

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Orkhan Hasanzade IVSB213831

**Quantum Threats to Asymmetric
Cryptography:
Analysing Vulnerabilities and Enhancing
Security**

Bachelor's thesis

Supervisor: Mohammad Tariq
Meeran
PhD

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Orkhan Hasanzade IVSB213831

**Asümmeetrilise krüptograafia kvantohud:
haavatavuste analüüs ja turvalisuse
tugevdamine**

Bakalaureusetöö

Juhendaja: Mohammad Tariq
Meeran
PhD

Tallinn 2024

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Orkhan Hasanzade

11.05.2024

Abstract

The computational power of quantum computers is rapidly evolving. Even though this progress is promising in most fields, it poses threats to classical asymmetric cryptography. Since the currently used asymmetric algorithms including DH (Diffie-Hellman), DSA (Digital Signature Algorithm), and RSA (Rivest–Shamir–Adleman) are threatened in this context, the need for analysing their potential vulnerabilities and exploring more secure cryptographic solutions gains uttermost importance for securing the future.

The thesis focuses on the theoretical exploration of classical and post-quantum cryptography, having the core delve into their comparative analysis and proposals for quantum-safe cryptography. The vulnerabilities of the classical asymmetric algorithms are identified through the review of their base mathematical foundations and the specific attack vectors.

The theoretical approach adopted by the thesis aims to explore the conceptual and underlying aspects of the current and future state of asymmetric cryptography.

This thesis is written in English and is 42 pages long, including 6 chapters, 10 figures and 3 tables.

List of abbreviations and terms

AES	Advanced Encryption Standard
CIA	Confidentiality Integrity Availability
CVP	Closest Vector Problem
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
LWE	Learning With Errors
MITM	Man-in-the-middle
MSS	Merkel Signature Scheme
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PQC	Post-quantum Cryptography
QC	Quantum Cryptography
QKD	Quantum Key Distribution
RSA	Rivest–Shamir–Adleman
SHA	Secure Hashing Algorithm
SVP	Shortest Vector Problem
XMSS	eXtended Merkel Signature Scheme

Table of contents

Author’s declaration of originality	3
Abstract.....	4
List of abbreviations and terms	5
Table of contents	6
List of figures	8
List of tables	9
1 Introduction	10
1.1 Motivation	10
1.2 Research Problem	10
1.3 Research Objectives	11
1.4 Limitations.....	11
2 Background Information.....	12
2.1 Basics of Cryptography	12
2.2 Overview of Asymmetric Cryptography	13
2.2.1 Diffie-Hellman Overview	14
2.2.2 Foundations of DSA	15
2.2.3 RSA Overview.....	17
2.3 Essentials of Quantum Computing and Cryptography	20
2.3.1 Understanding Quantum.....	20
2.3.2 Superposition.....	21
2.3.3 Uncertainty	21
2.3.4 Entanglement.....	22
2.3.5 Linear Algebra.....	22
2.3.6 Outline of Quantum Cryptography	23
3 Methodology.....	25
3.1 Research Design	25
3.2 Analysis Framework.....	26
4 Analytical Review	27
4.1 Quantum Vulnerabilities of Asymmetric Cryptography	27

4.1.1 Mathematical Background of Asymmetric Algorithms	27
4.1.2 Large Number Factorization Problem	27
4.1.3 Discrete Logarithm Problem	28
4.2 Recognizing the Threat.....	30
4.2.1 Current Trends in Secure Cryptography.....	30
4.2.2 The Shor's Algorithm.....	31
4.3 Post-quantum Cryptography	32
4.4 Comparative Analysis of Classical and Post-quantum Cryptography.....	35
4.4.1 Security Considerations.....	35
4.4.2 Compatibility and Practicality	36
4.4.3 Standardization	37
4.5 Summarizing Analytical Review	38
5 Results and Discussion	39
6 Summary.....	42
References	43
Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis	47

List of figures

Figure 1. Public Key Encryption Scheme.	14
Figure 2. Diffie-Hellman-based Key Exchange	15
Figure 3. DSA Signature Generation and Verification.....	16
Figure 4. RSA Encryption.	19
Figure 5. Sycamore – A quantum computer by Google.	20
Figure 6. Quantum Key Distribution process.....	24
Figure 7. Research Design.....	25
Figure 8. RSA Key Security.....	28
Figure 9. Shor's Algorithm	32
Figure 10. Performance Analysis of PQC Algorithms.....	37

List of tables

Table 1. Recommended prime number size.	29
Table 2. Secure cryptographic field sizes.	30
Table 3. Qubit growth timeline.....	36

1 Introduction

The ever-evolving landscape of digital threats prompts the transition to strengthened safeguards in cyber security. Within this context, the security of conventional asymmetric cryptographic algorithms including DH (Diffie-Hellman), DSA (Digital Signature Algorithm), and RSA (Rivest–Shamir–Adleman) is threatened by the recently rising technology – quantum computing. This thesis delves into the domain of cryptography by having a specific concentration on the analysis of vulnerabilities of selected asymmetric cryptographic algorithms to quantum attacks. The thesis also concentrates on the comparative review of the classical and the post-quantum cryptography.

1.1 Motivation

The critical necessity for preparing for the impending quantum age is the main drive behind this research. The possibility of exploiting potential vulnerabilities that are identified in the classical cryptographic algorithms by quantum computers is terrifying. These urges to strengthen the cryptographic solutions in a way that they become unbreakable even by quantum computers. The analysis of quantum technology regarding their threat to cause possible vulnerabilities in cryptographic algorithms and mitigating them to safeguard the data during transition, and ensuring its subsequent security is a paramount task for cyber security professionals.

1.2 Research Problem

The core focus of this research is the emerging vulnerabilities of the classical asymmetric cryptographic algorithms caused by the evolving landscape of quantum computing. Acknowledging the threat in this context and getting prepared for this is quite necessary even though the highly advanced quantum computers that are capable of breaking the currently used cryptographic algorithms are still far in the future. Enhancing the security of cryptographic algorithms carries uttermost importance as there are attacks like store-now, decrypt-later through which the encrypted data is collected, and the decryption is

delayed until access to quantum computers is granted to everyone [1]. Such attacks are notable threats, especially for financial and medical data.

1.3 Research Objectives

The primary objective of this study is to conduct an analysis of classical and post-quantum asymmetric cryptography by having a special focus on their vulnerabilities. Apart from the analysis of the vulnerabilities, the research objectives also include the examination of strengthened cryptographic solutions. Ultimately, the thesis is aimed at analysing the vulnerabilities of the selected asymmetric cryptographic algorithms caused by quantum computers and achieving enhanced security to ensure the security of digital data in the quantum age.

1.4 Limitations

Even though this research is aimed at providing a thorough analysis of cryptographic algorithms, certain constraints exist. Considering the wide range of the asymmetric algorithms and their metrics, this is not possible to cover the whole specifications and challenges. Moreover, the research is limited to three asymmetric cryptographic algorithms – DH, DSA, and RSA. Symmetric and hashing ones are not in the scope of this thesis. However, the study provides significant observations for contributing to the research on the security of asymmetric cryptography in the quantum era.

2 Background Information

In this section, an overview of the existing studies on (asymmetric) cryptography and quantum computing is conducted. The literature review involves the following parts: Basics of Cryptography, Overview of Asymmetric Cryptography, and Essentials of Quantum Computing and Cryptography.

2.1 Basics of Cryptography

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it [2]. The essence of cryptography for cybersecurity can be explained with the following services it is fulfilling: confidentiality, integrity, authentication, and non-repudiation [3]. To achieve the highlighted security features, cryptography makes use of mathematical principles and algorithms.

The implementation of cryptographic techniques and their corresponding infrastructure is called a cryptosystem. A basic cryptosystem generally includes the components - plaintext, cryptographic algorithm(s), key(s), and ciphertext. The encryption algorithm takes the plaintext which is the data to be converted and produces a ciphertext based on the associated algorithm. Cryptographic keys participating in the encryption and decryption processes are also inseparable parts of the cryptosystem. The security of the keys is an uttermost important task for safeguarding the data. [4]

The main types of cryptographic keys are symmetric and asymmetric ones. This difference is based on the usage place and logic of the keys. While the former is the only key in the cryptosystem and functions as the means of both encryption and decryption, the latter comes as a pair of different keys, one as public, and another as private (secret). The keys in an asymmetric cryptosystem are mathematically related but this is unfeasible to calculate the secret key from the public one due to one-way functions. [5]

2.2 Overview of Asymmetric Cryptography

Even though traditional (symmetric) cryptography is advantageous for the efficient processing of stationary data, it is not the best method for securing data in transit [6]. This need prompts the implementation of more suitable methods, and the challenge is overcome by applying asymmetric cryptography [7].

Asymmetric cryptographic algorithms make use of different keys for encryption and decryption purposes. The public key of the recipient is used to encrypt the message, and the recipient uses the associated private key to decrypt the message. As their names suggest, the public key is made publicly available since the sender must be able to encrypt data with it. However, the private key has to be kept secret because of its capability to decrypt the confidential data. [8] The main advantage of using asymmetric encryption is the establishment of a secure channel for key exchange. Moreover, asymmetric encryption is considered more secure due to the utilization of two different keys rather than a single one like in the symmetric cryptosystem [9].

For asymmetric cryptosystems, each user possesses their own encryption and decryption processes, which are denoted as E and D respectively. In all cases, E is publicly available, and D must be kept secret. For the following essential procedures of asymmetric cryptography that are the cornerstone of asymmetric cryptosystems; M symbolizes the message to be encrypted:

1. E and D are easily computable.
2. Even though E is publicly available, it is not easily achievable from a mathematical perspective to infer D from E .
3. Decrypting an encrypted message gives the original message back: $D(E(M)) = M$.
4. Reverse procedure still yields the original message: $E(D(M)) = M$. [10]

The process of asymmetric encryption is visualized in the figure below [11].

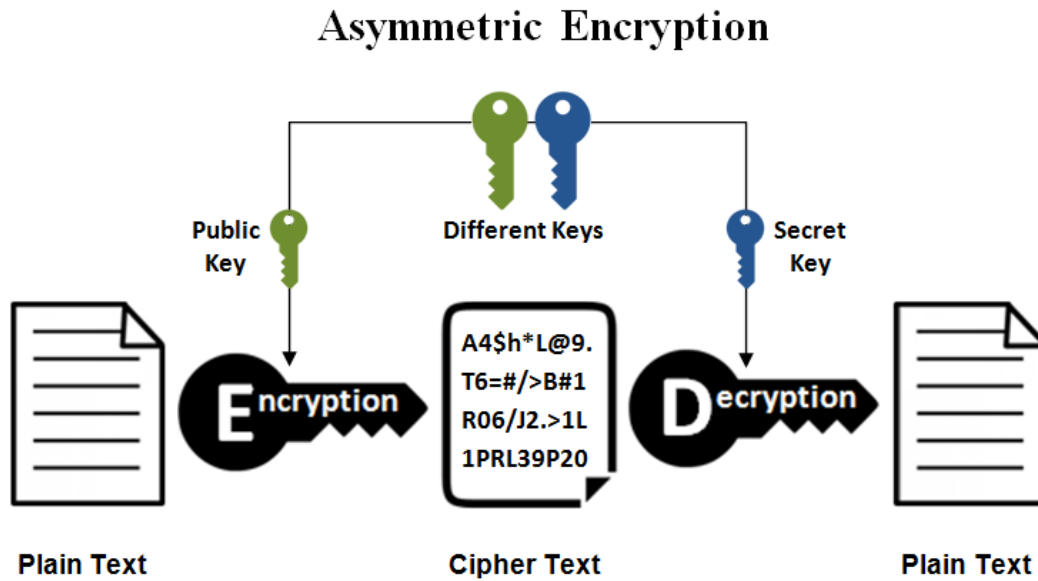


Figure 1. Public Key Encryption Scheme.

2.2.1 Diffie-Hellman Overview

In cryptography, key exchange is a strategy by which cryptographic keys are exchanged between two parties and those keys are utilized as a part of cryptographic algorithms. Utilizing those keys sender and recipient exchange encrypted messages. Public key cryptography provides a secure strategy for exchanging secret keys. [12] The Diffie-Hellman algorithm (DH) is used for exactly this purpose – the key exchange.

Establishing a secure channel over an insecure medium has been one of the most fundamental challenges of Cryptography. The Diffie-Hellman key exchange algorithm proposed in 1976 by Whitfield Diffie and Martin Hellman has played an essential role in resolving this dilemma [12]. The DH algorithm enables two parties to establish a shared key securely without prior communication. The working principle of DH is as follows:

- A large prime number p and the base number g , which is less than p are agreed on.
- Parties select secret numbers; x and y in this context.
- Respective public keys ($a = g^x \bmod p$ and $b = g^y \bmod p$) are calculated and sent to the other party.

- Lastly, the shared secret is calculated by using the received public key; $K = b^x \bmod p = a^y \bmod p$. [13]

The process is described in Figure 2 [14].

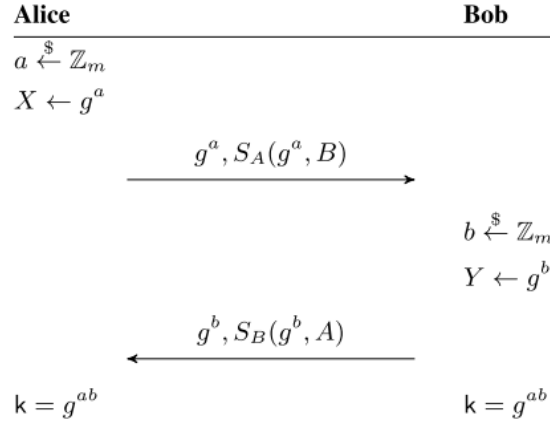


Figure 2. Diffie-Hellman-based Key Exchange

The mathematical background and security of the DH algorithm is based on the discrete logarithm. The discrete logarithm problem is defined as: given a group G , a generator g of the group, and an element h of G , to find the discrete logarithm to the base g of h in the group G . Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups. [15]

Taking account of the computational challenges of retrieving the discrete logarithm (exponent), especially for large numbers, the Diffie-Hellman key exchange algorithm is considered secure by now.

The main and currently the only vulnerability of DH is the Man in the Middle (MITM) attack which might intercept the communication and cause spoofing by the attacker in the way that the public key of the adversary is sent, or a shared key known to the adversary as well is generated [16]. Hence, digital signatures can be used together with the key exchange to provide an authentication mechanism that prevents MITM attacks [17] [14].

2.2.2 Foundations of DSA

Encrypting the transmitted data is not the sole means of providing private communication over insecure channels. Verifying the authenticity of the sender is another significant task for keeping the traffic secured. The digital signature which is committed to similar

purposes as handwritten signatures fulfils this significant task and even more – ensuring non-repudiation and integrity [18]. This way, the recipient can confirm the identity of the sender and assure the integrity (immutability) of the received message which results in achieving non-reputability. [19]

Within the context of asymmetric cryptography, the importance of digital signatures should especially be highlighted. In contrast to data encryption algorithms, like RSA which encrypt data with public key and decrypt with private key, the digital signature ones use the reverse methodology. The working principle of digital signatures is based on authenticating the sender which means only the expected sender (having the private key) can make the signature. However, as the decryption key is publicly available, anybody can verify the identity of the claimed sender. [19] [20]

The Digital Signature Standard (DSS) published by the National Institute of Standards and Technology (NIST) makes use of the Digital Signature Algorithm (DSA) which is based on the Secure Hash Algorithm (SHA) [19]. The DSA algorithm is a more competent version of the ElGamal Signature Scheme which satisfies today’s security standards in smaller bit lengths; While a DSA signature has a bit length of 320, ElGamal has a length of 2048. A similar set of numbers applies the signature verification process as well, which is done with two modular exponents of bit length 160 in DSA and three exponents with a minimum of 1024 bits in ElGamal [21].

The figure provided below describes the general signature generation and verification processes [19].

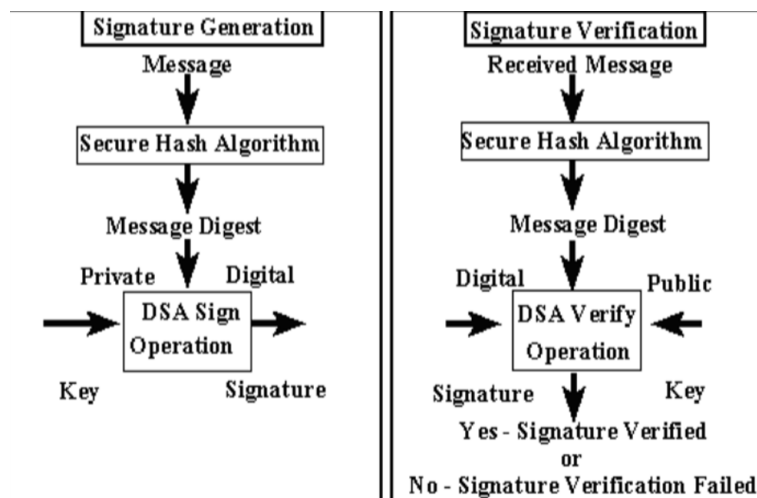


Figure 3. DSA Signature Generation and Verification.

The DSA algorithm commences with generating the keys like the other cryptographic algorithms:

- The prime numbers p and q such that $2^{511+64j} < p < 2^{512+64j}$ and $2^{159} < q < 2^{160}$ for $j \in \{0, 1, \dots, 8\}$ are chosen.
- p and q satisfy the conditions that; $q \equiv 0 \pmod{(p-1)}$, which means q is dividable by $(p-1)$.
- An $x \in \{1, \dots, p-1\}$ such that $x^{(p-1)/q} \not\equiv 1 \pmod{p}$ and corresponding variable g which is evaluated as $g = x^{(p-1)/q} \pmod{p}$ are calculated.
- A randomly generated $a \in \{0, 1, \dots, q-1\}$ is chosen. Then, the last component of the public key is calculated; $A = g^a \pmod{p}$. [21]

Considering the calculated values, the public key is (p, q, g, A) and the corresponding private key is a . The main components of the DSA keys, p and q have a direct influence on the security of the keys. The larger the numbers, the enhanced security. Thus, for a longer period of security, larger prime numbers within the context of p and q must be chosen. [21]

The security of the keys is associated with the feasibility of calculating the private key from the relevant public key, which for the DSA algorithm is based on the discrete logarithm problem and the algebraic properties of modular exponentiation. More precisely, the DSA algorithm is considered secure as solving the discrete logarithm is infeasible with the current advancement of computing technology.

2.2.3 RSA Overview

The RSA algorithm that was presented in 1977 by Rivest, Shamir, and Adleman is the first and still the most widespread public-key algorithm. This asymmetric algorithm secures data transmissions from e-mails to secure online shopping. RSA is also the pioneer cryptosystem for signing each message to prove the identity of the sender. [22]

The usage of the keys in RSA is flexible in the sense that it allows encryption and decryption with either of them. This way the requirements of CIA triad and non-reputability are satisfied [23]. Because the RSA algorithm is quite ubiquitous nowadays,

protecting the cryptographic keys is still the most fundamental task for securing the cryptosystem [24].

In the context of RSA, the components of the cryptographic keys – n , d , and e have to meet the following conditions:

- n should be the product of two very large random prime numbers; marked as p and q .
- d is relatively prime to $(p - 1)(q - 1)$, which is evaluated as $\gcd(d, (p - 1)(q - 1)) = 1$.
- $e \cdot d \equiv 1 \pmod{(p - 1)(q - 1)}$. In simpler terms, e is such a number that dividing its product with d by $(p - 1)$ times $(q - 1)$ results in 1 as a remainder.

The following mathematical foundations are the cornerstone of the encryption procedure with the RSA algorithm: The message to be encrypted is denoted with M , which is an integer from 0 to $n - 1$, where n represents the second element of the public key (e, n) . The encryption process is committed by raising M to the e^{th} power module n which results in the ciphertext represented as C :

$$C \equiv E(M) \equiv M^e \pmod{n}.$$

The decryption process works similarly as well. Considering the same expressions as in the encryption, decryption can be elucidated as follows:

$$M \equiv D(C) \equiv C^d \pmod{n}.$$

In other words, the ciphertext is raised to d which is the first component in the corresponding private key, module n . [10] [22]

Figure 4 visually demonstrates the encryption process of the RSA algorithm.

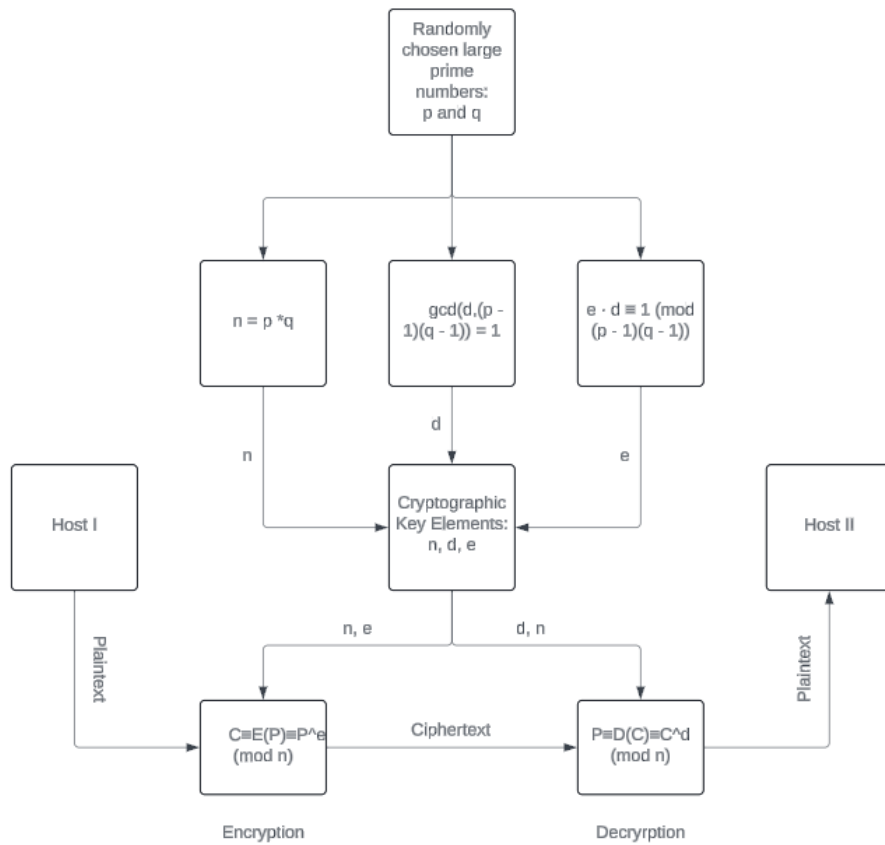


Figure 4. RSA Encryption.

The security of the RSA algorithm and messages encrypted using the algorithm relies on the difficulty of factoring the value of n . If n could be easily factored into the corresponding values of p and q , then one could easily find the value of d [22].

For the given public key (e, n) and the corresponding ciphertext $C = M^e \pmod{n}$ this is hard to find the original message (M) if n is an adequately large randomly generated number and the value of M is a random integer from 0 to $(n - 1)$. This verdict is the foundation of the RSA algorithm and is named the RSA assumption.

In simpler words, the security of the RSA algorithm is based on factoring n . Currently, no algorithm known to us is capable of breaking large numbers like 200 digits in an adequate timeframe. Thus, RSA is considered secure as of today. [22]

2.3 Essentials of Quantum Computing and Cryptography

Quantum computing is a modern way of computing that is based on the science of quantum mechanics [25]. In another way, quantum computing uses the properties of quantum mechanics and thermodynamics to secure sensitive information instead of binary bits. This unprecedented computational power is achieved through less energy consumption and provides exponential speed compared to classical computing methodologies. Certain problems that are considered practically impossible for classical computers are foreseen to be effortlessly solved with quantum computers [26]. For example, a specific computationally challenging task took 200 seconds to the Sycamore quantum computer by Google in 2019. For this similar task, a supercomputer requires 10,000 years [27]. A snippet of the Sycamore quantum computer is illustrated in Figure 5 [28].



Figure 5. Sycamore – A quantum computer by Google.

2.3.1 Understanding Quantum

Recalling again that the working principles of quantum computing are based on quantum mechanics which utilize subatomic particles. This phenomenon is essentially a general model of physics and a modern way of computing. The computers that are using the concepts of quantum computing (mechanics) are quantum computers [29]. Unlike the traditional computers that use binary bits (in 0's and 1's), the quantum ones use quantum bits – the qubits. Quantum computers are not using traditional hardware components, like

transistors, integrated circuits, logic gates, and so on. Instead, they utilize the subatomic particles – atoms, electrons, photons, and ions as the units of information by taking advantage of their spins and states. Quantum computers offer exponentially faster computation on specific tasks, especially related to cryptography, scientific calculations, simulations, and so on. Even though this revolutionary way of computing is in its preliminary stages, and it promises more sophisticated and accelerated solutions to most challenging problems, understanding the risks it brings, which in this context is mainly associated with threats to cryptography is essential for being safe in the quantum age.

2.3.2 Superposition

The cornerstone of quantum computing is the concept of superposition, which is the simultaneous existence of particles in multiple states. A prime example could be the representational comparison between bits and qubits. While bits account for either 1 or 0, qubits represent both values at the same time. More precisely, a quantum particle has a certain probability to be in the state of 1, and a certain probability to be in the state of 0 [30]. The principle of superposition only belongs to the subatomic particles, which are quantum systems. Within the context of subatomic particles, the superposition is represented as turning left and right at the same time. This phenomenon is translated to classical computing as being 1 or 0. The superposition principle enables more combinations by parallel running which leads to memory efficiency and powerful computing. [29] [31]

2.3.3 Uncertainty

Apart from superposition, quantum mechanics is heavily dependent on the principle of uncertainty (probability). In the world of quantum, every possible state of a qubit is linked to a probability, called the probability amplitude. Measuring the qubit ends up with its collapse to either 0 or 1 based on the corresponding probability. Hence, the potential state of the qubit is determined by its probability of occurrence. Within this context, the quantum world is irreducibly small, so it is impossible to measure a quantum system without having an effect on that system as our measurement device is also quantum mechanical [31]. Thus, forecasting the entities of a particle is practically impossible. This indeterminacy principle postulates that the particles do not possess undefined properties till they are measured.

2.3.4 Entanglement

Entanglement is another significant domain of quantum computing which makes the quantum computers capable of performing multiple calculations parallelly. In other words, the entanglement principle enables transferring quantum systems between two distant systems [32]. This way, many qubits are measured simultaneously instead of each one being manipulated individually. Put differently, a global system is established when qubits become entangled. A global system is such an arrangement that it cannot be written as the combination of the states of quantum subsystems [30]. Such a system also prevents individuals from being described independently. The global system is capable of preserving its state even over large distances. This feature enables correlations between the subsystems so that any process/ operation occurring over one subsystem correlates with the other one as well.

2.3.5 Linear Algebra

The role of linear algebra in quantum computing can be compared to the role of Boolean algebra in classical computing. Linear algebra is the language of quantum, and it represents how its building blocks (qubits) are behaving and interacting with each other. Hence, understanding the notion of vectors and the working principles of matrix multiplication plays a vital role in understanding the way quantum computers work [33]. The notation used for qubits is called the bra-ket notation or by its other name the Dirac notation. Preliminary information for qubit representation is provided below:

- 0 qubit is written as $|0\rangle$ and is called as ket 0.
- 1 qubit is written as $|1\rangle$ and is called as ket 1.
- Qubit is written as $|\psi\rangle$ and is called the general quantum state.
- Ket and bra notations are given respectively:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv \langle 0| = [1 \ 0] \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv \langle 1| = [0 \ 1]$$

- Vector addition example: $|\psi\rangle = \alpha(|0\rangle) + \beta(|1\rangle) = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Considering the normalized state of the qubit, in which the length of the qubit state is 1, the last equation becomes: $|\alpha|^2 + |\beta|^2 = 1$. [33][34][35]

2.3.6 Outline of Quantum Cryptography

Quantum cryptography is a branch of cryptography that exploits the principles of quantum mechanics to achieve secure communication [36]. While classical cryptographic solutions are based on complex mathematical algorithms, quantum cryptography uses fundamental properties of quantum, like superposition (see Section 2.3.2) and entanglement (see Section 2.3.4).

To elucidate further, quantum cryptography is mainly dealing with the manipulation and transmission of qubits. Their ability to exist in superposition enables the production of cryptographic keys that are encoded with an unmatched degree of unpredictability and complexity [37]. The uncertainty principle (see Section 2.3.3) is another core concept behind quantum cryptography and it is the key to the basis of Quantum Key Distribution (QKD), whose main purpose is to detect any possible eavesdropper. QKD works by encoding keys into qubits and sending them via a quantum channel. Later measurement of the qubits reveals the presence of the intruder. Hence, this is an important feature of quantum cryptography, which is not addressed in classical cryptography. The necessary steps the QKD is following are provided below:

- The photons are transmitted over a filter that randomly provides either of the 4 polarizations or bit designations. While vertical and 45 degrees right stand for 1 bit, horizontal and 45 degrees left represent 0 bits.
- The photons arrive at the receiver party and go through two beam splitters, which are optical devices used for splitting the light into transmitted and reflected beams [38]. The beam splitters are the types of horizontal/vertical and diagonal and are tasked with reading the polarization of each photon. The receiver does not have prior knowledge of which exact splitter to utilize and does this on a random basis.
- Later, the photos are processed by the splitters, and the receiver informs the sender of the order of the splitters used for each photon. Then, the sender checks this data against the sequence of polarizations it applied when sending the key. Any

photons read with the wrong beam splitter are removed. The remaining sequence of bits generates the cryptographic key. [36][37]

The detection of intrusions on the transmission of the keys is based on the possible state changes of the photons. Put differently, it is not feasible to read or alter the photons without triggering a state change. In case there is an intruder reading each photon, then the intruder themselves should pass the photon to the receiver, and this causes changes in the quantum state of the photons. This change is followed by an error in the key, and it proves that the key has been compromised. The process is visually demonstrated in Figure 6 [37].

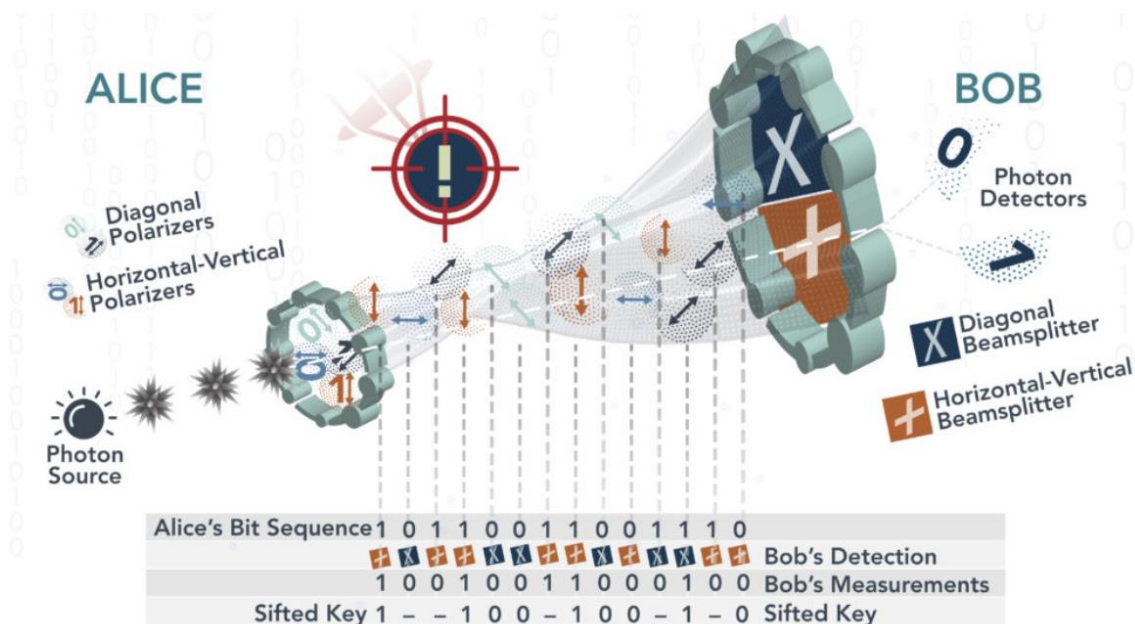


Figure 6. Quantum Key Distribution process.

Currently, QKD is the most common type of QC, which is already (practically) proven. There is ongoing research for implementing similar quantum solutions in digital signatures, direct data encryption, and other kinds of quantum cryptography. Hence, the application of quantum mechanics in cryptography is limited to key distribution (QKD) by now.

3 Methodology

In this section, we outline the methodology utilized to investigate how vulnerable classical asymmetric cryptographic algorithms are to quantum computing, assess the readiness of post-quantum cryptography solutions, and explore ways to achieve quantum-proof cryptographic solutions.

3.1 Research Design

The implications of quantum computing technology on classical cryptography techniques are analysed through a literature review and analysis approach. Scholarly articles, research papers, and online sources are examined to understand the vulnerabilities posed by quantum algorithms and the current state of post-quantum cryptography. By having a review of such diverse sources, we aim to have a vivid image of the vulnerabilities brought about by quantum algorithms. This way, we intend to have significant observations regarding safeguarding data in the quantum age. The research design is illustrated in Figure 7.

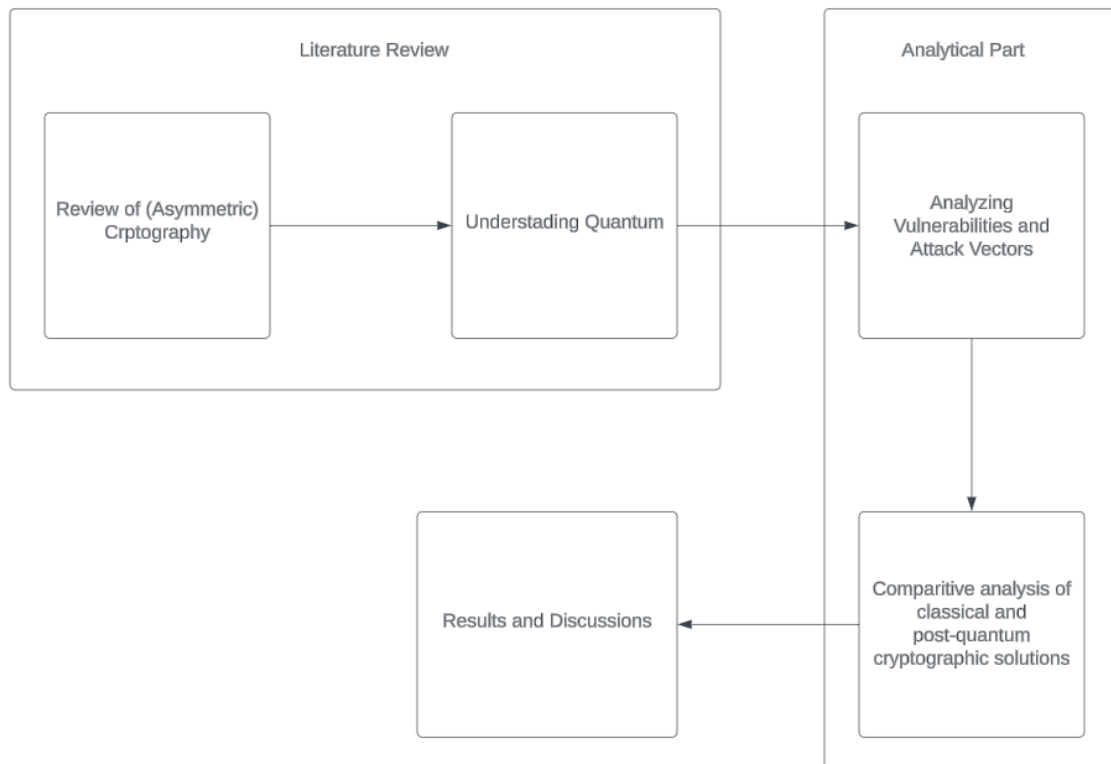


Figure 7. Research Design

3.2 Analysis Framework

A structured approach is employed to assess post-quantum and classical cryptography. The components of the utilized framework are intended to provide an extensive comprehension of the impact of quantum computing on asymmetric cryptography.

The study begins with evaluating the susceptibility of the classical asymmetric algorithms to quantum technology based on their mathematical foundations. Having reviewed the working principles of the selected algorithms, the specific methods they can be exploited will be discovered.

Next, a comparative analysis between the traditional and post-quantum cryptographic algorithms is to be conducted. This way, the suitability of the post-quantum algorithms in terms of being a substitute for the classical algorithms in the quantum age will be assessed. This part of the analysis includes assessing compatibility with current cryptographic systems, security parameters, computing efficiency, and a few other features. This analysis will discover the feasibility of implementing quantum-resilient algorithms.

Then, the necessity for potential modifications to classical cryptographic algorithms will be explored. Having a comparative and coherent analysis in the previous steps will enable us to gain insights for offering solutions to achieve enhanced security.

4 Analytical Review

In this chapter, we begin by examining the vulnerabilities of asymmetric algorithms based on their mathematical foundations. This analysis is followed by exploring the corresponding attack vectors. Later, we will go through an overview of post-quantum cryptographic algorithms and have a relative analysis of them with the classical ones.

4.1 Quantum Vulnerabilities of Asymmetric Cryptography

Classical cryptographic algorithms are based on complex mathematical problems that are considered practically impossible to solve with conventional computers. Thus, they are thought to be secure until a revolutionary method of computing arrives. The extensive computational power that quantum computers promise is the actual threat in this context.

4.1.1 Mathematical Background of Asymmetric Algorithms

The working principles of the asymmetric algorithms are based on mathematical problems that are easy to solve in one direction, but hard to compute in the other. This asymmetry forms the basis of their security.

4.1.2 Large Number Factorization Problem

The RSA algorithm has two main entities that make up the keys – randomly selected large prime numbers (See section 2.2.3). Their product results in the public modulus – n . Having the components of the public key, e , and n , the intruder is subject to factor n to gain the private exponent – d . The security of RSA is based on factoring n .

Prime factorization example:

- $497 = 7 \times 71$. The prime factors are 7 and 71.
- $1176 = 2^3 \times 3 \times 7^2$. So, the prime factors are 2, 3, and 7.

As shown in the above examples, a simple division method can be used for factoring small numbers. However, this and other similar strategies do not work for large numbers like 150 digits that are used in RSA key generation. Within the context of RSA, this is particularly hard as the public exponent is the factor of exactly 2 large prime numbers.

Currently, there is no practically applicable way known to us that enables factoring large numbers with sufficient resources. According to estimations, this can take millions of years to break RSA with conventional ways of computing [39]. Figure 8 demonstrates the proven and estimated security of RSA based on its private key size [40].

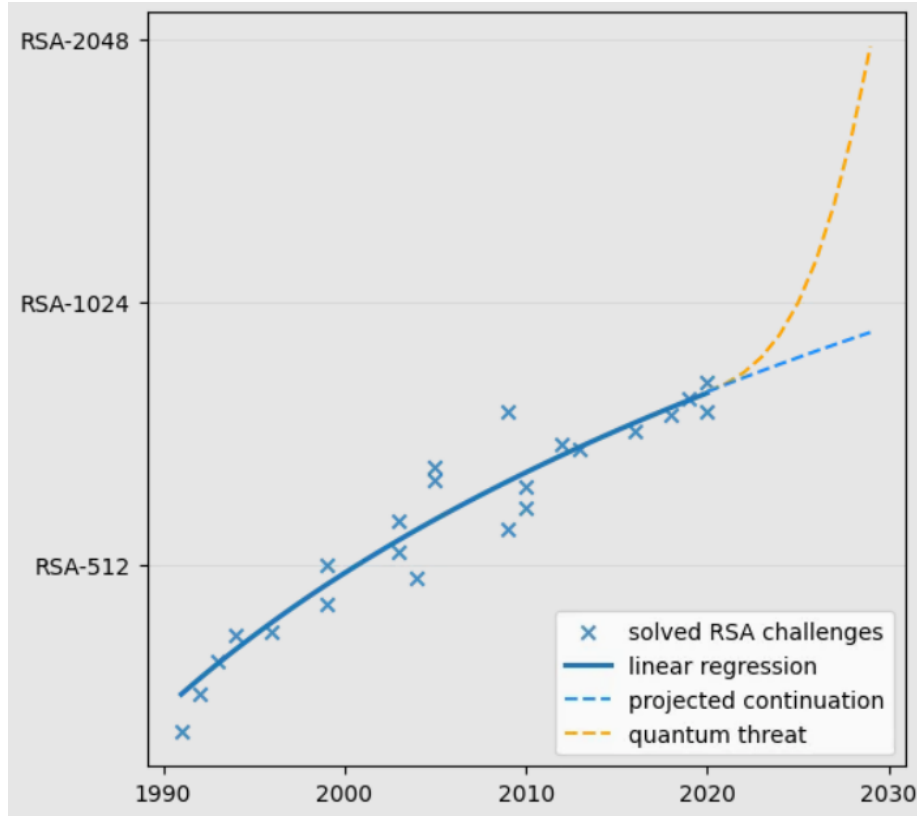


Figure 8. RSA Key Security.

4.1.3 Discrete Logarithm Problem

The discrete logarithm problem is the basis for Diffie-Hellman and Digital Signature Algorithms (See sections 2.2.1 & 2.2.2). Thus, the hardship of solving this problem has been a cornerstone in ensuring the security of data encoded with the highlighted algorithms.

The discrete logarithm problem emerges in the context of finite fields and cyclic groups. The objective of the problem is to find x such that $g^x = h \pmod{p}$, where g represents a group generator, h is a given element of the group, and p is a prime number modulus. The complexity of this problem relies on the size of the group and the modulus p . Hence,

large numbers are used to ensure a sufficient level of security in cryptosystems [15]. Simple examples are provided below:

- For the group Z_7^* , and the generator is 4, then the discrete logarithm of 1 is 3. Because $4^3 = 1 \pmod{7}$.
- For the group Z_{16}^* , and the generator is 6, then the discrete logarithm of 4 is 2. Because $6^2 = 4 \pmod{16}$.

Despite there are some conventional methods used to solve the discrete logarithm problem in cyclic groups like linear search, baby-steps giant-steps, and the Pohlig-Hellman algorithm, none is useful for numbers with long digits. In fact, smaller key sizes are more vulnerable.

Within the context of Diffie-Hellman, the keys with around 900 bits are already broken. Hence, the keys with either 1024 bits or 2048 bits which is for a longer period of security are currently in use [15].

A key size of at least 2048 bits is recommended by NIST to secure DSA [41]. The tables provided below illustrate the recommended key size of the prime number q and the cryptographic field size p for the following years [15].

Table 1. Recommended prime number size.

Year	Bit length of q
2010	138
2020	151
2030	165
2040	179
2050	193

Table 2. Secure cryptographic field sizes.

Year	Bit length of p
2010	1369
2020	1881
2030	2493
2040	3214
2050	4047

Even though the increased security parameter and the key sizes are estimated to secure the specified cryptographic algorithms still in the future, the presumed calculations are based on classical ways of computing. Considering the extensive computational power offered by quantum computers, this can be unfeasible to securely implement the crypto algorithms.

4.2 Recognizing the Threat

Having reviewed the mathematical backgrounds of the selected classical asymmetric algorithms, the next step is identifying the actual threat.

4.2.1 Current Trends in Secure Cryptography

As a matter of fact, cryptographic algorithms have always undergone extensive tests to prove their capabilities to resist a wide variety of possible attack vectors. As stated in the previous sections, there is no applicable algorithm discovered to break the base algorithms of RSA, DSA, and Diffie-Hellman, which are large-number factorization and discrete logarithm problems. The “resistance” referred to in this sense is also associated with the sizes of the corresponding key and security parameters of the aforementioned algorithms. While reviewing the historical data regarding the recommended metrics of the related parameters (See Table 1 & Table 2), this becomes blatant that the more computational power is achieved, the longer keys are compromised. In other words, each time the commonly used keys are broken by algorithms that are applied by conventional computing, there emerges a need to switch to longer key sizes to secure data encoded with these algorithms. While this trend does not look threatening at first glance, quantum computing, more precisely, Shor’s algorithm is capable of breaking the classical algorithms in hours instead of millions of years as conventional algorithms can do in

theory. The actual threat in this context is the uncertainty related to the bonding of the quantum computers. While there are presumptions made about the approximate time the conventional algorithms can break the aforementioned algorithms and strengthen the security parameters respectively, this is unfeasible to make similar estimations due to the exponentially growing power of the quantum computers.

4.2.2 The Shor's Algorithm

The algorithm suggested by the American mathematician Peter Williston Shor in 1994 (also known as Shor's algorithm) poses a terrifying threat against classical cryptography [42]. Shor's algorithm exploits the quantum properties of entanglement and superposition and solves the two fundamental problems of the asymmetric algorithms – large number factorization and discrete logarithm in polynomial time which is significantly lower than the conventional algorithms that are solving the problems in exponential time. This remarkable time reduction enables Shor's algorithm to break the cryptosystems quite efficiently. The Shor's algorithm works as follows:

1. Choose the number to factor – N . Make sure it is neither prime, nor even, nor of the form $N = x^a$.
2. Choose a random number $a \in [1 \dots N]$
3. Check $GCD(a, N) = 1$. Meaning that a and N should be coprime. Otherwise, a is already a factor of N .
4. Find minimum r that satisfies $a^r \equiv 1 \pmod{N}$. If r is odd, another a needs to be selected, and the process starts over with the second step.
5. The factors are $GCD\left[\left(a^{\frac{r}{2}} \pm 1\right), N\right]$. [43]

The main step the quantum computer will be involved is the fourth step. It will check the values of r simultaneously and find the sought-for value in a significantly lower time. This step can further be elucidated as follows:

- A new incremental variable k is defined and evaluated as $k = 1$.

- Calculate the value of $(k \times a) \bmod N$. Iterate the process until the remainder is 1. In the next iteration, the value of k is updated with the value of the remainder.
- The value of r is the number of iterations that we are making to result in 1 as the remainder.

The general process diagram is visualized in Figure 9.

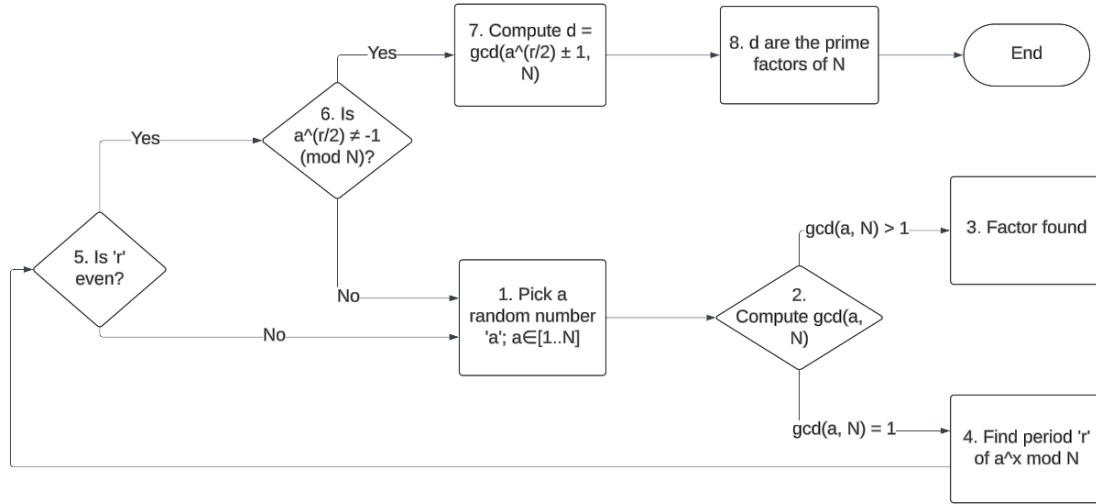


Figure 9. Shor's Algorithm

The Integer Factorization Problem and the Discrete Logarithm Problem are considered similar from the quantum perspective. Both are generalized to discrete logarithms and solved with the help of Shor's algorithm. [44] Currently, this algorithm is not applicable as it requires extensive quantum resources. Hence, the biggest number the Shor's algorithm factored so far is 21 [45]. With further advancement of quantum technology and the increased number of qubits, Shor's algorithm will be an actual threat to classical cryptography.

4.3 Post-quantum Cryptography

The cryptographic algorithms designed to resist attacks from quantum computers are referred to as post-quantum cryptography [37]. The primary distinction between the post-quantum algorithms and the quantum ones is associated with their working principles. In other words, while the quantum algorithms make use of the principles of quantum physics and can only be implemented with the help of special hardware, the post-quantum ones

are based on quite complex mathematical algorithms that even quantum computers are not considered to be capable of solving. In this sense, they are similar to classical cryptographic algorithms that both utilize hard mathematical problems. Despite this similarity in their working logic, there is a noteworthy difference between their capabilities to resist quantum attacks. Although conventional algorithms have known vulnerabilities that can possibly be exploited by particularly designed algorithms operating on quantum computers, such as Shor's algorithm, no vulnerabilities of post-quantum algorithms have been discovered so far. Several candidates have been proposed for post-quantum cryptography and they are based on various problems that are presently seen to be unsolvable even by quantum computers [46]. General outlines of the suggested schemes are provided below:

- Code-based cryptography – relies on decoding general error-correcting codes. In other words, its security is based on the difficulty of decoding linear error-correcting codes for which no practical method is known. Error-correcting codes (ECC) in general are meant for sending a message encoded with redundancy. More precisely, the concept of error correction is based on encoding data with redundant bits that the decoder corrects through these bits [47]. The key point making this methodology secure is the usage of a certain secret knowledge which is often based on the specific cryptographic scheme or the key generation process [48]. The secret generally includes random values, cryptographic seeds, and other sensitive parameters. The public key is a generator matrix or the linear random code, and the corresponding private key is derived from the public key through secret knowledge. Without the secret knowledge, this is impossible to retrieve the private key and decrypt data. This idea was first introduced by Robert McEliece in 1978 and is seen as a competent technique for PQC. [49]
- Lattice-based cryptography – relies on particular challenges of mathematical lattices. Lattice-based cryptographic schemes are based on hard problems associated with lattices which are the discrete collections of points in n -dimensional Euclidean spaces [50]. These points are generated by combining the integer combinations of a collection of vectors, called as basis of the lattice. The reason the lattices are seen as promising is related to certain computationally challenging problems like the Shortest Vector Problem (SVP), Closest Vector

Problem (CVP), and Learning With Errors (LWE). SVP is aimed at finding the shortest non-zero vector in a lattice while having its basis. The objective of CVP is to find the closest vector to the given vector [51]. LWE entails finding the coefficients of a randomly generated linear equation having its noisy version [52]. In fact, all the specified algorithms are related to one another, and they can essentially be reduced to the SVP. The key generation process is generally similar to the one in code-based cryptography. Random entities are added to the generated matrix, and it becomes the public key. The private key is derived from the secret information, and this is done by manipulating the public key in a way that certain mathematical properties are maintained. Again, without the private key, this is impossible to decrypt the message. Lattice-based problems are seen as quite hard for quantum computers as well, and no method capable of solving these challenges in polynomial time discovered yet.

- Hash-based cryptography – relies on the security of the chosen hash function. Even though unlike most of the other candidate PQC schemes, hash-based cryptography does not rely on complex mathematical structures, it offers vigorous security and especially simplicity. The working principle of the hash functions is quite simple: they take input data and output a fixed-size digest. SHA-2, SHA3, and Blake2 are commonly used hash functions that produce hashes of bit sizes from 256 to 512 [53]. As highlighted, the security of the generated signatures is based on the selected hash algorithm. Within this context, candidate hash algorithms like SHA-2 provide robust security against today's supercomputers and are thought to be secure against quantum computers as well. Even if the base algorithms are to be broken in the future, the integrity of the signatures can be restored by transitioning to more secure algorithms that have not been broken [54]. This feature makes hash-based cryptography an attractive and quantum-proof approach. Today, XMSS - the extended version of MSS (Merkel Signature Scheme) is considered the most prominent signature scheme of hash-based cryptography, and it mainly works based on constructing signatures through recursive hashing message blocks with a binary tree. [55]

4.4 Comparative Analysis of Classical and Post-quantum Cryptography

Having reviewed the conventional asymmetric algorithms, their vulnerabilities, and proposed substitutes, the next step is having a comparative analysis of them to assess their actual applicability in the quantum age.

4.4.1 Security Considerations

The field of cryptography in terms of security is undergoing significant changes mostly triggered by advancements in (quantum) computing technologies. As elucidated in the previous chapters, the conventional asymmetric algorithms are based on complex mathematical problems that the classical algorithms and the classical ways of computing are not capable of solving. In other words, they are considered secure with the current state of computing technology. Even though there emerges a need to increase the sizes of security parameters and eventually the keys from time to time, they are still considered secure as no revolutionary algorithm running on classical computers has been discovered.

However, the method of achieving enhanced security by increased key size does not seem to be promising against quantum attacks. This can be helpful in the early ages of quantum as quantum computers are not going to possess tremendous computational power at first. With further advancement of quantum computers, the need to migrate to quantum-proof algorithms will be necessary. To elucidate further, the need to transition to PQC schemes is caused by uncertainty. The degree of computational power that quantum computers are going to achieve is quite uncertain right now. In other words, they can reach a certain amount of computing power in a significantly shorter time than anticipated. Within the context of cryptography, this can threaten the classical algorithms with increased key sizes. Considering the existence of quantum algorithms that are capable of solving the foundational challenges of asymmetric cryptography by running on polynomial time instead of exponential (e.g. Shor's Algorithm), the approach of increased size of the security parameters will not be a durable solution. Table 3 illustrates the number of qubits reached by the specified periods [56].

Table 3. Qubit growth timeline.

Year	Qubit Number
2000	5 and 7
2006	12
2008	28
2012	84
2015	1000
2017	2000
2022	5000
2023	100000

To wrap up, while the classical cryptographic algorithms are expected to be quantum-resistant in the early quantum ages, their everlasting utilization through enhanced security parameters is not the ultimate solution. From the security perspective, the eventual migration to PQC is a must.

4.4.2 Compatibility and Practicality

While evaluating the most optimal cryptographic schemes for the quantum era, compatibility and consequently practicality are not the features to omit. Even though the PQC schemes have been designed to provide enhanced security, their large-scale adoption is not a straightforward process. Initially, the process of transitioning to PQC involves not only updating the classical algorithms but also modifying the current protocols and standards to ensure compatibility. Relative investments in the infrastructure are also a necessity. The possible consequences on regulatory compliance and legal frameworks of migration to PQC are also necessary matters to consider. In fact, the PQC algorithms are based on more complex mathematical problems so that their utilization can result in performance overhead regarding memory, bandwidth, and computational resources. This complexity may impact the performance of cryptographic operations and lead to higher resource utilization, which is especially inefficient for resource-constrained systems.

On the other hand, the fortified versions of classical algorithms do not require many changes to the deployed infrastructure. They offer a more seamless transition by utilizing the existing cryptographic infrastructure and frameworks. Moreover, their efficiency has been proven throughout the years and today they are empowering all the gadgets around

the world. While enhanced key sizes affect the operational performance, this impact is significantly less than the PQC ones, and this makes the classical algorithms possess an optimal balance between security and performance.

4.4.3 Standardization

The requirement of a swift transition to quantum-proof cryptosystems has been acknowledged by standardization organizations [57]. Standardizing cryptosystems is essential for their widespread adoption and deployment. This also ensures relative interoperability, compatibility, and efficiency.

Standardization of PQC is currently an ongoing process. Some outstanding work in this manner has been done by NIST (National Institute of Standards and Technology). In 2017, NIST announced a public competition for the standardization of PQC algorithms. After a 5-year long selection process, four algorithms out of 69 submitted were selected for standardization. While CRYSTALS–Dilithium, FALCON, and SPHINCS+ are intended to be implemented as digital signature algorithms, CRYSTALS–KYBER is thought to serve as the primary public-key algorithm [58]. Figure 10 illustrates significant observations regarding the performance evaluation of the selected algorithms [56].

Algorithm	Type	Performance
CRYSTALS-KYBER	Lattice-based	Overall performance of CRYSTALS-KYBER in software, hardware, and hybrid settings is excellent.
CRYSTALS-Dilithium	Lattice-based	It uses pseudorandomness and truncated storage techniques to improve performance. The scheme does not use floating-point arithmetic, which is an advantage. Highly efficient and relatively simple in implementation.
Falcon	Lattice-based	The verification process is fast and requires low bandwidth. It is the best choice for some constrained protocol scenarios.
SPHINCS+	Hash-based	Key generation and verification are much faster than signing

Figure 10. Performance Analysis of PQC Algorithms.

Even though the specified algorithms have been selected for standardization, their wide-scale deployment is still far in the future. Building a centralized view of their PKI and related systems could be one of the first steps for organizations to get ready for the transition to PQC. Prioritizing the cryptosystems and implementing corresponding automation are significant tasks for adopting PQC schemes [59].

On the other hand, classical algorithms like RSA have undergone a standardization process a long time ago and have been deployed on a large scale. They have already been operating with a wide range of different systems and platforms. Hence, their fortified versions are not going to go under any significant standardization and testing processes.

4.5 Summarizing Analytical Review

Having analysed the mathematical properties of the selected asymmetric algorithms - DH, DSA, and RSA this can be concluded that the security of these algorithms is heavily dependent on the hardness of the large number factorization problem and the discrete logarithm problem. Within this context, Shor's algorithm poses an actual threat as it has the potential to solve the above-mentioned problems in a polynomial time. Cryptographic schemes based on various problems related to error-correcting codes, lattices, hashes and so on that are thought to be secure against even algorithms running on quantum computers (like Shor's Algorithm) have been proposed.

Comparing the candidate post-quantum algorithms and the classical asymmetric ones concerning specific features like security, compatibility, and standardization has revealed significant observations. First of all, the post-quantum ones are considered secure as of now since no vulnerability of them has been discovered yet. On the other hand, they still have a long way to go to become the main cryptographic schemes deployed to a great extent. Their utilization can lead to performance issues, especially for resource-constrained systems. The corresponding standardization process should particularly ensure interoperability, compatibility, and performance efficiency. Only after the post-quantum algorithms have gone under extensive testing procedures and their practicality is proven, migrating to them should be considered, and this needs to be done in the smoothest manner possible.

5 Results and Discussion

The literature review and the comparative analysis of classical and post-quantum cryptography highlight noteworthy insights concerning the future of cryptographic systems. Classical cryptographic algorithms like DH, DSA, and RSA have been the key actors in asymmetric cryptography and have been empowering a wide range of digital platforms around the world. However, the ever-advancing power of quantum computing poses a terrifying threat to these algorithms and urges transitioning to more secure cryptographic schemes.

The study has carefully reviewed the basics of cryptography and the selected asymmetric algorithms, which especially enabled the examination of their working principles. Apart from classical cryptography, the threat – quantum technology and its primary principles have been reviewed as well. The simultaneous processing capabilities of quantum computers are the foundational point that their utilization with specifically designed algorithms threatens the security of conventional algorithms.

Laying this groundwork, the mathematical foundations of the aforementioned algorithms have been examined and this enabled identifying corresponding vulnerabilities. Understanding the working principles of Shor's algorithm and reviewing related data from different sources elucidates that the modified classical algorithms will not be able to resist quantum attacks in the long term. They will be secure only in the early ages of quantum in which the quantum computers will not possess enough processing power.

Even though the number of qubits is not the only factor determining the competence of quantum computers, their role is vital, and corresponding historical data reveals that this is unfeasible to make accurate predictions regarding the maturity of quantum computers. In other words, when the sufficient computational power the quantum computers will gain to break the conventional schemes is still unclear. This uncertainty requires more robust preparation and urges adopting quantum-proof schemes at the earliest possible time.

Our review indicates that the proposed PQC algorithms offer resilience against quantum attacks by building upon more complex solutions that are thought to be secure even against quantum attacks. In other words, due to the extensive mathematical complexity

of the candidate algorithms, no associated vulnerability has been detected that by leveraging them the adversaries can compromise the cryptosystem.

The comparative analysis of the primary features of classical and post-quantum cryptography provides essential observations in this regard. While modified conventional algorithms provide security for the initial stages of the quantum era, we cannot ultimately rely on them. Due to the discussed security principles, for quantum-safe cryptography, eventual migration to PQC schemes is a must. However, this process is not as straightforward as thought. Standardization, compatibility, interoperability, and working efficiency should be ensured. This indicates that the total integration of PQC to the deployed digital platforms is still a long-term work to be done.

To conclude, the classical asymmetric algorithms are already compatible with a wide range of digital systems for a long time and their only deficiency is the vulnerability to be exploited by quantum attacks – the security concerns. On the other hand, the current state of PQC schemes has exact opposite features. They are not capable of inter-operating with other subsystems, however, they offer resilience against quantum attacks and do not have any known vulnerability yet. Achieving their large-scale compatibility is still a complex and ongoing process.

The result we can infer from this analysis is that the classical asymmetric algorithms will not provide ultimate security against quantum attacks in the future. The PQC schemes will eventually substitute them. The study suggests a hybrid approach for the migration. The digital systems cannot solely rely on PQC algorithms in the beginning. Their interoperability and efficiency in actual scenarios will still be questionable in the early ages of deployment, even though some tests will have already been conducted in advance. Based on the fact that the conventional algorithms do not have similar risks and have already been in use for decades, the hybrid approach containing both the classical and PQC algorithms is the most optimal solution for the early quantum ages. Since the classical algorithms will already be modified with increased key size, their security will not be threatened. Hence, the hybrid approach will mainly focus on the actual integration of PQC schemes into the existing infrastructure. Any failures will be compensated as the classical algorithms will also be in place. After the successful implementation of PQC and reliability is assured, they can operate as the only means of cryptographic solution. This solution will cause performance overhead, but it is essentially the only way of

integrating new cryptographic schemes into the existing infrastructure. As stated, once the PQC algorithms are seen to be capable of operating on their own, the hybrid approach is to be substituted with only the PQC algorithms, and this will optimize the performance and working efficiency.

The suggested approach offers a more seamless transition to the new cryptographic schemes. Performance-related issues will be present at the beginning of the quantum era. The further replacement – from Hybrid to PQC will be the eventual solution for safeguarding cryptography in the quantum age.

6 Summary

To conclude, our analysis highlights the essence of PQC schemes for getting prepared for the impending threat of the extensive power of quantum computers. Through the analysis of the selected classical asymmetric cryptographic algorithms and the possible PQC solutions, the study provides significant insights into the future trends in the security of cryptography.

Our analysis indicates that even though the classical asymmetric cryptographic algorithms have been playing a pivotal role in securing digital communication for decades, the rise of quantum technology requires transitioning to more secure cryptographic solutions. The candidate schemes are built upon quite complex mathematical problems and do not currently possess any vulnerability.

Moreover, the study underlines the importance of the ongoing standardization process for ensuring interoperability, compatibility, and security of the implementation of cryptographic solutions on various platforms. All these efforts provide a seamless integration of the PQC schemes to the deployed systems. Apart from the efforts by standardization agencies, the organizations are also subject to optimizing their cryptographic infrastructure for successful implementation of the new schemes.

In summary, our analysis reveals the significance of the PQC algorithms for securing digital data in the quantum age. The study also highlights that the smooth transition to the PQC schemes is quite a crucial process for successful implementation and suggests a hybrid approach for the early and middle stages of quantum. By providing the analysis of the selected asymmetric algorithms and the candidate substitute ones, the study contributes to the research of post-quantum cryptography.

References

- [1] J. Hekkala, M. Muurman, K. Halunen, and V. Vallivaara, 'Implementing Post-quantum Cryptography for Developers', vol. 4, p. 365, 2023, doi: 10.1007/s42979-023-01724-1.
- [2] 'What is Cryptography? Definition, Importance, Types | Fortinet'. Accessed: Feb. 28, 2024. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/what-is-cryptography>
- [3] Malaysian Software Engineering Conference 9. 2015 Kuala Lumpur, R. Atan, Malaysian Software Engineering Conference 9 2015.12.16-17 Kuala Lumpur, and MySEC 9 2015.12.16-17 Kuala Lumpur, *2015 9th Malaysian Software Engineering Conference (MySEC2015) 16-17 December 2015, Kuala Lumpur, Malaysia*. IEEE, 2015.
- [4] A. Kumar, S. Srivastava, V. Wadhawan, and I. Khatri, 'CRYPTOGRAPHY AND ITS COMPONENTS', *International Journal For Technological Research In Engineering*, vol. 7, no. 4, 2019, Accessed: Feb. 28, 2024. [Online]. Available: www.ijtre.com
- [5] 'Classification of Cryptographic Keys'. Accessed: Feb. 28, 2024. [Online]. Available: <https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties>
- [6] 'An Introduction to Cryptography', 1991. [Online]. Available: www.pgp.com
- [7] S. Haque, Z. Eberhart, A. Bansal, and C. McMillan, 'Semantic Similarity Metrics for Evaluating Source Code Summarization', in *IEEE International Conference on Program Comprehension*, IEEE Computer Society, 2022, pp. 36–47. doi: 10.1145/nnnnnnn.nnnnnnn.
- [8] 'Asymmetric Cryptography'. Accessed: Mar. 01, 2024. [Online]. Available: https://ptgmedia.pearsoncmg.com/images/013100851X/samplechapter/013100851X_ch04.pdf
- [9] P. P. Santoso *et al.*, 'Systematic literature review: comparison study of symmetric key and asymmetric key algorithm', doi: 10.1088/1757-899X/420/1/012111.
- [10] E. Milanov, 'The RSA Algorithm', 2009, Accessed: Mar. 01, 2024. [Online]. Available: https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf
- [11] 'Symmetric vs. Asymmetric Encryption - What are differences?' Accessed: Apr. 18, 2024. [Online]. Available: <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>
- [12] S. Kallam, 'Diffie-Hellman:Key Exchange and Public Key Cryptosystems'.
- [13] R. N. Wright, 'Cryptography', *Encyclopedia of Physical Science and Technology*, pp. 61–77, Jan. 2003, doi: 10.1016/B0-12-227410-5/00843-7.
- [14] K. M. Vallejos, 'Diffie-Hellman based key exchange', 2019.
- [15] 'Discrete Logarithm Problem'. Accessed: Mar. 12, 2024. [Online]. Available: <https://www.doc.ic.ac.uk/~mrh/330tutor/ch06s02.html>
- [16] C. Gupta and N. V. S. Reddy, 'Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography', in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Jan. 2022. doi: 10.1088/1742-6596/2161/1/012014.

- [17] M. Mamatha and M. P. Kanchan, 'Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing', *International Journal of Scientific and Research Publications*, vol. 5, no. 6, 2015, [Online]. Available: www.ijsrp.org
- [18] D. Bansal, M. Tech Scholar, M. Sharma, and A. Mishra, 'Analysis of Digital Signature based Algorithm for Authentication and Privacy in Digital Data', *Int J Comput Appl*, vol. 161, no. 5, pp. 975–8887, 2017, doi: 10.1007/s13389.
- [19] P. Kaur and N. Arora, 'A Comprehensive Study of Cryptography and Digital Signature'. [Online]. Available: www.ijcset.net
- [20] 'DSA Algorithm: An In-depth Overview - CyberTalents'. Accessed: Mar. 11, 2024. [Online]. Available: <https://cybertalents.com/dsa-algorithm>
- [21] Buchmann Johannes, 'The Digital Signature Algorithm (DSA)'. Accessed: May 11, 2024. [Online]. Available: <https://www.cryptrec.go.jp/exreport/cryptrec-ex-1003-2001.pdf>
- [22] M. D. Kelly, 'The RSA Algorithm: A Mathematical History of the Ubiquitous Cryptological Algorithm', 2009.
- [23] S. Nisha and M. Farik, 'RSA Public Key Cryptography Algorithm-A Review', *Article in International Journal of Scientific & Technology Research*, vol. 80, p. 7, 2017, [Online]. Available: www.ijstr.org
- [24] 'RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained | Splunk'. Accessed: Mar. 04, 2024. [Online]. Available: https://www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html
- [25] S. Teja Marella and H. Sai Kumar Parisa, 'Introduction to Quantum Computing', in *Quantum Computing and Communications*, IntechOpen, 2022. doi: 10.5772/intechopen.94103.
- [26] 'What Is Quantum Computing? - Caltech Science Exchange'. Accessed: Mar. 16, 2024. [Online]. Available: <https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-computing-computers>
- [27] F. Arute *et al.*, 'Quantum supremacy using a programmable superconducting processor', *Nature*, vol. 574, p. 505, 2019, doi: 10.1038/s41586-019-1666-5.
- [28] 'Google Quantum Processor "Delivers Quantum Supremacy"'. Accessed: May 07, 2024. [Online]. Available: <https://www.iotworldtoday.com/quantum/google-quantum-processor-demonstrates-quantum-supremacy->
- [29] 'Quantum Could Solve Countless Problems—And Create New Ones | TIME'. Accessed: Mar. 18, 2024. [Online]. Available: <https://time.com/6249784/quantum-computing-revolution/>
- [30] 'Understanding quantum computing - Azure Quantum | Microsoft Learn'. Accessed: Mar. 21, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/azure/quantum/overview-understanding-quantum-computing>
- [31] '(17) QUANTUM COMPUTING Documentation | Manoj Kanturi - Academia.edu'. Accessed: May 11, 2024. [Online]. Available: https://www.academia.edu/40032269/QUANTUM_COMPUTING_Documentation
- [32] 'Azure Quantum | Entanglement'. Accessed: Mar. 21, 2024. [Online]. Available: <https://quantum.microsoft.com/en-us/explore/concepts/entanglement>
- [33] 'Linear algebra for quantum computing - Azure Quantum | Microsoft Learn'. Accessed: Mar. 21, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/azure/quantum/overview-algebra-for-quantum-computing>

- [34] E. Şahin, Ç. Onsekiz, and M. Üniversitesi, ‘Implementation of Addition and Subtraction based on Quantum Fourier Transform on IBM Quantum computer’. [Online]. Available: <https://www.researchgate.net/publication/365471214>
- [35] ‘Quantum Computing with Silq Programming’. Accessed: Mar. 25, 2024. [Online]. Available: <https://subscription.packtpub.com/book/programming/9781800569669/2/ch02lv11sec03/introducing-linear-algebra-for-quantum-computing>
- [36] ‘What Is Quantum Cryptography? | IBM’. Accessed: Apr. 01, 2024. [Online]. Available: <https://www.ibm.com/topics/quantum-cryptography>
- [37] ‘Quantum Cryptography, Explained | Quantum Xchange’. Accessed: Apr. 01, 2024. [Online]. Available: <https://quantumxc.com/blog/quantum-cryptography-explained/>
- [38] D. N. Makarov, ‘Theory for the beam splitter in quantum optics: quantum entanglement of photons and their statistics, HOM effect’.
- [39] N. Krzyworzeka, ‘Asymmetric cryptography and trapdoor one-way functions’, *Automatyka/Automatics*, vol. 20, no. 2, p. 39, 2016, doi: 10.7494/automat.2016.20.2.39.
- [40] ‘Will Quantum Computers break the Internet? - neXenio’. Accessed: Apr. 06, 2024. [Online]. Available: <https://www.nexenio.com/blog/2022/will-quantum-computers-break-the-internet/>
- [41] ‘Algorithms and key sizes - IBM Documentation’. Accessed: Apr. 07, 2024. [Online]. Available: <https://www.ibm.com/docs/en/zos/2.4.0?topic=2-algorithms-key-sizes>
- [42] M. E. Sabani, I. Galanis, I. K. Savvas, and G. Garani, ‘Implementation of Shor’s Algorithm and Reliability of Quantum Computing Devices’, 2021, doi: 10.1145/3503823.3503895.
- [43] ‘Shor’s Algorithm (classically) — Computing in Physics (498CMP)’. Accessed: Apr. 10, 2024. [Online]. Available: <https://courses.physics.illinois.edu/phys498cmp/sp2022/QC/Shor-Classical.html>
- [44] ‘Quantum Attack Resource Estimate: Using Shor’s Algorithm to Break RSA vs DH/DSA VS ECC – Kudelski Security Research’. Accessed: Apr. 11, 2024. [Online]. Available: <https://research.kudelskisecurity.com/2021/08/24/quantum-attack-resource-estimate-using-shors-algorithm-to-break-rsa-vs-dh-dsa-vs-ecc/>
- [45] ‘What is Shor’s Algorithm? - Utimaco’. Accessed: Apr. 08, 2024. [Online]. Available: <https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-shors-algorithm>
- [46] ‘BSI - Post-quantum cryptography’. Accessed: Apr. 12, 2024. [Online]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie/post-quanten-kryptografie_node.html
- [47] ‘Error-correcting code | Technology | Siglead’. Accessed: Apr. 12, 2024. [Online]. Available: <https://siglead.com/en/technology-eg/errorcorrectioncode/>
- [48] V. Weger, N. Gassner, and J. Rosenthal, ‘A Survey on Code-based Cryptography’, 2024.
- [49] ‘What is Code-based Cryptography? - Utimaco’. Accessed: Apr. 12, 2024. [Online]. Available: <https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-code-based-cryptography>

- [50] Z. Zheng, ‘Financial Mathematics and Fintech Modern Cryptography Volume 1 A Classical Introduction to Informational and Mathematical Principle’. [Online]. Available: <https://link.springer.com/bookseries/16497>
- [51] ‘Post-quantum cryptography - lattice-based cryptography’. Accessed: Apr. 13, 2024. [Online]. Available: <https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography>
- [52] O. Regev, ‘The Learning with Errors Problem’, Accessed: May 11, 2024. [Online]. Available: <https://cims.nyu.edu/~regev/papers/lwesurvey.pdf>
- [53] ‘What is Hash-based Cryptography? - Utimaco’. Accessed: Apr. 13, 2024. [Online]. Available: <https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-hash-based-cryptography>
- [54] ‘Math Paths to Quantum-safe Security: Hash-based Cryptography - ISARA Corporation’. Accessed: Apr. 13, 2024. [Online]. Available: <https://www.isara.com/blog-posts/hash-based-cryptography.html>
- [55] J. A. Buchmann, D. Butin, F. Göpfert, and A. Petzoldt, ‘Post-Quantum Cryptography: State of the Art’.
- [56] A. Horpenyuk, I. Opirskyy, and P. Vorobets, ‘Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms’.
- [57] J. Lange, ‘Post-quantum cryptography’, *Nature*, vol. 549, no. 7671, pp. 188–194, 2017, doi: 10.1038/nature23461.
- [58] ‘NIST Releases Four PQC Algorithms For Standardization’. Accessed: Apr. 16, 2024. [Online]. Available: <https://thequantuminsider.com/2023/08/24/nist-releases-four-pqc-algorithms-for-standardization/>
- [59] ‘NIST Releases Quantum-safe Cryptography Standards: What Happens Now? | DigiCert’. Accessed: Apr. 16, 2024. [Online]. Available: <https://www.digicert.com/blog/nist-pqc-standards-are-here>

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis¹

I Orkhan Hasanzade

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Quantum Threats to Asymmetric Cryptography: Analysing Vulnerabilities and Enhancing Security”, supervised by Mohammad Tariq Meeran.
 - 1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
 - 1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

11.05.2024

¹ The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.