jamk.fi

Post Quantum Cryptography

Impact to the public key cryptography

Juha Luukkanen

Master’s thesis
May 2022
Information and Communication Technologies
Master's Degree Programme in Information Technology,
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Luukkanen, Juha	Type of publication Master’s thesis	Date May 2022
		Language of publication: English
	Number of pages 133	Permission for web publication: x

Title of publication

Post Quantum Cryptography

Impact to the public key cryptography

Degree programme

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Saharinen Karo

Hautamäki Jari

Assigned by

Insta DefSec Oy, Lamminmäki Janne

Abstract

Public key cryptography plays an important role in people's daily lives, in the world of business and in critical functions of society. A quantum computer is a computer that uses the special properties of quantum mechanics to process, create and manipulate data. Quantum computing is a new and radically different computing technology that is believed to effectively solve problems that classical computers cannot. A quantum computer powerful enough is believed to be able to break the public key cryptography.

The aim of the study was to find out how a quantum computer works and is able to break the public key cryptography. The aim was also to interpret when a quantum computer threat is realized in public key cryptography, what the methods are to protect against it and how the threat should be or should already have been considered in advance. A literature review was used to gather existing information on the research topic. Thematic interviews were used to gather data on the key informants’ opinions and views on the future of quantum computing and its implications for public key cryptography.

Based on the research results, it is likely that a general-purpose quantum computer capable of breaking public key encryption will be developed in the future. The first quantum computer that threatens the security of public key cryptography is likely to be developed by a well-known player with sufficient resources and already involved in the development process. The realisation timeframe for a quantum computer capable of breaking the encryption of the public key is difficult to estimate reliably, but it is expected to happen within the next 15 years. Based on the research interviews, the best way to protect against the threat posed by quantum computers to public key cryptography is to use quantum-safe algorithms.

Keywords/tags (subjects)

Public key cryptography, post quantum cryptography, quantum computer

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t) Luukkanen, Juha	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Toukokuu 2022
		Julkaisun kieli: Englanti
	Number of pages 133	Verkkojulkaisulupa myönnetty: x

Työn nimi
Post Quantum Cryptography
Vaikutus julkisen avaimen salaukseen

Tutkinto-ohjelma
Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)
Saharinen Karo
Hautamäki Jari

Toimeksiantaja(t)
Insta DefSec Oy, Lamminmäki Janne

Tiivistelmä

Julkisen avaimen salauksella on merkittävä rooli ihmisten jokapäiväisessä elämässä, yritysten liiketoiminnassa sekä yhteiskunnan kriittisissä toiminnoissa. Kvanttitietokoneella tarkoitetaan tietokonetta joka, käyttää tietojen prosessointiin, luomiseen ja manipulointiin kvanttimekaniikan erikoisominaisuuksia. Kvanttilaskenta on uutta ja radikaalisti erilaista tietotekniikkaa, jonka uskotaan tehokkaasti ratkaisevan ongelmia, joihin klassiset tietokoneet eivät pysty. Riittävän tehokkaan kvanttitietokoneen uskotaan pystyvän murtamaan julkisen avaimen salaus.

Tutkimuksen tarkoituksena oli selvittää, miten kvanttitietokone toimii ja pystyy murtamaan julkisen avaimen salauksen. Tavoitteena oli myös tulkita, milloin kvanttitietokoneen aiheuttama uhka toteutuu julkisen avaimen salauksessa, millä menetelmillä sitä vastaan voidaan suojautua ja miten uhka olisi otettava tai on jo mahdollisesti otettu huomioon etukäteen. Kirjallisuuskatsauksen avulla kerättiin olemassa olevaa tietoa tutkimusaiheesta. Teemahaastattelujen avulla kerättiin aineistoa avainhenkilöiden mielipiteistä ja näkemyksistä kvanttilaskennan tulevaisuudesta ja sen vaikutuksista julkisen avaimen salaukseen.

Tutkimustulosten perusteella on todennäköistä, että tulevaisuudessa kehitetään yleiskäyttöinen kvanttitietokone, joka pystyy murtamaan julkisen avaimen salauksen. Ensimmäisen kvanttitietokoneen, joka uhkaa julkisen avaimen salauksen turvallisuutta, kehittää tunnettu toimija, jolla on riittävät resurssit ja joka on jo nyt mukana kvanttitietokoneiden kehittämisessä. Julkisen avaimen salauksen murtamiseen kykenevän kvanttitietokoneen toteutumisaikataulua on vaikea arvioida luotettavasti, mutta sen arvioidaan tapahtuvan seuraavan 15 vuoden kuluessa. Tutkimushaastattelujen perusteella paras tapa suojautua kvanttitietokoneen julkisen avaimen salaukselle aiheuttamaa uhkaa vastaan on hyödyntää kvanttiturvallisia algoritmeja. Suojautuminen tulee kuitenkin aloittaa riittävän ajoissa.

Avainsanat (asiasanat)
Julkisen avaimen salaus, Post Quantum cryptography, kvanttitietokone

Muut tiedot (Salassa pidettävät liitteet)

Contents

Figures

Tables

1 Introduction

A quantum computer is a computer that uses special properties of quantum mechanics, such as entanglement and superposition, to process, create and manipulate data. Quantum computers are based on quantum mechanics, a field of physics that studies randomly behaving subatomic particles. It is a new and radically different computing technology that is believed to solve certain computational problems much more efficiently than traditional computers.

The classic computer uses bits, representing ones and zeros, to solve different problems. A classical computer can handle one set of inputs and solve one calculation at a time, then move on to the next. Thanks to the quantum superposition principle, qubits in a quantum computer can hold one and zero values at the same time. In this way, the quantum processor can simultaneously solve multiple calculations that have multiple inputs. Interest in quantum computing has increased and dozens of governments, universities and corporate research institutes are investing in high-profile projects to conduct competitive research on quantum computing. The first working, but still rather modest, quantum computers have already been demonstrated and are being sold for limited use. The goal is to develop a universal fault-tolerant quantum computer by increasing the capacity of existing quantum computers from tens of qubits to hundreds, thousands, and millions, and to develop quantum error correction technologies(Swan, Santos & Witte, 2020, 2).

Many countries have been quick to set up applied research programmes to accelerate progress in the development of quantum technologies:

- In 2018, the EU launched the EU Quantum Flagship project to support quantum technology development with €1 billion over ten years (Quantum Flagship, 2018)
- The US National Quantum Initiative Act of 2018 is a five-year programme to accelerate quantum research and development. The value of the program is 1,275 billion US dollars (The National Science and Technology Council, 2021).
- India's 2018 budget allocates $1.12 billion over five years for quantum technology development (Padma, 2020).
- Finnish government funds the purchasing and development of a quantum computer with 20.7 million euros for 2020-2024 (Vasara, Pursula & Rantasalo, 2020).
- Germany transfers €2 billion from its pandemic fund to research on quantum technologies by 2020. The aim of the funding is to achieve German leadership in the European effort to move the sector from research to the mainstream (Burke, 2020).

- France presented its national strategy for quantum technologies in January 2021. Five-year €1.8 billion plan to fund research in quantum computing, communication, and sensing (Pelé, 2021).
- Large private players such as IBM, Google, Microsoft, Intel, Biogen, D-Wave, Honeywell, Rigetti and Alibaba are investing heavily in quantum computing and collaborating with academic partners and other institutions (Carter & Manley, 2020).

The above list does not include even a fraction of the funding that quantum computing has received in recent years. However, it gives a good idea of how important quantum computing is considered to be and how much effort is being put into its development.

Quantum processors are advancing rapidly, and manufacturers are introducing more powerful quantum computers every year. At the time of writing, in March 2022, the largest and third largest quantum computers in the number of qubits are located in the United States and the second largest is developed by China. In November 2021, IBM introduced the current number one quantum processor in terms of qubit count, which exceeds 100 qubits. A quantum processor named Eagle contains 127 qubits (IBM, 2021). The second largest quantum processor at the moment, the 76 qubit Jiuzhang processor developed by the University of Science and Technology of China was unveiled in 2020 (Ball, 2020). Google's fastest quantum processor at the moment is Sycamore, introduced in October 2019, which contains 72 qubits (Google, 2019). In chapter 3.2.3.3 Quantum volume of this research, the metrics used to compare different types of quantum computers are described in more detail.

When will a sufficiently powerful quantum computer be possible? The development of quantum computing is thought to be at a very early stage and there is no complete understanding of how and when to prepare for future breakthroughs. However, there is considerable uncertainty surrounding the development of quantum computing and it may be well ahead of where it is perhaps widely believed to be (Swan et al., 2020, 2).

Quantum computing is believed to offer the computational power to solve problems that cannot be solved by today's classical computers. Quantum machines are expected to provide help in areas such as chemistry, quantum simulation, geography and optimisation, pattern recognition and machine learning, drug development, artificial intelligence, finance, and logistics simulation.

While the development of the quantum computer will contribute to the advancement of many scientific disciplines, it also poses threats. The development of quantum computing has implications for cybersecurity. The public key cryptography is based on complex mathematical functions, which cannot be solved by a classical computer. These constraints no longer apply to the quantum computer, an efficient general-purpose quantum computer can reveal the prime numbers that underlie the public key cryptography of almost all current security systems. (Lewis, Ferigato, Travagnin & Florescu, 2018, 7).

The first actor to develop a quantum computer will have a significant advantage over other players. The fear is that competing actors such as governments or companies could use quantum supremacy to break the encryption of sensitive data and exploit it without others knowing. If quantum computing is implemented on a large scale, it will have a significant impact on cybersecurity. It is feared that quantum computing will affect almost all cryptographic systems based on factoring and discrete logarithms.

Today's data encryption is based on standardised algorithms protocols and products. The main categories of encryption algorithms are symmetric and asymmetric algorithms. Asymmetric algorithms are also known as public key algorithms. Public key cryptography is widely used and has a significant impact on the day-to-day functioning of society, affecting individuals, organisations, governments, and critical infrastructure. Public key cryptography is used in algorithms, protocols, and ecosystems such as RSA, Diffie Helman, ECC, SSH, TLS, Digital X.509(v3) certificates, Public Key Infrastructure, S/MIME, SSH and IPsec. Also, many systems such as VPNs, many Wi-Fi networks, smart cards, Hardware Security Modules utilise public key technology.

The growing use of IOT devices is expected to increase the use of public key cryptography in the future (Entrust, 2021).

An example of the extensive use of public key cryptography is the use of SSL certificates on the Internet to identify a trusted website. According to statistics from the BuiltWith technology tracking website, there were 174.9 million SSL-secured websites in use in March 2022 (BuiltWith, 2022).

Encrypted data can be captured today, and the encryption broken later, when technology such as the development of the quantum computer makes it possible. The retention periods for encrypted data can be very long. Act on the Openness of Government Activities 31 § specifies that the period of secrecy of a public authority document is 25 years (Oikeusministeriö, 1999). Act on Information Management in Public Administration 14 § transmission of data over a data network specifies that the public authority must carry out the transmission of data over a public data network using an encrypted or otherwise secure communication link or method if the data to be transmitted is confidential. In addition, the transfer must be organised in such a way that the recipient is verified or identified in a sufficiently secure manner before the recipient has access to the confidential data transferred (Valtiovarainministeriö, 2020). How information that is protected today should be protected so that it is not compromised in the future.

Many large companies, especially cloud service providers such as Google (Kirk, 2016), Oracle (Darrow, 2018), Amazon Web Services (Hopkins, 2019) and many others have already started to look for and implement solutions to protect their business against the potential threat of quantum computing. When should Finnish companies and organisations start preparing for the threat of quantum computing?

It is important to be able to identify and assess the threat posed by a quantum computer to the public key cryptography methods currently in use in order to prepare for it in time. As the predicted lifetime of currently deployed systems based on public key cryptography methods extends over decades, it is important to assess the threat that a quantum computer poses to, for example, encrypted data.

Previously, we have described the extensive use of public key cryptography techniques in our everyday world. It also describes how much governments and private companies are investing in the development of quantum computing. Various players have succeeded in developing more efficient quantum computing processors. It is therefore extremely important for anyone working in public key cryptography to understand what advances in quantum computing mean.

In Finland, Business Finland's Digital Trust programme funds the development of quantum-safe cryptographic technologies in the Post-Quantum Cryptography, PQC project. The total size of the programme is EUR 6 million, of which Business Finland will provide around EUR 3 million. The project started in 2020 and will be completed in 2022. Business Finland's PQC project aims to accelerate the generation of new innovations and business growth by leveraging Finland's trust capital: security and trust in solutions and services from the perspective of both solution providers and users. The programme supports the exploration of the opportunities and threats of new technologies such as quantum computing. The research project involves private companies, research organisations and public authorities important for national security (Business Finland, 2020).

Insta is one of the companies participating in the PQC project. Insta makes products and provides services that utilise public key encryption. This research was commissioned by Insta to better understand the impact of quantum computing on public key cryptography. This research promises to answer questions how a quantum computer works, how it can break the public key cryptography and how it can protect against it.

2 Research basis

2.1 Problem statement

Research can be described as organised collection and analysis of information with the aim of understanding the world around us (Baldwin, 2018, 3).

There are no unified criteria for science; scientists and philosophers present very different views on the nature of reality and knowledge. Science criteria include criticality, objectivity, independence, mysticality, and impartiality. Science understands, describes, and explains reality by creating theories that are sets of claims formed using concepts. It is important that scientific information is well-founded. (Puusa & Juuti, 2020, 27)

Depending on the choice of research approach, qualitative research may have different objectives, such as acquiring new knowledge, deepening understanding, describing, or interpreting a phenomenon, and making or questioning a theoretically meaningful interpretation. (Puusa & Juuti, 2020, 73)

The purpose of the study is investigate the impact of Post Quantum Cryptography to the public key cryptography.

- The purpose of the study is to describe how a quantum computer works and is able to break the public key cryptography. The goal is to interpret when a quantum computer threat is realized in public key cryptography and how the threat should be considered in advance.
- The study consists of facts that describe the current real state of the quantum machine, but also seeks to interpret the impact of the quantum machine in the future from the perspective of public key cryptography use cases.
- The study has aimed at objectivity
- As the subject of study is constantly evolving, it is study view of the current situation.

2.2 Research questions

Research questions must be researchable, which means that they must be answered by collecting and analysing data (Baldwin, 2018, 11).

The questions that concern the researcher are:

1. How does a quantum computer break public key cryptography?
2. Who will develop the first quantum computer powerful enough to break public key cryptography, and what is the motivation for development?
3. When will the first quantum computer that threatens public key cryptography become a reality?
4. What are the methods to protect public key cryptography against the threat posed by quantum computers?

The nature of the study is thus descriptive, and a qualitative research approach was chosen as the research approach.

The reasons for choosing a qualitative research method are: there is no previous knowledge, hypothesis, or theory about the research topic. A deep understanding of the complex topic to be studied is desired.

A qualitative research approach is well suited to research when one is interested in the detailed structures of events rather than their general distribution. (Syrjälä, 1994, 12-13)

Qualitative research is conducted because a detailed understanding of a complex problem is needed. Qualitative research is also used to understand the contexts or settings in which research participants address a problem or issue (Creswell & Poth, 2018, 103).

Qualitative research includes a verbal description of real-life situations (Silverman, 2006, 28).

Qualitative research is useful if the subject of the study has not previously been studied or it is difficult to know in advance the directions of the responses to be received during the study.(Hirsjärvi & Hurme, 2015, 34).

Due to the nature of qualitative research, the research questions prepared at the beginning of the study are preliminary, and the things found during the study may produce new questions, alter existing ones, or render them irrelevant (Saldana, 2011, 71)

The goal of qualitative research is not to test a pre-set hypothesis, but the research design is flexible. In accordance with the principle of the hermeneutic circle, the researcher can return to refine the research question after collecting the material, after finding something new and unexpected (Puusa & Juuti, 2020, 73).

Qualitative research is a suitable method when researchers want to understand a concept or a concept that has been studied little. If the researcher does not know in advance the important research variables related to the topic, qualitative research is exploratory and useful. An approach may be needed if existing theories are not suitable for research, the subject is new, or the subject has never been addressed by a specific sample or group of people. The approach chosen is also influenced by the researchers' personal educational background and experience. It should also be noted that qualitative approaches allow room to be innovative and more action within the framework designed by researchers. They allow for a more creative, written style of writing (Creswell, 2009, 18).

One of the key ideas of qualitative research is to obtain information from participants about the problem or issue being researched, using best practices to obtain that information. The qualitative research process is evolving in nature. As an example, the original stages of research may change after the researcher has started collecting material. Research questions, data collection methods or interviewees may change during the study (Creswell & Poth, 2018, 100) .

Qualitative research offers rich and convincing real-world perspectives and experiences in ways that are entirely different from, but sometimes also complement, the information available through quantitative methods (Braun & Clarke, 2014).

Qualitative research examines things in natural environments, trying to make sense of or interpret the meanings of the phenomena that people give them (Denzin & Lincoln, 2018, 43).

2.3 Scope

The research focuses on the impact of quantum computing on public key cryptography.

The purpose of the research is to describe how a quantum computer works and how it can break the public key cryptography. The goal is to interpret when a quantum computer threat is realized in public key cryptography, what are the methods to protect against it and how the threat should be/have already been considered in advance.

The target audience of the study are national cryptanalysts who want to understand the impact of quantum computing on public key cryptography.

The impact of quantum computing on symmetric encryption was excluded. The principle of the Grover algorithm for symmetric key breaking is briefly discussed in chapter 3.4.1.1 Grover´s Algorithm, but otherwise symmetric algorithms are left outside the scope of the topic.

The mathematical description and proving of problems related to quantum computing were also excluded from the scope of the study.

2.4 Research method

The interviews used in this qualitative study were conducted as a semi-structured interview in which the researcher formulates thematic questions based on research questions and research themes.

Information is needed to solve the research problem and the research questions derived from it. Information is obtained by collecting data. Research data is collected using data collection methods. The methods used depend on the chosen research approach. Typical sources of research data for qualitative research are documents, interviews, thematic interviews, and observations. Transparency, achieved through adequate and accurate documentation, is important in scientific work. The initial situation of the thesis, the choices of the research approach and methods are justified, so that readers and evaluators outside the thesis can evaluate the different stages of the research process and the reliability of the results (Kananen, 2017, 67)

The theoretical framework and methods chosen by the researcher should correspond to what he wants to achieve by research and the choices made must be made consciously (Braun & Clarke, 2006, 80).

The reliability of empirical research depends in part on how the data has been collected and analysed (Duran et al., 2006, 37)

Typical data collection methods in qualitative research are survey, interview, observation, and information collected from various documents (Tuomi & Sarajärvi, 2018, 82).

Existing material is called secondary material that can be used as such. For example, books, letters, memos, recordings, or videos can be used as material for qualitative research. The data collected for the research problem is called primary data. Primary data are processed using analytical methods, the choice of which is influenced by the nature of the data. (Kananen, 2015, 81)

The most used method of data collection in qualitative research is interview because it is a very flexible method and is suitable for many different research purposes. (Hirsjärvi & Hurme, 2015, 34). The aim of the interview is to collect data that can be used to draw reliable conclusions about the phenomenon under study (Hirsjärvi & Hurme, 2015, 66)

The use of the interview as a data collection method is supported by its flexibility. The interviewer can repeat the question, ask to elaborate on the wording of the expressions, correct misunderstandings, and have a conversation with the informant. The order of questions in the interview can be changed depending on the researcher's view and how the interview progresses. The interviewer acts as an observer who also records non-verbal observations. The downsides of the interview are that it is a time consuming and expensive form of data collection (Tuomi & Sarajärvi, 2018, 84-85).

The interview often discusses issues related to the past. There are many different forms of interviews, and they can be classified as individual or group interviews according to the number of interviewees. Depending on the type of question used, an interview can be broken down by question type into a form, thematic or open-ended interview. A form interview is a type of survey in which the questions are pre-defined. The form interview is structured, in other words, exact. The structured survey has pre-defined questions and their answer options. (Kananen, 2017, 88-89)

Structured questions can be used to understand the context of a qualitative phenomenon. The subject of the study and the phenomena are linked to the real world with factual data. The information can also be used to understand the phenomenon. (Kananen, 2017, 94).

An open interview, also referred to as a deep interview, is based solely on the topic being discussed. An open interview has no preconceived questions or themes (Kananen, 2017, 88-89)

In a thematic interview, the researcher has pre-defined the themes to be discussed with the informant. The themes are topics for discussion and very general in nature. Typically, the themes are based on the research framework, i.e., the information what is already known about the phenomenon under study (Tuomi & Sarajärvi, 2018, 87).

Themes are general questions like: what is this or what this is all about. (Kananen, 2015, 68)?

In the thematic interview, the researcher and the informant discuss issues related to the phenomenon. Theme refers to the subject being discussed. The theme is broader than the question. A thematic interview may include several rounds of interviews, in which case the second round can be used to discuss issues raised in the analysis of the material from the first round (Kananen, 2017, 95).

The thematic interview aims to use themes to gain insight and understand the phenomenon under investigation. The researcher tries to use the questions and the answers to them to build a detailed picture of the whole, which, through the analysis phase, will form a holistic picture and understanding of the subject of the research (Kananen, 2017, 89-91)

To formulate the topics of discussion, i. e. the themes, the researcher must have a prior understanding of the phenomenon being studied. Based on these, a framework for a thematic interview is drawn up, covering the phenomenon to be studied. Any new themes that emerge during the interview should also be discussed. The discussion will be as open and general as possible, with the interviewee answering how he or she experiences, understands, and structures the topic (Kananen, 2017, 95-98).

Questions used in an interview can be divided into four groups:

- Sensitizing questions – are questions leading to the phenomenon, such as: What is happening, what actors are involved, what is the meaning of the situation for the actors, and how do they define it? What are the different actors doing? Are their meanings and definitions similar or different?
- Theoretical questions- help to understand the processes and differences associated with the phenomenon, and to establish connections between concepts.
- Practical questions - which help to develop the structure of the theory and guide the theoretical sampling.
- Guiding questions - that guide the collection of documents, observations, interviews, and their analysis

(Corbin & Strauss, 2008, 93-94)

The content of a thematic interview consists of words, phrases and gestures, the meaning of which is not always unambiguous. The interview is conducted in colloquial language, where words and concepts are not precisely defined and are used quite broadly (Kananen, 2017, 89-90).

Qualitative research seeks to understand a particular activity, to describe an event or phenomenon, or to form a theoretical interpretation of the phenomenon under study. However, qualitative research does not aim to make statistical generalizations. For this reason, it is important that the persons from whom the data are collected have experience and that they know as much as possible about the phenomenon being investigated. (Tuomi & Sarajärvi, 2018, 97).

The interviews conducted in this qualitative study were key Informant interviews focusing on specific interview themes. The interview structure made use of a semi-structured interview framework.

The informants were selected in a targeted and appropriate manner based on the specific information they are expected to have. This specific information may relate to the knowledge, skills, personal experiences or other matters of the informants related to the research problem. The best possible informants are needed to obtain the required information (Robert G. Burgess, 2003, 155).

A key informant refers to an expert source of information. Due to his or her social status or personal skills, the key informant can provide a deeper understanding and more information on the topic related to the research question (Marshall, 1996, 92).

Robert G. Burgess (2003) presents the following criteria for the selection of key informants:

- Role in the community. The formal role of informants should expose them to the information needed to resolve the research question.
- Knowledge: In addition to having access to the information sought by the researcher, the informant must meaningfully absorb the information.
- willingness: Informant should cooperate as optimally as possible and to be willing to communicate their information to the researcher.
- Communicability: Informatics must be able to communicate their information in a way that the researcher understands.
- Neutrality: Key informants should be objective and neutral. The interviewer should be made aware of any factors that distort the answers.

(Robert G. Burgess, 2003, 155)

The advantage of using key informants is to obtain high-quality information in a brief period of time (Marshall, 1996, 93). However, it is worth remembering that key informants do not always represent a general view of the subject under investigation, or that their views may be biased (Williams, 1967, 28)

Potential key informants were selected together with the client's supervisor and researcher, based on criteria previously described. Interviewees were invited by email, followed by a phone call to arrange a suitable time. The duration of the interview was limited to one hour and the number of themes to four in order not to waste the valuable time of the informants.

It is ethically justified to tell informants beforehand what subject the interview is about. To ensure the success of the interview, it is also an innovative idea to tell them in advance about the themes of the interview (Tuomi & Sarajärvi, 2018, 84). The subject and themes of the interview were communicated to the informants in a leaflet sent as an attachment (Appendix 1.) with the invitation email, so they had time to familiarise themselves with the themes beforehand. The interviews were conducted as online meetings using Microsoft Office 365 Teams software that used both audio and video connections. Interviews were audio-taped, and transcription was purchased from an external service provider.

It is possible to estimate the sufficient size of the material based on saturation. Saturation means that the material begins to repeat itself; informants do not provide new information for solving the research problem. Due to limited resources and schedule, the number of informants interviewed in qualitative theses is generally small compared to quantitative research. The thesis is the work of its author, whose aim is to demonstrate the expertise in his or her field. Therefore, the size of the thesis research data should not be considered as the most significant assessment criterion (Tuomi & Sarajärvi, 2018, 96-99).

The sufficient number of interviewees depends on the purpose of the study. The number of interviewees in qualitative research is typically too small or too large. With a small number of interviewees, statistical generalizations cannot be made while a large number of interviewees it is difficult to make in-depth interpretations.(Kvale, 1996, 102).

A typical feature of a key informant interview is that the interview framework is individually tailored to the purpose of the interview, the topic, and the interviewees. The purpose of the interview is to deepen information obtained and to seek justification for the opinions expressed. Therefore, a semi-structured interview approach is appropriate, practical, and useful for this study.

The interview protocol was designed so that at the beginning the researcher formally introduced himself to the participant and briefly explained the nature of the study. In this introduction, the researcher also revealed his personal interest in research and research background. The participants were presented with a participant information form and asked for their consent to discuss the topic with the researcher and for permission to record and transcribe the conversation. The participants were told that the research was confidential, and that the information obtained from the interviews will not be presented in the research in a way that could identify the participants. Information was also provided on the handling of the survey data during and after the survey. Informants were given the contact details of the researcher and encouraged to contact him if they had any questions after the interview.

At the beginning of the interview, the researcher told the interviewees the first theme of the interview and the participants were free to deviate from it. The interviewer intervened in the discussion only to clarify things or present a new theme.

2.5 Analysis method

The analysis method of is used to find a solution to the research problem or answers to research questions from the research data. The analysis method is linked to the research approach and data collection methods (Kananen, 2017, 68).

Qualitative research typically proceeds in such a way that data collection and analysis alternate. After analysis, new data is collected and analysed. Since in qualitative research it is not possible to know in advance what data will be needed and how much, there may be several cycles of data collection and analysis in succession (Kananen, 2017, 131).

One of the most commonly used methods of analysis in qualitative research is thematic analysis (Howitt & Cramer, 2017, 396). As a useful and flexible research tool, thematic analysis can provide detailed and rich information about the subject of research (Braun & Clarke, 2006, 80).

The basic task of the thematic data analysis method is to simplify and organize the complexity of data into manageable and meaningful themes, categories, and codes (Peel, 2020, 7).

There is no standardised or generally accepted method for conducting the thematic analysis. For example, there are differences in the way different researchers conduct thematic analysis (Howitt & Cramer, 2017, 397-398).

Regardless of the data analysis method used, it is important that researchers describe the processes they use so that others can transparently follow the logic of the study (Duran et al., 2006, 37-38). If it is not known how the researcher has analysed the data or what assumptions the analysis has been based on, it is difficult to compare the study with other studies in the same topic (Attride-Stirling, 2001, 402).

Thematic analysis can be a realistic or essentialist method that describes the meanings and experiences of the participants' reality. It may also be a constructionist method, which looks at the ways in which events, experiences, meanings, realities, and so on are influenced by different discourses in society. Thematic analysis involves decisions that the researcher must make before data collection or at the latest during the analysis, which must be taken into account and discussed. A theme is a data set or patterned answer that contains important information related to a research question. The theme may appear in data among several cases, but it does not necessarily mean that the theme is more important than others. Moreover, the importance of a theme does not necessarily depend on a quantifiable measure, but rather on whether it highlights something important for the whole research question. Themes as a whole may capture an important element for research. The flexibility of thematic analysis is represented by the fact that themes can be defined in a number of different ways. It is important that the definition of themes is consistent throughout the analysis (Braun & Clarke, 2006, 82-83).

The researcher should determine the type of analysis to be performed, as well as the claims to be made from the data set to be used. Whether to provide a comprehensive thematic description of the entire data set to give the reader an insight into dominant or important themes. In this case, some depth and complexity are lost, but a rich overall image is maintained. Alternatively, the analysis can focus on a single theme or group of themes and provide a more detailed and nuanced explanation. (Braun & Clarke, 2006, 82-83).

The identification of themes for thematic analysis can be done inductively or by a bottom-up method. The themes identified in the inductive approach are strongly related to the data. No attempt is made to fit the data to be encoded into the set of analytical preconceptions of the researcher or an existing coding framework (Patton, 2015, 161-162).

The theoretical type of thematic analysis provides a comprehensive analysis of the data from a particular perspective but is less comprehensive in terms of the whole. The analysis would usually be based on the researcher's theoretical or analytical interest in the area and is therefore more clearly analysis driven (Braun & Clarke, 2006, 84).

The identification of themes can take place on a semantic or explicit level as well as on a latent or interpretive level. Thematic analysis usually focuses on one level. The semantic approach involves recognizing themes in their explicit meaning, and no other meanings are sought in the background of the participant’s sayings or writings. Semantic analysis of the latent level begins to explore and identify underlying ideologies, assumptions, concepts, and ideas to shape and enrich semantic content. Latent thematic analysis involves interpretation work, in which case the end result is not only a description, but also a theory (Attride-Stirling, 2001, 84).

The epistemology of research controls what can be told from the material and how meanings are theorised. The result and focus of the thematic analysis differ depending on whether it is carried out with realistic/essentialist or constructed paradigm. An essentialist/realistic approach can theorize meaning, experience and motivation in a straightforward way, since a simple, largely one-way relationship is assumed between experience, language and meaning. in contrast, from a structural perspective, meaning and experience are produced and reproduced socially rather than inherited within individuals. Thematic analysis in a constructionist context does not focus on individual psychology or motivation but seeks to theorise structural conditions and socio-cultural contexts (Braun & Clarke, 2006, 85).

The recordings of the interviews were transcribed, i.e., converted into written form, so that they can be processed manually or programmatically by various analysis methods. The transcription convention used general language transcription, in which the text has been modified to the literary language, eliminating dialect and colloquial expressions. transcription is part of the analysis phase where the researcher becomes familiar with the data collected. (Howitt & Cramer, 2017, 369)

Despite the fact that a transcription made by the researcher himself would have been an advantage in terms of familiarising himself with the material, the transcription was purchased from an external service provider due to time constraints.

The analysis of data collected by interviews and then transcribed was carried out according to the steps presented in Table 1. (Braun & Clarke, 2006, 87).

Table 1 Phases of typical thematic analysis

Phase		**Description of the process**
I.	Familiarisation with the data:	Transcribing, reading, and re-reading the information collected, taking notes. Preliminary ideas.
II.	Creating first codes:	Coding the interesting things in the data systematically from the whole data set and collecting the information related to each code.
III.	Finding themes	Compiling the codes into possible themes and collecting all the information related to each possible theme.
IV.	Review of themes	Checking whether the themes are working in relation to the coded extracts and the data as a whole and creating a thematic "map" of the analysis.
V.	Naming and defining themes	Ongoing analysis to refine the overall story and details told by the analysis of each theme and to create clear names and definitions for each theme.
VI.	Writing a report	One last opportunity for analysis. Selection of convincing and vivid extracts, final analysis of the selected extracts, linking the analysis to the research question and the literature, writing a scientific report on the analysis.

The phases of the thematic analysis of the research data are described below:

Phase 1. Familiarizing with data

The first step was to familiarize with the collected data, by reading it through several times and while at the same time trying to understand their depth and scope. An attempt was made to read the entire data set in an active way, looking for purposes and patterns in the data. During the reading, notes were taken, and possible coding ideas were recorded.

Phase 2. Creating first codes

Coding is part of the analysis (Miles & Huberman, 1994, 56). In coding, the data set is arranged into appropriate groups (Tuckett, 2005, 77-78). Initial codes are formed from the data set. The initial codes are of interest to the researcher or are considered relevant to the phenomenon. The codes describe the properties of the data (semantic or latent content) (Braun & Clarke, 2006, 88).

The researcher can conclude that the data analysis is complete when he is satisfied with the results of the analysis and can provide evidence that his interpretation comprehensively and significantly describes the analysed data in the sense of problem formulation (Duran et al., 2006, 38)

The entire dataset was reviewed, identifying interesting aspects that can form the basis for repeating patterns (themes). Full and equal attention was paid to the entire material. All actual data extracts were encoded and aggregated within each code. As it was not certain which themes / patterns were interesting, an attempt was made to code as many as possible. If necessary, the encoding took into account the surrounding data in order to maintain a connection to the context.
The phase is complete when all the data is encoded, sorted, resulting in a code list for the entire dataset.

Phase 3. Finding themes

In this phase, the analysis is focused on themes instead of codes. The codes are sorted, and the associated data extracts are compiled into identified themes. the relationships between different levels of codes and themes were sought to be outlined. Some codes became main themes while others formed sub themes or were rejected. Some of the codes did not fit into any existing theme, but temporary themes were created for them. At the end of the phase, a collection of candidates for themes and sub-themes and related coded information extracts were available. The meanings of individual themes began to emerge at this point. Not a single theme was rejected at this stage, as in the next step they will be examined in detail and may be that themes are merged, separated, or destroyed (Braun & Clarke, 200690-91).

Phase 4. Review of themes

In phase 4, there are two levels where previously formed themes are considered and refined. At the beginning, all data extracts composed of themes were read and considered whether them form a coherent pattern. If the themes did not fit the intended model, it was considered whether the problem was in the theme, or if some of the information contained in it did not fit the theme. To solve the problem, the theme could be modified, the code could be placed in another theme, or a completely new theme might be created. The theme may also have been rejected. During the phase, themes were identified that were merged into one and themes that were not desired themes. The next step was to assess whether the individual themes were valid in relation to the whole dataset, as well as whether it reflects the meanings associated with the whole data set. The themes were also encoded with additional information that had been ignored at previous stages. As a principle, when evaluating the themes, it was used that the information within the themes can be combined meaningfully, while there should be clear and identifiable differences between the themes. If the resulting thematic map seemed to work, it was possible to move on to phase 5. If the map did not fit in the data set, it was necessary to return to modifying the codes until the thematic map was satisfactory. At this point, it is also possible to identify new themes that were coded. At the end of the phase, the data collected formed a thematic map (Braun & Clarke, 200690-91).

Phase 5. Naming and defining themes

At this point, the essentials of each theme were identified, and the information contained in them was analysed. Extracts from the themes were reviewed and organized into coherent narratives. The themes were not only formulated but sought to identify what is interesting about them and why. A detailed analysis of each theme was written. In this context, it was considered how it fits into a broader general question and how to answer the research question. The aim was to identify sub-themes from themes that can be used to form complex theme structures and a hierarchy of meanings. At the end of Phase 5, the goal is to be aware of what themes are used in writing a report and what not. A rule may be used to test the readiness of a theme that the content and scope of a theme should be descriptive in a single sentence. If this does not happen, the theme needs to be further refined. The themes were also given short, descriptive, and striking names to be used in the final analysis (Braun & Clarke, 2006, 90-91).

At the end of the phase, all the necessary themes are known that are required to write the final analysis

Phase 6. Writing a report

Using the themes created in the previous created in previous phases are used to write a report that describes the data collected and contains an analytical report that answers the research question with justification (Braun & Clarke, 200690-91).

A qualitative research tool called MAXQDA was used for the thematic analysis. Transcripts and interview recordings were uploaded to the program. These were used to carry out the coding and analysis according to the steps described above.

2.6 Reliability assurance and ethics

Theses written in higher education institutions must meet scientific criteria (Kananen, 2015, 119). The aim of science is to produce new scientifically validated knowledge (Kuula, 2011, 15).

By its very nature, research is prone to unconscious or conscious errors caused by the researcher or the data. The purpose of the reliability assessment of the study is to reduce errors (Kananen, 2015, 338).

The researcher must demonstrate to the reader that the report can be trusted. This is achieved by providing evidence and analysis supporting the claims described. The requirement can be met by different methods, such as triangulation, analysing data using different methods or comparing evidence from different sources. If the evidence does not support each other, it is worth noting the differences (Duran et al., 2006, 38).

According to Aaltonen and Puusa (2020, 194), reliability means the independence of research results from random and irrelevant factors.

Reliability and validity are used as indicators for assessing the reliability of the study. Reliability means whether the phenomenon is reliably investigated with the chosen measures so that the results are not influenced by factors outside the measurement, and validity assesses whether the phenomenon is investigated exactly as it was promised to be investigated (Kananen, 2017, 81).

In the case of qualitative research, it is often argued that it is difficult to assess the quality and reliability of the research using the concepts of validity and reliability. (Tuomi ja Sarajärvi, 2018, 162).

However, the concepts of reliability and validity can also be applied in qualitative research, as long as it is understood that the nature of qualitative research and the meaning of the concepts are different from quantitative research. In qualitative research, validity means, for example, the integrity of the research subject. Reliability can be increased so that two researchers using different parallel research methods get the same result, or two different rounds of research on the same subject get the same result. When considering reliability, it should be noted that qualitative research is context-dependent and it cannot be assumed that the findings of two different researchers are completely identical (Aaltonen ja Puusa, 2020, 195-196).

Good and reliable research practice requires that the research sets out criteria against which the reliability of the research can be assessed. The reliability of a qualitative study cannot be expressed as an assessment of a quantitative or objective measure but must be examined within the framework of the study in question, taking into account, for example, the type of qualitative methods used in the research. The research report must convince the reader of the accuracy of the interpretations and thus the reliability of the research results (Aaltonen ja Puusa, 2020, 104).

In order for the results of scientific research to be credible and ethically acceptable, the research must be carried out in accordance with scientific practice. The research followed the key principles of scientific practice set out by The Finnish National Board on Research Integrity TENK, which applied to the research conducted.:

1. Observing practices recognised by the scientific community, such as general diligence, accuracy, and integrity in the conduct of research, in the recording and presentation of results, and in the evaluation of research and its results.
2. Research is carried out using research, data collection and evaluation methods that are ethically sustainable and comply with the criteria of

scientific research. The results of the research will be published with the transparency and accountability that is inherent in scientific knowledge.

3. Research takes appropriate and respectful account of the work and achievements of other researchers.
4. The design, implementation, reporting and storage of the resulting data take into account the requirements for scientific knowledge.
5. The rights, principles, responsibilities, and obligations of authorship are explained to the people interviewed in the study. They will also be informed about how the collected data will be stored and the rights of access to it.
6. Relevant affiliations and sources of funding will be disclosed to the participants and reported in the results.
7. The researcher will refrain from making decisions and evaluations related to the research in which he/she considers him/herself to be unfit to act.

(Launis, Helin, Kaisa & Jäppinen, 2012).

3 Theoretical basis

The theoretical part of the study presents the relevant theories and previous studies related to the research problem. In the theoretical part, the researcher explains what is known so far about the topic and the research problem (Kananen, 2017, 72).

3.1 Quantum mechanics

Heisenberg's article "Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen", published in 1925, is considered the beginning of quantum mechanics. The article is considered the beginning of the formation of the laws of quantum mechanics and a separation from the concepts of classical atomic physics, which could not describe molecules or atoms (Heisenberg, 1925, 382-396).

Quantum Mechanics is a physics theory that describes the behaviour of matter at the macroscopic, atomic, and subatomic scale. Quantum mechanics can be used to determine the properties of physical systems such as light, molecules, atoms, or materials in a condensed phase. Quantum phenomena are such that classical physics cannot explain. Particle in classical mechanics means a part of a substance, a point-formed, permanent grain. In a quantum world, a particle describes an object like a photon or an electron (Band & Avishai,2013, 1-2).

Quantum mechanics involves properties that are difficult to understand by common sense. In his book The Fabric of Reality, David Deutch (Deutsch, 1998, 150) describes the reality of the quantum world, which cannot be explained by current knowledge" When Shor's algorithm factored a number using about 10 500 times more computational resources than what can be seen or proven in the classical sense, where was the number factored? If the scale of physical reality were the visible universe, nowhere near all the resources needed to factor such a large number would fit into physical reality. Where and how would the calculation be performed and who would factor the number? The many-worlds Interpretation discussed in the following chapters also pushes the limits of human understanding.

Understanding quantum mechanics provides the basis for understanding quantum computing. The following chapters discuss the properties of quantum mechanics that can be used in quantum computing and quantum computers.

3.1.1 Quantum properties

The following chapters discuss some of the most common quantum particles or properties associated with quantum mechanical events.

3.1.1.1 Quantum particles

The matter of the universe is made up of 12 quantum particles called elementals. The elementals are also known as fundamental particles. Quantum fundamental particles are: electron, muon, tau, electron neutrino, muon neutrino, tau-neutrino, down quark, bottom quark, top quark, up quark, strange quark and charm quark. What they have in common is that they cannot be broken down into whole smaller particles. At the quantum level, fundamental particles form subatomic particles such as neutrons or protons. Similarly, subatomic particles - protons, electrons, and neutrons - form atoms, which in turn form molecules and elements, etc. Each quantum fundamental particle has a property charge, mass, and spin (Grimes, 2019, 19).

3.1.1.2 Spin (Electron)

All particles like electrons, protons and neutrons have a quantum property called spin. The quantum property was named spin because the magnetic field of the particle was initially thought to be due to its rotation around its axis. Later it was discovered that the phenomenon was not due to rotation, but the name was still preserved. Spin represents a magnetic dipole on each particle, which is like a small magnet. When the spin direction is observed, it can point in two directions and thus represent the different states of the qubit. The spin direction can be influenced by electricity, as well as by magnetic optical fields. (Grimes, 2019, 19-20)

3.1.1.3 Charge

Charge refers to the property of an elementary particle, how strongly it interacts with an electric field. The charge is represented as a multiplication of the elementary charge E, in which case, for example, the charge of the electron is negative -1e. For example, the charge of the up quark is two-thirds of the charge of the electron, and the charge of the down quark is negative one-third of the charge of the electron. Since a proton consists of two up quarks and one down quarks, its charge is the sum of these (2/3 + 2/3 — 1/3) = 1 which is equal but opposite direction than the electron. (Grimes, 2019, 19-20).

3.1.1.4 Photons

Light is formed by particles called photons whose properties are energy and momentum. According to quantum theory, light has properties of both particle and electromagnetic waveform. Polarization refers to the dependence of the direction of the amplitude of the light oscillations in a plane perpendicular to the direction of propagation. The electron field of photons of ordinary non-polarizing light oscillates randomly in all directions in a plane perpendicular to the direction of propagation of the photon. The wave motion of photons of fully polarized light occurs only in one direction in a plane perpendicular to the direction of propagation of the wave. Polarization of Photons can be influenced by polarizing filters. The direction of polarization of the photon can be used to describe the different states of the qubit (Hidary, 2019, 4).

3.1.1.5 Ions

Each stable atom contains an equal number of charge negative neutrons as well as positive protons. Such an atom has no net reservation in either direction. Ions are atomic particles with a total net charge - in other words, atoms with an unbalanced number of electrons and protons. Depending on the electron-proton imbalance, Ion is either positively or negatively charged. Quantum computers form ions by heating an atom located in vacuum to a very high temperature using a laser. Next, superheated atoms are fired with electrons, which leads to the atom losing an electron and the net charge of the atom becomes positive. The atoms typically used in quantum computers are calcium and ytterbium (Grimes, 2019, 51).

3.1.2 Special properties of quantum mechanical objects

The following chapters describe some special properties and principles of quantum mechanical objects that are useful in quantum computing.

3.1.2.1 Uncertainty principle

According to Heisenberg's uncertainty principle, the more accurately the position of a quantum particle is measured, the less accurately its amount of motion can be known, and vice versa. According to the uncertainty principle, it is impossible to accurately measure the values of certain pairs of characteristics of a particle. The principle also applies to other conjugate pairs such as time and energy. However, it is not possible to generalize the principle for all quantum properties: for some pairs of characteristics, it is possible to measure the values of both properties without problems. The uncertainty principle only matters when looking at small objects such as atoms or parts thereof (Grimes, 2019, 17)..

For example, it can be noted that the more accurately the speed of an electron is known, the less you know its place at the same time. Similarly, if the energy of particle is measured, it is impossible to tell exactly at what time of measure the energy was equal to the measured value (Sutor, 2019, 141).

The uncertainty principle is not due to the inaccuracy of the measuring instruments. No matter how accurate the measuring apparatus is, if the first value of the connected quantum characteristic pair is measured, it is simply impossible to accurately measure the second value (Grimes, 2019, 17).

3.1.2.2 Superposition

Superposition is a key feature of quantum mechanics, according to which a particle can be in all possible states until its state is observed, giving only one response. As a real world example, one can think of a lamp switch which is switched on and off at the same time, until the state is observed by looking at the lamp.

To illustrate the superposition, the paradox of Ervin Shrödinger's Quantum cat is often used. The description presented by Schrodinger goes as follows: In the opaque box is located a cat, a bottle of fast-acting poison, radioactive substance, as well as a Geiger meter. The Geiger meter detects a potential degradation reaction in the radioactive material. The poison bottle is connected to the Geiger meter so that when the meter reacts, the poison bottle breaks down and the cat dies. The degradation of a radioactive atom, which occurs randomly, is a quantum phenomenon. The idea of the example is that the cat is alive or dead at the same time until we open the box and check it out. There is only a probability that the cat will survive or die. The example is often misinterpreted by stating that the cat has already died before opening the box. The quantum world works so that the cat is at the same time perfectly alive and completely dead until exactly the moment the box is opened, the cat dies or continues to live. (Grimes, 2019, 20-22)

Superposition can be described by the polarisation of light. The polarisation can be selected with a polarising filter in which case one of the two states of the qubit is described by vertical polarisation and it can be denoted by $| \uparrow\rangle\ or$ and the other by horizontal polarization which can be denoted by $|\rightarrow\rangle$. A polarizing filter is used to select vertical polarization and then a second filter is placed orthogonally to the first filter. In this case, no light can pass through the second filter because the horizontal $|\rightarrow\rangle$ is orthogonal to the first filter. In this case, no horizontal polarization comes through from the first vertical filter. Now the second filter is rotated at a 45° diagonal angle to the first filter. Some light passes through this filter because the vertical polarization can be expressed by the superposition of the diagonal components. One 45° diagonal state,$|\nearrow\rangle$, which can be equivalently described as a superposition of vertical polarization states, passes through the second filter. Since the state $|\nearrow\rangle$ is only one of the terms in the superposition, only part of the light passes through the second filter(Hidary, 2019, 4-5).

In another example, the qubit state can describe the spin of an electron, which has two states understood as spin-down and spin-up. The classic bit is in one of two states at a given time. The qubits of a quantum mechanical system can simultaneously exist in a coherent superposition of both levels or states of the system. This property shows that the computational potential of a quantum system is greater and is therefore one of the essential properties of quantum mechanics (Swan et al., 2020, 48)

If the qubit starts in state 0-0-0 the superposition is in states 1-0-0, 1-0-1 and 1-1-1. The quantum states of a qubit in superposition can have weights in all possible classical states simultaneously. Performing the various steps of the quantum algorithm mixes the states into even more complex superpositions. In the next step, each of the three components of an example superposition states divides into several states. Compared quantum states to classical states, they have much more depth and richness. This can allow faster problem solving compared to a classical computer (Swan et al., 2020, 49).

3.1.2.3 Observer effect

According to the Observer effect, observing the state of the quantum system changes it, so that the state in the Superposition collapses into one final classical state. It is undeniably proven that the observer effect exists, but it is not known for sure why it happens. It is assumed that a measurement operation affects the system in some way, thus reducing the number of probable answers to one. It is generally impossible to observe the state of the system without affecting the target particle of observation in any way. As an example, the detection of an electron requires it to interact with the photon, thereby changing the trajectory of the electron. Similarly, to measure a photon, it must collide with the sensor from which it bounces forward (Grimes, 2019, 21-23)

According to Copenhagen interpretation, when measuring the collapse of a quantum wave function, it decays from many probable possibilities to a single final state. So, measuring the quantum state of a superposition collapses all possible simultaneous states into one final answer. The observation that creates the resulting collapse is interference (Grimes, 2019, 22).

3.1.2.4 Quantum tunnelling

Quantum tunnelling or electron tunnelling, a phenomenon where a particle passes through an obstacle that in the classical sense cannot be exceeded. According to quantum mechanics, there is a possibility that a particle passes through an obstacle even though its kinetic energy is less than the potential energy of the obstacle. The phenomenon is explained by the Heisenberg principle of uncertainty (Grimes, 2019, 21-23).

3.1.2.5 Wave function collapse,

The double-slit experiment was first conducted by Thomas Young in 1801 by using light. Since then, the experiment has been repeated several times, for example, in 1961 with electron beams and 1974 atoms. In the experiment, a light source, such as a laser, is used to transmit a beam of light towards the background. Between the laser and the background is an opaque plate with a thin vertical slit through which light can pass. When a beam of light is directed through the slit, it hits directly to the background. This observation supports the particle property of light. When the plate is replaced with plate containing two parallel narrow vertical slits, it is observed that the photon forms an interference pattern on the shadow, consisting of darker and light points. The pattern is explained as an interference, that is, the interaction of light waves. Light passes through both slits of the plate, dividing into two waveforms, whose interaction alternately reinforces and alternately weakens the pattern drawn on the back plate. This observation supports the waveform of light. When a sensor is inserted into the second slot to detect which slot the photon passes, it is observed that the interference pattern disappears, i.e. the wave function collapses. In other words, the light behaves same as if there is only one slit in the plate located between the light source and the background (Grimes, 2019, 11).

3.1.2.6 Many-worlds Interpretation

When the system is observed, the universe divides into branches, each of which shows a single value of system. The observer is located in the branch where the measured value is located. According to the theory, each quantum collapse creates a new set of new worlds corresponding to all alternative answers in the probability wave function before the collapse. The end result is an infinite number of parallel universes (Grimes, 2019, 23).

3.1.2.7 No-cloning theorem

On a traditional computer, a copy of its status can be taken during the execution of the program. Due to the observer effect, it is impossible to copy the state of a quantum computer in the middle of an execution without changing the state of its quantum phenomenon. Copying quantum state is possible, but it must be done in an indirect way. The uncloning theory must be taken into account when designing a quantum computer. As a result, error correction, for example, cannot be done as simply as on a classic computer. On the other hand, the clone-free distribution theory is useful in Quantum key distribution (QKD) solutions, where it can be used to detect potential eavesdropping attempts (Grimes, 2019, 23).

3.1.2.8 Entanglement

Entanglement is a natural process that occurs when a quantum particle interacts with another quantum particle. Entanglement refers to the property of two or more quantum particles in which they correlate each other. In the entangled state, particle groups are connected to each other and can interact in such a way that the quantum state of a single particle cannot be described without considering the state of other particles. The above is true even if the particles are located at great distances from each other. (Swan et al., 2020, 69).

As the state of another particle in an entangled state change, the state of another entangled quantum particle also changes immediately at the same time. Such properties include polarization, spin, moment, and charge. The interlacing is preserved even if the particles are moved apart. However, in order to create an entanglement, the particles must be close each other's. The phenomenon occurs when observing the state of a particle: if the state of one particle is known, the other particle is also in the corresponding state. If an attempt is made to change the state of the entangled pair of particles, the entanglement between the particles disappears immediately (Grimes, 2019, 23-25).

3.1.2.9 Decoherence

The quantum system is said to be coherent when its state is genuinely superposition. However, the coherence state is not permanent and without strict isolation of the system from the rest of the world, the quantum particle in the system very quickly interacts with the external factors of the system and begins to entangle with other particles. This is called decoherence. One of the major challenges facing quantum systems is how to avoid premature decoherence before the final measurement can be performed. The quantum system must be kept isolated from the external world so that it cannot influence the operation of the machine. Unwanted connections with the external world cause the unwanted entanglement, resulting in decoherence causing the wave function to collapse and leads to the collapse of the quantum particles in the superposition into the classical state. The quantum state observation instruments are made of quantum particles and must interact with the object being observed. The observation changes the state of the system. We want to keep the decoherence of the system as controlled and as low as possible until we are ready to observe the final result (Grimes, 2019, 25-27).

Decoherence is one of the biggest challenges in implementing increasingly powerful quantum computers (Deutsch, 1998, 152).

3.1.2.10 Probability principle

According to the probability principle, we cannot predict the state of a quantum property before measuring it. We can indicate the answer alternatives and their probabilities based on a predefined mathematical theory, if the test is carried out a sufficient number of times. However, we must wait for the result of the measurement to see what result was actually measured and observed. The state that a quantum property has when measured at a given moment in time is random. In classical physics, the answer can be calculated in advance if all the variables involved in the experiment and their magnitudes are known. The result measured at the end of the test corresponds to the answer calculated beforehand. In quantum mechanics, the exact position of a quantum property such as an electron in orbit can only be described by probabilities. When measuring the state of a particular quantum property, the result is in wider ranges than the probability estimates for any single measurement. The randomness of a state or response is not a coincidence but a natural and fundamental feature of quantum mechanics. Although we cannot know the specific answer, we do know the possible range of measurement responses. When we know the probability of a given quantum state of a discrete quantum system, we can describe it with a mathematical formula called the wave function. Wave functions are used to predict and describe what will happen over a wide range of probabilities for a given quantum property or interaction (Grimes, 2019, 16).

For a more practical calculation, amplitudes can be converted into probabilities, where the probability is the square of the absolute value of the amplitude (Swan et al., 2020, 69).

Even if the particles in quantum mechanics and their interactions are well known, the response of a particular measurement is not known, but the range of probable responses is known, and the probabilities of possible responses can be predicted. The wave function is a complete map of a quantum particle. It can be used to describe mathematically all the information about a quantum object, including all its associated properties, what values these properties may have and the probability of their occurrence at the time of measurement. The wave function can be used to predict what will happen if different interactions occur between particles. The answer given by the quantum calculation may not necessarily be correct. Quantum answers are correct answers only under a given probability scenario. To obtain the correct answer, the quantum operation is repeated until there is sufficient statistical confidence to determine the correct answer (Grimes, 2019, 16).

Grimes (Grimes, 2019, 16) demonstrate this with an example of a weighted dice. One side of the dice is weighted so that the dice end up on that side more often than the others. The dice roller does not know which side is weighted. A single roll of the dice can result in any answer. When the rolls are repeated a sufficient number of times, the dice weighting state starts to appear in the final states more often than the other states. The probability of a quantum computer's answers is based on a similar phenomenon, where a measurement must be repeated a certain number of times to get the right result. When only one measurement is made, there is a chance that the answer is wrong.

3.1.3 Quantum supremacy

Quantum supremacy refers to the moment in time when a quantum computer can solve problems that a classical computer cannot logically solve (Preskill, 2012). Quantum advantage is the term used to describe the superiority of a quantum computer compared to classical computers. In this case, a quantum computer is only used because it can solve a problem much faster than a classical computer, regardless of its other properties (Manin, 1980). Google says it achieved quantum supremacy in December 2019, by using a 53 qubit Sycamore quantum processor to perform a computation that sorts a set of random numbers in a way that is estimated to take the best classical supercomputers around 10 000 years to complete (Arute et al., 2019).

3.2 Quantum computing

By definition, a quantum computer is called a device that uses the properties of quantum mechanics to solve problems (Hidary, 2019, 3).

Traditional computers solve problems in a row, one by one. Quantum computer features such as superposition, entanglement and uncertainty to allow a quantum machine to solve all problems that are not possible for classic computers at once (Grimes, 2019, 28).

The classical and quantum system differ significantly from each other as follows:

- A classical system can be in only one state at a time. According to the superposition principle, a quantum system may be in several states at same time.
- The state of the classical world system, consisting of several components, is found out by describing each component and identifying their states. The state of the system of the quantum world, consisting of multiple components, is formed by collecting only the states of some components.

(Mikio & Yoshitaka, 2014, 2)

In the early 1980s, researchers discovered that quantum mechanics offers new opportunities for data processing. Charles Bennett and Gilles Brassard demonstrated how the non-classical features of quantum mechanics allow the creation of a proven secure encryption key. Richard Feynman, Yuri Manin discovered that the entanglement property of particles is associated with a quantum phenomenon that cannot be simulated by the so-called Touring's machine. This arose the idea of whether the phenomenon could be used to speed up the calculation in general. Quantum computing is based on the phenomena of quantum mechanics. A physical system that implements quantum computing is called a quantum computer (Thompson, 2003)

The traditional computer experienced a significant step forward as a result of the invention of the transistor. In a quantum machine, quantum bits, qubits correspond to transistors. Qubits can be implemented in many ways and the methods of execution are based on one of the following four types of quantum particles: photon, electron, atom, and ion. The system used to process quantum data shall meet the following requirements:

1. Shall be initialisable to pure quantum state
2. Ability to control the quantum state of the system
3. Long enough coherence time
4. The quantum state of the system shall be measurable

(Thompson, 2003)

The advantage of a universal quantum computer is that it can be used in various processing scenarios. In general, it can be said that a universal quantum computer combines the functionality of a classic computer with the power of a quantum computer and enables the simulation of quantum mechanics. The disadvantage is that it requires a wide number of qubits. It is also the most challenging to implement (Grimes, 2019, 47).

3.2.1.1 Qubit (Quantum bit)

The fundamental information unit of quantum computing is called a quantum bit or qubit (Sutor, 2019, 303).

A classical computer uses bits with a value of either 0 or 1 to represent binary numbers. The association of values 0 and 1 with the physical state depends on the system used. The states can be related to voltages where 0 volts corresponds to state 0 and 3 volts to state 1. A quantum computer processes information in quantum bits $|\psi\rangle$ also called qubits. Qubits can be formed from either light (photons) or matter (atoms or ions) (Swan et al., 2020, 58).

Qubit takes the value $\mathbb{C}^2$ which is a two-dimensional complex vector. The two states of Qubit are named $|0\rangle$ and $|1\rangle$ according to the Dirac ket notation. (Foot, 2005, 61). In the theoretical discussion, the state of Qubit is described as unit vectors in the vector space $\mathbb{C}^2$ where the basic vectors are described $|0\rangle$ =(1, 0)^t and $|1\rangle$ = (0, 1)^t .

Figure 1. illustrates the differences between classical and quantum bits. On the left side of the figure is the classic bit, which can only have the values 0 and 1. The figure on the right shows all possible states of a qubit as points on a single sphere. $|0\rangle$ is up at the North Pole and $|1\rangle$ is down at the South Pole (Sutor, 2019, 322).

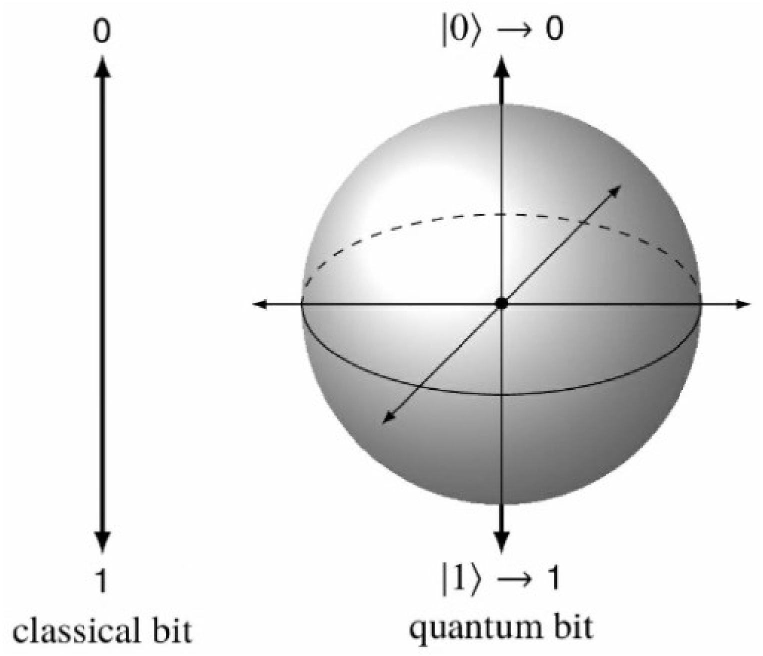


Figure 1: Classical and quantum bits

The association of vectors with physical states depends on the system used in data processing. In a photon-based system $|0\rangle$ describes a vertically polarized photon and $|1\rangle$ horizontally polarized photon. Vectors can represent other directions of polarization such as $|0\rangle$ can correspond to the direction | ⤢$\rangle$=$\frac{1}{\sqrt{2}}(|\updownarrow\rangle + | \leftrightarrow\rangle)$ and $|1\rangle$ correspond | ⤡$\rangle$= $\frac{1}{\sqrt{2}}(|\updownarrow\rangle - | \leftrightarrow\rangle)$. if vectors present the spin-1/2 states of the electron in which case $|0\rangle$ is equivalent to spin down $|m_{s=-1/2}\big)$ or $| \downarrow\rangle$ and $|1\rangle$ is equivalent to spin up $|m_{s=+1/2}\big)$ or $| \uparrow\rangle$.

A qubit in superposition mode can be represented as$|\psi\rangle = a|0\rangle + b|1\rangle with\ |a|^2 + |b|^2 = 1$. When the state of a qubit in a superposition is measured to learn if its state is $|0\rangle$ vai $|1\rangle$, outcome is 0 (1) in probability of $|a|^2$ $|b|^2$.

When measuring, Qubit provides the same amount of information as the classical bit, although it can contain an infinite number of different states. This is because when measured, the state of the qubit collapses into one of the eigenvectors. (Mikio & Yoshitaka, 2014, 17) .

As noted above, a qubit is a quantum information bit with two possible states. Because of its two states, qubits correspond to the current data infrastructure based on classical bits. There are also other types of quantum information bits with more states. Qutrits have three states, and ququats have four states. Quantum atoms are artificially made atoms that can be assigned an arbitrary number of states. The reason for using different quantum data unit formats is that because they have more states, they may be more efficient in all operations. (Swan et al., 2020, 320).

3.2.1.2 A quantum logic gate

The qubits of a quantum computer store information, which can be manipulated by logic circuits called gates (Mikio & Yoshitaka, 2014, 19)

A classical computer performs computations by passing bits through ports on logic circuits. A quantum computer also uses gates in quantum computing to transform the information contained in qubits into the wanted format. The qubits are converted by routing them through the gates of the logic circuit to solve the required computation. The superposition of qubits in the quantum system is also realized when using quantum logic gates. The qubit is in superposition as it passes through the quantum logic gates until it collapses to a classical value of 1 or 0 when measured. In the classical system, the states of the bits can be monitored at different phases of the computation, which is not possible in a quantum information system. The state of a quantum system is represented by a vector and quantum gates are matrices. In port operations, matrices are multiplied by a vector to move the vector in 3D space. The efficiency of quantum computing compared to classical systems is based on the exponential space of quantum states (Swan et al., 2020, 217).

The size of the vector describing the state of a quantum system is 2n for an n-qubit system. For example, in a 9-qubit system, the vector size is 512. At the start of the calculation, this 512-digit output vector is initialized to an output value, where typically all elements of the vector are initialized to zero. The calculation is started by applying each port to qubits and updating the vector with the output values of each port. Once the calculation is complete, the values of the vector are measured and the results are converted to classical values of 1 and 0. The classical result can be further processed by a classical computer (Swan et al., 2020, 217-218).

The three basic ports used in quantum computing are described below:

- The CNOT or controlled NOT port affects two qubits and can flip bits. CNOT is a 2 qubit IF condition that reverses the destination bit if the control bit is 1.

- The Hadamar gate affects one qubit and places the qubit in a superposition. The qubit is then a vector in Hilbert space, meaning that the vector is the sum of the 0-vector and the 1-vector. In this case, the vector is in all states of 3D space.
- The Toffoli gate is a classic logic gate that affects three or more qubits. Using a port, it is possible to perform the same boolean operations that are possible with ordinary classical ports. These operations are AND, conditional AND, OR, conditional OR, exclusive OR, and NOT

When using the Toffoli port, ancilla qubits may need to be used to perform debugging or operations. At ancilla, qubits use a property of qubit entanglement where the states of a qubit can be mapped to another qubit with which it is entangled. Ancilla qubits are used because it is difficult to measure the state of qubits without collapsing their superposition. Ancilla qubits can be used to process information contained in a qubit without damaging the original qubit (Swan et al., 2020, 218-219)..

Other well-known quantum gates are the Deutsh- Fredkin- and Ising gates (Swan et al., 2020, 219).

3.2.2 Quantum computer types

There are two types of quantum computers, universal and non-universal. The most important difference between the two types is that universal quantum computers can perform any computational task, while non-universal quantum computers can only perform certain limited tasks. (Mavroeidis, Vishi, Zych & Jøsang, 2018, 2).

Universal Quantum computer does not mean a quantum computer implemented with a specific technology, but is a generic term for a quantum computer whose operation is not related to a limited number of use cases. The original idea of a universal Quantum computer was presented by David Deutch from Oxford University in 1985(Pathak, 2013, 21-22). According to Deutch, a universal computer can do the following three things: To act as a Feynman's universal simulator. It can do all the same things that a general-purpose classic computer can do. And last of all, it can benefit from quantum parallelism and do things that a general-purpose classic computer can't do (Brown, 2001, 112).

Another definition of a universal quantum machine is a quantum Turing machine (QTM). QTM is the ultimate abstract quantum machine capable of utilizing all the power of quantum computing. In other words, it is capable of executing any quantum algorithm (Silva, 2018).

3.2.2.1 Nuclear Magnetic Resonance

Nuclear Magnetic Resonance (NMR) equipment was used in the first proof-of-concept implementations of quantum computing. Although NMR platforms are used to test quantum computing, it is unlikely to scale to fault-tolerant quantum computing (Hidary, 2019, 58).

Nuclear magnetic resonance (NMR) is based on the physics principle that atoms have an electric charge and spin that can be controlled by an external magnetic field. NMR uses a similar technique to that used in medical imaging. Nuclear magnetic resonance is one of the first methods used in quantum computing. The challenge of the nuclear magnetic resonance method is its difficult scalability to commercial needs (Swan et al., 2020, 61-62).

In 2001, IBM introduced the first experimental implementation of quantum computing, in which a 7-bit circuit performed the Shor's factorisation algorithm by factoring the number 15 into its prime factors of 3 and 5 (Vandersypen et al., 2001).

3.2.2.2 Neutral Atom

The neutral atom system is implemented by placing four laser beams around an atomic assembly. This is called a Magneto-Optical trap (MOT). The neutral atomic sequence usually uses either Rubidium (Rb) or Cesium (SD) atoms. With the quadruple laser system, the temperature of the atoms can be reduced down to mK degrees. Of these millions of atoms in the container, a small number can be transferred to an addressable array. Qubits based on a neutral quantum system are individually identifiable and addressable. They can keep their status and can be measured. The problem with the system is its poor scalability. On these bases, the system meets the DiVincenso criteria (Hidary, 2019, 49-50)

3.2.2.3 NV Center-in-Diamond

Nitrogen-vacancy (NV) colour centres are promising candidates for qubit implementations because of their atom-like properties, such as the long lifetime of spin quantum states and well-described optical transitions in solid-state devices. Nitrogen Vacancy defect centres are particularly attractive for quantum computing because they produce stable quantum states that can be initialised, measured, and manipulated at room temperature with high accuracy. Of the many types of point defects in the diamond, the NV centre is the most promising and scientifically studied for quantum computing applications. (Haque & Sumaiya, 2017).

Nitrogen-vacancy (NV) center-in-diamond solution two carbon atoms in the diamond lattice are missing. One of the missing carbon atoms is replaced by a nitrogen ion. This results in a system with a paramagnetic failure. The property can be used as a qubit. Qubit status can be read optically and manipulated by microwave fields (Hidary, 2019, 51).

The crystal lattice can be used in the development of quantum devices. Imperfections in the crystal lattice of diamonds can be caused by natural defects or by artificially intentionally added impurities. NV centres are produced by ion implantation techniques in both nanocrystalline and large crystalline single crystal particle nanocrystalline materials. For quantum computation, impurities are artificially added by implanting ions to form nitrogen-vacuum photon centres. The nitrogen vacancy in a diamond crystal is created by removing a carbon atom and replacing it with a nitrogen atom and then removing the adjacent carbon atom to create an empty space. The fault in the crystal lattice created by the nitrogen constant is called the colour centre, which has an unpaired electron. An unpaired electron produces a strong spin that can be manipulated and used as a qubit. The NV centre is very useful because the electron spin of its centres can be tuned by applying and changing electromagnetic radiation, electric field, magnetic field, or a combination of these. Its photoluminescence is also easy to detect. In terms of scalability and manageability, the challenge is posed by the random orientation and location of the grown NV centres in the natural diamond lattice. This affects the coupling of photon-NV centres, which are a requirement for practical applications based on quantum-mechanical theory. (Haque & Sumaiya, 2017).

3.2.2.4 Superconductive quantum machines

The early prototypes of quantum machines were based on superconductivity and are still one of the most common methods of implementation today. The implementation is based on two weakly connected superconductors located in side by side and separated from each other by a thin insulator. A set of even or connected electrons or fermions is passed from one superconductor through the insulation to another superconductor. This is called the Mesoscopic Josepson's junction, and the transition of electrons through the insulation occurs through a quantum tunnel. Superconductive qubits can be divided into three groups: to the charge-, phase- and flux-based qubits (Grimes, 2019, 44).

Superconducting quantum computing has two architectures, quantum annealing and the standard gate model. Of the two architectural models, quantum annealing was developed first, and different models are used to solve different problems. Quantum annealing is designed to solve quadratic unconstrained binary optimization problems (QUBO). QUBO problems concern the minimization of a quadratic polynomials over binary variables and belong to the class of NP-hard optimization problems. The universal gate model is a general-purpose computer whose applications are, as the name implies, general-purpose and not limited to one type of problems (Swan et al., 2020, 54).

Quantum annealing machines

In a quantum annealing machine, the problem is set at the beginning and the natural evolution of quantum states over time is used to solve the problem. During the problem-solving process, the system works in such a way that quantum physics follows its natural evolutionary path, and if all goes well and a final configuration is reached, the result will correspond to a useful answer to the problem (Swan et al., 2020, 54-55) .

Quantum annealing counting is started so that qubits are superposition in a state where each of them has an equal probability of outcome. Next, each qubit is subjected to a temperature-aided and quantum tunnelling annealing process using an external tool called electromagnetic coupler. The tool changes the probability of qubits from an equal state to a non-equal state. After that, quantum states try to switch to the state of the minimum possible energy. The quantum states with the least energy have the greatest probability of being the correct final answer. D-Wave has been using annealing quantum technology on its computers for a long time and managed to manufacture computers with allegedly the highest number of qubits (Grimes, 2019, 45).

Quantum annealing is an energy-based approach, based on the idea of fluctuations of spinning atoms that try to find the lowest energy state of a system. Adiabatic quantum evolution is used to solve optimization problems to find the ground state of the system. Adiabatic means that no heat is transferred into or out of the system. The quantum annealing process is started from the ground state, which is a quantum-mechanical superposition of all possible states of the system, where all states have the same weight. The system then evolves, according to the time-dependent Schrödinger equation, through natural physical evolution to settle into a low-energy state. A computational problem to be solved by a quantum computer is formulated as an energy optimization problem, where a low-energy state signals the answer (Swan et al., 2020, 54-55).

The biggest weakness of Quantum annealing computers is that they are only suitable for solving certain types of quantum problems, so-called optimization problems. Annealing computers cannot be utilized, for example, for equations involving large prime numbers such as the Shor’s equation (Grimes, 2019, 46-47).

Quantum annealing machines have the advantage that because annealing systems are constantly trying to achieve the lowest energy level, they are more resistant to errors compared to the gate model systems and therefore require much less debugging on a larger scale (Swan et al., 2020, 54-55) .

Standard gate model

In the Standard Gate model of a superconducting circuit, the qubits are formed by an electric circuit in which the oscillating current is controlled by electromagnetic fields (Wilhelm et al., 2020, 135).

The use of superconducting circuits in quantum computing was made possible by the discovery of high-temperature superconductors in 1986. (Bednorz & Müller, 1986). High temperature metals can have transition temperatures below 138K (-135°C) and can be cooled by liquid nitrogen. Materials previously known to be superconducting became superconducting when frozen with liquid helium below the critical temperature of 30K (-303°C). (Swan et al., 2020, 53).

The long-term goal is to implement a superconducting circuit that will work at room temperature. In 2015, it was found that hydrogen sulphide exhibits a superconducting transition near 203K (-70°C) when subjected to very high pressures of around 150 gigapascals. (Drozdov, Eremets, Troyan, Ksenofontov & Shylin, 2015).

A study in 2019 gave indications of the superconductivity of lanthanum superhydride at 206K (-13°C). Superconductors operating at near room temperature have only been experimentally demonstrated but are still far from practical implementation because they require special conditions to be produced (Drozdov et al., 2015).

Research on superconducting quantum bits uses superconductors consisting of elemental metals and alloys whose superconductivity is well known. Superconducting substrates used in quantum computing operate at low temperatures. Electric charge in superconducting circuits is carried by Cooper pairs, or elementary charge pairs. Due to superconductivity, the transmission of the elementary units of information is possible without losses, allowing quantum coherence to be maintained (Wilhelm et al., 2020, 135).

The key element in superconducting circuits is the Josephson junction. The feature is named after British physicist Brian David Josephson, who predicted the mathematical tunnelling behaviour of superconducting Cooper pairs in 1962. He was awarded the Nobel Prize in Physics for his work in 1973. This is a weak link between superconductors made of a superconducting material. It is usually implemented as Josephson tunnel crossings in electrical insulators (Josephson, 1962, 251-254).

The electrical resistance of a superconductor is zero when its temperature falls below a certain value. This allows electrons to travel freely through the material without losing energy. When the temperature falls below the critical level, two electrons with the same charge, which normally repel each other, form a weak bond. The bond formed by the electrons is called a Cooper pair. Cooper's pair allows a property known as quantum tunnelling, which means it has no resistance when passing through metal. This feature can be used in quantum computing (Swan et al., 2020, 52).

By its very nature, superconductivity is a reactive (non-energy consuming) element which, unlike the commonly known capacitor and inductor, is classically non-linear. The nonlinearity allows for a non- equidistant energy spectrum, which is essential to selectively use quantum states as computational states of the qubit. In this implementation, the linear inductors of a traditional circuit are replaced by Josephson junctions, a non-linear element that allows the formation of energy levels sufficiently far apart. These energy levels can be used as qubits (Wilhelm et al., 2020, 136).

Josephson Junctions-based superconducting integrated circuits are a solid-state-based quantum bit platform. It is used as a platform for both quantum circuit-based quantum computing and quantum thermal annealing/adiabatic quantum computing. The implementation of qubits is based on either a flex-qubit design or a transmon. Interfaces to other platforms and switching and control are transmitted via microwave transmission lines. Transmission lines transmit electromagnetic fields in the microwave frequency range. Due to the combination of the low operating temperature of the microwave regions and the energy scale, the preparation of the qubit space can be performed by cooling (Wilhelm et al., 2020, 135).

In a superconducting loop-shaped electrical circuit, a current circulates, and a corresponding magnetic field holds the qubit in place. The two different states of the qubit can be created by directing the current in different directions. The superconducting loop acts as a magnetic field measuring device (magnetometer) in a Superconducting Quantum Interference Device (SQUID). The SQUID contains two superconductors separated by thin insulating layers that form two parallel Josephson junctions. The non-linearity of the Josephson inductance breaks the degeneracy of the energy level gap. This allows the dynamics of the system to be restricted to 2-qubit states. Josephson junctions are important for the formation of qubits because without them the superconducting loop would just be a circuit. A Josephson junction is a non-linear element that produces energy levels at different distances from each other and can be used as a qubit (Swan et al., 2020, 52).

Google's quantum computer qubits are electronic oscillators made of aluminium that become superconducting when cooled below1° Kelvin (-272°C). The oscillator is capable of storing a small amount of electrical energy, which is used to present the Qubit states. The oscillator is in state 0 when it has no energy and in state 1 when it has one quantum of energy. The logical states of a qubit are the two states of an oscillator with a quantum energy of 1 or 0. The oscillators have a resonant frequency of 6 gigahertz which is equivalent to 300 millikelvins and sets the energy difference between states 1 and 0. It has high enough frequency to prevent the background thermal energy from interfering with the oscillation and causing errors. On the other hand, the frequency is also so low that the controller electronics can be built from commercial components that are readily available(Swan et al., 2020, 51-52).

The Rigett solution is composed of a single Josephson junction qubit on a sapphire substrate. The substrate is embedded in the cavity of a copper corrugated tube. The waveguide is coupled to the qubit transitions to perform quantum computation (Rigetti et al., 2012).

Implementations based on Josephson Junctions are considered one of the most promising candidates for implementing qubits. It is widely used by commercial and academic actors (Wilhelm et al., 2020, 136).

Typical sources of error in Josephson junction-based implementations are due to the system's concentrated environment and the requirement to manufacture system components, such as Josephson junctions, from heterogeneous materials (Wilhelm et al., 2020, 136).

Compared to implementations of the quantum annealing model, the goal of the Gate model is to allow the evolution of quantum states to be fully manipulated and controlled during computation. This makes it possible to solve more general and bigger problems. Considering the sensitivity of quantum mechanical systems, this is much more difficult than quantum annealing implementations and explains why gate implementations have much lower qubit counts (Swan et al., 2020, 54).

3.2.2.5 Topological Quantum Computer

Topological quantum computers are a relatively new area and their introduced qubit quantities have been quite small. Topological quantum computing aims to process and store information in a secure way using the topological phases of matter. Information encoded in the spatial space of non-Abelian anyons is not subject to local interference and environmental errors and is believed to provide a scalable approach to quantum computing.

Topology refers to a mathematical term describing the transition of the state of an object from one state to another without ruining or tearing the object. Topological quantum qubits are implemented using non-abelian anyons, which are two-dimensional "quasiparticles". A single anyon cannot form a qubit but needs a collection of anyons to do so. Anyons can be induced to produce a three-dimensional quantum braids consisting of a time and two spatial dimensions. Different quantum operations can be formed by moving collections of anyons around each other, and new particles can be created by moving them together. As a result of new particles and transfers, wrapped braid chains are created, which can be compared to a string with knots. The string can be changed or moved, but the quantum information contained in the nodes remains regardless of how the string is manipulated or what external influences interfere with it. A special feature of braids is that they preserve the history of previous quantum states, making it possible to observe how a quantum state has changed over time. Other types of quantum computers do not have a similar feature. Topological qubits have the advantage of being able to maintain coherence for several seconds and are more fault-tolerant than many other implementations. Wrapped anyon braids make it possible to implement hardware-level strong quantum logic gates (Grimes, 2019, 49).

Qubits are made using topological superconducting particles and they are controlled electronically by a computational model based on the "braiding" of their trajectories (Freedman, Kitaev, Lrsen & Wang, 2001).

Topological superconductors are new classes of quantum phases that arise in condensed matter, which is characterised by quantum computational states, i.e. Cooper pairing states. Cooper's pairing modes are a unique class of matter known as Majorana fermions. Topological invariants caused by the symmetry of the systems generate Majorana fermions and make them stable. The name topological superconductors originate from the observation that quantum states appear in the topology of a superconductor at the edge and the core. (Swan et al., 2020, 57)

Majorana Fermions are in a similar method as anyons. Majorana Fermions are created by dividing electrons into two smaller entangled quasi particles. The property also known as electron fractionalization. Quasiparticle’s form topologic qubits that behave similarly to anyons. Majorana fermions have a property where when two particles meet, they can destroy each other. Particles have counterparts (e.g., electrons and neutrons), but typically the same particle type does not act as antiparticles (Grimes, 2019, 50).

As Majorana's fermions are bouncing around, their trajectories remind of a braid made up of multiple strands. Braids are wave functions that are suitable for use in the development of logic gates in computational model. Majorana fermions are assigned to quantum states or modes and occur as particle-antiparticle pairs. The calculation model is based around the concept of a Majorana zero state exchange in a sequential process. The sequentially of the process is important because changing the order of the particle exchange operations also changes the outcome of the calculation. This feature is known as non-abelian, which means that the steps in the process are non-exchangeable with one another. Majorana's zero modes belong to a new class of quantum statistics, known as non-abelian statistics, where particle exchange operations are non-commutative. Majorana null states are modes that indicate a particular state of a quantum object. The mode is related to polarisation, charge, spinning or any other parameter and is a unique and important state of the Majorana fermion system. The advantage of non-abelian quantum statistics of Majorana zero states is the possibility to use them in wavefunction calculations. The sequential behaviour of the particle wave function is important for building efficient logic gates for quantum computation. It is believed that well-separated Majorana null spaces can be used to express non-abelian braid statistics suitable for uniform gate operations in topological quantum computation. (Swan et al., 2020, 57-58).

Majorana fermions are only realised at high magnetic fields close to -272 °C (1 K) temperature. Recently, proposals have been made for more reliable platforms to implement Majorana zero modes (MZM) (Robinson et al., 2019). It is believed that superconducting proximity parity in helical edge modes, such as topological insulators (TI), provides an exceptionally good platform for implementing Majorana zero modes. (Jäck et al., 2019)

Topological computers require error correction and qubit control. Decreasing the temperature and increasing the distance between the particles helps to the error correction. Computers may be more economical because the total number of qubits can be kept lower (Grimes, 2019, 50).

In topological quantum computing, error correction can be implemented directly in hardware, compared to software-based error correction, which is one of its main advantages. The initial error rates of the method are low compared to other qubit implementations (Freedman et al., 2001).

3.2.2.6 Ion Trap Quantum computers

Ion Trap Quantum computers are based on individual ions floating in a vacuum and controlled by slowly varying electric fields. Qubits can be controlled very accurately, and it forms a well isolated quantum system. The Ion Trap technique has been applied in the past in atomic clocks (Wilhelm et al., 2020, 27)

A charged particle located in an electromagnetic field is subject to much stronger forces than a neutral particle (Foot, 2005).

Earnshaw proved that: A charged particle cannot rest in a stable equilibrium due to the interaction of electrostatic forces alone. Because of this, it is not possible to limit the ion using only the electrostatic field (EARNSHAW, 1842).

Figure 2 shows an electric field formed along the Y axis between two equal positive charges at a fixed distance from each other. At point P, halfway between the two charges, a point is formed where the forces cancel each other, and no forces are applied to the ion. It can be noted that point P is the saddle point of the electrostatic potential ϕ. However, since all lines around point P do not align inward, it is not stable. If the ion shifts from the point slightly to the side, its velocity accelerates parallel to the field lines away from the charge. In the case of a negatively charged ion, one of the charges attracts it (Brown, 2001).

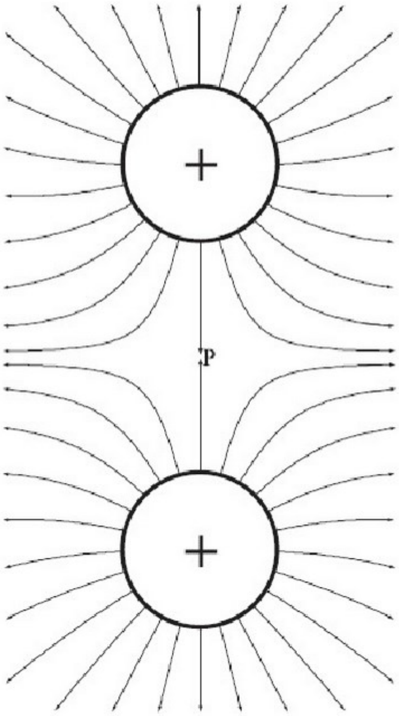


Figure 2. Field lines describing the electric field between two positive charges of equal magnitude.

The electrostatic potential energy of an ion eϕ has the same shape as the gravitational potential energy of a ball set on a saddle-shaped surface. However, the ball tends to spin from the other side off the surface. This is prevented by rotating the plane about a vertical axis at a suitable speed. Figure 3 illustrates how an electron stays on a saddle-shaped rotating surface (Brown, 2001).

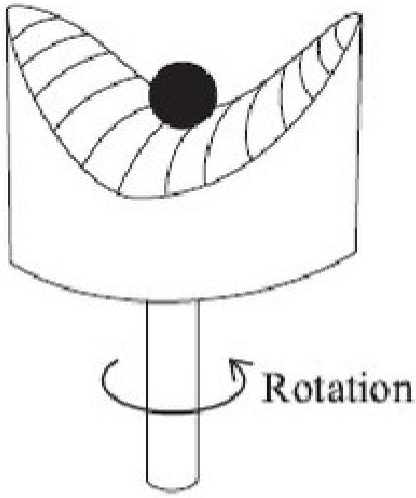


Figure 3. A ball located on a saddle-shaped surface

The rotating saddle-shaped plane has features similar to Paul’s linear trap. The principle of Paul's trap is shown in the Figure 4 (Brown, 2001).

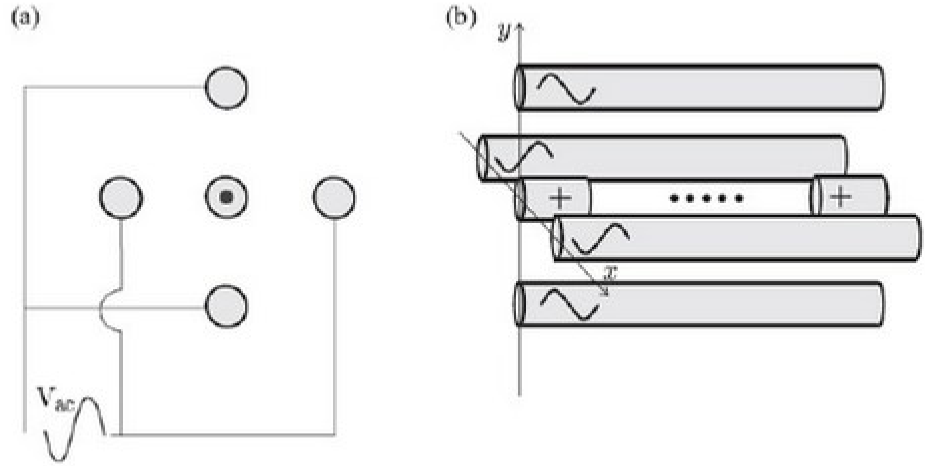


Figure 4. A principal image of Paul's linear trap

The Pauli linear trap consists of four rods parallel to the Z-axis, located at the corners of a square in the XY plane. An AC is applied to the rods, which has different phases in the diagonally opposite rods. There are equal magnitude positive electrodes at both ends of the trap that prevent positive ions from escaping the trap. The ions stored in the trap form a chain (Brown, 2001).

Electromagnetic fields can be used to trap ions of atoms. A typical trap configuration used for quantum computing purposes is called a Paul linear trap. An ionic string in such a trap is controlled by a combination of static and oscillating electric fields. Information contained in qubits is stored as states of electrons in ions. Qubits are consistently manipulated using microwave fields and lasers to control electron state transitions. Ions are completely isolated from the environment: they are locked in a vacuum and are typically located about 30 — 300 µm away from surfaces. (Gerard Higgins, 2019, 19-20)

Wolfgang Paul and Hans Dehmelt received the 1989 Nobel Prizes for their development of the first ion trap at the turn of the 1050s and 1960s (Thompson, 2003, 1).

Two trap types, the Paul radio frequency trap and the Penning trap, were introduced at about the same time. The principle of ion traps is to limit the movement of charged particles by electric and magnetic fields. From the point of view of realizing the trap, it would be ideal to create a static potential well, but the Eanshawn theorem prevents its use. Using static electric fields, it is only possible to create a potential saddle point. In the simplest case, the square potential is created by three electrodes (Thompson, 2003).

Quantum computing requires that there is more than one ion in the trap and in order to operate the system the ions must be cooled to their lowest vibrational level (Foot, 2005).

Ion qubits can be prepared, manipulated and read-out with great certainty. Entanglement operations between qubits can be performed with a small number of errors. Quantum data is stored in loosely bound external electrons whose states can be manipulated by laser or microwave magnetic fields. Ions can be trapped in chains of mutually repelling objects and can interact through vibrations. One-dimensional traps can communicate optically (Wilhelm et al., 2020, 27).

Ignacio Cirac and Peter Zoller found in 1995 that Ions can be used to implement qubits and ion lock the movement of bounded ion queues (string) can be exploited as logic gates between them. Trapped Ions can be cooled by laser to close to the lowest energy state (ground state) located near absolute zero point. When an ion band is kicked from one end, the motion proceeds through the entire strip and back as if the ions were a band of pearls. The movement of ions must be considered a collective motion, which can be described by normal states. Cirac and Zoller found that collective movement can be used to transfer information between qubits (National Academy of Engineering, 2003, 98)

The state of the ion qubit can be detected by tuning it with laser light. If the qubit is in state |↓, laser light scatters from the ion and is detectable with either a CCD camera or photomultiplier tube. If the qubit is in |↑ state, ion does not couple with laser light and neither does emit fluerizing photons. (Thompson, 2003)

When processing quantum information, the information contained in each ion corresponds to one qubit of information in the superposition of two long-lived internal states. The states can be initialized, processed, and read with laser light. The system is scalable using the entanglement. (Thompson, 2003)

Ion trap quantum computers can be implemented for traditional types of silicon chips that operate at room temperature. Ion trap computers coherence times are very long, 10 minutes or longer. Entanglement property is high class, all qubits can be connected to each other (which is not possible in my qubits implementation ways). The measurement results are very accurate compared to other quantum technologies. The difficulty is to increase the number of Ion traps so that individual control and measurement accuracy are maintained at the same time. Data transfer with ions is slow because the typical mass of an ion is 10^5 compared to electrons (National Academy of Engineering, 2003)

3.2.2.7 Quantum photonics

In quantum photonics, the technique uses single photons or compressed light states to represent qubits. In the computational model, they are controlled in cluster states, which are entangled states of multiple photons. For photon quantum computation, a cluster space of entangled photons needs to be formed. A cluster space is called a resource space formed by multidimensional highly entangled qubits. Quantum photonics can be implemented in a free space or in a computing circuit. Squeezed states of light or single photons are sent through a free space or chip to be counted and then measured by photon detectors located at one end. A typical process proceeds as follows: first, photons are produced, next they are entangled, then they are counted and finally the result is measured. One way to generate cluster spaces on qubit lattices with a phase transition, the so-called ISing-type interactions. The lattices are well suited to quantum photon computing. The cluster state is presented as a vector space, where the underlying vector is a combined subset of a d-dimensional lattice. Then the vector spaces are instantiated into a calculation schema with directed operations to complete the calculation (Swan et al., 2020, 58).

The higher speed of a quantum computer in comparison to a classical computer is due to superposition, which means that a quantum circuit can process all the inputs to a problem simultaneously. In photonic quantum computing, superposition can be used not only for problem inputs but also for gate processing. This adds even more speed to the quantum computing process. Quantum photonics allows overlapping gates, i.e. the counting is performed when photons pass through overlapping gates.

There is potential benefit gained from the overlapping computation of optical quantum circuits that is linear compared to standard quantum algorithms and exponential compared to classical algorithms (Procopio et al., 2015).

3.2.2.8 Linear Optics Quantum Computing (LOQC)

A gate-based quantum computer can be implemented using Photonics. Optical elements such as beam splitters, mirrors and phase shifters are used to process quantum information. These optical elements maintain the coherence of the input light and thus uniformly transmit a finite number of qubits. However, photons cannot interact with each other in a vacuum, so the interaction must take place indirectly through another carrier (Hidary, 2019, 52-53).

3.2.2.9 Neutral atoms

Unlike ions, which are charged because they have been stripped or have an electron added, neutral atoms are uncharged ordinary atoms that have a balanced number of electrons and protons. Qubits are formed from neutral atoms trapped in optical arrays or optical lattices. Lasers are used to trap neutral atoms in space. The optical lattice is made with laser beams from multiple directions that hold atoms in wells. Qubits are guided in the calculation by a second set of lasers. An alternative method of keeping atoms in an array is to use optical tweezers. Neutral atoms can be held tightly together and can be manipulated in a computation, unlike ions, which repel each other’s (Swan et al., 2020, 59).

3.2.2.10 Quantum dots

In 1997, a theoretical implementation based on quantum dots was proposed, enabling universal and scalable quantum computing that can be controlled by purely electrical methods. Quantum information encoded by the spin states of single electron quantum dots. Quantum dots are nanoparticles of semiconductor materials. They can be used to implement qubits in electron circuits trapped in the nanostructure of semiconductors. They are controlled by electronic pulses in the computation(Loss & DiVincenzo, 1998).

The semiconductor-based structure is manufactured using the same technology as classic processors. Electrostatic fields formed by metal electrons patterned on the semiconductor layer are used to trap individual electrons. Inside the semiconductor nanostructure are tiny silicon chambers that hold the electron in place long enough for it to hybridise its charge and rotate, manipulating the electron orbit interaction for computation (Petta et al., 2005).

Coherence interactions typically last longer in silicon than in other materials but may be difficult to manage (Kloeffel & Loss, 2013).

3.2.2.11 Error correction

One of the major challenges in implementing a general-purpose quantum computer is the implementation of quantum error correction. Qubits are more susceptible to errors than classical bits and errors that do occur must be able to be corrected by error correction (Swan et al., 2020, 64).

Error correction aims to identify whether data is damaged or destroyed. Error correction also allows the data to be restored to its original state (Swan et al., 2020, 76).

There are many outright errors and premature quantum decoherence in current quantum computers. Errors in quantum computing are typically caused by interactions with the world around. Errors can be caused by a range of reasons such as heat, noise, vibration, radiation, qubit structure, faulty gates, incorrect preparation of the initial state (Grimes, 2019, 38-39).

It is not yet possible to build quantum computers with enough qubits to perform perfect error correction. (Hidary, 2019, 196).

Even if it is possible to implement a perfect computing environment without any noise, it is likely that quantum computers will always need some level of error correction. The natural property of qubits to decay must be taken into account when implementing quantum computers. The excited state of qubits eventually decays to the ground state because it is coupled to the vacuum fluctuation. In order to be robust, qubits must be implemented in such a way that any errors can be corrected. The goal of quantum error correction is to make quantum computing usable so that a quantum computer can tolerate enough noise in the surrounding environment to be able to perform useful computations (Swan et al., 2020, 75-76).

Error correction protects the logical qubit from errors caused by state decay or environmental noise. Error correction is implemented by encoding an entangled logical qubit using several physical auxiliary qubits. The entangled qubits form a larger entity that forms a quantum processor. Error correction leads to a challenge for the scalability of quantum computers. If there is a quantum computer with 50 physical qubits, the error correction uses 9 of them for each logical qubit. This leaves only 5 qubits for data processing. From this we can form an implicit scaling rule 10, where each qubit requires 9 auxiliary qubits for error correction. It can be noted that a quantum computer can then use only one tenth of all available qubits for information processing (Swan et al., 2020, 79)

The need for error correction is different for different types of quantum computers. For certain types of optimization problems, the quantum annealing model utilises the natural evolution of quantum systems over time, where they settle into the lowest energy states (the minimum). The setting of energy states is automatic and cannot be controlled or manipulated. With less manipulation, fewer errors are generated, and with the current number of qubits, there is no need for error correction. Standard-gate model quantum computers aim to manipulate and control the evolution of the state of a quantum system at any given moment of time, meaning that they are also capable of solving more general and much broader problems (Swan et al., 2020, 64).

According to quantum error threshold theory, any quantum system is useful if it can correct errors faster than it creates them. When the number of qubits in a quantum system increases, also the rate of natural error increases. The number of errors can be expressed as the ratio of the quantum action time to the decoherence time. A usable quantum computer is considered to have an error rate of less than 1%. Developers of quantum computers are trying to find solutions to minimise the factors that cause quantum errors. Typical solutions include isolating the quantum components of a quantum computer from the outside world, improving coherence times, subcooling and increasing component performance to outperform errors (Grimes, 2019, 39).

The effect of errors on the final result can be countered by repeating the same calculation several times and storing the results in the classical world. The results are examined when the calculation has been repeated at least three times. If disagreements are identified when examining the results, the results that occur more often than others are taken into account. The method slows down the calculation in direct relation to the number of overlapping operations used. There is also no certainty that the repeated answer is the correct one (Grimes, 2019, 41).

Error correction can be implemented by so-called surface code, in which a single logical qubit is encoded in the space of several physical qubits. When measuring the states of physical qubits, it is possible to observe a pattern known as a syndrome. The syndrome is the consequence of a series of errors (Hidary, 2019, 197).

In error correction, extra qubits can be used as check qubits. Check qubits implement a logical checking method to detect and correct errors. A check qubit can be used to verify that the resulting qubyte sums in a certain way. In this case, the computer sets the check qubit to 0 or 1 so that the sum of all qubits has an even value. If the error check returns an odd value for the sum of the qubits, it is recognized that an error has occurred, and the quantum operation is repeated until the correct result is obtained. The method does not detect if there are multiple errors in the final result so that the checksum returns an even value (Grimes, 2019, 42).

In classical computing, the simplest way to implement error correction is to multiply the state into several classical bits. Classical information can be examined an arbitrary number of times to determine whether it has changed. When there are multiple copies of data, redundancy allows the use of a mechanical majority voting mechanism to identify the error-free version of the data. Quantum state qubits cannot be directly copied because of the observer principle and the no-cloning theorem (Hidary, 2019, 196).

However, indirect copies of qubits can be made by using property called entanglement. The entanglement bonds are fragile and are easily lost when decoherence occurs (Grimes, 2019, 41).

Entanglement can be used to perform quantum error correction. Quantum particles in qubits are not separate or isolated but correlated not only with each other but also with the history of the system. The past states of the system and quantum particles are correlated as part of the information set of the quantum computer.

Entanglement allows to measure the relationships between qubits instead of measuring the values stored in the qubits itself (Swan et al., 2020, 75-76).

The idea of entanglement quantum error correction is to store the information of a single qubit in the entangled state of multiple qubits. In this case, the information stored in a qubit is protected by spreading its information across a larger system of multiple physical qubits. The auxiliary qubits are known as an ancillary or ancilla qubits. The integrity of a qubit can be checked by examining the information it contains through indirectly entangled qubits using parity measurements (Swan et al., 2020, 76).

Shor's code is one of the first quantum error correction codes. In Shor's code, an ancilla requires at least nine qubits to ensure the integrity of the logical qubit. Shor’s code is redundant, which means that the amount of logical qubits it protects is significantly smaller than the amount of physical qubits it uses. It checks different pairwise sequences for possible flips on the X, Y or Z axes of the qubit. Pairwise checks examine whether the first and second qubits contain the same state and also whether the second and third qubits contain the same state. Pairwise checks can be performed in both space and time. If the value of one qubit differs from the other two qubits, it can be corrected by setting it to the same value as the others. However, the checks cannot be used to determine what the value is. Because the original qubit and the ancillary qubits are intertwined, any errors can be identified and corrected. An erroneous qubit can be corrected to the original phase or to an irrelevant phase that does not affect the information in the original qubit. As the states of the system are the eigenstates of all operators whose eigenstate is one, the measurement has no effect on the total state. Shor code is also non-local, which means that the information in a logical qubit travels in an entanglement between several physical qubits, which protects it from local depolarization and decoherence (Swan et al., 2020, 77).

Error checking methods based on repeated computations and ancilla qubits are inefficient because they perform error checking and correction only at the very end. Answers from quantum computing are probabilistic in nature and may therefore return a different answer at each run, regardless of error levels (Grimes, 2019, 42).

Holographic codes are suggested as special quantum error correction codes. The holographic principle is a property that appears in quantum gravity theories, according to which a region of space can be encoded in its lower dimensional boundary (Susskind, 1995).

3.2.3 Concepts related to quantum computing

3.2.3.1 The DiVincenzo criteria

The Divincenzo criteria have been suggested as standards that describe the five elements associated with the implementation of a well-functioning quantum computer.

DiVincenzo's (2000) seven requirements for a quantum computer:

1. scalable physical system of well-characterized qubits
2. The ability to initialize the state of the qubits to a simple fiducial state
3. Long (relative) decoherence times, much longer than the gate-operation time
4. A universal set of quantum gates
5. A qubit-specific measurement capability
6. The ability to interconvert stationary and flying qubits
7. The ability to faithfully transmit flying qubits between specified locations

(771-784)

3.2.3.2 NISQ-devices

Noisy Intermediate-Scale Quantum (NISQ) - devices mean modest-sized, imperfect quantum computing machines (Preskill, 2018, 1).

NISC devices are small systems, a few qubits in size, that are part of the development path. NISQ devices serve as proof of concept. The challenge is to find suitable problems for which existing 50-100 qubit systems without error correction are suitable. Quantum computers smaller than 50 qubits are considered the limit below which the most powerful existing classical supercomputers can simulate. Noise reflects the incompleteness of today's qubits and places serious limitations on what quantum computers will be able to do in the near future (Preskill, 2018, 4-5).

NISQ devices are not suitable for solving computationally difficult problems such as breaking an RSA key with Shor’s factorization algorithm or solving symmetric keys with Grover's algorithm. NISQ devices may have potential applications in the fields of machine learning, cryptography, simulation, or learning (Swan et al., 2020, 71).

NISQ equipment is expected to demonstrate quantum advantage, which refers to the superiority of a quantum computer over a classical computer (Swan et al., 2020, 72).

3.2.3.3 Quantum volume

The number of qubits in noisy intermediate-scale quantum (NISQ) systems currently under development does not necessarily indicate the performance of the system. The performance of individual qubits can be compared using methods such as state and process tomography (Paris & Řeháček, 2004),   gate set tomography (Merkel et al., 2013) or randomized benchmarking (Magesan, Gambetta & Emerson, 2012). These methods do not take into account, for example, errors due to qubit interactions. Measuring the overall performance of a quantum computer requires a concise representation of complex operations. To make it easier to compare quantum computers, a single number metric was implemented to measure the capability and error level of the quantum computer. Determining the quantum volume involves many factors and complex calculations. The definition takes into account, among other things, the number of qubits, error rates and connectivity of qubits. The quantum volume expresses the size of the largest random circuits of equal width and depth that a quantum computer can implement. The architecture of the quantum computer has no influence on the form of the circuit, but the compiler can optimise and adapt it to take advantage of the computer's capabilities. Quantum volume makes it possible to compare the quantum quantities of different architectures (Cross, Bishop, Sheldon, Nation & Gambetta, 2019).

3.3 Public key cryptography

Public key cryptography, also called asymmetric cryptography, is based on the use of key pairs. A key pair consists of a public and a private key. A public key, as the name implies, can be shared publicly, while a private key must be kept only known to its owner (Boyles, 2010).

The public key cryptography method enables authentication, confidentiality, and non-repudiation. Confidentiality is achieved when a public key is used for encryption, which can only be decrypted using a private key. In authentication and non-repudiation, encryption is performed with a private key and can only be decrypted with the public key associated with the private key (Boyles,2010).

3.3.1.1 RSA

RSA (Rivest–Shamir–Adleman) public key encryption method is named after the researchers who developed it, Ron Rivest, Adi Shamir and Leonard Adleman. Researchers published RSA's principle of operation and applied for a patent for it in 1977 (Rivest, 1978, 120-126). Cifford Cocks, who worked for the British Government Communications Headquarters (GCHQ), had invented the same algorithm as early as 1973 but had been classified as secret. The strength of RSA-based cryptography is based on the problem called prime factorization. The problem is based to the fact that it is very difficult to find factors of very large composite number factors, if the factors are prime numbers. Generating large numbers is easy by multiplying the two factors. However, finding two major prime factors for the product of a large number is exponentially difficult (Hidary, 2019, 14).

The security of the RSA algorithm is based on the assumption that decrypting without a cryptographic key being available will take too long in time, even if computing capacity develops in the future (Grobman, 2020, 55).

Suppose Alice wants to send Bob the number K using RSA encryption: In the first step, Bob forms two large primes, denoted by p and q, randomly and independently of each other. The prime numbers generated must be approximately the same length of approximately 300 decimal system numbers, corresponding to 1024 binary numbers. The numbers are used to calculate N = pq which is called modulus. Next, d is chosen such that $d\ e \equiv 1 \pmod{(p-1)(q-1)}$.

Next, Bob looks for a relatively small integer e that has no common factors with previously formed numbers p and q. Bob disposes of numbers p and q. N and d forming a secret key that Bob keeps secret. N and e form the public key that Bob sends to Alice.

Alice raises the number K to the power of e and divides it by N. The remainder is called mod N, which Alice sends to Bob.

Bob is able to factor Alice's original value K using the known factors N and d.

The security of the system is based on the fact that a potential eavesdropper cannot use the value N to form factors p and q. (Bernhardt, 2019a)

The RSA algorithm is the fundamental encryption standard on which most security and network encryption solutions in use today are based (Grobman, 2020, 55)

3.3.1.2 Elliptic Curve

A public key cryptosystem based on elliptic curves was proposed in 1985 by Victor Miller and Neal Koblitz (G. Seroussi, 1999).

TLS 1.2 introduced support for Elliptic Curve Cryptography (ECC) in 2008 (Dierks & Rescorla, 2008).

The security of elliptic curve cryptography is related to the one-way discrete logarithm problem, whose security is based on the fact that the exponentiation operation inverse computation problem is mathematically intractable. The argument that the problem is intractable is based more on anecdotal than mathematical evidence. In other words, there is a possibility that the problem is not actually as difficult to solve as has been assumed (Blahut, 2014).

Elliptic curve cryptography allows the use of much smaller key sizes than RSA. Compared to the commonly used 2048-bit RSA key, the elliptic curve can achieve the same level of security using 256-bit parameters (Smart, 2016)

The equation of an elliptic curve defines all the points on the curve. The curve is defined by the coordinates x and y, which solve the equation. It was discovered that a group can be built over elliptic curves. Most of the curves used today are based on a few standards. The most commonly used on the Internet is the NIST P-256 curve which is one of the 15 curves defined in the NIST FIPS 186-4, "Digital Signature Standard" annex. The P-256 curve is determined by the Weierstrass equation "y2 = x3 + ax + b mod p" (Wong, 2021)

3.4 Post-quantum cryptography

Post-quantum cryptography, or PQC, refers to cryptographic algorithms that are believed to be resistant to the threat posed by a quantum computer. It is believed that a powerful enough quantum computer will be able to break the current widely used public-key cryptographic algorithms based on RSA, DSA and ECC. PQC algorithms are believed to be resits to classical computer and quantum computers.

So far, there is no known method such as "Shor's algorithm" that can break PQC algorithms.

3.4.1 Quantum algorithms

Quantum algorithms are commonly described as much faster than traditional algorithms are. The rationale is that due to the superposition, all possible input values can be given as input, after which the algorithm is executed in superposition. Instead of one traditional classical input executed at once, the algorithm utilizes the "quantum parallelism" feature, where all inputs are processed simultaneously. However, it remains open how many simultaneous responses can be used. When we make a measurement, we get one random answer. Probability of getting the wrong answer is more likely than the right one. The real benefit of quantum algorithms is their ability to manipulate superpositions so that measurements provide useful answers to the solution sought. The effectiveness of quantum algorithms is not based on the fact that they are accelerated classical algorithms that utilize brute force. The power of quantum algorithms is based on their ability to utilize quantum properties in an efficient way (Bernhardt, 2019b).

The performance of quantum algorithms is evaluated in terms of various measures such as efficiency, speed, and implementation of quantum circuits (Soltan Agh, Zukarnain, Mamat & Zainuddin, 2009)

Quantum gates are described by orthogonal arrays. Quantum circuits consist of combinations of gates corresponding to the multiplication of orthogonal matrices. Since the result of the multiplication is an orthogonal matrix, it follows that any quantum circuit can be represented by an orthogonal matrix. Compared to classical computing, quantum computing provides more opportunities to examine the problem. Problems solved by a quantum computer must have a structure that only becomes visible when it is converted using an orthogonal matrix. (Bernhardt, 2019)

3.4.1.1 Grover´s Algorithm

The search algorithm created by Lov Grover can speed up searches by a quantum mechanical system to a directory where the data is in a completely random order. Grover's search algorithm speeds up data search polynomically compared to traditional classical computer search. If the target is a randomly organized directory that contains N items, only one of which satisfies the desired search condition. The most effective classic algorithm for retrieving data is to view items one by one until the searched item is found. A classical computer requires an O (N) step to solve the problem, which means an average of 0.5N. Utilizing quantum mechanical system duality properties of photons can be used to make non-interacting measurements. The presence (or absence) of an object can be inferred by allowing a small probability that the photon will interact with the object. By allowing a certain probability to examine the desired object, it is enough to allow a small interaction for the measurement, and it is possible to find the subject of the search problem without examining all the items. Using the same amount of hardware as in the traditional case, but using input and output in superpositions of states, we find the object in quantum mechanical phases in O (√N) steps instead of the classical phases in O (N) steps. The same problem can be solved by Grover's algorithm in O (√N) steps (Bernhardt, 2019).

3.4.1.2 Shor´s algorithm

Peter Shor published his remarkable study in 1994: Algorithms for Quantum Computation: Discrete Logarithms and Factoring (Shor, 1994, 124-134)

The Shor’s algorithm makes it possible to identify the factors of the prime numbers used in RSA encryption and break the encryption. The algorithm is special because it runs significantly faster on a quantum computer than on a traditional classical computer. The approach provided by Shor’s algorithm is exponentially faster than the sub-exponential time general number field sieve, which is currently the fastest known factoring capability available on traditional classical computers (Shor, 1994, 123-134).

The following chapter describes the main features of the operation of the Shor‘s algorithm in a simplified manner. Shor’s algorithm takes advantage of Euler's theorem, continued fraction expansions from number theory, requires knowledge of complex analysis and the discrete Fourier transform.

The factoring of large numbers into components is slow on classical computers, but the algorithm developed by Shor makes it possible to factor large numbers into two prime factors using a quantum computer. (Hidary, 2019, 14) .

Using Shor’s algorithm, it is possible for a quantum computer to factor prime numbers faster than using the brute-force method used by a classical computer (Grimes, 2019, 77-78).

Shor's algorithm is based on the observation that long series of numbers contain periodicity that can be detected by mathematical analysis. Shor's algorithm utilizes Fourier analysis to identify periodicities of number sequences. Theoretically, this can also be achieved with a classic computer by looking at each possibility alternately, but with long number sequences this takes longer than the age of the universe. (Gribbin, 2014, 137)

The algorithm includes quantum and classical components. Quantum computing section includes phase estimation, order search, modular exponentiation and Quantum Fourier transformation (Sutor, 2019, 540).

The Shor’s method makes a purely random guess of a single prime number, and then new guesses are made closer to the desired prime number, until the correct searched prime number is found. Shor's method utilizes the mathematical relationship of prime numbers in a way that reduces the number of guesses required. A large number of guesses are still needed, but due to the quantum property of superposition, they can be created on a quantum computer in a short time. The correct prime number is identified by all guesses by converting guesses with a Fourier transformation into a sine wave. Sine waves are added together with other sine waves in all possible combinations. The two searched values, form together a sine wave with the greatest amplitude, meaning the peaks are the highest and the valleys are the lowest. Incorrect guesses affect each other so that their amplitude remains smaller (Grimes, 2019, 77-78).

Shor's algorithm exponentially accelerates the solution of components and discrete logarithm problems compared to classical methods. Shor's algorithm solves the problem of finding the prime factors of the given integer N. Shor's integer factorization algorithm includes two steps: The first step is to reduce the factoring problem to an ordering problem, which can also be done effectively with a classical computer. The second step, called phase evaluation, involves formulating the period-retrieval problem as a phase evaluation problem and solving it with a quantum algorithm. A key component of the second phase is the quantum Fourier transform, which allows for exponential acceleration compared to classical algorithms (Stanescu, 2017, 306).

Stanescu (2017) describes an algorithm that is a key part of finding the order of Step 2:

1. Randomly choose an integer a < N; compute the greatest common divisor gcd(a;N); if gcd(a;N) 6= 1, return it and stop (a nontrivial factor of N has been found); otherwise, continue.
2. Apply the order-ending subroutine to find the period r of the function fa(x) = ax (mod N).
3. If *r* is odd or $aa^{r/2} = -1\ (mod$ N), go back to step 1, otherwise continue.
4. At least one of the integers $p\ = \gcd\left(a^{r/2} + 1, N\right)$ and $q\ = \gcd\left(a^{r/2} - 1; N\right)$ is a non-trivial factor of N; test which one and return it; stop.

(Stanescu 306-307).

The problem of dividing the factors of a number into prime numbers decreases when the coefficient *a* is found, because the found factor can be used to divide the original number, and thus identify smaller factors. Shor's method for finding the factor *N* of any number is to find the period *r* of a particular function *F* and use this information to find the factors. Increasing the key size of encryption keys does not provide significant additional security because requirements for quantum machine increase much more slowly compared to the length of the encryption key used (Deutsch, 1998, 149).

The operation of Shor's algorithm has been proven by researchers Isaac Chuanf and partners in an experiment in which they factored the number 15 using the nuclear magnetic resonance system (Sherwood, 2001, 883-887)

Today's quantum computers are incapable of breaking the key sizes currently used in public key cryptography using Shor's algorithm (Gidney & Ekerå, 2019).

According to David Deutch (Deutsch, 1998, 149) Shor's algorithm is exceptionally simple. It does not require a universal quantum computer to operate but operates on much more modest hardware. Deutch predicts that the quantum factor engine will be built before the entire quantum computing area is technically implemented.

3.4.2 Crypto break

The complete security of the RSA system is already uncertain. It is possible that someone captures and stores an RSA encrypted message and will be left waiting until there is a sufficient level of quantum factoring available to decrypt the encryption. All that remains of the complete security of RSA encryption is the likelihood that it will last quite a long time. This could be centuries or decades. (Deutsch, 1998, 149).

3.4.3 Preparing

Mosca’s Inequality

There is a strong interest in post-quantum cryptography, although the realisation of a sufficiently powerful quantum computer is uncertain and will only take place in the future. The transition to quantum safe cryptography will take several years, subject to decades. A good example of a similar transition is the SHA1 hash function which has been considered unsafe since 2014 (Horowitz & Grumbling, 2019, 109).

In practice, the transition to safe SHA2 hash functions really started when browser manufacturers removed SHA1 support from browsers.

Most of today's applications and solutions use algorithms that are not post-quantum safe. In 2015, Michelle Mosqa introduced the equation x + y ≥ z, also known as “Mosca's inequality” shown in the Figure 5. (Michele Mosca, 2015).

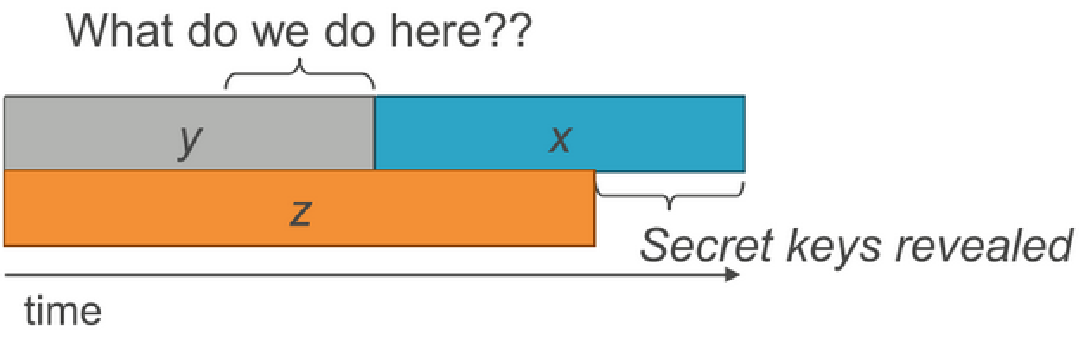


Figure 5. Mosca’s inequality

The variable X in the equation describes in years how long the encryption we use must be safe. The variable Y describes the time in years that we estimate for the transition from classic data protection methods to Post-Quantum methods. The variable Z describes the time in years until quantum computers are able to break down the classic methods of data protection. If a requirement is that the data protected must remain encrypted for 15 years and the transition to a quantum safe method is estimated to take 5 years, the transition to the post-quantum system shall begin 20 years before the estimated quantum period is realized (Michele Mosca, 2015, 20).

According to Kiviharju (2021, 1)the theorem proposed by Mosca is very general and only takes into account the worst-case scenario. The use cases and targets of systems threatened by a quantum computer are not identical. Encryption keys expire quickly, the information to be protected is not secret, but it is not allowed to change. Kiviharju questions whether Mosca's inequality can be applied to all critical information infrastructure (CII) areas and all encryptions use cases. There are currently no methods to answer the questions of how best to protect against a quantum computer threat, whether protective updates are necessary and how quickly should they be installed, or how to take into account the requirements of the target system.

Kiviharju proposes the Quantum Computing risk management model as a solution to more accurately assess the impact of quantum computing to systems using vulnerable cryptosystems.

The risk management model consists of the following three aspects:

1. An estimate of the time, resources and scalability needed to develop quality control implementations
2. Qualitative classification of the strengths of quantum resistive methods by type
3. Qualitative classification of risk levels by cryptographic and asset use case.

3.5 Quantum-resistant algorithms

The security of post-quantum cryptographic algorithms is based on mathematical problems that are widely believed to be difficult to solve using quantum computation. Since it is possible that a quantum computer will be able to break public key encryption in the future, interest in quantum-safe algorithms is growing. The ongoing NIST competition is expected to produce standards for quantum key exchange and standardisation. It is important to understand that the adoption of new algorithms also depends on how well they can be implemented in applications and communication protocols (Soltan Agh et al., 2009, 1).

3.5.1 Major types of Post-Quantum Algorithms

The following chapters describe the major types of post-quantum algorithms and what kind of protection they provide against a quantum computer attack.

3.5.1.1 Code-Based Cryptography

Code-based encryption is a method relying on mathematical algorithms that deliberately add errors to the plaintext content so that the original content is encrypted/covered. Code-based cryptography is also called as algebraic encryption or error correction codes (ECC). An equivalent error-correcting algorithm / code can be used to decrypt, restoring the content back to its original form. Code-based encryption uses complex error correction algorithms that are very difficult to solve without knowing the key used for encryption (Grimes, 2019, 135-136).

The first code-based cryptosystem was developed by Robert McEliece in 1978 (McEliece, 1978). Code-based encryption systems have not achieved the same level of popularity as, for example, RSA, which is the same age, or Elliptic-curve-cryptography, which is about 10 years younger. The strength of code-based encryption schemes is better than RSA, which is more security is decreased from exponential to subexponential (Lange, 2020, 2). Breaking the parameters proposed by McEliece in 1978 for 64-bit security was not successful until 2008 and required 264 operations (Bernstein, Lange & Peters, 2008).

The original McEliece uses Goppa codes to generate the private key. Goppa codes developed by the Russian Valery Denisovich Goppa in the 1970s and 1980s are widely used in encryption (Goppa, 1970).

There are two technical challenges associated with code-based cryptography: Compared to other types of encryptions, the use of Goppa code-based systems results in a large public key size, which is their greatest weakness (Lange & Steindwandt Rainer, 2018, 4). The size of the public key used for encryption can be more than 300,000 bits long. The ECC algorithms used in code-based cryptography are intended to correct errors, and if this is not taken into account, errors that have passed the encryption may prevent decryption with the correct encryption key. The error is called self-induced, denial-of-service looping event. The problem is usually taken into account in the design of code-based cryptography algorithms, so that they tend to prevent such errors, but there is always a theoretical risk of error (Grimes, 2019. 135-136).

3.5.1.2 Supersingular Elliptic Curve Isogeny-based Cryptography

Isogeny-based public key cryptography uses maps between elliptic curves. The first Isogeny-based implementation was introduced in 2006 by Couveignes (Couveignes, 2006) and Rostovtsev & Stolbunov (Rostovtsev & Stolbunov, 2006)

A key exchange system that use isogenies between ordinary elliptic curves over finite fields is called by the name CRS (Charles, Goren & Lauter, 2006). Shor's algorithm does not weaken the implementation, but CRS can be broken by a sub-exponential quantum attack (Childs, Jao & Soukharev, 2014) .

Supersingular elliptic curve isogeny equations are considered the most challenging mathematical problems ever developed. Isogeny cryptography is based on mathematical equations that produce supersingular elliptic curves and isogeny graphs. Elliptical curves are created with mathematical formulas representing algebraic curves. The "super" section in the name refers to unusually large curves. All supersingular curves are nonsingular, which means algebraic curves that do not self-intersect. Isogeny denotes discrete algebraic groups that share the intersection of interrelated values. Supersingular elliptic curve isogeny implementation does not have the same weaknesses as the previously described CRS key-exchange implementation and provides exponential security against quantum attacks. The supersingular isogenicity implementation was introduced by Jao and De Feo in 2011 (Feo, Jao & Plût, 2011).

Isogenic encryption is based on two different algorithm equations that form an isogenic connection. Algorithm equation can be used for both encryption and decryption. The public key used for encryption is formed of a pair of elliptical curves and the private key is the isogeny between them.

The advantages of isogenic encryption are very small key sizes compared to other quantum-safe methods and it allows perfect forward secrecy implementation. Its weakness is considered to be that it is a fairly new encryption method and has not been tested as much as other post-quantum encryption methods. However, many speed-ups have been found and its safety is better understood (Couveignes, 2006, 2).

Perfect forward secrecy means that the compromise of one key does not compromise all encrypted information. For example, the compromise of a long-term private key does not compromise a session key derived from a set of long-term private and public keys. In systems where new session keys are negotiated for each session, any compromise of the key will only compromise that session. The term Forward Secrecy differs from Perfect forward secrecy in that the subsequent compromise of another key derived from the same long-term key material does not compromise the previously derived key (Grimes, 2019, 140).

A Chinese team of researchers carried out the first quantum-safe digital signature based on supersingular elliptic curve isogenies and multivariate cryptography (Xu, 2019).

3.5.1.3 Hash-Based Cryptography

Hash-based cryptography is based on cryptological hashes and is used in digital signatures rather than encryption. Hash refers to a one-way function that forms a set of bits describing the source material pattern that is unique to the target material. In other words, if the source material does not change, the hash taken from it always produces the same bit pattern. If, on the other hand, the source material changes by at least one character, the hash formed from it also changes.

Ralph C. Merkle introduced Hash-based signatures (Merkle, 1979)

Hash functions are one of the most widely used tools in cryptography. They are used for a wide range of purposes, from hashing passwords to checksums for files. Hash functions are used in almost all cryptographic implementations (Smart & Lange, 2021, 9).

The main feature of hash-based approaches is their well-understood security against both classical and quantum computing threats. The security of HBS schemes relies on well-known security notions related to hash functions, including pre-image and collision resistance (Misoczki, 2).

Hash-based cryptography is considered quantum safe because it is not vulnerable to Shor’s algorithm. Grover's algorithm affects the hash effect by a square root and removes half of the encryption strength. However, this can be compensated by using key sizes twice as long. However, there is a limit to the number of messages that can be protected before the hash outputs will become prematurely redundant for all possible unique inputs they are attempting to hash. An attacker gets a strong idea of the private key if the hash cryptography mistakenly repeats the same one-time key for two separate inputs. The risk can be reduced by increasing the accuracy of the hash algorithm in extracting individual content. In this case, a unique hash output is formed for each unique entry. The challenge is that the key space used by the hash is more limited than the content it compresses. The size of the Hash key can be increased so that it is possible to have more digested results. Large hash sizes can cause performance and storage problems. There are different views according to which high quality hashes, using its inherent algorithmic accuracy, do not necessarily produce large key sizes. Others believe that large key sizes are the only way to ensure accurate hash without result redundancy. A stateful hash is a way to prevent keys from recurring. A stateful hash maintains a list of each one-time secret used to ensure that it is not reused. If a reused key is identified, the algorithm is re-executed and another part of the longer key stream is selected to generate a unique one-time key. The use of stateless and stateful hashes comes with its own disadvantages and advantages. Stateless hashes cannot guarantee unique keys and use larger key sizes. Stateful keys allow for smaller key sizes, but secure maintenance and storage of the status table can cause security, resource, and capacity issues (Grimes, 2019, 136-138).

Because hash functions are so widely used, their security is well understood. It is also known that quantum machines cannot significantly reduce the security of hash functions. At worst, the impact can be as large as square-root factor speed-up (Smart & Lange, 2021, 9).

3.5.1.4 Lattice-Based Cryptography

Lattice means a repetitive, dimensionally distributed geometric pattern or arrangement of something, such as points in space. Lattices occurs everywhere in nature, such as in crystals and molecules. Lattice is the result of many mathematical formulas and algorithms. Most Lattice-based encryption algorithms are based on the Shortest Vector Problems (SVPs), which require super-exponential time to solve (Grimes, 2019, 138).

The most common lattice problems with encryption use are Learning With Rounding (LWR), Learning With Errors (LWE), Module Learning With Errors (MLWE), Ring Learning With Errors (RLWE). Different types of problems have their own advantages and disadvantages. For example, RLWE include new mathematical structures with no long-term experience, but it uses a smaller key size and is generally faster than LWE. Hard-to-solve lattice problems have been used to develop public key cryptography and digital encryption systems. These are considered to have the advantage of being robust against classical and quantum computers. Lattice-based encryption is based on a mathematical work-load problem that is equivalent to or greater than the amount of work required to construct large prime numbers. However, Lattice-based encryption is not based on large prime numbers, which is why it is not considered vulnerable to quantum algorithms that form prime factors, such as Shor's algorithm (Grimes, 2019, 138-139).

For Lattice encryption, a complex Lattice function is created that acts as a private key. Content is encrypted using a public key. The public key is a modified version of the original Lattice function that acts as a private key. Decryption is performed with the original (private key) lattice function (Smart & Lange, 2021, 9-10).

The weakness of Lattice-based encryption is considered to be relatively large key sizes compared to other encryption types. The overall security of SVP-based lattice encryption is not fully understood and has been the subject of theoretical attacks which have significantly undermined confidence in its security. It is feared that Lattice-based encryption will be found to be weaker than expected in the future. (Grimes, 2019, 138-140)

3.5.1.5 Multivariate Cryptography

The name multivariate comes from the words “multiple variables”. Multivariate encryption uses complex mathematical polynomial equations to generate encryption primitives (multivariate polynomial math equations) such as x + y + z = n. If the variables of the Multivariate polynomial equation are raised to another power x2 + y + z it is called *multivariate quadratic (MQ) polynomial equation cryptography.* Multivariate Cryptography has been rated as quantum safe because it does not use large prime numbers in encryption and, when properly implemented, cannot be solved in polynomial time. Due to its performance and features, Multivariate Cryptography can also be implemented on a hardware basis, such as by utilizing field-programmable gate arrays (FPGAs) or application-specific integrated circuits (ASICs). (Grimes, 2019, 139)

3.5.1.6 Zero-Knowledge Proof

The Zero-Knowledge Proof (ZKP) method has two parties, the first of which (referred to as Prower) indicates to the other party (verifier) that they know the value A. In the method, the parties do not have to communicate to each other than the confirmation of the value of A without providing that value or passing on any other unnecessary or additional information. An example of a ZKP method is user authentication to a service using the challenge-response method. ZKP encryption typically involves proving something related to encryption, such as a discreet logarithm function, without revealing the function itself.

3.6 NIST Post-Quantum Contest

The NIST Post-Quantum Cryptography Process is a competition that began in February 2016 with the goal of selecting post-quantum cryptographic standards for public key exchange and digital signatures. 82 proposals were submitted, of which 69 were selected by NIST to go forward to the first round. The algorithms that participated in the competition must provide at least one of the following functions: public key encryption, key exchange, or digital signature. In January 2019, 17 asymmetric encryption and 9 digital signature schemes were selected from the first round of candidates to proceed to the second round (Chen, Moody & Liu, 2017, 13).

The Round 3 candidates were announced July 22, 2020. NIST announced that the analysis of Round 2 participants has been finished and seven finalists and eight alternatives have been selected from the competitors to proceed to the third round. NIST will evaluate the algorithms of the finalist group and the selected ones will be recommended for standardisation at the end of the third round. The algorithms of the finalist group are presented in Table 2 (Alagic, et al., 2020, 8).

Table 2 Third Round Finalists

Public-Key Encryption/KEMs		**Digital Signatures**	
Classic McEliece	Code	CRYSTALS-DILITHIUM	Lattice
CRYSTALS-KYBER	Lattice	FALCON	Lattice
NTRU	Lattice	Rainbow	Multivariate
SABER	Lattice		

A group of alternative algorithms were selected because they may provide better security, performance, and suitability for some applications. According to NIST, alternative algorithms still require further analysis. Alternate Candidates are presented in Table 3 (Alagic, et al., 2020, 8).

Table 3 Alternate Candidates

Public-Key Encryption/KEMs		**Digital Signatures**	
BIKE	Code	GeMSS	Multivariate
FrodoKEM	Lattice	Picnic	Zero-knowledge proog
HQC	Code	SPHINCS+	Hash
NTRU Prime	Lattice		
SIKE	Isogeny		

The winner of the NIST competition, such as AES and SHA3 algorithms, usually becomes U.S. federal standards through NIST Federal Information Processing Standards (FIPS) release documents. NIST believes it will standardize on more than one algorithm to provide options for different usage needs (such as speed, memory consumption, power consumption, etc.) (Basu, Soni, Nabeel & Karri, 2) All computers used by the US government and contractors must comply with the standards. Since the US government is the largest single purchaser of computers, computer manufacturers find it more cost-effective and easier to include the standards in all computers sold than to make dedicated versions for the government. US standards will become global standards, except for a few big countries like Russia and China which have their own strong standards (Alagic, et al., 2020).

3.6.1 NIST Security Strength Categories

All algorithms participating in the NIST Post-Quantum competition are required to implement certain methods equivalent to current quantum-resistant symmetric cryptographic algorithms and hashes. The strength categories defined by NIST and the peer algorithms are described in the Table 4 (Grimes, 2019, 149).

Table 4. NIST Security Strength Categories

NIST security level	Equivalent security
1	AES-128 (Key search)
2	SHA256/sha3-256 (Collision search)
3	AES-192 (Key search)
4	SHA-384/sha3-384 (Collision search)
5	AES-256 (Key search)

According to NIST, all five classes are resistant to quantum computers, although the lowest class, Class 1, is described as "likely to be safe in the near future unless quantum computers improve faster than expected". Most of the participants in the NIST competition submitted versions of their algorithms corresponding to NIST security levels 1, 3 and 5. The majority did not submit versions for levels 2 and 4 (Grimes, 2019, 149).

3.6.2 Round 3 Finalists

3.6.2.1 Classic McEliece

McEliece is based on the public key cipher presented by Robert J.McEliece in 1978. McEliece is a code-based cipher based on Goppa codes which is still considered secure (McEliece, 1978). The original McEliece is also quantum secure and fast compared to the RSA algorithm. The downside of McEliece is the large key sizes which are often over 1Mb. Attempts have been made to develop the algorithm to use smaller key sizes, but these have been less secure than the original implementation (Grimes, 2019, 145)

With Classic McEliece, the team participating in the NIST competition has managed to modify the implementation so that using smaller key sizes achieves quantum security without decryption errors. The group includes a well-known cryptographer, Daniel J. Bernstein. The advantages of Classic McEliece are speed in device-based implementations and small ciphertext size. Its public key size is the second largest among the participants in the first round (Alagic, et al., 2020, 9).

3.6.2.2 CRYSTALS-Kyber

The name CRYSTALS comes from Cryptographic Suite for Algebraic Lattices. CRYSTALS consists of two Lattice based cryptographic primitives: Dilithium, EUF-CMA Secure digital signature algorithm and cyber CCS-secure KEM. CRYSTALS-Kyber is built on a previous MLWE-based encryption problem, while use a square rather than a rectangular matrix as the encryption key and polynomial rings. The advantages of CRYSTAL are good scalability to use larger key sizes if required and good performance (Smart & Lange, 2021, 13-14).

3.6.2.3 NTRU

NTRU, or N-th degree Truncated Polynomial Ring, was originally developed in 1996 and is therefore well researched. NTRU is a lattice-based NTRU encryption scheme. It is the first identified asymmetric cipher that is not susceptible to the Shor's algorithm. In addition, NTRU, together with McEliece, is one of the first public key cryptosystems that does not rely on factorization or the discrete logarithm problem.

The lattices used by NTRU contain more structure than the average lattice implementation. As a result, generating secure keys and encryption is remarkably faster than classical public key methods like ECC and RSA. NTRU is one of the fastest implementations of the first round.

NIST round 1 participants NTRU Encrypt and NTRU-HRSS-KEM merged into one for the second round. The underlying ciphers of NTRU have been released under the public domain in 2013 (Grimes, 2019, 149).

3.6.2.4 SABER

SABER is a lattice-based CPA-secure encryption and CCA-secure KEM suite, with security based on the hardness of solving module-learning-with-rounding (MLWR) problems. Saber only implements encryption but not signing. It is flexible, requires less randomness to be secure, performs well and uses little bandwidth (Alagic, et al., 2020, 11).

3.6.2.5 CRYSTALS-Dilithium

The name CRYSTALS comes from the words Cryptographic Suite for Algebraic Lattices.

CRYSTALS comprises two lattice-based cryptographic primitives which are Kyber: the CCA-aware KEM and Dilithium, the EUF-CMA-strongly secure digital signature algorithm, CRYSTALS-Dilithium. Crystals takes advantage of an interactive proof-of-knowledge idea similar to ZFK systems, known as Fiat-Shamir aborts (Lyubashevsky, 2009).

Dilithium provides a level of security equivalent or better to AES-128 but using relatively small public keys and forming small digital signatures. Dilithium forms a small private key that acts as a seed value when pseudo-randomized to another value, used by the algorithm to generate the public key and digital signature. A vulnerability was found in the first-round version of CRYSTAL-Dilithium in random number generation. The error was found to be a simple two-line coding implementation error and was corrected by the implementers (Smart & Lange, 2021, 16-17).

3.6.2.6 FALCON on NTRU lattice-based

FALCON, or Fast Fourier Lattice-based Compact Signatures over NTRU, is an NTRU lattice-based digital signature algorithm whose security is based on the ring short integer solution (SIS) problem. SIS problems are very difficult to solve. Falcon uses floating-point arithmetic based on 54-bit precision. In addition, Falcon is also based on work published in 2008 to implement a framework known as Gentry, Peikert and Vaikuntanathan (GVP) for secure HASH and lattice-based signatures (Grimes, 2019, 157).

Falcon utilises a "hash-then-sign" paradigm that first hashes the message and signs the hash instead of the message. The implementation does not have the same problem with long message signature as Dillithium does with the Fiat-Shamir paradigm.

FALCON has been designed with high performance in mind, especially for environments where memory is limited. Falcon uses one of the smallest public key sizes and creates a small signature equivalent to a 2048-bit RSA signature. However, it uses floating-point math, leading to poor performance on platforms that do not support floating-point (Grimes, 2019, 157).

3.6.2.7 Rainbow

Rainbow is a multivariate EUG-CMA secure digital signature algorithm. Rainbow uses a multi-layered Unbalanced Oil & Vinegar implementation. There are different implementations of the algorithm depending on whether one wants to prioritise security, performance, or size. It uses the SHA2 algorithm from 256bit to 512 bits depending on the chosen security level (Ding & Schmidt, 2008).
Rainbow was created as early as 2005 and is one of the most tested post-quantum algorithms. In 2008 it had to be modified following a successful attack but since then, for more than 10 years, no vulnerabilities have been discovered (Thomae, 2012).

Signature sizes are small and signature execution time is very fast. While signature sizes are among the smallest, the private and public keys being used are some of the largest (Grimes, 2019, 160).

3.6.3 Hybrid methods

A hybrid method refers to the simultaneous use of two (or more) algorithms in a so-called "hybrid mode". For example, both traditional (e.g., elliptic curve Diffie-Hellman) and post-quantum algorithms can be used together for different reasons. Typical reasons for using hybrid algorithms may be that they meet government or industry regulations which have not yet been updated, but also meet the security requirements of a post-quantum algorithm. It may also be that, in the early stages, users want to take advantage of the possibilities offered by post-quantum algorithms but do not want to rely solely on a new and relatively untested algorithm (Crocckett, Paquin & Stebila, 2019, 2).

In Information Technology, redundancy aims to avoid the impact of a single component failure on the whole system. Redundancy has been used in cryptography, for example, to improve the security of the DES algorithm by performing multiple encryptions in succession (Merkle & Hellman, 1981) It has also investigated tolerant encryption systems that remain secure even if one or more of their components fail (Herzberg, 2005)

The security of classical algorithms such as factorization or discrete logarithm has been much more studied than the assumptions underlying the security of post-quantum cryptography algorithms such as syndrome decomposition or learning with errors. Combining classical and PQC algorithms into a single system is considered a good idea from a safety perspective (Huguenin-Dumittan & Vaudenay, 2021, 1).

The aim of the hybrid method is to ensure that the intended safety feature is maintained as long as one of the subsystems used remains intact. In terms of key exchange, this means that if one of the key exchange mechanisms used is intact, the session key will also remain secure. For authentication, it is required that the protocol provides secure authentication if one of the digital signatures is intact at the time of session establishment (Huguenin-Dumittan & Vaudenay, 2021, 5-6).

Combining both PKE/KEM and PQ, the ideal case is an encryption system that is secure as long as one of the two systems is secure. Such systems are called hybrid systems, and the method of combining the systems used to implement them is called a combiner. If the resulting hybrid system is safe as long as any of the systems used is safe, the combiner is said to be robust (Huguenin-Dumittan & Vaudenay, 2021, 1).

Protocols may have been designed with algorithm agility in mind, allowing multiple cryptographic algorithms to be supported by the parties of the connection. Algorithms are often defined for different classes of functions such as symmetric encryption, hash function, key exchange, public key authentication, etc. The agility described above has been considered in the design of TLS and SSH, among others. SSH and TLS include a mechanism for the parties of the connection to negotiate the cryptographic method to be used. The negotiation can take place either as a complete negotiation or on an "a la carte" basis. The negotiation mechanism allows for parties of the connection who support subsets of different algorithms to choose a combination of ciphers that suits both parties, as long as they have at least one overlapping supported algorithm in each class. The negotiation mechanism however supports only one algorithm at a time for each action class. To support the hybrid method, the protocol must be modified to support the negotiation of a combination of algorithms in hybrid mode (Crocckett et al., 2019, 4).

The hybrid protocol should be backwards compatible, meaning that it should also work with applications that do not support hybrid algorithms. Other requirements for a hybrid method are adequate performance, so the implementation must not use too much processing power, and low latency (Huguenin-Dumittan & Vaudenay, 2021, 6).

A typical way to combine private key encryption (PKE) and key exchange (KEX) is to first perform encryption on both systems. The end result is a shared secret per system used, for which an XOR operation is performed, resulting in a single shared secret. For protocols such as TLS, where the session key is derived by feeding a premaster secret obtained by public key cryptography into a key derivation function (KDF), there is also the possibility to create one premaster secret per system and feed a concatenation of two premaster secrets into the KDF (Smart & Lange, 2021, 22).

For signatures, the two systems are usually used independently of each other. In this case, there are always two signatures, one for each system. There will also be two key pairs.

3.7 Literature review

A literature review is considered an effective tool to deepen knowledge on issues where there is existing research data. (Tuomi & Sarajärvi, 2018, 138). The researcher typically has a preliminary understanding of the topic to be studied, which he or she deepens through a literature review. (Puusa & Juuti, 2020, 88). In the literature review, the researcher presents previous research and literature relevant to the problem (Kananen, 2015, 24). The literature review provides a theoretical basis for the research and also shows how the phenomenon has been studied before, how successful it has been, what gaps have been left in the research area and where it would be useful to focus new research. (Hirsjärvi & Hurme, 2015, 13).

3.7.1 Sources for the literature review

The scope of the literature review was limited to the quantum computer implementation, the estimated timeframe for implementation and the protection against the quantum computer threat. As the development of the quantum computer is progressing rapidly, the age of the material used in the literature review was limited to ten years. The literature review was based on four major research reports on the development of quantum computing, books on the subject and selected articles.

In recent years, a few studies have been carried out on the implementation method and timing of a quantum computer capable of breaking public key cryptography. In 2019, Michelle Mosca and Marco Piani conducted their first Quantum Threat Timeline Report on cyber risks associated with quantum crypto analysis. The survey was conducted as a questionnaire survey with the participation of 22 experts (Mosca & Piani, 2019).

The survey was renewed the following year under the name Quantum Threat Timeline Report 2020. In addition to 21 existing respondents, 23 new respondents from around the world took part in the survey. The respondents consist of 44 leading experts from universities and industry on four continents. Experts were asked to assess how quantum computers are evolving and when they will be able to pose a threat to cybersecurity. The study was conducted as an online survey. The aim of the study was to describe not only the current state but also the changes in opinions (Mosca & Piani, 2021).

In 2018, the Joint Research Centre (JRC) of the European Commission carried out a study of the emerging field of quantum computing using an online survey of the expert community. The aim of the study was to get an idea of the impact of quantum computing on different sectors and an assessment of the timetable for implementation. A total of 131 people responded to the survey, of whom more than 100 considered themselves to have a high level of expertise in quantum computing (Lewis et al., 2018).

A study by the Federal Office for Information Security, Status of quantum computer development, discusses the state of the physical implementation of quantum computing and the algorithms that run on it, focusing on cryptanalysis applications. The first version of the study was published in autumn 2017, the first update in early 2019 and the second update in early 2020 (Wilhelm et al., 2020, 3).

Roger Grimes (Grimes, 2019) describes in his book Cryptography Apocalypse a comprehensive overview of quantum computing, from quantum mechanics to different types of quantum computers and how quantum computers are used in today's cryptographic methods. The book also describes how to protect against the threat posed by the quantum computer.

3.7.2 Quantum computer implementations

Mosca and Pianini (Mosca & Piani, 2021, 2) describe that survey participants were asked to rank the physical implementations of quantum computing in order of preference, with the goal of creating a digital quantum computer with 100 logical qubits in the next 15 years. Based on the responses, superconducting systems and trapped ions are currently the leading implementations. Comments from respondents mentioned that it is unlikely that implementations based on topological cubes will work but they will lead the competition if they can be made to work. The responses also highlighted hybrid systems that combine the benefits of different platforms. In hybrid systems, material qubits, quantum dots, ions, NV centres, etc. interconnected using interlinked optical measurements.

One aspect of the JRC's research was to understand which physical implementation platforms for quantum computers are superior and which are not popular. Respondents were asked to evaluate possible physical platforms for building a quantum machine. Superconducting qubits were rated as the most likely implementation (80 respondents), followed by trapped ions, photonics, and semiconducting qubits (50 respondents). Topological qubits were ranked third most likely (40 responses). Other approaches identified included were nitrogen vacancy (NV) centres in diamond, hybrids of superconducting and optical/photonic technique and cold atoms. The five most popular options have strong support, and no clear distinction can be seen between them (Lewis et al., 2018, 88).

Status of quantum computer development research report (Wilhelm et al., 2020, 25)) proposes a five-level model for evaluating the evolution of quantum computers, as outlined in Figure 6. (Wilhelm et al., 2020, 25).

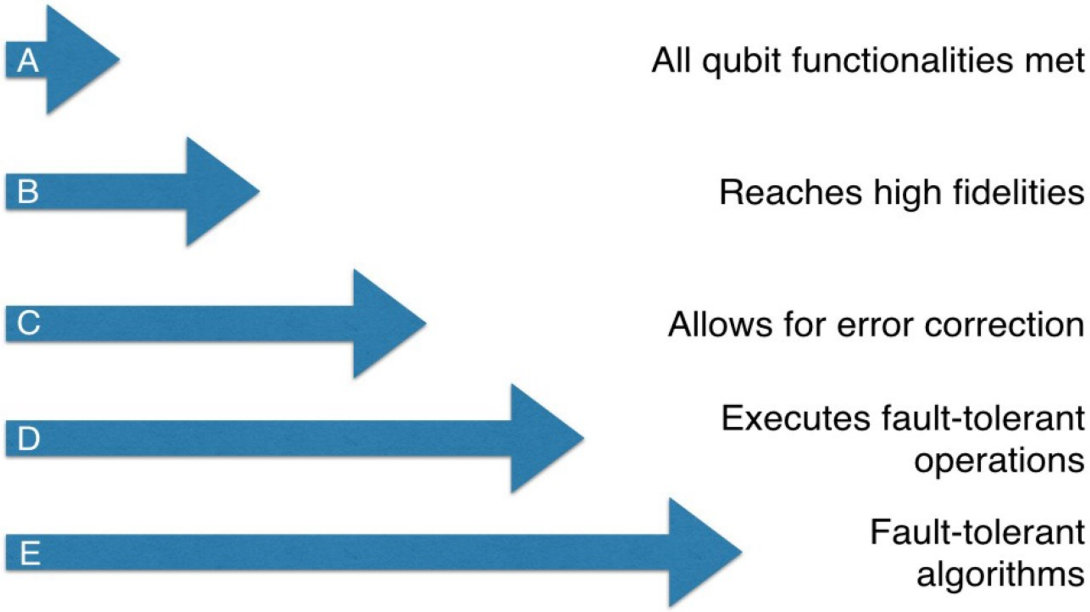

A
All qubit functionalities met
B
Reaches high fidelities
C
Allows for error correction
D
Executes fault-tolerant operations
E
Fault-tolerant algorithms

Figure 6. Quantum computer development levels

The levels of the model are:

A. Basic functionality
Candidate demonstrates all the basic functions of a quantum processor in the same experiment using more than two qubits (qubits, initialization, readouts, gates, coherence)
B. Quality of operations
The error rates for all significant activities are measured and they are compatible with error correction thresholds. All the elements of fault-tolerant architecture have also been demonstrated.
C. Error correction
Effective error correction is proven. Logical error rates are lower than physical error rates
D. Fault tolerant operation
The operations performed on logical qubits using common ports are implemented in a fault-tolerant manner.
E. Algorithms
Highly sophisticated complex algorithms and functions have been implemented.

Quantum computers based on the trapped ions implementation are classified as level C. Justification for this classification is that the quantum processor achieves all the elements, has a high quality of operation, and has demonstrated simple error correction(Wilhelm et al., 2020, 27).

According to the study, quantum computers based on superconducting circuits are of most interest to industry. There are different implementations of superconducting qubits which are classified into different levels. Flux qubits are superconducting loops and resemble classic superconducting electronics. They are easily interconnected and achieve long coherence times. The problem is the difficulty of implementation because it is difficult to form qubits that work consistently and predictably. Flux qubits are classified as level B for gate-based computation. A quantum error correction variation has been implemented for implementations based on superconducting circuits that implements level C elements but cannot be extrapolated with certainty. Two-dimensional transmons carrying quantum information through electromagnetic vibrational modes are classified as level C. Transmons are single Josephson resonators that achieve very long coherence. Three-dimensional transmons reach level B. They are resonators similar to their two-dimensional versions but surrounded by a superconducting cavity on all sides (Wilhelm et al., 2020, 27).

The existence of topological qubits has not been unquestionably confirmed and is therefore classified as Level A. Semiconductor nanowires implementations are considered promising candidates because topological error protection is carried out at material level and is not sensitive to correlated errors. Topological implementations are expected to quickly reach level D if level A is properly managed and theoretical predictions are correct (Wilhelm et al., 2020, 29).

Photon-based implementations are classified as Level A. A key challenge is the implementation of the two qubit gates because the quantums of light do not interact with each other. Therefore, the debugging required for level B cannot be performed due to insufficient properties of the two qubit ports. It is also difficult to build a scalable system (Wilhelm et al., 2020, 29).

3.7.3 When a quantum computer threatens public key cryptography

Michelle Mosca and Marco Piani (Mosca & Piani, 2021, 22) asked experts to estimate when and how likely a quantum computer would be able to crack an RSA 2048-bit key in less than 24 hours. The majority of researchers agreed that the probability of developing a quantum computer capable of cracking the current public key cryptosystem in the next 5 years is less than 1% or relatively unlikely.

More than half of the respondents thought that the threat of a quantum computer would materialise in the next 10 years was less than 1%. 11 out of 44 respondents agreed that the probability is about 50% or higher than 70% (Mosca & Piani, 2021, 24).

Just over half (23 out of 44 respondents) thought that a quantum computer was about 50% likely to become a reality within the next 15 years. However, the other half (21 respondents) agreed that the probability of realisation is less than 30% or even lower (Mosca & Piani, 2021, 24).

38 out of 44 respondents (86%) thought that a quantum computer was about 50% likely to become a reality within the next 50 years. In the opinion of 12 respondents, the probability is greater than 95% or higher than 99%. The answers suggest that the quantum threat will occur before 20 years pass is likely (Mosca & Piani, 2021, 24).

All but 1 respondent were in favour of a probability of around 50% in the next 30 years. 36 out of 44 respondents agreed that the quantum threat is real (Mosca & Piani, 2021, 24).

A large majority of 28 out of 43 respondents expect investment in quantum computing to grow over the next two years. 10 respondents expect investment to increase significantly, while 12 expect investment to remain at about the same level as now. Only 2 out of 43 respondents expect investment to decrease (Mosca & Piani, 2021, 32).

Sevilla and Riedel (Sevilla & Riedel, 2020, 18) states that the possibility that the RSA-2048-bit public key will be broken by Shor's algorithm before 2039 is less than 5 %. In order to ensure that the break-in takes place before this, progress must be made more quickly than has happened so far.

A study conducted by JRC (Lewis et al., 2018, 7) suggests that Sceptics believe that quantum computing still has many scientific and technological issues to resolve and will only have a significant impact in the long term, or possibly never. The majority of survey respondents believe that the technological outlook for quantum computing is positive and that the benefits outweigh the risks. The study identified quantum computing as an important area in the future that will play a significant role in the European Union's digital single market policy, industry and growth. The economic impact of quantum computing was estimated to be equal to or even greater than traditional information technology has had. Quantum computing was also estimated to create new jobs.
Respondents agreed that quantum computing is safe and likely to be useful, although it is believed that it could compromise existing encryption systems in the long term. Quantum computing was perceived to need only light regulation. Quantum computing is expected to be feasible within 10-15 years and capable of cracking the encryption protocols currently in use within less than 20 years (Lewis et al., 2018, 8).

Roger Grimmes gives four timeframe scenarios for a quantum computer to break the public key:
In the first scenario, the quantum crypto break and Quantum Supremacy have already taken place by a single actor. If the breakthrough has been carried out by the

government of a country, it might have every reason to keep the achievement a secret for as long as possible. In this case, other operators would still trust traditional public key cryptography to be secure to use. Grimes himself believes that this scenario has a 15% chance of being realized (Grimes, 2019, 90-91).

In the second scenario, Grimes suggests that Quantum Crypto Break and Quantum Supremacy are only a few years away, or even more likely. Google, IBM and many others have said they have already achieved quantum supremacy, or that it is probably about a year away. Achieving quantum supremacy, allowing a quantum computer to do things that a classical computer cannot, is unlikely to change the world in an instantly measurable way. A significant question is how quickly quantum computers with 100 stable qubits can be expanded to more than 4,000 qubits. Is it likely that once the stabilization and error correction of qubits can be made work with individual qubits, their scalability will increase rapidly? Grimes predicts that the feasibility of this option will be about 30% (Grimes, 2019, 91-92).

As a third option, Grimes (Grimes, 2019, 92) suggests that the quantum computing breakthrough will occur after the period of the “next few years”. This can be compared to the typical future prediction phrase "within the next 10 years". Scientists do not know exactly when the quantum crypto break is likely to occur, but they believe it will happen. Scientists developing quantum computers believe that the quantum computer will not be a reality in ten years, but rather in five to seven. Grimes estimates the probability of this scenario at 50%.

As a final option, Grimes presents a scenario in which a small minority of quantum computing experts believe that the remaining problems of quantum computing are insurmountable, and that the quantum computer will never materialise. Researchers believe that every type of quantum computer in the pipeline will run into a problem that will prevent them from truly evolving beyond current devices such as the crude abacus-like contraptions. According to Grimes, researchers involve some of the world's leading scientists who have a deep understanding of quantum computing, and their views cannot be ignored. Since "never" is a long time, Grimes gives this option a probability of 5% (Grimes, 2019, 92).

Aaronson Scott states in his book Quantum Computing since Democritus: “it’s entirely conceivable that quantum computing is impossible for some fundamental reason. If so, then that’s by far the most exciting thing that could happen for us. That would be much more interesting than if quantum computing were possible, because it changes our understanding of physics” (Aaronson, 2013, 218).

It is unlikely that within the next ten years a quantum computer will be built that threatens the security of RSA-2048. The reason for this is the current state of quantum computing and recent progress rates (National Academies of Sciences, Engineering, and Medicine, 2019, 157).

According to a report by Enisa (Smart & Lange, 2021, 25) not all developments related to a quantum computer are public and it considers it very likely that the first large fully functional quantum computer will not be made public.

Grimes (Grimes, 2019, 96) says that many countries use billions to develop quantum computers to be the first to implement quantum supremacy and the ability to break encryption. A scenario has been put forward where different countries reach their quantum targets within a few years of each other. States want to protect their secrets and limit damage by keeping information secret before bringing their quantum computer skills into the public eye. The scenario can be equated with how nations treat nuclear weapons. Acquiring a nuclear weapon requires a high cost and, after acquiring them, they are highly protected. States that possess nuclear weapons try to prevent new states from acquiring them. Strong encryption is considered a national secret. Even today, the export of cryptographic technology or know-how to some countries is prohibited and punishable.

Various formulas, also known as laws, have been used to try to describe the increase in power of machines in relation to time.

According to Moore's law, the number of transistors in the classical world in the same space doubles every 18 months or two years. (G. E. Moore, 2006).

Named after Hartmut Neven, "Neven's law" describes the increase in computing power of quantum computers relative to classical computers. The power growth of classical computers described by Moore’s law is called exponential growth. Exponential growth means that something increases by the power of two: $2^1=2$, $2^2=4$, $2^3=8$, and so on. According to Neven's law, the computing power of quantum computers increases proportionally to classical computers at doubly exponential rate. Doubly exponential growth means that the computing power increases by powers of powers of two: $2^{2^\wedge 1}$ =4, $2^{2^\wedge 2}$=16, $2^{2^\wedge 3}$ =256 and so on. According to Neven, the double exponential speed of quantum computers is due to two exponential factors that connect to each other. The inherent exponential advantage of the quantum computer over classical computers is the first advantage. If a classic computer has 16 standard bits, the quantum computer only needs four qubits to achieve the corresponding computing power. Another exponential factor is the rapid pace of development of quantum computers. Neven uses the example of the exponential growth of Google's chips, which has been driven by the reduction in error rates that has enabled the construction of larger quantum processors. (Hartnett, 2019).

Caution should still be exercised in interpreting Newen's law, as its conclusions are based on a few prototypes and a relatively short period of time. Quantum processors will become more powerful and complex, so that problems that are currently not significant may become more important. Moore's Law is not based on fundamental laws of nature, but on empirical observations. It has accurately predicted the evolution of computing for about 50 years. Neven's Law will have implications that go far beyond simply predicting the performance of quantum computing if Neven's observation turns out to be as accurate as Moore's Law (Rossi & Gonzalez-Zalba, 2019).

Grimes (Grimes, 2019, 96) makes the argument that the cost of developing quantum computers will be so high that quantum computers capable of breaking public secrets will only be available to states or companies with sufficient resources to make or afford to buy or lease performance time from quantum computers. The quantum calculation carried out by new, complex and hard-to-implement quantum computers will be economically highly expensive for several years. It will take decades from the release of the first working quantum computer to the advent of affordable, all-available quantum computers (Grimes, 2019, 96).

It is possible that governments will create laws that prohibit quantum computer manufacturers from allowing public key cryptography to be broken. This is comparable to preventing printing paper currencies on printers and copier machines.

According to Grimes, in the most likely scenario, the first to use large-scale quantum computing will be governments and the agencies, universities and businesses that work with them. If a quantum machine is developed by one of the big companies like IBM, Microsoft, Google, governments will be their first customers. Quantum computers are rapidly being used by companies of all sizes for a wide range of applications, so that within a decade quantum-based applications will be available to all. Quantum technology is either implemented in hardware or the hardware is connected to quantum computing services that perform the required quantum computation.

3.7.4 Preparing for the quantum break

Quantum Key Distribution (QKD) provides a secure way, guaranteed by the laws of physics, to distribute the secret keys required by cryptographic protocols. However, it does not provide authentication or message confidentiality, which still requires the use of mathematical encryption algorithms (Smart & Lange, 2021, 26).

The safest strategy to move to PQC algorithms is to wait for the national authorities to standardise PQC algorithms and then implement them during the transition period. Information that must remain confidential for more than 10 years must be protected from now on. As the NIST competition is still ongoing, there are two viable options for protecting information (Smart & Lange, 2021, 4).

Crocckett, Paquin and Stebila (Crocckett et al., 2019, 1) point out that there are several steps in the implementation of new algorithms, it is therefore important to plan the transition to post-quantum algorithms as early as possible. The first step is to identify whether there are features in the product into which the post-quantum algorithms are to be integrated that make implementation difficult. Such challenging features include the inability to override or negotiate encryption algorithms or size limits on keys or packets. A decision must then be made on how to incorporate the new algorithm into the existing implementation. The decisions to be made include cryptographic choices, like how the key material is used, and technical choices, like how keys and parameters are represented in network packets. In addition to the things described above, it must be considered how to maintain backward compatibility with implementations that have not yet been updated to support post-quantum algorithms, while achieving the desired protocol functionality for updated products.

The first option is to use hybrid implementations based on a combination of pre-quantum and post-quantum systems. An implementation's pre-quantum encryption scheme typically refers to RSA or ECDH algorithms. Post-quantum system refers to post-quantum algorithms. Using two different methods ensures safety as long as at least one of the two methods used is safe. However, implementations come at a price, and it is therefore worth carrying out a thorough risk and cost-benefit analysis before adopting a practice (Smart & Lange, 2021, 22).

Another implementation is to include the stored shared secret information in the key derivation, in addition to the key material obtained by a public key operation. This comes at the cost of storing pairwise data and is therefore only an alternative for systems that store states and have a limited number of peers. An example of such an implementation is ZRTP (Smart & Lange, 2021, 23-24)

Enisa's (Smart & Lange, 2021, 26) report reminds us that the quantum cryptography application is not immune to traditional crypto analysis or quantum crypto analysis.

4 Research results

The research data was collected by interviewing three key informants. The interviews, the coding of the interview material and the method of analysis used are described in more detail in chapter 2.4 Research method and 2.5 Analysis method.

The following seven themes were identified during the thematic analysis:

- Developers of the first usable quantum computer
- Quantum computer development challenges
- Motivation to develop a quantum computer
- Estimated timeframe for the realisation of the quantum threat
- Quantum computer threat
- Protecting against quantum threat
- Raising awareness of quantum computing

Themes and results of the analysis of the interviews are described below:

4.1 Developers of the first usable quantum computer

Developers of the first usable quantum computer describes the developers likely to develop the first quantum computer that threatens public key cryptography. The theme also discusses the publicity of development.

Developers of the first usable quantum machine are likely to be those who have money and resources to invest in development. These are known actors such as Google, IBM, Honeywell, IonQ Rigetti and D-Wave. These companies already have the best proposals for the equipment to be implemented and a strong lead in development. Honeywell and IonQ are developing quantum computer technology based on ion traps. Google, IBM and Rigetti use technology based on superconducting qubits. According to an interviewee familiar with the current state of quantum computing development, superconducting and ion trap-based quantum computers are currently the most promising technologies. The ability of countries to develop quantum computers is not clear, as there is no public information on the machines being developed for military or government needs. A state actor might have an interest in collecting data traffic, and breaking the secrets contained in it when the technology is mature enough. China and Russia believe the US has the motivation and ability to develop quantum computing and are seeking for ways to protect themselves against this by developing their quantum key distribution (QDK) capabilities. A quantum computer falling into the hands of criminals, either developed by them or sold by someone, is seen as a dangerous scenario. However, this is not considered realistic because they lack sufficient knowledge and resources. It should also be noted that breaking public key cryptography is illegal, and does not provide a commensurate benefit in terms of investment to companies that are capable of doing so. The topological quantum computer being developed by Microsoft is seen as a black horse because it may prove to be easily upward scalable.

Interviewees were asked whether it is possible that the first quantum computer will be developed by some as yet unknown small player. The general opinion of all interviewees was that it is difficult to predict, but the option cannot be completely ruled out. One interviewee described a possible scenario in which a small operator makes a breakthrough in the area for each of the other actors interpreted as infertile. Topological quantum computers could be those in which a breakthrough would lead to the rapid development of a quantum computer.

The first threat to public key cryptography is likely to be a general-purpose error-corrected quantum computer. The idea of a general-purpose quantum computer is to implement universal quantum computation and to be able to do any quantum calculations such as Shor's algorithm.

General-purpose quantum computers are being developed by companies such as IBM, Google, Aalto University and the black horse Microsoft with its topological computer. The topological machine is still in its infancy, but if it can be made to work, it is expected to jump straight to the most mature stage. The development path for general-purpose quantum computers is perceived as slower but more secure. It is also seen as possible that the first quantum computer capable of running Shor's algorithm would not be fully general-purpose but also not fully developed to solve a single problem.

4.2 Quantum computer development challenges

Quantum computer development challenges describes the problems encountered in quantum computer development, which currently limit the development of larger quantum computers.

Interviewees believe that scalability, noise levels and error correction are the major challenges in developmet of the quantum computer. In older quantum computers, qubit volumes have been higher, but in newer qubits the quality is better. When discussing quantum computers, people usually talk about the number of qubits, but the main problem is not how many qubits are available, but how to keep them in good quality for a long enough time before decoherence breaks down the information stored in the qubits. The biggest problem with today's quantum computers is seen as operational noise, which is perceived as an engineering problem to reduce. Although there will always be some noise in the physical qubits, there is a need to push the noise level below a certain threshold in order for the qubits to be usable. After that, the error rate of qubits can be reduced using theoretical methods such as error correction. A sufficient noise level depends on the implementation of the quantum computer. Error correction can be achieved by representing one logical qubit by several physical qubits. A lot of work is being done to improve the noise level of qubits. Current quantum computers of the Noisy intermediate Scale Quantum computing era are not yet capable of breaking the encryption of the public key.

A requirement for the implementation of a viable quantum computer is a sufficient number of qubits. Error correction may require hundreds of qubits to represent a single logical qubit, with a much higher overhead than classical correction methods. So far, there has been no success in building a physical quantum computer large enough to test error correction. The most mature state of maturity for quantum technologies is that noise and errors can be pushed down sufficiently and the quantum state is maintained long enough to complete the quantum algorithm with sufficiently large parameters.

One of the interviewed informants pointed out that comparing quantum computers based on different implementations is sometimes difficult. To describe the power of a quantum computer, a quantity called the quantum volume has been developed. Quantum volume includes the number and noise level of qubits. The lower the noise level of a quantum computer, the higher the quantum volume. However, quantum volume does not tell the whole truth about the efficiency of a quantum computer.

One of the key features of a quantum computer, which quantum volume does not take into account, is how long it takes to perform a single operation. Quantum volume ignores performance, which is why developers of ion-based machines such as IonQ and Honeywell prefer it. Ion-based quantum computers operate at significantly slower speeds than superconducting machines, which have lower noise levels. Quantum machine runs are typically repeated several times and the results of the runs are used to produce statistics from which the final result can be interpreted. If the program is run several times, the effect of slowness is also multiplied.

A limitation of current quantum computers is condidered to be the coupling of qubits to each other. In order to perform universal computation on qubits, the system must be able to perform operations on two qubits. The coupling of qubits affects which qubits the operations can be done between. Different types of couplability are required for different quantum gates. There are differences in coupling depending on the quantum computer implementation. The qubits of machines based on ions are fully coupled, allowing the operation to be done between any two qubits. Not all qubits of superconducting machines are connected. For operations, the qubits must be moved next to each other which causes latency, increases noise and the possibility of errors.

4.3 Motivation to develop a quantum computer

The theme aims to describe motivations and reasons for developing quantum computers. An interesting question for research is whether breaking the public key is sufficient motivation to develop a quantum computer.

Calculating Shor's algorithm and breaking a public key is not seen as the primary motivation for developing a quantum computer. Funding for the development of the quantum computer will come from other applications and the resulting technology may be used to calculate Shor's algorithm. It is likely that a public actor will first develop a viable technology on a small scale. Once the technology is proven scalable, an entity with sufficient capital and resources can develop a quantum computer capable of breaking the public key, something universities cannot afford. On the other hand, breaking the public key was also seen as a reason to develop a quantum computer because Shor's algorithm is the most famous and one of the only algorithms known to be able to perform exponentially faster on a quantum computer than on a classical one. It was questioned whether the benefits of breaking RSA is sufficient reason to develop a quantum computer, especially since most of the protection of important information will shift to some secure method when the quantum computer becomes a reality. Realistic applications for the use of quantum computing are seen in areas such as utilizing increasing computing capacity, simulating quantum mechanics for quantum chemistry, studying protein folding in pharmaceutical research, pattern recognition, artificial intelligence and machine learning in a quantum context. Quantum computer applications are also created during development and when the machine is completed, when its characteristics become better known. It is comparable to a classical computer whose development did not anticipate what forms a computer could take or what everything it is used for today. The very fact that we want to prove the feasibility of a quantum computer, the promotion of science, the development of engineering research and skills is seen as a reason to develop a quantum computer.

The motive for breaking the RSA is seen as the de-encryption of a public key in relation to governmental information exchange. Most of the usefulness of encrypted information on the internet becomes obsolete before encryption can be broken. Breaking authentication and non-repudiation is not considered so important. On the other hand, public key decryption gets more hype than what its true meaning really is.

4.4 Estimated timeframe for the realisation of the quantum threat

For the secure use of public key cryptography, it is important to understand when a quantum computer is able to break the encryption. This theme examines the assessments of the experts interviewed on the timetable for the realisation of the quantum data computer.

According to the estimates of current quantum computer developers, the development of machines will continue to progress rapidly. The evolution of the quantum computer is progressing in jumps, new insights and new technologies are being developed that will move forward with in a jumps. For example, a recent paper has published a study in which the number of qubits required by Shor's algorithm has been reduced significantly from the previous estimate by utilising quantum memory. The development of a quantum computer was compared to the development of artificial intelligence that began in the 60s, where there have been periods of intense hype going forward until it hits a wall. After this, there may be a long period of silence until someone makes another breakthrough and things move forward again for a while. There is a lot of hype and activity going on in quantum computers at the moment. The plans of the developers of quantum computers are bold. Currently, quantum computers have a capacity of approximately 100 qubits. In the near future, the number of qubits should increase to thousands, tens of thousands and be in one million qubits before the end of the decade.

All interviewees agreed that the threat of a quantum computer to public key cryptography is realistic, at least for information that needs to be encrypted for a long time. This view was justified by the fact that the current development of the quantum computer is so strong and the scientific community has strong opinions about its realisation. Estimating when a quantum computer will break the RSA key is difficult because potential problems could delay development for several years. The interviewees' estimates of the implementation schedule were placed in a 10-year window: A quantum machine capable of breaking a public key is not expected to be realised at least within the next five years, but it is estimated that it will be completed in the 2030s or early 2040s. It is very possible that exponentially evolving technologies may surprise forecasters. According to this prediction, the quantum computer performs exponential acceleration of development, making the exponential model too slow. The exponential forecast model works for classical technology, where the transistor density increases with a specific formula that is exponential. If the density of qubits increases at the same rate, the growth is twice as exponential, making development even faster. There may also be surprising breakthroughs in the development of algorithms used by quantum computers. Breaking the Elliptic-curve cryptography key is likely to occur first, as the amount of qubit it requires is somewhat lower.

4.5 Quantum computer threat

The Quantum computer threat theme describes how a quantum computer threatens public key cryptography and what kind of data is affected.

The threat to the quantum machine is seen as its ability to solve the underlying mathematical problems of cryptoprimitives, such as discrete logarithms and factorization of integers. The threat posed by the quantum machine is also seen as a perverse threat, with new methods being used to protect against it that may not be as well researched or are poorly implemented. Poorly implemented solutions may cause short-term weaknesses in new algorithms before they can be fixed.

Protecting against the threat of a quantum machine is affected by the timeframe of the quantum machine's realisation. The threat scenario is different if it is to protect against an attacker with sufficient capability and quantum capacity in the near future compared to a threat that is to prepare for a possible quantum machine threat that may materialise in the future. The threat is also affected by what is done with public key encryption, whether it is used to exchange long age secrets over a radio link, where a third party can record the traffic and decrypt it later, making the probability of the threat high. In another contrasting example, the session authentication keys are exchanged, but breaking them later does not matter because the session is already expired.

The most vulnerable to the threat posed by a quantum computer is high-security communication over a medium that someone can listen and intercept to. Examples of such traffic include diplomatic or banking transactions, which rely on the confidentiality of communications and may contain long-standing secrets. In the beginning, quantum computers will be only a few in numbers and will be valuable, probably worth several million to billions. The processing time of an expensive quantum computer should only be used to process the most relevant information.

The debate about breaking a public key with a quantum computer - also called crypto apocalypse - is considered more hype than its true meaning will be. Rather, it is considered a disturbance, but since the threat is known well in advance, there will be time to react in advance. Preparing for a threat requires studying and developing public key methods and updating systems. It is necessary to develop a new foundation that typically also creates new innovations in cryptology. Although Shor's algorithm poses a clear threat to public key cryptography, the quantum computer's potential is seen as greater than the threat it poses.

Opinions were divided on the use of quantum technology for key distribution. Quantum key distribution (QKD) already has commercial implementations and infrastructure is being built around the world. Quantum key distribution shows clear benefits and has its own applications. QKD's importance to data transfer protection is no longer so great because PQC implementations solve protection more flexibly and are more cost effective.

The rapid realisation of a quantum computer in the present would surprise an unprepared society and cause real chaos for a moment, because computing could no longer be trusted and no updates or fixes are yet available. A low-probability but high-risk scenario would be that a Microsoft-type topological quantum computer could be made to work on a large scale. If a small country can get hold of the technology and manage to keep it secret, it has the potential to benefit politically, commercially and militarily.

Two different ways of breaking the public key are identified, one of which is done in secret from the public. This option is likely to be the goal of governmental actors, allowing them to be the first to exploit the quantum computer and gain capabilities that others do not have. A working quantum computer is not reported if it is developed for military or government use. The intelligence sector is considered to be warming inwards and, by its very nature, covert, so reactions from the quantum machine may not be visible to the public eye. It is likely that governmental actors do not yet have the technology capable of breaking the public key, because quantum technology is still at such an early stage, and governmental actors cannot be so far ahead of private programmes. The second option, where the developer of the first public key crypto-threatening quantum computer is a public actor, a company, a university, or a collaboration between them. Development is carried out transparently, it is known how it is progressing and it is possible to predict, at least to within a few years of accuracy, when the encryption of the public key will be broken.

Developments are closely monitored behind closed doors. So far, we are still a long way from the implementation of a quantum computer using Shor's algorithm.

4.6 Protecting against quantum threat

This theme describes different ways to prepare for the threat of a quantum computer.

Many people see a quantum machine as a very distant thing. For companies and products, quantum capability is seen as an image issue: products to be released in three to five years that use public key cryptography or PKI must also have PQC capability implemented. In general, it was considered important to monitor the development and standardisation of quantum proof algorithms and how they are being deployed. One should keep up with development and at the beginning favor simple and conservative methods.

None of the interviewees can say with certainty that it will one day be possible to build a quantum computer capable of breaking the encryption of the public key. However, there is a desire to prepare for the realisation of the quantum computer by researching and developing quantum secure cryptography, whether or not quantum computers are forthcoming. Preparation should start with a threat assessment and an overview of current procedures, which in large companies can be complex and consist of many different security measures. The big picture makes it easier to decide whether to introduce hybrid algorithms or new PQC algorithms if they seem reasonable. The longer the data is wanted to be protected, the earlier it is needed to start preparing for the threat posed by the quantum computer.

One interviewee considered it a good thing that we are well on the way to preparing for the quantum threat, as the winners of the NIST PQC algorithm competition will be announced within two to three years. He then continues by noting that the worst pitfalls of PQC algorithm development are now beginning to be avoided.

According to the informants, algorithms that participated in the NIST competition can already be studied and implemented if the company or organisation considers that it has sufficient knowledge of the subject matter. After the NIST competition is over, the authorities will start requiring PQC implementations for products, so it is better for safety if something is implemented even if it is not the winning algorithm of the NIST competition. The implementation description in the standard, usually in pseudo-code syntax, is typically not a good and safe implementation and requires further research and development. Algorithms implement new things that have not been used in current methods and are mathematically more complex. A security proof means confidence that the new algorithm is good and secure. Security proofs of algorithms are based on mathematical realities that are difficult to implement in practice on computers. There is a risk of trying to mitigate the problems that arise using different methods, which may cause further problems. The algorithms of the NIST competition are not conceptually equivalent to the algorithms currently in use. For example, the key exchange mechanism does not correspond to encryption, which has to be taken into account in the implementation and it should be remembered that the new algorithm does not replace the existing one-to-one. When implementing algorithms, care must be taken until the algorithms are fully ready. It is predicted that approximately four years ahead of this moment (2021) PQC algorithms will be ready. At the moment, we are still in an interim phase where the threats are real. The algorithm to be implemented can also be a hybrid solution, combining classical and new algorithms. Also embedded components with a long life cycle should be moved well in advance. A lot of hopes are placed on lattice-based algorithms. They have the advantage of consistently moderate performance across multiple applications, tolerable key size as well as support from U.S. authority NSA. Despite its lage key size, the code-based McMcEliece will be used in applications where conservative security is required and performance is not so important.

It is likely that there will be more than one winner in a PQC algorithm competition. NIST has announced that it will publish more algorithms as a family. One of the interviewees believes that the future will show which algorithms will gain popularity. Will there be a general-purpose algorithm, suitable for multiple uses, which will be studied and optimised and will become a de facto standard.

Classical algorithms have been thoroughly studied for a long time but the understanding of quantum algorithms is still limited and based on the fact that no one knows a method that would challenge them. Quantum algorithms have not been proven safe in quantum complexity theory. Cryptologists are needed to develop a good encryption algorithm. In Finland, cryptological research is quite scarce and there are not enough resources to develop algorithms. The development of the encryption algorithm is also a political issue, not just a mathematical one. The impartiality of NIST competitions has sometimes been questioned. NIST has been working to increase the transparency of its competitions and thereby gain credibility for its algorithms. The algorithm proposals submitted to the competitions are made by multinational teams, which reduces the possibility of implementing things in the algorithms that do not get into the public domain. NIST's PQC race has received a lot of academic notices and the algorithms presented are widely studied around the world. The EU could organise a similar competition and perhaps gain confidence in the results within the EU. An EU-level competition would not necessarily receive the same level of scientific attention, and whether the winner would be chosen on the right criteria.

Hybrid methods, using new algorithms with old ones, will be introduced for Internet communications within the next five years. There are indications that the authorities are favouring hybrid algorithms before the NIST standardisation is completed. By combining the elliptic curve and the appropriate Lattice algorithm, we obtain a balanced solution with a classical known robust algorithm and a quantum-resistant algorithm. This is a way to protect against possible unknown weaknesses of new methods, but also to gain experience with new algorithms. The problem with hybrid methods is that they are seen as a performance issue, which is why they are used with high security data and as a temporary solution before the transition to NIST-standardised PQC algorithms. Another problem with the hybrid algorithm is that it complicates the overall algorithm and may introduce new unknown bugs. If the threat of a quantum computer is quickly realised, hybrid methods may provide a fast-deployable, security patch that is used initially for critical systems and later all the way to ordinary Internet users.

4.7 Raising awareness of quantum computing

Raising awareness of quantum computing describes how the quantum computer would affect different sectors of society and how they are aware of the issue. The theme also briefly discusses quantum computing education.

The quantum threat is expected to affect the financial and healthcare sectors where sensitive data such as patient information is processed and stored, as well as industry. These sectors are perceived as conservative and slow to innovate. On the healthcare side, there were also problems that are more important for the sector to solve than the quantum threat. Energy and food supply were not seen as critical sectors for quantum threat.

Quantum threats should be prepared for well in advance, preferably 10-20 years before a quantum machine can possibly break RSA. The preparedness to the threat posed by a quantum computer cannot be expected to be corrected automatically, nor are people experts on the issue. People also have misconceptions about quantum computing, which is understandable given the technical nature of the field. For this reason, quantum consciousness must be maintained in a debate that must be as realistic as possible without unnecessary hype. Through education, awareness of quantum knowledge is transferred to the business world. Special courses in quantum computing are held in upper secondary schools, and quantum computing, for example, has just been added to the curricula of the University of Helsinki and Aalto University. The courses held in upper secondary schools specifically demo quantum mechanics and attract students' interest. The interviewees had no knowledge of courses in quantum computing in the Bachelor's degree programmes. Aalto University's second-year curriculum includes a compulsory course in quantum information, which also covers quantum computation. The course is a concrete part of the curriculum. According to interviewees, quantum awareness is moderately trained in schools and universities.

Information on PQC requirements is available. For example, trainings have been held on the subject, which have involved a wide range of actors from different business areas. Awareness of PQC has been punched through and PQC will be taken into account when developing encryption. Education must take into account future NIST PQC algorithm standards that must be able to be implemented. This requires implementation training and implementation expertise.

5 Conclusions

The first conclusion of this study is that it is very likely that breaking public key cryptography in the future will be done using Shor's algorithm with either an ion trap or a superconducting quantum computer. Shor's algorithm requires 4099 logical qubits to crack the most commonly used 2048-bit RSA key. Error correction may require hundreds of qubits to implement a single logical qubit, which could result in a large total number of physical qubits required to break the RSA key. It is estimated that it would take around 20 million qubits to decrypt 2048-bit encryption.

The most promising technologies for the development of a quantum computer are solutions based on superconductivity or ion traps. Scalability, error correction and high noise levels are seen as the main obstacles to implementing a quantum computer. The first threat to public key cryptography is a general-purpose error-corrected quantum computer.

The second conclusion of the study is that the first quantum computers that threaten the security of a public key are likely to be developed by a well-known player with sufficient resources and already involved in the development process. However, the primary motivation for developing a quantum computer is not to break the encryption of the public key, but other use cases.

The first efficient general-purpose quantum machine is more likely to be developed by a company, a university, or a joint project between them than by a governmental actor. It is possible that the principle of a scalable quantum computer will be developed by a university and a larger player with sufficient resources will develop a more powerful quantum computer capable of challenging even public key cryptography.

The main motive for the development of quantum computing is seen as to utilise the increase in computing capacity, simulating quantum mechanics for quantum chemistry, studying protein folding in pharmaceutical research, pattern recognition, artificial intelligence, and machine learning in a quantum context. As quantum computers evolve, new applications are also being identified.

Quantum computing is expected to continue to develop rapidly in the future. The third conclusion of the study is that a quantum computer capable of cracking the 2048-bit RSA key will be implemented in about 15 years. Implementation may be faster than estimated due to the exponential acceleration of quantum computing. The quantum computer that threatens public key cryptography is expected to become a reality in the 2030s or early 2040s.

The fourth conclusion of the study is that the best way to protect public key cryptography against the threat of a quantum computer is through developing quantum secure protocols. The most vulnerable to the threat posed by a quantum computer is high-security communication over a medium where someone can intercept and record the communication. Information that is wanted to be kept encrypted for long periods of time is also at risk. Preparing for the threat of quantum computing to public key cryptography solutions should be started well in advance. The threat to public key cryptography posed by quantum computers is real, but it can be protected against.

However, the threat posed by the quantum computer to public key cryptography was more as a disruption than a threat because NIST's PQC algorithm competition is well underway, and the results of the competition are expected within a couple of years. The fear is that there will be weaknesses in the implementation of algorithms that compromise security. Hybrid algorithms combining classical and PQC algorithms are seen as a likely transitional solution.

People often have misconceptions about quantum computing, which is perfectly understandable due to the technicality of the field. Preparing for the coming of a quantum computer is about sharing accurate and unvarnished information with people. Schools have an important role to play in transferring quantum skills to businesses. Quantum education is already taught in secondary schools and universities.

6 Discussion

6.1 Discussion of results

This thesis focuses on describing the threat posed by quantum computing to public key cryptography and how to protect against the threat. The impact of quantum computing on symmetric encryption and the methods of quantum encryption are excluded. The study also does not describe in depth how a quantum computer works from a mathematical point of view. However, it is essential to understand the basics of how a quantum computer works and what it can and cannot do.

The first research question is how a quantum computer breaks public key cryptography. It is very likely that breaking public key cryptography with a quantum computer will succeed in the future. This conclusion is supported by the fact that all informants interviewed for the study believe that an efficient error-corrected general-purpose quantum computer is feasible. A number of different players already have functional quantum computers. Today's universal quantum computers are small, about 15-130 qubits, and do not yet pose a threat to the security of the RSA key. Annealing Quantum processor-based computers have already been presented with implementations of 5760 qubits, but they are not general-purpose and are most effective in optimisation problems and thus do not threaten public key cryptography. Breaking a 2048-bit RSA key using Shor’s algorithm requires a general-purpose quantum computer with about 4000 error-corrected logical qubits.

Informants interviewed for this study estimate that ion trap and superconducting qubit-based technologies are currently the most promising for the implementation of a quantum computer. The relatively recent studies discussed in the literature review also confirm the advantage of the same technologies. Both interviews and previous studies rated topological qubit-based technologies as a black horse, but a breakthrough in research could make it a winner in the quantum computing race.

The answer to the second research question, who will develop the first quantum computer powerful enough to break public key cryptography, and what is the motivation for development, is a little more complex. The question may seem irrelevant, what does it matter who develops the quantum computer? When the question is put in the context of the research, the threat posed by the quantum computer to public key cryptography, it is understood that it affects the visibility of progress in development. The progress of public research projects can be monitored, and it is possible to know in advance when they will start to threaten the encryption of the public key. There is no visibility of the progress of secret projects, and there is no way of knowing for sure whether an actor is already in possession of an advanced quantum computer today.

Based on the results of this study, the first quantum computers that threaten the security of a public key are likely to be developed by a well-known player with sufficient resources and already involved in the development process. Those interviewed for the study naturally have no knowledge of quantum computers, which may be developed in secret from the public. The interviewees' opinion is that the developer of the first quantum machine that threatens the security of public key cryptography is more likely to be a company, university, or their joint venture than a government actor.

Informants did not see breaking public key cryptography as the primary motivation for developing a quantum computer but were thought to be motivated by general interest, such as quantum chemistry, pharmaceutical research, artificial intelligence and machine learning. However, it is true that the ability of a quantum computer to break public key cryptography will be of interest to many actors who will use a generic quantum computer when its capability reaches a sufficient level.

It is difficult to predict the exact timing of the implementation of a quantum computer that breaks the encryption of the public key. The answer to the third research question, when a quantum computer breaks the public key cryptography, is that a quantum computer capable of cracking a 2048-bit RSA key will be implemented in about 15 years. The informants interviewed for the study expect the quantum computer to become a reality within 10-20 years. In previous studies, such as the quantum threat timeline report 2020, the majority of respondents predict that a quantum computer will be capable to factor 2048 bits of the RSA key in about 20 years (Mosca & Piani, 2021, 23-29).

Why is the quantum crypto break happening in 15 years, why not in 5 or 20 years? The likely answer to the question is that nobody knows the exact date yet, so 15 years is a safe answer because it is not too close but it's far enough away. We know for sure that current technology is not mature enough to implement a sufficiently powerful quantum computer in the next couple of years. On the other hand, so much is being invested in the development of quantum computers today that it is likely that significant steps will be made in the next 10-20 years.

Developers of quantum computers have already declared that they have achieved quantum supremacy, where a quantum computer can perform a task faster than a classical computer. The calculations used to achieve the claimed quantum supremacy have been simple compared to breaking a public key using Shor’s algorithm. Quantum machine manufacturers have presented schedules in which the number of qubits in quantum computers will increase rapidly in the future. The rapid development of quantum computing is justified by doubly exponential rate of development due to its quantum nature. The study identified noise reduction and error correction as the main challenges in quantum computing development. It is possible that the development of a quantum computer will slow down due to some fundamental problem.

The answer to the last research question, what are the methods to protect public key cryptography against the threat posed by quantum computers, is that the best way to protect public key cryptography against the threat of a quantum computer is through developing quantum-safe protocols. But developing protocols alone is not enough: it is needed to start preparing for quantum threats early enough. The threat posed by a quantum computer against public key cryptography should be assessed using a threat assessment method and the best protection chosen on a case-by-case basis. Based on research interviews, the threat posed by a quantum computer is not considered intolerable because the development of quantum-safe algorithms is well under way. The NIST PQC competition standard draft release is expected to take place between 2022 and 2024. It has been suggested that one should wait for the announcement of the winner of the competition before starting to implement the algorithms (Grimes, 2019, 164). Two of the interviewees see no obstacle to starting to implement the algorithms proposed in the competition if the implementer has sufficient understanding and know-how. The operating principles of PQC algorithms differ from the traditional algorithms currently in use. The requirements of the new algorithms shall be carefully implemented. The informant interviewed for the study raised the risk that at least at the beginning there may be errors in the implementation of algorithms that compromise data security. Experts suggest that hybrid algorithms, which use both the traditional and PQC algorithms together, are a viable option for the transition period.

Although the realisation of a powerful general-purpose quantum computer is still theoretical and will probably not happen for another ten years, perhaps several decades, the threat it poses must be recognised. The PQC algorithms now under development will be able to protect the information after it is implemented in products and solutions. Use cases where data is encrypted using public key for long periods of time and data is transferred in encrypted form over a shared transmission medium may already today be vulnerable to the threat posed by a quantum computer. The threat posed by a quantum computer should be taken into account in the design of solutions that are difficult to update afterwards, such as satellites or some IoT devices. The question arises as to how to protect against the threat of a quantum computer right now. Quantum-safe methods have already been presented in the NIST PQC competition. However, they have not yet been standardised or implemented in products and solutions on the market. Hybrid algorithms for transition protection are also not yet widely available. At the moment, we are at a stage where the solution seeking extreme quantum safety must rely, for example, to the exchange of symmetrical keys by courier or to utilise methods such as Quantum key distribution (QKD). Often neither of the methods mentioned earlier makes sense because of usability or cost. Those using long-term public key cryptography are currently in a difficult state waiting for quantum-safe algorithms because there are no ready-made solutions that are suitable for everyone.

The study also revealed that in the future we will need experts who can implement new PQC algorithms. Quantum computing is already taught in secondary schools and universities and the skills are expected to be transferred to businesses. Increasing knowledge in quantum computing will place new demands on education programmes at different levels of education.

6.2 The reliability of thesis

Chapter 2.6 Reliability assurance and ethics describes the methods used to ensure the credibility and reliability of research results. This chapter aims to assess the success of the research and the reliability of the results.

The reliability of scientific research is measured by using commonly used indicators of validity and reliability. Validity refers to doing the right things, including designing the study and doing the data analysis correctly. Reliability is used to assess the implementation of the research (Kananen, 2017, 174-175).

The reliability/authenticity of the study was ensured by documenting the implementation of the study as accurately as possible. In this case, an external evaluator (member checking) can assess the reliability of the work's feasibility, the integrity of the reasoning path and the correctness of the conclusions.

The literature review discusses previous studies that have been referred to when discussing the results of the research.

The research data was collected by interviewing three informants. As the number of observation units was relatively small, it is questionable whether the saturation is sufficient. On the other hand, all the key informants requested participated in the interviews, representing the main sectors of the PQC study area in a comprehensive way.

Reactivity or contamination was avoided by asking research questions and discussing them in a way that the researcher did not direct or lead the informants.

During the analysis phase of the study, the researcher asked himself whether the themes of the interview should have been described and delimited more precisely or whether the interviewer should have guided the direction of the interviews more decisively. Now the informants approached the themes from different angles, leaving some key aspects of the themes less discussed in some interviews. Due to the limited number of interviews, it was not possible to compare the opinions of all interviewees at the analysis phase. In these cases, the findings were compared with previous studies discussed in the literature review in order to confirm the claims made and interpretations of the phenomenon. This can also be seen as a richer interpretation made possible by qualitative research compared to, for example, quantitative research. Now, the interviewees approached the topics from their own areas of expertise, resulting in a broad and holistic view of the research topic.

Quantum mechanics and quantum computing are very complex subjects, and the researcher had no previous educational background in the subject. As a result, it is possible that the researcher's analyses may contain errors of interpretation or incorrect conclusions due to the fact that the researcher has examined the topic through his own limited perspective. Efforts were made to reduce this error already at the design phase of the study by keeping the level of abstraction of the study high and by excluding mathematical proofing, among other things.

Criterion validation, i.e. the use of the results of other studies to support our own research results, has been used wherever possible, i.e. where previous research results have been available.

The reliability of the study was improved by using material triangulation. The interpretations from the interviews were compared with the previous findings discussed in the literature review. The researcher's own interpretations were given confidence and reliability if other studies had already produced the same conclusions.

6.3 Suggestions for development and further research topics

The study described the current state of PQC algorithms. Further research is needed to understand how the PQC algorithms in the final round are suitable for real-life applications. Can they directly replace existing algorithms in applications or is it necessary to change the way applications work? How the key sizes and speed of new algorithms affect their usability? Can new algorithms also be used in hardware-based implementations? Full utilization of public key cryptography and Public Key Infrastructure (PKI) also requires hardware support for the algorithms used. In a variety of devices, the key associated with public key encryption needs to be protected by hardware-based implementations so that unauthorized copies of the private key cannot be made. The Certification Authority's (CA) private key is the foundation of trust for the entire system and its exposure should be protected as well as possible. In a trusted CA solution, private keys of CA certificates are typically protected by Hardware Security Module (HSM) devices. So, it is not enough that only the CA application supports PQC algorithms, hardware must also be supported. It would be important to understand what requirements the PQC algorithms place on the hardware, and whether there is already existing support for the algorithms.

Hybrid algorithms are planned to provide a cross-over solution for the transition from the current algorithms to pure PQC algorithms. Some implementations of hybrid algorithms already exist, but official specifications are not yet available. As noted in the findings of the study, there are countless combinations of classical and PQC algorithms. There is a need for further research-based recommendations on hybrid algorithms suitable for the most common applications and their potential limitations.

References

Aaronson, S. 2013. Quantum computing since democritus. Cambridge: Cambridge University Press. https://janet.finna.fi/Record/jamk.993628760206251.

Alagic,G, Alperin-Sheriff, J. Apon, D. Cooper, D. Dang, Q. Kelsey, J. Liu, Y-K. Miller, C Moody, D. Peralta, R. Perlner, R. Robinson,A. Smith-Tone, D, July 2020, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8309

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., . Martinis, J. M. 2019. Quantum supremacy using a programmable superconducting processor. Nature, 574, 7779, 505-510. doi:10.1038/s41586-019-1666-5. https://doi.org/10.1038/s41586-019-1666-5.

Attride-Stirling, J. 2001. Thematic networks: An analytic tool for qualitative research. Qualitative Research : QR, 1, 3, 385-405. doi:10.1177/146879410100100307. https://janet.finna.fi/PrimoRecord/pci.cdi_crossref_primary_10_1177_146879410100100307.

Band, Y. B.Avishai, Y. (2013). Quantum mechanics with applications to nanotechnology and information science. Academic Press.

Baldwin, L. 2018. Research concepts for the practitioner of educational leadership. Boston: BRILL. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=5570533.

Ball, P. 3.12.2020. Physicists in China challenge Google's 'quantum advantage'. Nature. https://www.nature.com/articles/d41586-020-03434-7

Basu, K., Soni, D., Nabeel, M. & Karri, R. NIST post-quantum cryptography- A hardware evaluation study. https://eprint.iacr.org/2019/047.pdf:

Bednorz, J. G. & Müller, K. A. 1986. Possible highTc superconductivity in the Ba−La−Cu−O system. Zeitschrift Für Physik B Condensed Matter, 64, 2, 189-193. doi:10.1007/BF01303701. https://doi.org/10.1007/BF01303701.

Bernhardt, C. 2019a. Quantum computing for everyone. https://janet.finna.fi/PrimoRecord/pci.cdi_askewsholts_vlebooks_9780262350945.

Bernhardt, C. 2019b. Quantum computing for everyone. The MIT Press. http://common.books24x7.com.ezproxy.jamk.fi:2048/book/id_145580/book.asp.

Bernstein, D. J., Lange, T. & Peters, C., 2008. Attacking and defending the McEliece cryptosystem. Springer International Publishing.

Blahut, R. E. (2014). *Cryptography and secure communication*. Cambridge University Press.

Boyles, T. 2010, CCNA Security: Study Guide, Sybex,ISBN:9780470527672

Braun, V. & Clarke, V. 2014. What can "thematic analysis" offer health and wellbeing researchers? Null, 9, 1, 26152. doi:10.3402/qhw.v9.26152. https://doi.org/10.3402/qhw.v9.26152.

Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 2, 77-101. doi:10.1191/1478088706qp063oa. http://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa.

Brown, J. 2001. Quest for the quantum computer. New York [u.a.]: Touchstone.

BuildWith. 5.2.2022. SSL Usage Distribution on the Entire Internet. https://trends.builtwith.com/ssl/traffic/Entire-Internet.

Burke. Fintan. August 2020. Qubit to get ahead: Germany is racing to catch up with the quantum revolution. https://sciencebusiness.net/news/qubit-get-ahead-germany-racing-catch-quantum-revolution

Business Finland, 01.06.2020, Post-Quantum Cryptography project develops quantum-secure encryption technology. Business Finland. https://www.businessfinland.fi/en/whats-new/news/2020/post-quantum-cryptography-project-develops-quantum-secure-encryption-technology

Carter, Ash. Manley Laura, 2020. Tech factsheets for policymakers. Quantum Computing. Belfer Center for Science and International Affairs Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/2020-10/tappfactsheets/QC.pdf

Charles, D., Goren, E. & Lauter, K. 2006. Cryptographic hash functions from expander graphs.

Chen, L., Moody, D. & Liu, Y. 2017. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf:

Childs, A., Jao, D. & Soukharev, V. 2014. Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology, 8, 1, 1–29. doi:10.1515/jmc-2012-0016. http://dx.doi.org/10.1515/jmc-2012-0016.

Corbin, J. & Strauss, A. L., 2008. Basics of qualitative research : Techniques and procedures for developing grounded theory. 3rd ed p. Los Angeles: Sage. https://janet.finna.fi/Record/jamk.991663224806251.

Couveignes, J. 2006. Hard homogeneous spaces.

Creswell, J. W. 2009. Research design : Qualitative, quantitative, and mixed methods approaches. 3rd ed p. Los Angeles: SAGE.

Creswell, J. W. & Poth, C. N., 2018. Qualitative inquiry & research design : Choosing among five approaches. Fourth edition. International student edition p. Los Angeles: SAGE Publications, Inc. https://janet.finna.fi/Record/jamk.993328924806251.

Crocckett, E., Paquin, C. & Stebila, D. 2019. Prototyping post-quantum and hybrid key exchange
and authentication in TLS and SSH. IACR Cryptol. ePrint Arch., https://ia.cr/2019/858.

Cross, A. W., Bishop, L. S., Sheldon, S., Nation, P. D. & Gambetta, J. M. 2019. Validating quantum computers using randomized model circuits. Physical Review A, 100, 3, doi:10.1103/physreva.100.032328. http://dx.doi.org/10.1103/PhysRevA.100.032328.

Denzin, N. K. & Lincoln, Y. S., 2018. Handbook of qualitative research. 5th p. SAGE Publications, Inc.

Deutsch, D. 1998. The fabric of reality. East Rutherford: Penguin Publishing Group. https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=6048486.

Dierks, T. & Rescorla, E. 2008. The transport layer security (TLS) protocol version 1.2.

Ding, J. & Schmidt, D. 2008. Rainbow, a new multivariable polynomial signature scheme. Applied cryptography and network security. 164-175. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/11496137_12.

Divincenzo, D. P. 2000. The physical implementation of quantum computation. Fortschritte Der Physik, 48, 9-11, 771-783. doi:10.1002/1521-3978(200009)48:9/113.0.CO;2-E. https://janet.finna.fi/PrimoRecord/pci.wjAID-PROP771%3E3.0.CO;2-E.

Drozdov, A., Eremets, M., Troyan, I., Ksenofontov, V. & Shylin, S. 2015. Conventional superconductivity at 203 kelvin at high pressures in the sulfur hydride system. Nature, 525, 73. doi:10.1038/nature14964.

Duran, R. P., Eisenhart, M. A., Erickson, F. D., Grant, C. A., Green, J. L., Hedges, L. V., Schneider, B. L. 2006. EDUCATIONAL RESEARCHER-2006-AERA highlights-33-40. American Educational Research Association. Educational Researcher, 35, 6, 33-40. doi:https://doi.org/10.3102/0013189X035006033.

EARNSHAW, S. 1842. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. Transactions of the Cambridge Philosophical Society, 7, 1, 97.https://search-proquest-com.ezproxy.jamk.fi:2443/docview/1310503851.

Entrust, 2021, 2021 Global PKI and IoT trends study. Ponemon Institute. https://www.entrust.com/-/media/documentation/reports/2021-pki-iot-trends-study-executive-summary-re.pdf

Feo, L. D., Jao, D. & Plût, J. 2011. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.

Foot, C. J. 2005. Atomic physics. Oxford: Oxford University Press, Incorporated. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=422882.

Freedman, M. H., Kitaev, A., Lrsen, M. J. & Wang, Z. 2001. Topological quantum computation. v2, https://arxiv.org/abs/quant-ph/0101025.

G. E. Moore. 2006. Cramming more components onto integrated circuits, reprinted from electronics, volume 38, number 8, april 19, 1965, pp.114 ff. doi:10.1109/N-SSC.2006.4785860.

G. Seroussi.Elliptic curve cryptography. Paper presented at the - 1999 Information Theory and Networking Workshop (Cat. no.99EX371), 41. doi:10.1109/ITNW.1999.814351.

Gerard Higgins. 2019. A single trapped rydberg ion. Cham: Springer. doi:10.1007/978-3-030-33770-4. https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=5966964.

Gidney, C. & Ekerå, M. 2019. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. https://arxiv.org/abs/1905.09749v2.

Google. 23.11.2019. Quantum Supremacy Using a Programmable Superconducting Processor. https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

Goppa, V. D. 1970. A new class of linear correcting codes. Problemy Peredachi Informatsii, 6(3), 24-30.

Gribbin, J. 2014. Computing with quantum cats : From colossus to qubits. Amherst: Prometheus. https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=5890858.

Grimes, R. A. 2019. Cryptography apocalypse: Preparing for the day when quantum computing breaks today's crypto. John Wiley & Sons. http://cds.cern.ch/record/2705137.

Grobman, S. 2020. Quantum computing's cyber-threat to national security. Prism : A Journal of the Center for Complex Operations, 9, 1, 52-66.http://ezproxy.jamk.fi:2048/login?url=https://www.proquest.com/scholarly-journals/quantum-computings-cyber-threat-national-security/docview/2455929484/se-2?accountid=11773.

Haque, A. & Sumaiya, S. 2017. An overview on the formation and processing of nitrogen-vacancy photonic centers in diamond by ion implantation. Journal of Manufacturing and Materials Processing, 1, 1, doi:10.3390/jmmp1010006. https://www.mdpi.com/2504-4494/1/1/6.

Hartnett, K. 2019. A new law to describe quantum computing's rise? Quantamagazine, https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/.

Heisenberg, W., 1925, Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen, European Physical Journal, DOI:10.1007/978-3-642-61659-4_26

Herzberg, A. 2005. On tolerant cryptographic constructions. Topics in cryptology – CT-RSA 2005. 172-190. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-540-30574-3_13.

Hidary, J. D. 2019. Quantum computing: An applied approach. Springer International Publishing. doi:https://doi.org/10.1007/978-3-030-23922-0. http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9783030239220.

Hirsjärvi, S. & Hurme, H., 2015. Tutkimushaastattelu : Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press. https://janet.finna.fi/Record/jamk.992838484806251.

Howitt, D. & Cramer, D., 2017. Research methods
in psychology. 5th p. Pearson Education Limited.

Huguenin-Dumittan, L. & Vaudenay, S.FO-like combiners and hybrid post-quantum cryptography. Paper presented at the Cryptology and Network, 225-244.

IBM. 16.11.2021. IBM Unveils Breakthrough 127-Qubit Quantum Processor. https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.

"Introduction to the Quantum Flagship", Quantum Flagship. March 2, 2022, https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/

Jäck, B., Xie, Y., Li, J., Jeon, S., Bernevig, B. A. & Yazdani, A. 2019. Observation of a majorana zero mode in a topologically protected edge channel. Science, 364, 6447, 1255–1259. doi:10.1126/science.aax1444. http://dx.doi.org/10.1126/science.aax1444.

Josephson, B. D. 1962. Possible new effects in superconductive tunnelling. Physics Letters, 1, 7, 251-253. doi:https://doi.org/10.1016/0031-9163(62)91369-0. https://www.sciencedirect.com/science/article/pii/0031916362913690.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu. https://janet.finna.fi/Record/jamk.993276444806251.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas : Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu. https://janet.finna.fi/Record/jamk.992835104806251.

Kiviharju, M. 2021. Refining mosca's theorem: Risk management
model for the quantum threat applied to IoT
protocol security.

Kloeffel, C. & Loss, D. 2013. Prospects for spin-based quantum computing in quantum dots. Annual Review of Condensed Matter Physics, 4, 1, 51–81. doi:10.1146/annurev-conmatphys-030212-184248. http://dx.doi.org/10.1146/annurev-conmatphys-030212-184248.

Kuula, A, 2011., Tutkimusetiikka, aineiston hankinta, käyttö ja säilytys, Ouuskunta Vastapaino, ISBN 978-951-768-513-9

Kvale, S. 1996. InterViews. Thousand Oaks [u.a.]: Sage.

Lange, T. 2020. WG 2 SD8 (post-quantum cryptography) -- part 4:
Code-based cryptography.

Lange, T. & Steindwandt Rainer. 2018. Post-quantum
cryptography, 9th international conference, PQCrypto 2018.
doi:https://doi.org/10.1007/978-3-319-79063-3.

Launis, V., Helin, M., Kaisa, S. & Jäppinen, S. 2012. Hyvä tieteellinen käytäntö (HTK). Finnish Advisory Board on Research Integrity.

Lewis, A. M., Ferigato, C., Travagnin, M. & Florescu, E. 2018. The impact of quantum technologies on the EU's future policies: Part 3 quantum computing. Joint Research Centre (JRC), the European Commission's science and knowledge service. doi:10.2760/737170.

Loss, D. & DiVincenzo, D. P. 1998. Quantum computation with quantum dots. Physical Review A, 57, 1, 120–126. doi:10.1103/physreva.57.120. http://dx.doi.org/10.1103/PhysRevA.57.120.

Lyubashevsky, V.Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. Paper presented at the Advances in Cryptology – ASIACRYPT 20, 598-616.

Magesan, E., Gambetta, J. M. & Emerson, J. 2012. Characterizing quantum gates via randomized benchmarking. Physical Review A, 85, 4, 042311. doi:10.1103/PhysRevA.85.042311. https://link.aps.org/doi/10.1103/PhysRevA.85.042311.

Manin, Y. 1980. Computable and uncomputable. Radio, Moscow.

Marshall, M. N. 1996. The key informant technique. Family Practice, 13, 1, 92-97. doi:10.1093/fampra/13.1.92. https://janet.finna.fi/PrimoRecord/pci.cdi_proquest_miscellaneous_78099868.

Mavroeidis, V., Vishi, K., Zych, M. D. & Jøsang, A. 2018. The impact of quantum computing on present cryptography. http://urn.nb.no/URN:NBN:no-75086.

McEliece, R. J. 1978. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

Merkel, S. T., Gambetta, J. M., Smolin, J. A., Poletto, S., Córcoles, A. D., Johnson, B. R., Steffen, M. 2013. Self-consistent quantum process tomography. Physical Review A, 87, 6, 062119. doi:10.1103/PhysRevA.87.062119. https://link.aps.org/doi/10.1103/PhysRevA.87.062119.

Merkle, R. C. 1979. Secrecy, authentication and public key systems.

Merkle, R. C. & Hellman, M. E. 1981. On the security of multiple encryption. Commun.ACM, 24, 7, 465–467. doi:10.1145/358699.358718. https://doi.org/10.1145/358699.358718.

Mikio, N. & Yoshitaka, S., 2014. Quantum information and quantum computing : Proceedings of the symposium. Singapore: World Scientific Publishing Co Pte Ltd. http://ebookcentral.proquest.com.ezproxy.jamk.fi:2048/lib/jypoly-ebooks/detail.action?docID=1069829.

Miles, M. B. & Huberman, A. M., 1994. Qualitative data analysis : An expanded sourcebook. London: Sage. .https://janet.finna.fi/Record/jamk.99283474806251.

Misoczki, R. WG 2 SD8 (post-quantum cryptography) -- part 2:
Hash-based signatures.

Mosca, M. & Piani, M. 2021. Quantum threat timeline report 2020.

Mosca, M. & Piani, M. 2019. Quantum threat timeline report.

National Academies of Sciences, Engineering, and Medicine. 2019. Quantum computing: Progress and prospects. Washington, DC: The National Academies Press. doi:10.17226/25196". https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects.

National Academy of Engineering. 2003. Frontiers of engineering : Reports on leading-edge engineering from the 2002 NAE symposium on frontiers of engineering. Washington, D.C.: National Academies Press. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=3375434.

Oikeusministeriö. 1999. Act on the openness of government activitie . .2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621#a23.6.2005-495.

Padma, T.V. 3.2.2020. India bets big on quantum technology. Nature. https://www.nature.com/articles/d41586-020-00288-x/

Paris, M. & Řeháček, J., 2004. Quantum state estimation. 1 p. Berlin, Heidelberg: Springer. doi:https://doi.org/10.1007/b98673.

Patton, M. Q. 2015. Qualitative research & evaluation methods : Integrating theory and practice. 4th edition p. Thousand Oaks, California: SAGE Publications, Inc. https://janet.finna.fi/Record/jamk.992838304806251.

Peel, K. L. 2020. A beginner's guide to applied educational research using thematic analysis. Practical Assessment, Research, and Evaluation, 25, 2, doi:10.7275/ryr5-k983. https://scholarworks.umass.edu/pare/vol25/iss1/2.

Pelé, Anne-Françoise. 22.1.2021. French President Details €1.8b Quantum Plan. Times Europe. https://www.eetimes.eu/french-president-details-e1-8b-quantum-plan/

Petta, J. R., Johnson, A. C., Taylor, J. M., Laird, E. A., Yacoby, A., Lukin, M. D., . . . Gossard, A. C. 2005. Coherent manipulation of coupled electron spins in semiconductor quantum dots. Science, 309, 5744, 2180-2184. doi:10.1126/science.1116955. http://science.sciencemag.org/content/309/5744/2180.abstract.

Preskill, J. 2018. Quantum computing in the NISQ era and beyond. Quantum, 2, 79. doi:10.22331/q-2018-08-06-79. https://janet.finna.fi/PrimoRecord/pci.cdi_doaj_primary_oai_doaj_org_article_b27bd39720084a80ba9c8e79c469a945.

Preskill, J. 2012. Quantum computing and the entanglement frontier. https://arxiv.org/abs/1203.5813.

Procopio, L. M., Moqanaki, A., Araújo, M., Costa, F., Alonso Calafell, I., Dowd, E. G., Walther, P. 2015. Experimental superposition of orders of quantum gates. Nature Communications, 6, 1, doi:10.1038/ncomms8913. http://dx.doi.org/10.1038/ncomms8913.

Puusa, A. & Juuti, P., 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. 1 p. Gaudeamus.

Rigetti, C., Gambetta, J. M., Poletto, S., Plourde, B. L. T., Chow, J. M., C 'orcoles, A. D., . . . Steffen, M. 2012. Superconducting qubit in a waveguide cavity with a coherence time approaching 0.1 ms. Phys.Rev.B, 86, 10, 100506. doi:10.1103/PhysRevB.86.100506. https://link.aps.org/doi/10.1103/PhysRevB.86.100506.

Rivest, R. 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21, 2, 120-126. doi:10.1145/359340.359342.

https://janet.finna.fi/PrimoRecord/pci.cdi_crossref_primary_10_1145_359340_359342.

Robert G. Burgess. 2003. Field research: A sourcebook and field manual. Taylor and Francis. doi:10.4324/9780203379998. https://www.taylorfrancis.com/books/9781134897506.

Robinson, N. J., Altland, A., Egger, R., Gergs, N. M., Li, W., Schuricht, D., . . . Konik, R. M. 2019. Nontopological majorana zero modes in inhomogeneous spin ladders. Physical Review Letters, 122, 2, doi:10.1103/physrevlett.122.027201. http://dx.doi.org/10.1103/PhysRevLett.122.027201.

Rossi, A. & Gonzalez-Zalba, M. F. 2019. Neven’s law: Why it might be too soon for a moore’s law for quantum computers. The Conversation, https://theconversation.com/nevens-law-why-it-might-be-too-soon-for-a-moores-law-for-quantum-computers-120706.

Rostovtsev, A. & Stolbunov, A. 2006. Public-key cryptosystem based on isogenies.

Saldana, J. 2011. Fundamentals of qualitative research. Cary: Oxford University Press, Incorporated. .http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=665394.

Sherwood, M. H. 2001. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. Nature (London), 414, 6866, 883-887. doi:10.1038/414883a. https://janet.finna.fi/PrimoRecord/pci.cdi_proquest_miscellaneous_72393441.

Shor, P. W.Algorithms for quantum computation: Discrete logarithms and factoring. Paper presented at the doi:10.1109/SFCS.1994.365700. https://janet.finna.fi/PrimoRecord/pci.cdi_ieee_primary_365700.

Silva, V. 2018. Quantum computing: Bending the fabric of reality itself. doi:10.1007/978-1-4842-4218-6_2. https://janet.finna.fi/PrimoRecord/pci.cdi_springer_books_10_1007_978_1_4842_4218_6_2

Silverman, D. 2006. Interpreting qualitative data : Methods for analysing talk, text and interaction. 3. ed p. London: SAGE Publications. https://janet.finna.fi/Record/jamk.991001044806251.

Smart, N. 2016. Cryptography Made Simple. Springer. ISBN:9783319219356

Smart, N. & Lange, T. 2021. POST-QUANTUM CRYPTOGRAPHY current state and quantum mitigation. European Union Agency for Cybersecurity (ENISA). doi:10.2824/92307.

Soltan Agh, M. R., Zukarnain, Z. A., Mamat, A. & Zainuddin, H. 2009. A hybrid architecture approach for quantum algorithms. Journal of Computer Science, 5, 10, 725-731. doi:10.3844/jcssp.2009.725.731. https://thescipub.com/pdf/jcssp.2009.725.731.pdf.

Stanescu, T. D. 2017. Introduction to topological quantum matter & quantum computation. Boca Raton: CRC Press. doi:10.1201/9781315181509. https://www.taylorfrancis.com/books/9781482245943.

Submission Requirements and Evaluation Criteria for the Post-Quantum cryptography Standardization Process. 2016, National Institute of Standards and Technology, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

Susskind, L. 1995. The world as a hologram. Journal of Mathematical Physics, 36, 11, 6377-6396. doi:10.1063/1.531249. https://doi.org/10.1063/1.531249.

Sutor, R. S. 2019. Dancing with qubits, How quantum computing works and how it can change the world. Birmingham ; Mumbai: Packt Publishing.

Swan, M., Santos, R. P. d. & Witte, F., 2020. Quantum computing: Physics, blockchains, and deep learning smart networks. Vol. 2 p. World Scientific. http://cds.cern.ch/record/2743451.

Syrjälä, L. 1994. Laadullisen tutkimuksen työtapoja. Helsinki: Kirjayhtymä. https://janet.finna.fi/Record/jamk.99162864806251.

The National Science and Technology Council. December 2021. NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT’S FY 2022 BUDGET. https://www.quantum.gov/wp-content/uploads/2021/12/NQI-Annual-Report-FY2022.pdf

Thomae, E. 2012. A generalization of the rainbow band separation attack and its applications to multivariate schemes. IACR Cryptol. ePrint Arch., 223.https://eprint.iacr.org/2012/223.pdf.

Thompson, R. 2003. Physics with trapped charged particles : Lectures from the les houches winter school. Singapore: Imperial College Press. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=1647259.

Tuckett, A. G. 2005. Applying thematic analysis theory to practice: A researcher's experience. Contemporary Nurse : A Journal for the Australian Nursing Profession, 19, 1-2, 75-87. doi:10.5172/conu.19.1-2.75. https://janet.finna.fi/PrimoRecord/pci.cdi_pubmed_primary_16167437.

Tuomi, J. & Sarajärvi, A., 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos p. Helsinki: Kustannusosakeyhtiö Tammi. https://janet.finna.fi/Record/jamk.993376414806251.

Valtiovarainministeriö. 2020. Act on information management in public administration. https://www.finlex.fi/fi/laki/alkup/2019/20190906.

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H. & Chuang, I. L. 2001. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414, 6866, 883–887. doi:10.1038/414883a. http://dx.doi.org/10.1038/414883a.

Vasara, Antti. Pursula, Pekka. Rantasalo, Leena. 3.6.2020. Building of Finland's first quantum computer underway and on schedule at VTT, VTT Research. https://www.vttresearch.com/en/news-and-ideas/building-finlands-first-quantum-computer-underway-and-schedule-vtt

Wilhelm, F. K., Steinwandt, R., Langenberg, B., Liebermann, P. J., Messinger, A., Schuhmacher, P. K. & Misra-Spieldenner, A. 2020. Status of quantum computer development. Federal Office for Information Security.

Williams, T. R. 1967. Field methods in the study of culture. New York [u.a.]: Holt, Rinehart and Winston.

Wong, D. 2021. Real-world cryptography. New York: Manning Publications Co. LLC. https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=6766359.

Xu, X. 2019. Strongly secure authenticated key exchange from supersingular isogenies. doi:10.1007/978-3-030-34578-5_11. https://janet.finna.fi/PrimoRecord/pci.cdi_springer_books_10_1007_978_3_030_34578_5_11

Appendices

Appendix 1. Information leaflet on the content of the research interview

Research interview

- **Title of the study:** Post Quantum Cryptography, Impact to the public key cryptography
- **Background:** The research this interview is related to is part of Business Finland's Post-Quantum Cryptography project. Business Finland's Digital Trust program provides the Post-Quantum Cryptography, PQC, project appr. a three million euro funding. The aim of the project is to develop quantum-secure encryption technologies. The objective is to increase Finland's trust capital by utilizing the emergence of new innovations and the growth of business in security and trust solutions and services – from the perspectives of both the solution providers and the users.
- **The purpose of the study:** To describe how a quantum computer works and is able to break the public key cryptography. The goal is to interpret when a quantum computer threat is realized in public key cryptography, what are the methods to protect against it and how the threat should be/have already been considered in advance.
- **Objectives for the interview:** The aim of the interview is to gather material for analysis on key informants opinions and views on the future of the quantum computing and its implications for public key cryptography.
- **Information about the thesis:**
    - School: JAMK University of Applied Sciences
    - Degree Programme: Master’s Degree Programme in Cyber Security
- **Researcher:** Juha Luukkanen, Senior Security Specialist from Insta Defsec Oy Fifteen years of experience in Public Key Infrastructure related issues such as products, managed services and professional services. Has been involved in the implementation of public key cryptography projects requiring high security and availability for both the public and private sectors.
- **Motivation:** It is assumed that quantum computing will have a significant impact on public key cryptography in the future. In connection with his own work, the researcher is interested in what threats quantum computing poses or how it can be exploited. It is also interesting what things should be considered when designing public key cryptography solutions today.
- **Supervisors:**
    - Saharinen Karo, JAMK
    - Janne Lamminmäki, Insta Defsec Oy
- **The method and duration of the interview:** The interview is conducted as a thematic interview, in which the interviewer explains the topic he wants to discuss with the interviewee. The topic is discussed freely without restrictions, after which the interviewer gives a new theme to be discussed. This will continue until all the themes of the interview have been covered. The estimated duration of the interview is 60 minutes. The interview will be conducted in Finnish if there is no justified reason to use English. The themes of the interview were shared with the interviewees in advance so that they could familiarise themselves with the topic
- **Permission to record the conversation:**
  Participation in the interview is confidential. The identity of the interviewees will never be revealed at any stage of the research. The interview will be recorded and transcribed in to written form. After the interview, two backups of the recording will be made and kept on two memory sticks until the interview is transcribed.

Transcribe the interview is carried out by a third party. Upon completion of the thesis, the recordings, transcriptions and other material during the research will be destroyed. After completing the interview, you will have the opportunity to contact the interviewer via email about the interview. I ask for your permission to record the interview and use other material you have submitted for the research purposes of the thesis.

Interview themes

1. BY WHOM, WHY, WHEN, WHERE, AND HOW A QUANTUM COMPUTER BREAKS PUBLIC KEY CRYPTOGRAPHY? WHAT HAPPENS THEN?
2. WHAT DOES THE DEVELOPMENT OF A QUANTUM COMPUTING MEAN FROM A CRYPTOGRAPHIC PERSPECTIVE?
3. HOW POST QUANTUM'S SECURE PUBLIC KEY CRYPTOGRAPHY SOLUTION WILL BE IMPLEMENTED? WITH WHAT CERTAINTY ARE THE SOLUTIONS SAFE IN THE FUTURE AS WELL?
4. TRANSITION TO QUANTUM SECURE PUBLIC KEY CRYPTOGRAPHY METHODS, WHAT TO DO AND WHY?

Appendix 1.: Support material related to theme 4.

Key industries in terms of security of supply:

- Energy supply
- Food supply
- Financial secto
- Industry
- information society
- Logistiics
- Public health care

Source: https://www.huoltovarmuuskeskus.fi/

Themes and support questions

For interviewer use only

1. **BY WHOM, WHY, WHEN, WHERE, AND HOW A QUANTUM COMPUTER BREAKS PUBLIC KEY CRYPTOGRAPHY? WHAT HAPPENS THEN?**
   1.1. What you consider to be the biggest challenge in the development of a quantum computer
   1.2. Describe how you think a quantum computer threatens traditional cryptography methods such as public key cryptography
   1.3. When do you expect the threat of a quantum computer to be realized?
   1.4. Whether the development of a quantum computer will proceed slowly or will occur quickly as a result of some breakthrough
      a) What are the main factors that affect to when a quantum computer is completed?
   1.5. Who develops the first usable quantum computer?
      a) Describe what the first usable quantum computers will be like: whether it is general purpose or made for a specific purpose
      b) Will technology be available to everyone or will it be restricted?
      c) When will it come to the public consciousness?
      d) How long is used before existence becomes public
   1.2. What is the motive for the development of the first quantum computer
      a) How important a motive for the development of a quantum computer is considered to be a breaking of encryption
   1.3. Is the threat posed by a quantum computer to public key encryption realistic?
2. **WHAT DOES THE DEVELOPMENT OF A QUANTUM COMPUTING MEAN FROM A CRYPTOGRAPHIC PERSPECTIVE?**
   2.1. How you estimate that a quantum computer affects the security of public key cryptography
      a) In the near future
      b) In the long term
   2.2. When quantum break occurs, how it affects from the perspective of cryptography solutions: whether it rigs existing implementations or rather opens up new opportunities (1.4)
   2.3. If quantum Supremacy happens quickly by a few actors, how will it affect existing actors and structures?
3. **HOW POST QUANTUM'S SECURE PUBLIC KEY CRYPTOGRAPHY SOLUTION WILL BE IMPLEMENTED? WITH WHAT CERTAINTY ARE THE SOLUTIONS SAFE IN THE FUTURE AS WELL?**
   3.1. How to protect against the threat posed by a quantum computer
   3.2. Should the threat posed by quantum computers to public key encryption methods be considered today and if so, how?
   3.3. What are your thoughts around crypto agility?
      a) Can a hybrid implementation be used to prepare for existing or yet unidentified threats?
   3.4. How do you estimate the results of the NIST PQC Standardization Program will affect the public key cryptography methods used in Finland in the near future and in the longer term?

4. TRANSITION TO POST QUANTUM SECURE PUBLIC KEY CRYPTOGRAPHY IMPLEMENTATIONS: WHAT TO DO AND WHY?

4.1. How organizations or companies should prepare for Post Quantum cryptography

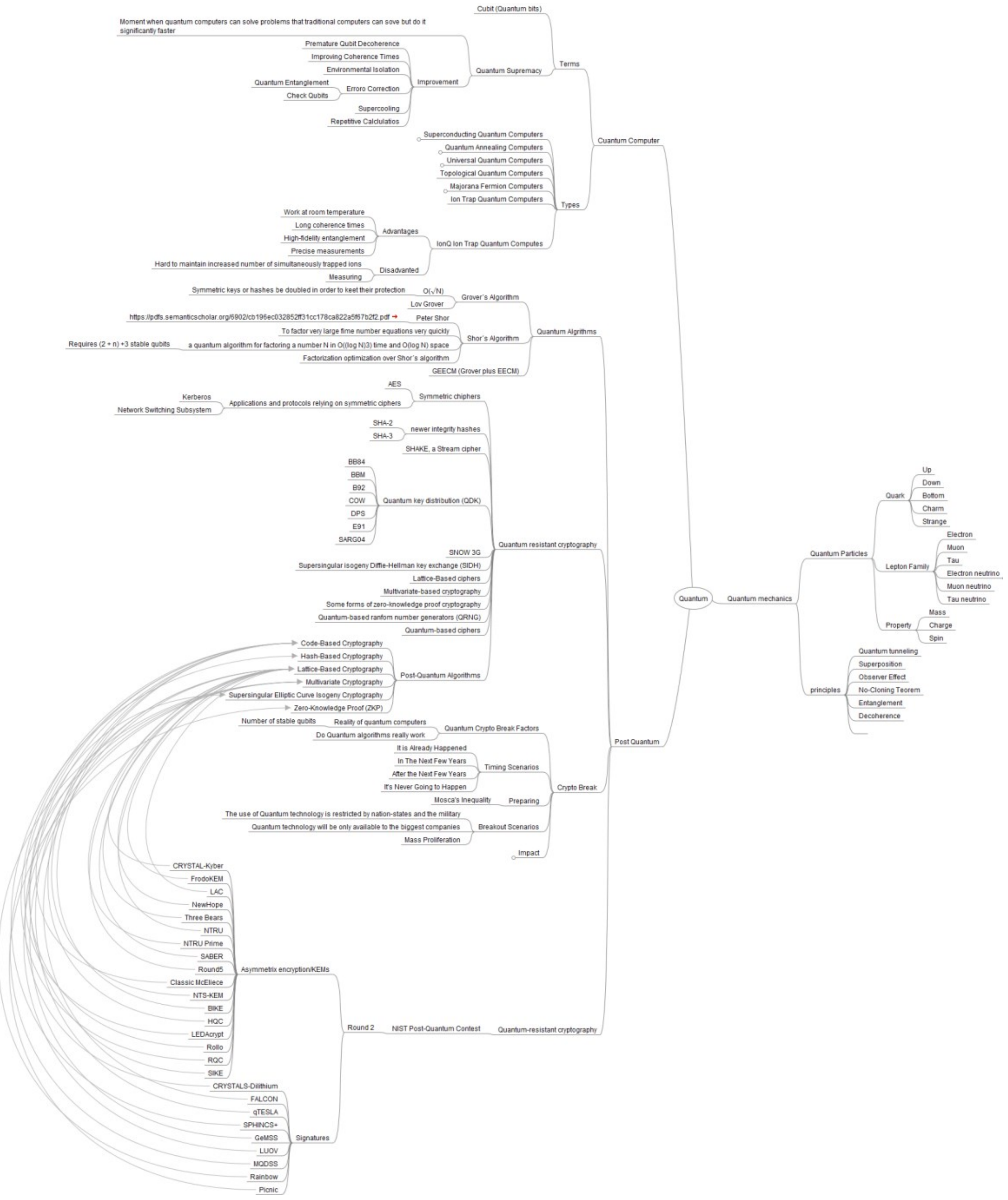
a) Impact on different sectors/societies

4.2. Should we wait for the winning algorithms selected by NIST PQC or does it make sense to start implementing non-standardized quantum-resistant public-key cryptographig algorithms in practice?

4.3. Who is the right party to take PQC algorithm research/requirements/development forward and at what level (global / EU / national)

4.4. How do you think quantum secure encryption technology should be developed? Should development be national or carried out in cooperation globally with other countries, or should development responsibility be left to large companies? Please justify your opinion.

Appendix 2. Mindmap diagram used to structure the research problem


Cubit (Quantum bits)
Moment when quantum computers can solve problems that traditional computers can sove but do it significantly faster
Premature Qubit Decoherence
Improving Coherence Times
Environmental Isolation
Quantum Entanglement
Erroro Correction
Check Qubits
Supercooling
Repetitive Calclulatios
Improvement
Quantum Supremacy
Terms
Superconducting Quantum Computers
Quantum Annealing Computers
Universal Quantum Computers
Topological Quantum Computers
Majorana Fermion Computers
Ion Trap Quantum Computers
Types
Cuantum Computer
Work at room temperature
Long coherence times
High-fidelity entanglement
Precise measurements
Advantages
IonQ Ion Trap Quantum Computes
Hard to maintain increased number of simultaneously trapped ions
Measuring
Disadvanted
Symmetric keys or hashes be doubled in order to keet their protection
O(√N)
Lov Grover
Grover´s Algorithm
https://pdfs.semanticscholar.org/6902/cb196ec032852ff31cc178ca822a5f67b2f2.pdf →
Peter Shor
To factor very large fime number equations very quickly
Requires (2 + n) +3 stable qubits
a quantum algorithm for factoring a number N in O((log N)3) time and O(log N) space
Shor´s Algorithm
Factorization optimization over Shor´s algorithm
Quantum Algrithms
GEECM (Grover plus EECM)
AES
Symmetric chiphers
Kerberos
Network Switching Subsystem
Applications and protocols relying on symmetric ciphers
SHA-2
SHA-3
newer integrity hashes
SHAKE, a Stream cipher
BB84
BBM
B92
COW
DPS
E91
SARG04
Quantum key distribution (QDK)
Quantum resistant cryptography
SNOW 3G
Supersingular isogeny Diffie-Hellman key exchange (SIDH)
Lattice-Based ciphers
Multivariate-based cryptography
Some forms of zero-knowledge proof cryptography
Quantum-based ranfom number generators (QRNG)
Quantum-based ciphers
Code-Based Cryptography
Hash-Based Cryptography
Lattice-Based Cryptography
Multivariate Cryptography
Supersingular Elliptic Curve Isogeny Cryptography
Zero-Knowledge Proof (ZKP)
Post-Quantum Algorithms
Number of stable qubits
Reality of quantum computers
Quantum Crypto Break Factors
Do Quantum algorithms really work
It is Already Happened
In The Next Few Years
After the Next Few Years
It's Never Going to Happen
Timing Scenarios
Mosca's Inequality
Preparing
Crypto Break
Post Quantum
The use of Quantum technology is restricted by nation-states and the military
Quantum technology will be only available to the biggest companies
Mass Proliferation
Breakout Scenarios
Impact
Quantum
Quantum mechanics
Quantum Particles
Quark
Up
Down
Bottom
Charm
Strange
Lepton Family
Electron
Muon
Tau
Electron neutrino
Muon neutrino
Tau neutrino
Property
Mass
Charge
Spin
principles
Quantum tunneling
Superposition
Observer Effect
No-Cloning Teorem
Entanglement
Decoherence
CRYSTAL-Kyber
FrodoKEM
LAC
NewHope
Three Bears
NTRU
NTRU Prime
SABER
Round5
Classic McEliece
NTS-KEM
BIKE
HQC
LEDAcrypt
Rollo
RQC
SIKE
Asymmetrix encryption/KEMs
Round 2
NIST Post-Quantum Contest
Quantum-resistant cryptography
CRYSTALS-Dilithium
FALCON
qTESLA
SPHINCS+
GeMSS
LUOV
MQDSS
Rainbow
Picnic
Signatures