bank (ECB) Economic Bulletin, Issue 8/2021. 2021. URL: https://www.ecb.europa.eu/press/economic-bulletin/focus/2022/html/ecb.ebbox202108_01~e8ceebe51f.en.html (visited on Apr. 1, 2024).

[65] *What is a data breach?* IBM. URL: https://www.ibm.com/topics/data-breach (visited on Apr. 2, 2024).

[66] Jessica Farrelly. *High-Profile Company Data Breaches.* Electric Blog. Mar. 21, 2024. URL: https://www.electric.ai/blog/recent-big-company-data-breaches (visited on Apr. 2, 2024).

[67] *Threat Landscape 2020 - Cyber espionage.* Tech. rep. European Union Agency for Cybersecurity (ENISA), Oct. 20, 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage (visited on Apr. 2, 2024).

[68] David Joseph et al. "Transitioning organizations to post-quantum cryptography". In: *Nature* 605 (May 2022), pp. 237–243. DOI: 10.1038/s41586-022-04623-2.

[69] D. Alan Heslop. *The functions of government.* Britannica Online. URL: https://www.britannica.com/topic/political-system/Stable-political-systems (visited on Apr. 2, 2024).

[70] Pallavi Rao. *These are the EU countries with the largest economies.* World Economic Forum. Feb. 1, 2023. URL: https://www.weforum.org/agenda/2023/02/eu-countries-largest-economies-energy-gdp/ (visited on Apr. 2, 2024).

[71] Veronica Vella. "Is There a Common Understanding of Dual-Use?: The Case of Cryptography". In: *Strategic Trade Review* 3.3 (Apr. 2017). ISSN: 2506-9691.

[72] Thea Riebe et al. "U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance". In: *European Journal for Security Research* 7.1 (July 2022), pp. 39–65. ISSN: 2365-1695. DOI: 10.1007/s41125-022-00080-0. URL: https://doi.org/10.1007/s41125-022-00080-0.

[73] U.S. Department of Commerce, Bureau of Industry and Security. *76 FR 1059 - Publicly Available Mass Market Encryption Software and Other Specified Publicly Available Encryption Software in Object Code*. Jan. 2011. URL: https://www.govinfo.gov/app/details/FR-2011-01-07/2010-32803.

[74] Edward Robin. *Unlocking the Secrets Exploring the Laws that Mandate Data Encryption*. Aug. 2023. URL: https://www.newsoftwares.net/blog/the-laws-that-mandate-data-encryption/#United_States_Data_Encryption_Laws (visited on Apr. 13, 2024).

[75] U.S. Deaprtment of Health and Human Services Office for Civil Rights. *Summary of the HIPAA Privacy Rule*. Oct. 2022. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (visited on Apr. 13, 2024).

[76] U.S. Federal Trade Commission. *FTC Safeguards Rule: What Your Business Needs to Know*. May 2022. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (visited on Apr. 13, 2024).

[77] Council of the European Union. *The general data protection regulation*. Dec. 2023. URL: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/.

[78] Council of the European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)". In: *Official Journal of the European Union* 119 (May 2016). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1707132925013.

[79] Exec. Order No. 14073, 87 Fed. Reg. 27909 (May 4, 2022). URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee/.

[80] European Commission. *The European Quantum Communication Infrastructure (EuroQCI) Initiative*. 2019. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (visited on May 2, 2024).

[81] Andrea G. Rodríguez. "A quantum cybersecurity agenda for Europe - Governing the transition to post-quantum cryptography". In: *Europe's Quantum Frontier* (July 2023). (Visited on May 2, 2024).

[82] European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parlament and the Council - The EU's Cybersecurity Strategy for the Digital Decade*. Oct. 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (visited on May 2, 2024).

[83] European Union Agency for Cybersecurity (ENISA). *Post-Quantum Cryptography - Current state and quantum mitigation.* May 2021. URL: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation (visited on May 2, 2024).

[84] Dan Schiappa. *Our survey reveals what data businesses are encrypting, what data they're not, and why.* Sophos News. Jan. 19, 2016. URL: https://news.sophos.com/en-us/2016/01/19/encryption-survey-results/ (visited on May 7, 2024).

[85] Ponemon Institute LLC and Entrust. *2021 Global Encryption Trends Study.* Apr. 2021. URL: https://apexassembly.com/wp-content/uploads/2021/07/Entrust__2021_Global_Encryption_Trends_Study.pdf (visited on May 7, 2024).

[86] Ponemon Institute LLC and Entrust. *2022 Global Encryption Trends Study.* June 2022. URL: https://helpransomware.com/wp-content/uploads/2022/07/Entrust-Global-Encryption-Trends-Study-PDF-HelpRansomware-2.pdf (visited on May 7, 2024).

[87] Charlie Bell. *Building a quantum-safe future.* May 2023. URL: https://blogs.microsoft.com/blog/2023/05/31/building-a-quantum-safe-future/ (visited on May 15, 2024).

[88] Matthew Campagna. *Preparing today for a post-quantum cryptographic future.* July 2022. URL: https://www.amazon.science/blog/preparing-today-for-a-post-quantum-cryptographic-future (visited on May 15, 2024).

[89] Eric Crockett, Christian Paquin, and Douglas Stebila. *Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.* Cryptology ePrint Archive, Paper 2019/858. https://eprint.iacr.org/2019/858. 2019. URL: https://eprint.iacr.org/2019/858.

[90] Stefan Kölbl, Rafael Misoczki, and Sophie Schmieg. *Securing tomorrow today: Why Google now protects its internal communications from quantum threats.* Nov. 2022. URL: https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms?hl=en (visited on May 15, 2024).

[91] Devon O'Brien. *Protecting Chrome Traffic with Hybrid Kyber KEM.* Chromium Blog. Aug. 10, 2023. URL: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html (visited on Apr. 3, 2024).

[92] *About NIST.* U.S. National Institue of Standards and Technology. Jan. 11, 2022. URL: https://www.nist.gov/about-nist (visited on May 8, 2024).

[93] National Institute of Standards and Technology. *Federal Information Processing Standards Publication: Data Encryption Standard (DES).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) 46. Gaithersburg, MD: U.S. Department of Commerce, Jan. 15, 1977. DOI: 10.6028/NIST.FIPS.46.

[94] Morris J. Dworkin et al. *Federal Information Processing Standards Publication: Advanced Encryption Standard (AES).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) 197. Gaithersburg, MD: National Institute of Standards and Technology U.S. Department of Commerce, Nov. 26, 2001. DOI: 10.6028/NIST.FIPS.197-upd1.

[95] National Institute of Standards and Technology. *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms.* Oct. 2016. URL: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms (visited on May 15, 2024).

[96] Gorjan Alagic et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process.* Tech. rep. NISTIR 8240. National Institute of Standards and Technology U.S. Department of Commerce, Jan. 31, 2019. DOI: 10.6028/NIST.IR.8240.

[97] Gorjan Alagic et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process.* Tech. rep. NISTIR 8309. National Institute of Standards and Technology U.S. Department of Commerce, July 22, 2020. DOI: 10.6028/NIST.IR.8309.

[98] Gorjan Alagic et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.* Tech. rep. NISTIR 8413-upd1. National Institute of Standards and Technology U.S. Department of Commerce, Sept. 29, 2022. DOI: 10.6028/NIST.IR.8413-upd1.

[99] National Institute of Standards and Technology. *PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates.* July 2022. URL: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 (visited on May 15, 2024).

[100] National Institute of Standards and Technology. *Module-Lattice-based Key-Encapsulation Mechanism Standard (ML-KEM).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) NIST 203 ipd. Gaithersburg, MD: U.S. Department of Commerce, Aug. 24, 2023. DOI: 10.6028/NIST.FIPS.203.ipd.

[101] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard (ML-DSA).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) NIST 204 ipd. Gaithersburg, MD: U.S. Department of Commerce, Aug. 24, 2023. DOI: 10.6028/NIST.FIPS.204.ipd.

[102] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard (SHL-DSA).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) NIST 205 ipd. Gaithersburg, MD: U.S. Department of Commerce, Aug. 24, 2023. DOI: 10.6028/NIST.FIPS.205.ipd.

[103] National Institute of Standards and Technology. *Module-Lattice-based Key-Encapsulation Mechanism Standard (ML-KEM).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) NIST 203. Gaithersburg, MD: U.S. Department of Commerce, Aug. 13, 2024. DOI: 10.6028/NIST.FIPS.203.

[104] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard (ML-DSA).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) NIST 204. Gaithersburg, MD: U.S. Department of Commerce, Aug. 13, 2024. DOI: 10.6028/NIST.FIPS.204.

[105] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard (SHL-DSA).* Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) NIST 205. Gaithersburg, MD: U.S. Department of Commerce, Aug. 13, 2024. DOI: 10.6028/NIST.FIPS.205.

[106] National Institute of Standards and Technology. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards.* Aug. 2024. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (visited on Aug. 19, 2024).

[107] Federal Office for Information Security. *BSI - Technical Guideline, Cryptographic Mechanisms: Recommendations and Key Lengths.* Feb. 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7.

[108] William Barker, William Polk, and Murugiah Souppaya. *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms.* Tech. rep. NIST Cybersecurity White Paper. Gaithersburg, MD: National Institute of Standards and Technology U.S. Department of Commerce, Apr. 28, 2021. DOI: https://doi.org/10.6028/NIST.CSWP.04282021.

[109] *IBM Quantum Safe → Technology: Safeguard your data and modernize your cryptography for the quantum era.* IBM. URL: https://www.ibm.com/quantum/assets/quantum-safe/IBM_Quantum-Safe-Technology-Brochure.pdf (visited on June 18, 2024).

[110] *IBM Quantum Safe Explorer: Simplify the discovery of cryptography and the management of quantum security risks.* IBM. URL: https://www.ibm.com/downloads/cas/O5BOWXVZ (visited on June 18, 2024).

[111] Ponemon Institute LLC and IBM Security. *Cost of a Data Breach Report 2023.* July 2023. URL: https://www.ibm.com/downloads/cas/E3G5JMBP (visited on May 7, 2024).

[112] Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation, 70 Fed. Reg. 28907 (May 19, 2005). URL: https://www.federalregister.gov/documents/2005/05/19/05-9945/announcing-approval-of-the-withdrawal-of-federal-information-processing-standard-fips-46-3-data.

[113] Miles Smid. "Development of the Advanced Encryption Standard". In: *Journal of Research of the National Institute of Standards and Technology* 126.126024 (Aug. 2021). DOI: 10.6028/jres.126.024.

[114] David Leech, Stacey Ferris, and John Scott. *The Economic Impacts of the Advanced Encryption Standard, 1996-2017.* Tech. rep. Grant/Contract Reports (NISTGCR) - 18-017. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, Sept. 7, 2018. DOI: https://doi.org/10.6028/NIST.GCR.18-017.

[115] U.S. Cybersecurity and Infrastructure Security Agency and. *Transition to Advanced Encryption Standard (AES).* Tech. rep. U.S. Federal Partnership for Interoperable Communications, May 2024. URL: https://www.cisa.gov/sites/default/files/2024-05/23_0918_fpic_AES-Transition-WhitePaper_Final_508C_24_0513.pdf (visited on July 30, 2024).

[116] Ronald L. Rivest. *The MD5 Message-Digest Algorithm.* RFC 1321. Apr. 1992. DOI: 10.17487/RFC1321. URL: https://www.rfc-editor.org/info/rfc1321.

[117] Bart Preneel. “The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition”. In: *Topics in Cryptology - CT-RSA 2010*. Ed. by Josef Pieprzyk. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–14. ISBN: 978-3-642-11925-5.

[118] Xiaoyun Wang and Hongbo Yu. “How to Break MD5 and Other Hash Functions”. In: *Advances in Cryptology – EUROCRYPT 2005*. Ed. by Ronald Cramer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 19–35. ISBN: 978-3-540-32055-5.

[119] National Institute of Standards and Technology. *Secure Hash Standard (SHS)*. Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) 180. Gaithersburg, MD: U.S. Department of Commerce, May 11, 1993. DOI: `10.6028/NIST.FIPS.180`.

[120] Lily Chen. *NIST Comments on Cryptanalytic Attacks on SHA-1*. National Institute of Standards and Technology. Apr. 26, 2006. URL: `https://csrc.nist.gov/news/2006/nist-comments-on-cryptanalytic-attacks-on-sha-1` (visited on May 22, 2024).

[121] *NIST Retires SHA-1 Cryptographic Algorithm*. National Institute of Standards and Technology. Dec. 15, 2022. URL: `https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm` (visited on May 22, 2024).

[122] National Institute of Standards and Technology. *Secure Hash Standard (SHS)*. Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) 180-2. Gaithersburg, MD: U.S. Department of Commerce, Aug. 1, 2002. URL: `https://csrc.nist.gov/files/pubs/fips/180-2/final/docs/fips180-2.pdf`.

[123] *SHA-256 and SHA-3*. GeeksforGeeks. Mar. 21, 2024. URL: `https://www.geeksforgeeks.org/sha-256-and-sha-3/` (visited on May 22, 2024).

[124] National Institute of Standards and Technology. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Tech. rep. Federal Information Processing Standards Publications (FIPS PUBS) 202. Gaithersburg, MD: U.S. Department of Commerce, Aug. 4, 2015. URL: `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf`.

[125] Jacek Tchórzewski and Agnieszka Jakóbik. “Theoretical and experimental analysis of cryptographic hash functions”. In: *Journal of Telecommunications and Information Technology* 1 (2019), pp. 125–133.

[126] Red Hat. *What is software supply chain security?* Dec. 2022. URL: `https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security` (visited on July 10, 2024).

[127] Robert Ellison et al. *Evaluating and Mitigating Software Supply Chain Security Risks*. Tech. rep. CMU/SEI-2010-TN-016. May 2010. URL: `https://doi.org/10.1184/R1/6573497.v1` (visited on June 27, 2024).

[128] Ben Lutkevich and Shraddha Kakade. *Definition - bill of materials (BOM)*. TechTarget. June 2022. URL: `https://www.techtarget.com/searcherp/definition/bill-of-materials-BoM` (visited on June 27, 2024).

[129] *SBOM at a Glance*. National Telecommunications and Information Administration, U.S. Department of Commerce. Apr. 27, 2021. URL: `https://www.ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf` (visited on June 27, 2024).

[130] National Telecommunications and Information Administration. *The Minimum Elements For a Software Bill of Materials (SBOM)*. Tech. rep. U.S. Department of Commerce, July 12, 2021. URL: `https://www.ntia.doc.gov/sites/default/files/publications/sbom_minimum_elements_report_0.pdf` (visited on June 27, 2024).

[131] *Cryptography Bill of Materials (CBOM)*. CycloneDX. URL: `https://cyclonedx.org/capabilities/cbom/` (visited on June 27, 2024).

[132] *SPDX Security*. SPDX, The Linux Foundation Projects. URL: `https://spdx.dev/learn/areas-of-interest/security/` (visited on June 27, 2024).

[133] Nouri Alnahawi et al. *On the State of Crypto-Agility*. Cryptology ePrint Archive, Paper 2023/487. 2023. URL: `https://eprint.iacr.org/2023/487`.

[134] Dave Wichers et al. *Source Code Analysis Tools*. Open Worldwide Application Security Project (OWASP). URL: `https://owasp.org/www-community/Source_Code_Analysis_Tools` (visited on Aug. 28, 2024).

[135] Filippo Valsorda, Josh Bleecher Snyder, and David Buchanan. *mlkem768: A Go implementation of the quantum-resistant key encapsulation method ML-KEM (formerly known as Kyber)*. Github. URL: `https://github.com/FiloSottile/mlkem768` (visited on Aug. 6, 2024).

[136] integritychain and eschorn1. *ml-kem-rs: Pure Rust implementation of (draft) FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Github. URL: `https://github.com/integritychain/ml-kem-rs` (visited on Aug. 6, 2024).

[137] Giacomo Pope et al. *kyber-py: ML-KEM / CRYSTALS-Kyber Python Implementation*. Github. URL: `https://github.com/GiacomoPope/kyber-py` (visited on Aug. 6, 2024).

Selbstständigkeitserklärung

Hiermit erkläre ich, die vorliegende Masterarbeit "Strategic Approach to Post-Quantum Cryptography Migration" selbstständig ohne unerlaubte fremde Hilfe und nur unter Zuhilfenahme der aufgeführten Quellen und Hilfsmittel, verfasst zu haben. Alle Stellen der Arbeit, an denen Quellen wortwörtlich oder sinngemäß benutzt wurden, sind als solche gekennzeichnet. Über die gesamte Arbeit hinweg wurden zur Bearbeitung und Verbesserung von Rechtschreibung und Grammatik die in "Overleaf" (overleaf.com) integrierte Rechtschreibprüfung und das KI-basierte "LanguageTool" (languagetool.org) verwendet. Diese Arbeit wurde weder vollständig noch in Auszügen im Rahmen einer anderen Prüfungsleistung eingereicht.

Datum: ....

(Unterschrift)