Kanditutkielma

Tietojenkäsittelytieteen kandiohjelma

Kvanttikryptologia

Matias Tamsi

17.12.2021

Matemaattis-luonnontieteellinen tiedekunta

Helsingin yliopisto

Yhteystiedot

PL 68 (Pietari Kalmin katu 5)
00014 Helsingin yliopisto

Sähkopostiosoite: info@cs.helsinki.fi
URL: http://www.cs.helsinki.fi/

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Koulutusohjelma — Utbildningsprogram — Study programme
Matemaattis-luonnontieteellinen tiedekunta	Tietojenkäsittelytieteen kandiohjelma

Tekijä — Författare — Author

Matias Tamsi

Työn nimi — Arbetets titel — Title

Kvanttikryptologia

Ohjaajat — Handledare — Supervisors

FT Tommi Meskanen

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Kanditutkielma	17.12.2021	25 sivua

Tiivistelmä — Referat — Abstract

Tutkielmassa käydään läpi kvanttikryptologian keskeisiä asioita. Ennen kvanttikryptografiaa ja kvanttikryptoanalyysia, joihin kvanttikryptologia jakautuu, käsitellään taustatietoa kryptologiasta ja kvanttilaskennasta. Kvanttikryptografian osuus painottuu kvanttiavaimen jakoon, joka on tunnetuin menetelmä kvanttikryptografiassa. Kvanttikryptoanalyysi puolestaan painottuu kahteen tunnetuimmista kvanttialgoritmeista alalla eli Shorin ja Groverin algoritmeihin. Lisäksi tarkastellaan kvanttiturvallista kryptografiaa, joka liittyy läheisesti kvanttikryptologiaan. Lopussa pohditaan käsiteltyjä asioita sekä alan nykytilaa, tulevaisuutta ja haasteita.

Tutkielma on suunnattu aiheesta kiinnostuneille, mutta erityisesti kohdeyleisönä on tietojenkäsittelytieteen opiskelijat, joille kvanttikryptologia on käsitteenä uusi. Päämääränä on antaa katsaus kvanttikryptologiaan ja niihin aloihin, jotka liittyvät läheisesti kvanttikryptologiaan.

ACM Computing Classification System (CCS)
Security and privacy → Cryptography
Theory of computation → Computational complexity and cryptography
Hardware → Emerging technologies → Quantum technologies → Quantum computation → Quantum communication and cryptography

Avainsanat — Nyckelord — Keywords

kvanttikryptologia, kvanttikryptografia, kvanttikryptoanalyysi, kryptologia, kvanttilaskenta, salaukset

Säilytyspaikka — Förvaringsställe — Where deposited

Helsingin yliopiston kirjasto

Muita tietoja — övriga uppgifter — Additional information

Sisällys

1 Johdanto

Kvanttikryptologia on kvanttikryptografian ja kvanttikryptoanalyysin kattokäsite samaan tapaan kuin kryptologia on kryptografian ja kryptoanalyysin. Etuliite *kvantti* viittaa kvanttifysikaallisten ominaisuuksien hyödyntämiseen näillä aloilla. Usein alalla kryptologian sekä kvanttikryptologian eroa painotetaan kutsumalla kryptologiaa *klassiseksi kryptologiaksi*. Sama pätee siis kryptologian osa-alueille eli puhutaan *klassisesta kryptografiasta* ja *klassisesta kryptoanalyysista*. Tutkielmassa käytetään samaa käytäntöä, kun on tarpeellista painottaa alan, periaatteiden tai ilmiöiden klassisuutta.

Tutkielman pääasiallinen tarkoitus on antaa katsaus tämänhetkiseen edistykseen ("*state-of-the-art*") kvanttikryptografiassa ja -analyysissa. Täten saadaan myös käsitys kvanttikryptologian tilanteesta. Mainittakoon, että kvanttikryptografiaa ja -analyysia ei usein käsitellä yhdessä eikä kvanttikryptologia ole kovin vakiintunut termi. Tutkielmassa onkin otettu lähtökohdaksi se, että kvanttikryptografia ja -analyysi kuuluvat saman kattokäsitteen alle. Huomautuksena myös, että useille englanninkielisille alan termeille ei ole vastaavaa tai vakiintunutta suomenkielistä vastinetta. Oikeastaan joidenkin englanninkielistenkin termien kohdalla esiintyy epäjohdonmukaisuutta tai vakiintumattomuutta.

Ennen itse kvanttikryptografiaan ja kvanttikryptoanalyysiin perehtymistä käydään läpi taustatietoa niin kryptologiasta kuin myös kvanttilaskennasta. Kryptologian osuus jakautuu kryptografiaan ja kryptoanalyysiin. Lisäksi omaksi luvukseen on otettu kryptografian osa-alue *kvanttiturvallinen kryptografia*. Kvanttiturvallisen kryptografian voi ajatella ikään kuin kvanttikryptoanalyysin haastajaksi, joten sitä käsitellään varsinkin kvanttikryptoanalyysin yhteydessä.

Kvanttilaskennan osuuteen on puolestaan valittu tärkeimpiä perusteita, joiden avulla lukijan toivotaan kykenevän ymmärtää paremmin kvanttikryptografiaa ja -analyysia. Täten on välttämätöntä käydä läpi, mitä tarkoittaa kvanttilaskennan perusyksikkö *kubitti*, ja sen erikoinen ominaisuus nimeltään *superpositio*. Kappaleet *lomittumisesta* ja *konjugaattikoodauksesta* ovat valittu lähinnä kvanttikryptografiaa varten. Kvanttilaskenta osuuden lopussa käsitellään vielä lyhyesti kvanttilaskennan haasteita ja nykyisiä kvanttitietokoneita. Tämä auttaa myöhemmin hahmottamaan kvanttikryptologian tilannetta.

Kvanttikryptografia osuudessa tutustutaan *kvanttirahaan* ja satunnaislukujen generointiin kvanttilaskennan avulla, mutta pääosassa on *kvanttiavaimen jako*, joka on kvanttikryptografian tunnetuin tulos. Kvanttiavaimen jakoa käsitellään teoriassa, ja lisäksi käydään läpi sen

käytännön sovelluksia.

Kvanttikryptoanalyysin osuus keskittyy kvanttikryptoanalyysin tunnetuimpiin kvanttialgoritmeihin eli *Shorin algoritmiin* ja *Groverin algoritmiin*, jotka toimivat tavallisilla eli universaaleilla kvanttitietokoneilla. Sen jälkeen tarkastellaan *kvanttihehkutusta*, joka on universaalin kvanttitietokoneen kvanttilaskennasta eroava menetelmä, joka on lupaava keino saavuttaa kvanttikryptoanalyysin vaatima tarpeeksi tehokas kvanttitietokone. Kvanttikryptoanalyysi osuuden lopuksi tarkastellaan vielä, miten kvanttiturvallisessa kryptografiassa kvanttikryptoanalyysia vastaan ”taistellaan”.

Ennen yhteenvetoa pohditaan käsiteltyjä asioita. Erityisesti keskitytään siihen, miksi kvanttikryptologia ja sen tutkimus ovat niin tärkeitä tutkielmassa käsiteltyjen asioiden valossa. Kvanttikryptologiassa on tyypillistä arvioida ja ennustaa, kuinka pian saavutetaan sellainen kvanttitietokone, joka pystyisi murtamaan nykypäivänä käytössä olevia salauksia suorittamalla jonkin kvanttikryptoanalyysiin tarkoitetun kvanttialgoritmin. Ennustaminen on vaikeaa eikä ennusteita voida pitää varmoina, mutta se on kuitenkin tärkeää, jotta siihen voidaan varautua.

2 Taustatietoa

Tässä luvussa tutustutaan tutkielmassa esiintyviin käsitteisiin ja niiden perusteisiin, mistä on hyötyä myöhemmissä luvuissa. Katsaus on suppea ja käsittelee vain niitä asioita, jotka esiintyvät myöhemmin. Tarkoituksena on, että tarvittavilla taustatiedoilla kvanttikryptografiaan ja kvanttikryptoanalyysiin on helpompi perehtyä.

Kryptologian ja kvanttilaskennan välinen suhde on ollut esillä tutkimuksessa puoli vuosisataa, joten kvanttikryptologiaa voidaan pitää suhteellisen nuorena tieteenalana. Wiesnerin keksimää *kvanttirahaa* (*"quantum money"*) vuodelta 1968 pidetään ensimmäisenä kvanttikryptologian menetelmänä, koska silloin kvanttifysiikkaa sovellettiin ensimmäistä kertaa kryptografiassa. (Anne Broadbent, 2015.)

2.1 Kryptologia

Kryptologia on tieteenala, joka tutkii salaista kommunikaatiota, ja sen juuret yltävät tuhansien vuosien taakse. Kryptologia voidaan jakaa kahteen osa-alueeseen – *kryptografiaan* ja *kryptoanalyysiin*. (Massey, 1988.)

2.1.1 Kryptografia

Kryptografiassa pyritään löytämään tapoja lähettää viesti salassa ja turvata sen aitous (Massey, 1988). Kryptografisilla menetelmillä voidaan salaamisen lisäksi toteuttaa *digitaalinen allekirjoitus*. Digitaalinen allekirjoitus tarkoittaa menetelmää, jolla varmistetaan viestin lähettäjän identiteetti sekä viestin koskemattomuus (NIST, 1992).

Esimerkiksi armeijat ovat käyttäneet kryptografiaa jo vuosituhannet salatakseen kommunikaatiota. Ennen kryptografian tarve painottui julkisille tahoille, kuten valtioille, mutta nykyään yksityishenkilöilläkin on tarve kryptografialle. Yksityishenkilöt eivät välttämättä viesti valtiosalaisuuksia, mutta viestinnän sähköistyttyä yksityishenkilöt lähettävät digitaalisesti arkaluontoisiakin asioita, joten tarvitsee jokainen taho kryptografiaa viestinnän salaamiseen ja viestinnän aitouden turvaamiseen. (Massey, 1988.)

Moderni avainten jakoon perustuva kryptografia voidaan jakaa symmetriseen ja epäsymmetriseen kryptografiaan. Symmetrisessä kryptografiassa, esimerkiksi symmetrisen avaimen salauksessa, samaa yksityistä salausavainta käytetään sekä salaamiseen että salauksen pur-

kamiseen (Gheorghiu ja Mosca, 2019; Chandra et al., 2014). Yksityinen salausavain pitää jakaa salaisen kommunikaatikanavan kautta, sillä ulkopuolisen saadessa sen käsiinsä voi ulkopuolinen helposti muuttaa kryptotekstin eli salatun viestin takaisin selkokieliseksi tekstiksi. Symmetristä kryptografiaa tarvitaan, koska sillä voidaan toteuttaa epäsymmetristä kryptografiaa nopeampia ja vähemmän resursseja vieviä kryptografisia menetelmiä. Esimerkkinä edellä mainitusta on *AES* ("*Advanced Encryption Standard*"), joka on yksi tunnetuista symmetrisen kryptografian salausmenetelmistä (Chandra et al., 2014).

Epäsymmetrisessä kryptografiassa, joka tunnetaan myös julkisen avaimen kryptografiana, yksityisen salausavaimen lisäksi käytetään julkista salausavainta. Lähettäjä käyttää vastaanottajan julkista salausavainta hyväksi salatakseen viestin. Vastaanottaja voi purkaa salauksen yksityisellä salausavaimella. Menetelmä ei vaadi salaista kommunikaatiokanavaa, kuten symmetrinen kryptografia vaatii yksityisen salausavaimen jakamiseen. Yksi tunnetuista julkisen avaimen kryptografisista salausmenetelmistä on RSA (Gheorghiu ja Mosca, 2019; Chandra et al., 2014). Julkisen avaimen kryptografia mahdollistaa myös digitaalisen allekirjoituksen: yksityistä salausavainta käytetään digitaalisen allekirjoituksen luomiseen ja julkista avainta käytetään digitaalisen allekirjoituksen tarkistamiseen. Esimerkiksi *DSA* ("Digital Signature Algrorithm") on yksi digitaalisista allekirjoitusmenetelmistä (NIST, 1992).

Kryptografiassa keskeisessä roolissa ovat tiivistefunktiot ("*hash functions*"). Tiivistefunktiot kehitettiin aluksi turvaamaan informaation aitoutta. Tiivistefunktioita käytetään muun muassa salasanojen ja -lauseiden suojaamisessa, digitaalisessa allekirjoittamisessa (NIST, 1992; Preneel, 1994), erilaisissa protokollissa sekä salausalgoritmien perustana (Preneel, 1994).

2.1.2 Kryptoanalyysi

Kryptoanalyysissa pyritään murtamaan viestin salaus tai väärentämään sen aitous. Esimerkiksi armeijat ovat tarvinneet kryptoanalyysia vastustajan salauksien murtamiseen, kun taas yritykset ovat saattaneet vakoilla kilpailijaansa. Varsinkin kryptoanalyysin tieteellistä tutkimusta varjostavat esimerkiksi valtioiden poliittiset intressit. (Massey, 1988.)

Yhtenä esimerkkinä kryptoanalyysin metodeista on raakahyökkäys ("*brute-force attack*"). Raakahyökkäyksessä käydään läpi mahdollisia vaihtoehtoja esimerkiksi salausavaimelle tai salasanalle. Parhaimmassa tapauksessa ensimmäinen kokeilu on oikein, kun taas huonoimmassa tapauksessa käydään kaikki vaihtoehdot läpi. Keskimääräisesti pitää siis käydä läpi puolet vaihtoehdoista. Raakahyökkäys liittyy läheisesti kvanttikryptoanalyysiin, sillä sitä voidaan parantaa kvanttilaskennan avulla. (Jordan ja Liu, 2018.)

Toisena esimerkkinä kryptoanalyysin metodista on kryptografiassa käytettävien tiivistefunktioiden arvojen yhteentörmäyksien löytäminen. Voidaan osoittaa syntymäpäiväparadoksin avulla, että klassinen algoritmi kykenee tiivistefunktiosta $F : X \to Y$ ratkaisemaan $O(\sqrt{N})$ arvioinnilla törmäysongelman, jossa N on lähtöjoukon koko, ja sille pätee $N = |X|$. Törmäysongelmassa kyse on löytää törmäys eli sellaiset arvot $a, b \in X$, joilla pätee $F(a) = F(b)$ olettaen, että tällainen törmäys on olemassa (Brassard et al., 1997). Syntymäpäiväparadoksia voi havainnollistaa esimerkillä: jos henkilöiden syntymäpäivät ovat jakautuneet tasaisesti vuoden päiville, niin keskimääräisesti kahdella henkilöllä 24:stä henkilöstä on sama syntymäpäivä (Flajolet et al., 1992). Edellä mainittua hyökkäystä voidaan myös tehostaa kvanttilaskennan avulla.

2.1.3 Kvanttiturvallinen kryptografia

Kvanttiturvallinen kryptografia (”*postquantum cryptography*”) on klassisen kryptografian osaalue, joka pohjautuu laskennallisesti vaativiin ongelmiin, joita kvanttitietokoneet eivät pysty tehokkaasti ratkaisemaan. Kvanttiturvallista kryptografiaa voidaan pitää väliaikaisena ratkaisuna, sillä saattaa olla, että jonain päivänä kvanttiturvallisia salauksia voidaan murtaa kvanttialgoritmein. (Pirandola et al., 2020.)

2.2 Kvanttilaskenta

Kvanttilaskennassa laskeminen tapahtuu kvanttialgoritmeilla, joita suoritetaan kvanttitietokoneilla. Kvanttialgoritmien toiminta perustuu herkkiin vuorovaikutuksiin, jotka tuottavat eksponentiaalisen määrän erilaisia laskennallisia polkuja klassisiin algoritmeihin nähden (Jordan ja Liu, 2018). Laskennallisilla poluilla on todennäköisyyksiä, jotka saavat kompleksilukuarvoja. Kompleksilukuarvojen yhteenlaskeminen ei kasvata todennäköisyyttä, mikä johtaa joidenkin laskennallisten polkujen hylkäämiseen. Eli sen sijaan, että kvanttitietokoneet suorittaisivat klassisia tietokoneita nopeammin laskutoimituksia peräkkäin, niin kvanttitietokoneiden tehokkuus tulee kyvystä laskea klassisille tietokoneille käytännössä mahdottomalla tavalla (Wallden ja Kashefi, 2019).

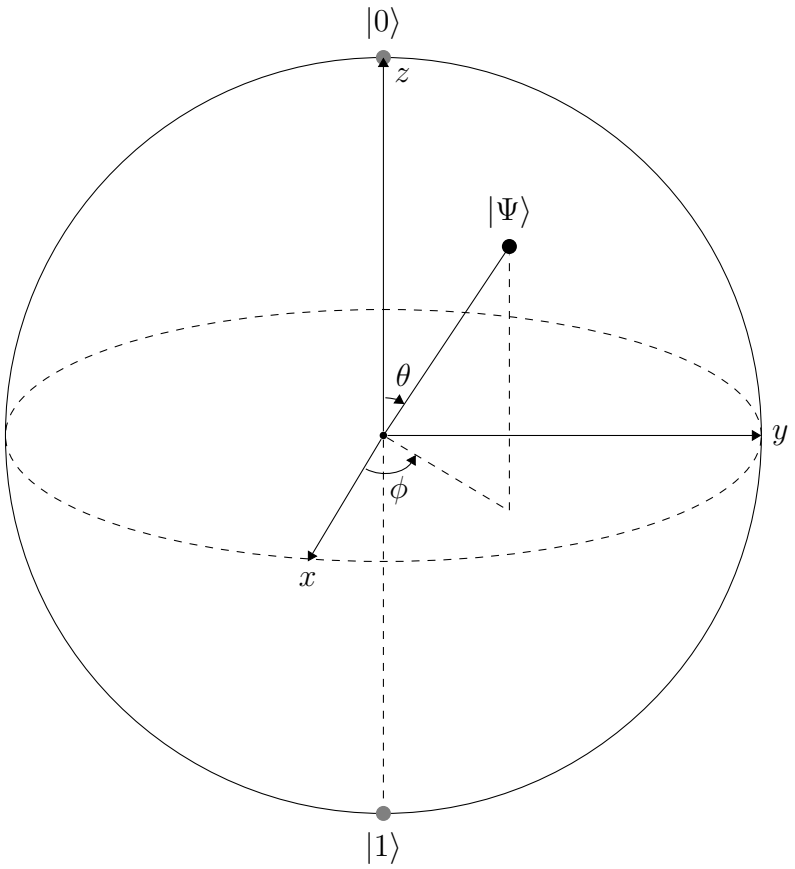
2.2.1 Kubitti ja superpositio

Klassisessa informaation käsittelyssä yksikkö on tunnetusti bitti, mutta kvanttiinformaatiossa yksikkö on kubitti. Kubitin tila voidaan kuvata vektorina, jonka pituus on yksi kaksiuloitteisessa kompleksissa vektoriavaruudessa. Olkoon kubitin tila $|\Psi\rangle$, jolloin ku-

bitin tila voidaan kuvata yhtälöllä $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Tilat $|0\rangle$ ja $|1\rangle$ muodostavat kannan kyseessä olevalle vektoriavaruudelle. Kompleksiluvuille α ja β pätee $|\alpha|^2 + |\beta|^2 = 1$, sillä kubitti ei voi saada muita arvoja mittauksessa kuin arvon 0 todennäköisyydellä $|\alpha|^2$ tai arvon 1 todennäköisyydellä $|\beta|^2$. Jos kumpikaan todennäköisyyksistä ei ole nolla, niin silloin kubitin sanotaan olevan tilojen $|0\rangle$ ja $|1\rangle$ superpositiossa. Kun kubitin tila mitataan, romahtaa se takaisin klassiseksi informaatioksi eli se menettää superposition. Toisin sanoen jäljelle jää joko 0 tai 1. (Anne Broadbent, 2015.)

Kubittia voidaan visualisoida *Blochin pallona* ("Bloch sphere"), kuten kuvassa 2.1 on tehty. Pallon säde on yksi, joka on yksikkövektorin pituus. Pallon pinnan muodostaa kaksiuloitteinen kompleksi vektoriavaruus, jossa on ääretön määrä pisteitä eli kubitilla on ääretön määrä mahdollisia tiloja. Kulmat ϕ ja θ määrittävät yksikkövektorin asennon, jolloin saadaan superpositio $|\Psi\rangle$. Oli superposition arvo mikä tahansa, niin mittauksesta saadaan joko 0 tai 1. (Nielsen ja Chuang, 2002.)

Kuva 2.1: *Blochin pallo* (Nielsen ja Chuang, 2002)



On tärkeää huomata, että kuvan 2.1 kulmat ϕ ja θ eivät ole kompleksilukuja α tai β, vaan koska $|\alpha|^2 + |\beta|^2 = 1$, niin

$$|\Psi\rangle = e^{i\gamma}(cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle), \tag{2.1}$$

ja koska tekijällä $e^{i\gamma}$ ei ole havaittavaa vaikutusta, niin saadaan yhtälö muotoon

$$|\Psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle, \tag{2.2}$$

josta nähdään kulmien ϕ ja θ merkitys. (Nielsen ja Chuang, 2002.)

Superposition luominen vaatii ympäristöstä aiheutuvien vuorovaikutuksien karsimista, sillä muuten niistä aiheutuva melu ("*noise*"), toisin sanottuna häiriö, pyyhkii kvanttifysikaalliset ilmiöt pois ennen kuin ne pystytään huomata. (Jordan ja Liu, 2018.)

Kahden tai useamman kubitin kvanttimekaanista tilaa voidaan kuvata tensoritulona. Esimerkiksi kaksi kubittia voivat muodostaa tilat $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ ja $|1\rangle \otimes |1\rangle$, jotka usein esitetään muodossa $|00\rangle$, $|01\rangle$, $|10\rangle$ ja $|11\rangle$. Eli n-kubitin systeemi voi olla mahdollisten tilojen ($|00...0\rangle$, $|00...1\rangle$,..., $|11...1\rangle$) superpositiossa. (Anne Broadbent, 2015.)

2.2.2 Lomittuminen

Lomittuminen ("*entanglement*") tarkoittaa kvanttimekaanista ominaisuutta, jossa kvanttisysteemien välillä on yhteys, vaikka ne olisivat fyysisesti erillään. Kun kaksi kvanttisysteemiä ovat lomittuneet, niin silloin niiden välillä on riippuvuus siten, että toisen kvanttisysteemin tilaa ei voi kuvailla viittaamatta toisen kvanttisysteemin tilaan. Ajatellaan esimerkiksi kahta kubittia, joista toinen on tutkijalla maan pinnalla ja toinen satelliitissa maan kiertoradalla. Jos nämä kaksi kubittia ovat 2-kubitin superpositiossa ja lomittuneet, niin tutkijan mitatessa maan pinnalla olevan kubitin tila, tietää hän myös satelliitissa olevan kubitin tilan. (Amer et al., 2021.)

2.2.3 Konjugaattikoodaus

Konjugaattikoodaus ("*conjugate coding*") on usean kvanttikryptograafisen protokollan taustalla. Konjugaattikoodaus perustuu lomittumiseen ja on suhteellisen yksinkertaista toteuttaa olemassa olevalla teknologialla. Konjugaattikoodaus perustuu siihen, että klassista informaatiota voidaan koodata ("*encode*") konjugaateiksi kvanttimekaanisiksi kannoiksi. Konjugaattikoodauksen perusperiaatetta voidaan yleisen terminologian mukaan kuvata rinnastamalla

kubitti fotoniin eli valohiukkaseen. Fotonin polarisaatiota voidaan käyttää kuvaamaan kvanttimekaanista vapausastetta. Fotonit voivat nimittäin polarisoitua horisontaalisesti, vertikaalisti tai diagonaalisesti oikealle tai vasemmalle. Muodostamalla näistä tiloista suoraviivainen ja diagonaalinen kanta, saadaan kaksi kantaa, joista kummatkin voivat koodata klassisen bitin. Näitä kahta kantaa kutsutaan konjugaateiksi. Konjugaattikoodauksen merkitystä voidaan kiteyttää kahden sen tärkeimmän ominaisuuden myötä. (Anne Broadbent, 2015.)

Ensinnäkin mitattaessa toisessa kannassa menettää konjugaatti eli toinen kanta siihen koodatun informaation. Tämä voidaan selittää *Heisenbergin epätarkkuusperiaatteen* avulla: kvanttihiukkasen sijaintia ja liikemäärää on mahdotonta mitata tarkkaan samanaikaisesti. Ajatellaan nyt, että kvanttihiukkasen sijainti on toinen kanta ja liikemäärä on sen kannan konjugaatti. Kun mitataan sijaintia, niin katoaa tieto kvanttihiukkasen liikemäärästä. (Anne Broadbent, 2015.)

Toisena konjugaattikoodauksen merkittävänä ominaisuutena on, että ulkopuolinen ei kykene luomaan samanlaista koodausta suurella todennäköisyydellä. Ulkopuolisen oletetaan olevan ilman tietoa käytetystä kannasta sekä pääsevän käsiksi vain yhteen tilaan. Ominaisuus perustuu *kloonaamattomuus* (”*no-cloning*”) teoriaan, jonka mukaan on fyysisesti mahdotonta kopioida kvanttimekaanista systeemiä, sillä kopiointivaiheessa kubittien tila häiriintyy. (Anne Broadbent, 2015.)

2.2.4 Kvanttilaskennan haasteet

Kvanttilaskennassa on paljon haasteita, joita koitetaan ratkaista. Laskennan nopeutta hidastaa muun muassa todennäköisimmän ratkaisun löytäminen mahdollisista ratkaisuista eli laskennan lopussa pitää arvioida, mikä mahdollisista laskennallisista poluista on todennäköisin. Lisäksi todennäköisimmän ratkaisun oikeellisuuden tarkistaminen hidastaa myös laskentaa. (Mavroeidis et al., 2018.)

Kubitit ovat alttiita virheille. Virheitä voi syntyä muun muassa ympäristön lämmön tai melun seurauksena. Kuten klassisessa tiedonsiirrossa voi esiintyä bittien arvojen vaihtumista, niin myös kubiteille voi käydä samoin. Kuitenkin kyseisten virheiden tarkistamista pitäisi välttää, koska tarkistamisessa kubitti menettää superposition. (Mavroeidis et al., 2018.)

Kubitit eivät pysty säilyttämään kvanttitilaansa pitkään. Vuonna 2018 maailmanennätyksenä pidettiin 35 sekuntia. Koossapysyvyys vaatii lämpötilan olevan lähellä absoluuttista nollapistettä ja esimerkiksi edellä mainitussa maailmanennätyksessä eristeenä käytettiin piin isotooppia karsimaan magneettista melua. (Mavroeidis et al., 2018.)

2.2.5 Kvanttitietokoneet

Kvanttitietokoneet, jotka voisivat murtaa nykyisiä salauksia, tarvitsevat skaalautuvuuden ja virhesietoisuuden lisäksi ainakin tuhansia kubitteja (Wallden ja Kashefi, 2019). Tehokkaimmat kvanttitietokoneet ovat vielä kaukana siitä.

IBM paljasti juuri kehittäneensä 127 kubitin kvanttiprosessorin, jota tullaan käyttämään kvanttitietokoneissa. Tällä hetkellä IBM tarjoaa 65 kubitin kvanttitietokonetta kenen tahansa käytettäväksi pilvipalveluna (IBM, 2021). Googlen Bristlecone nimisessä kvanttiprosessorissa on 72 kubittia (Kelly, 2021). Tutkielman kannalta on olennaista huomioida nykyisten kvanttitietokoneiden kubittien suurin piirteinen määrä. Mainittakoon vielä, että kvanttitietokoneiden tehokkuuden tarkastelussa tulisi ottaa myös muita asioita huomioon kuin vain kubittien määrä. Esimerkiksi virheenkorjauksen laiminlyönti aiheuttaa sen, että kubittien lisääminen ei enää tehosta laskentaa tietyn pisteen jälkeen (Lapedus, 2021).

Edellä mainitut kvanttitietokoneet ovat niin sanotusti universaaleja kvanttitietokoneita eli niillä voitaisiin laskea erilaisia ongelmia. Universaalien kvanttitietokoneiden lisäksi on kvanttihehkutukseen (”quantum annealing”) perustuvia kvanttitietokoneita. Kvanttihehkutuksessa ratkaistaan jokin tietty optimointiongelma (Kadowaki ja Nishimori, 1998; Jiang et al., 2018; Hauke et al., 2020). *D-Wave*:n dokumentaatiossa (D-Wave Systems Documentation, 2021, *What is Quantum Annealing?*) kerrotaan kvanttihehkutuksessa olevan kyse siitä, että ratkaistavan ongelman ratkaisu on kvanttisysteemin tilojen energioiden pienin summa. Esimerkiksi kvanttihehkutuksella voitaisiin ratkaista jokin lyhyimmän reitin etsimiseen liittyvä ongelma, sillä lyhin reitti edustaa kvanttisysteemin pienintä energiatilaa. Universaaleihin kvanttitietokoneisiin nähden kvanttihehkutuksella saavutetaan suurempia kubittien määriä (Hauke et al., 2020). Esimerkiksi *D-Wave*:n kvanttihehkutukseen perustuvassa kvanttitietokoneessa on yli 5000 kubittia (D-Wave Systems, 2021).

3 Kvanttikryptografia

Kvanttikryptografia hyödyntää kvanttimekaanisia ilmiöitä kryptografian tarpeisiin. Kvanttikryptografian tunnetuimman tuloksen, kvanttiavaimen jaon ("*quantum key distribution*"), lisäksi kvanttikryptografiaan kuuluu muun muassa *kvanttiraha* sekä esimerkiksi satunnaislukujen generointia kvanttimekaniikan avulla (Anne Broadbent, 2015). Lisäksi kvanttikryptografiaan kuuluu paljon muita menetelmiä, joita ei tässä tutkielmassa käsitellä, vaan pääpaino on kvanttiavaimen jaossa.

3.1 Kvanttiraha

Ensimmäinen kvanttikryptografian menetelmä eli Wiesnerin vuoden 1968 kvanttiraha ("*quantum money*") käyttää konjugaattikoodausta. Kvanttirahaa kutsutaan myös termillä kvanttisetelit ("*quantum banknotes*"). Konjugaattikoodauksessa käytetään satunnaisesti valittuja bittejä sekä kantoja. Täten kvanttiraha koostuu kubiteista, jotka ovat valittu satunnaisesti tiloista $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\nearrow\rangle$ ja $|\searrow\rangle$. Kvanttirahan lähettäjä, jota usein kutsutaan *pankiksi*, pystyy ainoana varmistamaan konjugaattikoodauksella luodun kvanttirahan aitouden (Anne Broadbent, 2015). Huolimatta Wiesnerin kvanttirahan merkityksestä ja sen aikaisesta edistyksellisyydestä, ei kvanttirahasta olla vielä saatu toteutettua käytännöllistä protokollaa. Syitä ovat muun muassa puute kvanttimuisteista ja käytännöllisestä tavasta varmistaa kvanttirahan aitous (Bozzio et al., 2018).

3.2 Satunnaislukujen generointi kvanttilaskennalla

Useimmat kryptografiset protokollat käyttävät satunnaislukugeneraattoreita toimiakseen. Satunnaislukugeneraattorien aidon satunnaisuuden toteuttaminen on kuitenkin vaikeaa. Satunnaislukujen epäsatunnaisuus voi johtaa ongelmiin, kun jokin satunnaiseksi oletettu ei olekaan täysin satunnaista. Esimerkiksi huomattavaa osaa verkosta kerättyjä RSA:n julkisia avaimia yhdisti sama alkuluku, joka voi puolestaan heikentää RSA:n turvallisuutta, jos tietoa käytetään murtamisyrityksessä. (Anne Broadbent, 2015.)

Klassinen fysiikka on deterministä, joten klassinen satunnaislukugeneraattori ei voi koskaan tuottaa täysin satunnaisia satunnaislukuja. Siksi satunnaisuuden riittävyyttä on arvioitava käyttötilanteen mukaan. Kvanttimekaniikan avulla kvanttisatunnaislukugeneraattorit voivat

tuottaa teoriassa aidosti satunnaisia lukuja. Otetaan esimerkiksi hyvin yksinkertainen kvanttisatunnaislukugeneraattori, jota suoritetaan luotettavalla laitteella eli sellaisella, johon ulkopuolinen ei pääse käsiksi. Ammuttaessa yksittäinen fotoni säteenjakajaan, niin kimpoaa fotoni 50 % todennäköisyydellä sensoriin A ja 50 % sensoriin B. Täten, jos A vastaa bitin arvoa 0 ja B vastaa bitin arvoa 1, niin kvanttisatunnaislukugeneraattori tuottaa aidosti satunnaisia bittejä. (Anne Broadbent, 2015.)

Kvanttisatunnaislukugeneraattori, joka tuottaa aidosti satunnaisia lukuja, on siis teoriassa mahdollista saavuttaa, mutta käytännössä toteutus on vaikeaa (kuten kvanttilaskennassa yleensä). Haasteita luovat muun muassa fyysinen toteutus aina fotonin luomisesta sen mittaamiseen asti. Esimerkiksi säteenjakajan toiminnan täydellisyyttä on vaikea taata. Lisäksi kaikki ulkoiset tekijät, kuten muutokset energialähteessä, vaikuttavat tuloksiin. Yleinen käytäntö on vielä vahvistaa satunnaisuutta klassisella laskennalla näiden vaikutusten minimoimiseksi. (Anne Broadbent, 2015.)

3.3 Kvanttiavaimen jako

Kvanttiavaimen jako on tunnetuimpia tapoja hyödyntää kvantti-informaatiota kryptografiassa. Kvanttiavaimen jaolla on niin merkittävä rooli kvanttikryptografiassa, että se usein rinnastetaan virheellisesti kvanttikryptografiaan (Anne Broadbent, 2015). Verrattuna kvanttiturvallisiin salauksiin, jotka ovat toistaiseksi turvallisia, kvanttiavain jakoa pidetään teoriassa murtamattomana. Kvanttiavaimen jakoa on kuitenkin käytännössä vaikea toteuttaa kunnolla ja monet ratkaisemattomat ongelmat kaipaavat ratkaisuja (Pirandola et al., 2020).

Kvanttiavaimen jako koostuu kahdesta päävaiheesta, jotka ovat kvanttikommunikointi (”*quantum communication*”) sekä sitä seuraava klassisesti tapahtuva jälkiprosessointi. Kvanttikommunikointia vastaavat taulukon 3.2 vaiheet 1-5 ja taulukon 3.3 vaiheet 1-7. Jälkiprosessointiin kuuluvat loput vaiheista.

Kvanttikommunikointi tapahtuu siten, että Alice koodaa sattumanvaraisesti klassisen muuttujan α instansseja kvanttitiloiksi, joka tarkoittaa taulukkojen 3.2 ja 3.3 vaiheita 1-3. Alice siis valitsee sattumanvaraisesti kannan ”$\times$” tai ”$+$” taulukosta 3.1 koodatakseen bitin. Esimerkiksi bitin ollessa ”0” ja sattumanvaraisesti valitun kannan ollessa ”$+$”, niin saatua kvanttitilaa kuvataan nuolella ”$\uparrow$”. Kyseiset tilat lähetetään kvanttikanavaa pitkin Bobille. Kvanttikanava voi olla esimerkiksi valokuitua tai optista tiedonsiirtoa. Salakuuntelija Eve voi päästä käsiksi kvanttikanavaan ja koittaa varastaa koodattua informaatiota. Taulukossa 3.3 vaiheet 4 ja 5 kuvastavat tällaista tilannetta. Kvanttimekaniikan lait kuitenkin estävät Even salakuunteluyritystä. Eve ei enää pysty täydellisesti kopioimaan lukemaansa kvanttikanavassa

liikkunutta kvantti-informaatiota ja saa vain osan informaatiosta tietoonsa samalla häiriten kvantti-tiloja. Bob mittaa kvanttikanavan toisessa päässä saapuvia signaaleja ja saa tulokseksi sattumanvaraisen klassisen muuttujan β, jota kuvastavat taulukossa 3.2 vaiheet 4 ja 5 kun taas taulukossa 3.3 vaiheet 6 ja 7. Toistettuaan tätä tarpeeksi monta kertaa, kuten taulukoissa bittejä on välitetty tavun verran $b_1, ...b_8$, Alice ja Bob jakavat korreloivien bittien α ja β raakadatan, jota vastaavat taulukon 3.2 vaihe 6 ja taulukon 3.3 vaihe 8. (Pirandola et al., 2020.)

Taulukko 3.1: Käytössä olevat kannat taulukkoja 3.2 ja 3.3 varten (Pirandola et al., 2020; Amer et al., 2021).

Kanta	0	1
$+$	$\uparrow$	$\rightarrow$
$\times$	$\nearrow$	$\searrow$

Taulukko 3.2: Kvanttiavaimen jaon vaiheita havainnollistettuna ilman salakuuntelija Eveä (Anne Broadbent, 2015; Pirandola et al., 2020; Amer et al., 2021).

		b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
1.	Alicen satunnainen bitti	0	1	0	1	0	0	1	1
2.	Alicen satunnainen lähettämiskanta	$+$	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$
3.	Alicen lähettämän fotonin polarisaatio	$\uparrow$	$\searrow$	$\nearrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\rightarrow$	$\searrow$
4.	Bobin satunnainen mittauskanta	$+$	$\times$	$+$	$+$	$+$	$\times$	$\times$	$\times$
5.	Bobin mittaaman fotonin polarisaatio	$\uparrow$	$\searrow$	$\rightarrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\searrow$
6.	Julkinen keskustelu käytetyistä kannoista								
7.	Jaettu salausavain	0	1		1	0	0		1

Bob ja Alice arvioivat kvanttikanavan ominaisuuksia kuten läpäisykykyä ja melua osalla jaetusta datasta. Näiden ominaisuuksien arviointi on tärkeää Alicelle ja Bobille, jotta he voivat arvioida jälkiprosessoinnin määrän tarpeen salausavaimen muodostusta varten. Tämän arvion pohjalta he korjaavat virheet, joita tiedonsiirrossa mahdollisesti aiheutui. Virheenkorjauksessa ("*error correction*") pyritään havaitsemaan virheitä ja korjaamaan ne. Kuten klassisessa tiedonsiirrossa saattaa bitti vaihtua nollasta ykköseksi tai toisin päin, niin saattaa kvanttikanavassa liikkuva kubitti vaihtaa tilaansa, joka saattaa aiheuttaa bitin muuttumisen. Virheen korjauksen jälkeen vuorossa on vielä yksityisyyden vahvistaminen ("privacy amplification"). Yksityisyyden vahvistamisessa yleensä käytetään kahta universaalia tiivistefunktiota, jotka muuttavat virheistä korjatun syötteen vielä lyhyemmäksi salausavaimeksi päämääränä vahvistaa sen yksityisyyttä. Kaiken tämän jälkeen Alicella ja Bobilla on salausavain. Kvanttiavaimen jaossa syntynyttä salausavainta käytetään sellaisen salausprotokollan

Taulukko 3.3: Kvanttiavaimen jaon vaiheita havainnollistettuna salakuuntelija Even ollessa Alicen ja Bobin välissä. Eve sieppaa polarisoidun fotonin, joka on lähtöisin Alicelta, mittaa sen satunnaisella kannalla ja lopuksi lähettää saamansa polarisoituneen fotonin eteenpäin Bobille. (Pirandola et al., 2020; Amer et al., 2021.)

		b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
1.	Alicen satunnainen bitti	0	1	0	1	0	0	1	1
2.	Alicen satunnainen lähettämiskanta	+	×	×	+	+	×	+	×
3.	Alicen lähettämän fotonin polarisaatio	↑	↘	↗	→	↑	↗	→	↘
4.	Even satunnainen mittauskanta	+	+	×	×	+	+	×	+
5.	Even mittaaman ja lähettämän fotonin polarisaatio	↑	→	↗	↗	↑	→	↗	→
6.	Bobin satunnainen mittauskanta	+	×	+	+	+	×	×	×
7.	Bobin mittaaman fotonin polarisaatio	↑	↗	→	→	↑	↗	↗	↗
8.	Julkinen keskustelu käytetyistä kannoista								
9.	Jaettu salausavain	0	0		1	0	0		0
10.	Virheet		X						X
11.	Salausavain virheiden poiston jälkeen	0			1	0	0		

kanssa, joka hyödyntää kertaluontoista salausavainta ja joka on todistetusti turvallinen (Pirandola et al., 2020).

Kuten taulukossa 3.3 tapahtuu, Evellä on mahdollisuus valita oikea kanta 50 % todennäköisyydellä. Bob puolestaan saa oikean tuloksen Even sieppaamasta fotonista 50 % todennäköisyydellä. Joten jos kvanttikanavassa on salakuuntelija, niin todennäköisyys fotonin sieppaamisen aiheuttamalle virheelle on 25 %. Kun Alice ja Bob haluavat tarkistaa onko heitä salakuunneltu, niin heidän tulee verrata tarpeeksi monta bittiä jaetusta salausavaimesta. Alicen ja Bobin pitää hylätä kyseiset julkisesti jaetut salausavaimen bitit, koska ne eivät ole enää salaisia. Todennäköisyys huomata salakuuntelija kasvaa, mitä enemmän bittejä verrataan. Taulukossa 3.4 on esimerkkejä todennäköisyyksistä havaita salakuuntelija eri määrillä verrattuja bittejä. Esimerkiksi vertaamalla vain yksi bitti todennäköisyys on 25 % ja vertaamalla 50 bittiä todennäköisyys on jo 0.999999... %.

Taulukko 3.4: Esimerkkejä todennäköisyyksistä havaita salakuuntelija, kun verrataan salausavaimen bittejä.

Bittien määrä	Todennäköisyys havaita salakuuntelu
1	$1 - (0.75)^1 = 0.25$
10	$1 - (0.75)^{10} = 0.943686...$
20	$1 - (0.75)^{20} = 0.996829...$
30	$1 - (0.75)^{30} = 0.999821...$
40	$1 - (0.75)^{40} = 0.999989...$
50	$1 - (0.75)^{50} = 0.999999...$

3.3.1 Käytännön sovellukset

Tässä osassa käytetään lähteenä ajankohtaista selvitystä (Amer et al., 2021) kvanttiavaimen jaon käytännön sovelluksista. Kvanttiavaimen jako vaatii siis vain yksittäisen kubitin lähettämistä kerrallaan, joten kvanttiavaimen jakoa sovelletaan jo sekä tieteellisesti että kaupallisesti. Tieteellisen teoreettisen tutkimustyön lisäksi töitä on tehty kvanttiavaimen jaon käyttöön ottamiseen nykypäivää sekä tulevaisuutta varten.

Kvanttiavaimen jakoa on muun muassa sovitettu yleisiin turvallisiin kommunikaatioprotokolliin, joista esimerkkejä ovat IPSec ja TLS. Jos protokollaa käyttävien osapuolien välillä on kvanttikanava, niin julkisen avaimen protokolla voitaisiin korvata kvanttiavaimen jaolla. Kvanttiavaimen jakoa voitaisiin käyttää muodostamaan alussa salausavain sellaisille protokollille, joiden toiminta perustuu etukäteen osapuolien välillä jaetulla salausavaimella salaamiseen. Tärkeä kysymys on myös, kuinka toteuttaa kvanttiavaimen jaon insfrastruktuuri, ja vuosien saatossa ympäri maailmaa onkin rakennettu erilaisia tietoverkkoja kvanttiavaimen jakoa varten. Ensimmäinen on *DARPA*:n jo vuodelta 2003, jonka jälkeen muun muassa Euroopassa ja Kiinassa on ollut useita projekteja.

Kaupallisia kvanttiavaimen jakoa tarjoavia yrityksiä on useita kuten myös niiden tarjoamia palveluita. Yksi suurimmista on sveitsiläinen ID Quantique, joka tarjoaa laitteita yksittäisen fotonin havaitsemiseen, satunnaislukujen generoimiseen kvanttifysikaallisesti sekä kvanttiavaimen jakoa, joka on suunniteltu helposti integroitavaksi nykyiseen datakeskuksien käyttämään teknologiaan. Kvanttiavaimen jako vaatii aidosti satunnaista satunnaislukujen generointia, joka voidaan toteuttaa kvanttimekaniikan avulla. ID Quantique:n ratkaisut generoivat aidosti satunnaisia tavuja 4-16 MB/s. Itse kvanttiavaimen jako, jota ID Quantique tarjoaa, kykenee jakamaan 20 000 symmetristä 256 bitin avainta tunnissa ainakin 50 kilometrin etäisyydellä. Puolestaan 100 kilometrin säteellä, avainten lukumäärä on 2000.

Toshiba, japanilainen yritys, on kehittänyt omaa patentoitua teknologiaa toteuttaakseen

kvanttiavaimen jaon. Toshiba markkinoi prototyyppinsä tarjoavan 1 MB/s siirtonopeudella tapahtuvaa avainbitin välitystä jopa 100 kilometrin säteellä. Toshiba:n mukaan alle 50 kilometrin säteellä teknologia mahdollistaa esimerkiksi videokonferenssin pitämisen.

Yhdysvaltalainen Qubitek erottuu standardeista järjestelmistä, joissa kubitti valmistellaan ja mitataan. Sen sijaan Qubitekk hyödyntää lomittumista, josta kerrotaan luvussa 2.2.3. Qubitekk tarjoaa pääasiassa kvanttiavaimen jakoa teollisten valvontajärjestelmien tarpeisiin. Kommunikointi voidaan toteuttaa tavallisella valokuidulla ainakin 20 kilometrin päähän siirtäen avainbittejä siirtonopeulla 100 kb/s.

4 Kvanttikryptoanalyysi

Kvanttialgoritmit voivat murtaa epäsymmetrisen kryptografian eli julkisen avaimen kryptografian menetelmiä. Jokapäiväinen turvalliseksi mielletty kommunikaatio-infrastruktuuri nojaa vahvasti julkisen avaimen järjestelmiin, jotka eivät ole turvallisia kvanttialgoritmeja vastaan (Amer et al., 2021). Taulukossa 4.1 on esimerkkejä tällaisista julkisen avaimen kryptografian algoritmeista.

Symmetrisiin funktioihin ja tiivistefunktioihin perustuviin kryptografisiin menetelmiin kvanttihyökkäykset ("*quantum attacks*") eivät tehoa yhtä paljoa kuin epäsymmetrisiin, mutta niillä voidaan saavuttaa parempia aika- ja tilavaativuuksia klassisiin hyökkäyksiin verrattuna (Gheorghiu ja Mosca, 2019; Brassard et al., 1997). Taulukosta 4.1 nähdään, kuinka symmetrisien salauksien turvallisuutta voidaan parantaa avaimen kasvattamisella ja tiivistefunkioiden turvallisuutta voidaan parantaa kasvattamalla tulostetta.

Nykyinen yhteisymmärrys on, että symmetrisissä salauksissa salausavaimen kaksinkertaistaminen on hyvä heuristiikka. Kvanttialgoritmeja vastaan strategiana pidetäänkin salausavainten kasvattamista, mutta kaikissa tapauksissa se ei ole taattu ratkaisu. Nimittäin voidaan osoittaa, että kvanttidifferentiaali- ja kvanttilineaarihyökkäykset ("*quantum differential and linear attacks*") ovat sitä vaarallisempia symmetrisiä salauksia kohtaan, mitä suuremmaksi salausavainta kasvatetaan. Tämä tuntuu järjenvastaiselta, mutta mitä pidempiä kryptotekstit tulevat olemaan, niin sitä suuremmiksi niiden turvallisuusvaatimukset kasvavat. (Kaplan et al., 2016.)

Taulukko 4.1: Kvanttilaskennan vaikutus yleisiin kryptografisiin algoritmeihin (Chen et al., 2016).

Algoritmi	**Tyyppi**	**Tehtävä**	**Parantaminen**
AES	Symmetrinen	Salaus	Avaimen kasvattaminen
SHA-2, SHA-3	—	Tiivistefunktiot	Tulosteen kasvattaminen
RSA	Julkinen	Allekirjoitukset, salaus	Ei enää turvallinen
ECDSA, ECDH	Julkinen	Allekirjoitukset, salaus	Ei enää turvallinen
DSA	Julkinen	Allekirjoitukset, salaus	Ei enää turvallinen

4.1 Shorin algoritmi

Vuonna 1994 Peter Shor kehitti kvanttialgoritmin, jolla voidaan laskea diskreettejä logaritmeja sekä jakaa kokonaislukuja tekijöihin polynomisessa ajassa (P. Shor, 1994). Diskreettejä logaritmeja voidaan laskea ajassa $O(n)$. Tekijöihin jako voidaan puolestaan suorittaa ajassa $O(n^3)$ (P. W. Shor, 1997; Jordan, 2021).

Shorin algoritmi koostuu kahdesta vaiheesta, jotka ovat *klassinen vaihe* ja *kvanttilaskennan vaihe*. Klassinen vaihe voidaan suorittaa klassisella laskennalla, jossa ongelma luvun tekijöiden löytämisestä muutetaan *järjestyksen löytämisen ongelmaksi* (*"order-finding problem"*). Kvanttilaskennan vaiheessa käytetään kvanttialgoritmia ratkaisemaan kyseinen järjestyksen löytämisen ongelma. (P. W. Shor, 1997.)

Shorin algoritmi voi murtaa RSA:n sekä siihen perustuvan digitaalisen allekirjoituksen, jos on mahdollista kehittää sen suoritukseen kykenevä kvanttitietokone (Jordan ja Liu, 2018; Wallden ja Kashefi, 2019; Kaplan et al., 2016; P. Shor, 1994; P. W. Shor, 1997; Jordan, 2021; Bhatia ja Ramkumar, 2020). Sama pätee Diffie–Hellman -avaimenvaihtoon (Jordan ja Liu, 2018). Lisäksi Shorin algoritmilla voidaan diskreettien logaritmien laskennan avulla murtaa elliptsiin käyriin perustuvia salauksia ja digitaalisia allekirjoituksia (Jordan ja Liu, 2018; Jordan, 2021).

Esimerkiksi Shorin algoritmilla 2048 bitin RSA:n murtamiseen vaaditaan 4098 vakaata kubittia. Shorin algoritmilla *ECDLP*:n eli elliptisen käyrän diskreetin logaritmin ongelman ratkaisuun vaaditaan 2330 vakaata kubittia 256 bitin salaukselta. (Roetteler et al., 2017.)

Jos tarkastellaan meluisien kubittien käyttöä, niin esimerkiksi optimoitu Shorin algoritmin variantti RSA-salauksen murtamiseen vuodelta 2019 kykenee yleisesti käytetyn 2048 bitin RSA-salauksen murtamiseen kahdeksassa tunnissa vaatien arviolta 20 000 000 meluisaa kubittia. Määrä kuulostaa suunnattomalta, mutta vuonna 2015 arvio kubittien määrästä oli miljardi. Ennuste kubittien tarpeen määrästä putosi siis lähes kaksi suuruusluokkaa. (Gidney ja Ekerå, 2021.)

4.2 Groverin algoritmi

Groverin algoritmi perustuu oikean arvon etsintään. Ajatellaan, että on jokin äärellinen joukko N johon muuttuja x kuuluu ja funktio f jolle pätee $f(x) = 1$. Tehtävänä on löytää x joukosta N. Ongelma on hankalin siinä tapauksessa, että $f(x) = 1$ toteutuu vain yhdellä muuttujan x arvolla. Klassisessa laskennassa muuttujan x arvon löytämiseen vaaditaan pahimassa tapauksessa $|N|$ kokeilua eli joudutaan käydä kaikki vaihtoehdot läpi. Lov Grover

osoitti vuonna 1996, että kvanttilaskennalla vaaditaan vain $\sqrt{|N|}$ kokeilua. (Grover, 1996.)

Groverin algoritmia voidaan käyttää esimerkiksi raakahyökkäyksessä symmetristä salausta vastaan parantaen raakahyökkäyksen ajassa $O(|N|)$ tapahtuvan aikavaativuuden tapahtumaan ajassa $O(\sqrt{|N|})$ (Gheorghiu ja Mosca, 2019; Jordan ja Liu, 2018). Kvanttiturvallisessa kryptografiassa tähän on vastattu kaksinkertaistamalla salausavaimen koko symmetrisissä salauksissa (Gheorghiu ja Mosca, 2019).

Groverin algoritmia voidaan myös käyttää tiivistefunktioiden törmäyksien löytämiseen. Kuten klassisen toteutuksen tapauksessa, josta kerrottiin luvussa 2.1.2, niin kvanttilaskennan avulla voidaan suorittaa syntymäpäivähyökkäys ("*quantum birthday attack*"). Groverin algoritmia hyödyntämällä aikavaativuus putoaa aikavaativuudesta $O(\sqrt{N})$ aikavaativuudeksi $O(\sqrt[3]{N})$. (Brassard et al., 1997; Mavroeidis et al., 2018.)

4.3 Kvanttihehkutus kryptoanalyysissa

Kvanttihehkutus saattaa tarjota kvanttikryptoanalyysille tehokkaan keinon murtaa jokin kryptografinen menetelmä, jos kyseisen kryptografisen menetelmän murtaminen voidaan muuttaa optimointiongelmaksi, jonka kvanttihehkutukseen perustuva kvanttialgoritmi voi ratkaista. Kvanttihehkutuksella voidaan laskea tekijöihin jakoa kubittien määrällä $O(log^2 N)$, jossa N on tekijöihin jaettava luku. (Jiang et al., 2018.)

Vähintäänkin kvanttihehkutuksella voidaan parantaa minkä tahansa klassisen etsimisalgoritmin aikavaativuutta aikavaativuudesta $O(N)$ aikavuuteen $O(\sqrt{N})$. Voidaankin osoittaa, että adiabaattisella kvanttilaskennalla ("*adiabatic quantum computing*") voidaan toteuttaa Groverin algoritmia vastaava kvanttialgoritmi. Adiabaattinen kvanttilaskenta sisältyy kvanttihehkutukseen, joten kvanttihehkutuksella voidaan toteuttaa Groverin algoritmi. (Dam et al., 2001.)

4.4 Kvanttiturvallisen kryptografian vastaus kvanttikryptoanalyysille

Julkisen avaimen kryptografia on vaarassa lähinnä Shorin algoritmin takia, kun tarpeeksi tehokas kvanttitietokone kehitetään. Klassinen kryptografia kuitenkin tarjoaa erilaisia julkisen avaimen kryptografisia menetelmiä, jotka eivät ole vaarassa Shorin algoritmilla suoritettavia hyökkäyksiä vastaan. (Chen et al., 2016.)

Yksi mielenkiintoa herättänyt kryptografian osa-alue on hilapohjainen kryptografia ("*lattice-*

based cryptography"). Syynä on muun muassa menetelmien suhteellinen yksinkertaisuus, tehokkuus ja rinnakkaistettavuus. Lisäksi jotkin hilapohjaiset systeemit voidaan todistaa turvallisiksi pahimman tapauksen vaativuuden mukaan sen sijaan, että kyseessä olisi keskiarvoinen tapaus. Hilapohjaisen kryptografian turvallisuus kvanttikryptoanalyysin tapauksessa on tosin vielä avoin kysymys, sillä on osoittautunut, että turvallisuuden todistaminen on ollut vaikeaa jopa klassisen kryptoanalyysin tapauksessa. (Chen et al., 2016.)

Koodipohjaisen kryptografian ("*code-based cryptography*") murtaminen on erityisen haastava laskennallinen ongelma. Yksi parhaimmista menetelmistä sen murtamiseen on raakahyökkäys, jota voidaan nopeuttaa kvanttilaskennalla, jolloin salausavaimen koko puolittuu (Chen et al., 2016). Huomattavaa on se, että koodipohjaisen kryptografian turvallisuuden takaamiseksi pätee sama ominaisuus kuin symmetriselle kryptografialle eli salausavain pitää kaksinkertaistaa, jotta se olisi turvallinen kvanttialgoritmeja vastaan. Koodipohjaisen kryptografian ongelma on kuitenkin sen avaimien todella suuret koot. Koodipohjaista kryptografiaa pidetään kuitenkin lupaavana vaihtoehtona korvaamaan käytettyjä julkisen avaimen kryptografian menetelmiä. Erityisesti koodipohjainen kryptografia voisi korvata julkisen avaimen salauksia kuten RSA:n (Chen et al., 2016; Kuznetsov et al., 2017).

Usean muuttujan polynomisen kryptografian ("*multivariate polynomial cryptography*") turvallisuus perustuu vaikeuteen ratkaista systeemit, jotka perustuvat usean muuttujan polynomeihin yli äärellisten kuntien. Monet kyseisenkaltaiset systeemit ovat kuitenkin murtuneet. Monimuuttuja polynominen kryptografia on ollut menestyksellisempää digitaalisissa allekirjoituksissa salauksien sijaan. (Chen et al., 2016.)

Tiivistefunktioihin perustuvat allekirjoitukset ("*hash-based signatures*") ovat osoittautuneet yhdeksi kryptografian osa-alueeksi, jota voitaisiin käyttää kvanttikryptoanalyysia vastaan. Tiivistefunktioihin perustuvien allekirjoituksien turvallisuus on hyvin tunnettu jopa kvanttialgoritmien muodostamien uhkien tapauksessa. Rajoittavia tekijöitä tehokkaille tiivistefunktioihin perustuville allekirjoituksille ovat muun muassa allekirjoittajan tarve pitää kirjaa allekirjoitettujen viestien määrästä ja kyky tuottaa ainoastaan rajallinen määrä allekirjoituksia. (Chen et al., 2016.)

Läpikäydyistä kvanttiturvallisen kryptografian menetelmien tyypeistä yhtäkään ei ole todistettu turvalliseksi kaikkia kvanttialgoritmeja vastaan. Jonain päivänä kvanttikryptoanalyysi saattaa tarjota sellaisen kvanttialgoritmin, joka murtaa jonkin edellä mainituista kryptografian osa-alueista. (Chen et al., 2016.)

5 Pohdintaa

Kvanttikryptologian avointa tutkimusta luulen varjostavan klassiselle kryptologialle tuttu salainen tutkimus (Massey, 1988). Onhan kvanttikryptologia kuitenkin kryptologiaa. Voi olla, että erinäiset tahot, kuten valtiot, ovat jo pidemmällä kehityksessä ja saavuttaneet läpimurtoja suljettujen ovien takana. Näitä läpimurtoja saatetaan kohdella valtiosalaisuuksina, kuten historiassa on tehty. Singhin kryptologian historiaa käsittelevä kirja (Singh, 1999) tukee tätä väitettä.

Universaalien kvanttitietokoneiden tehokkuus saattaa riittää esimerkiksi Shorin algoritmille jo alle kymmenen vuoden päästä. Google pyrkii kehittämään miljoonan kubitin kvanttiprosessorin vuoteen 2029 mennessä ja jos IBM jatkaa samanlaista kehitystä, niin saatetaan nähdä kvanttitietokone, jolla voidaan murtaa esimerkiksi RSA jo aiemmin (Lapedus, 2021). Olen törmännyt varteenotettaviin arvioihin kymmenistä vuosista, ja kyseisistä arvioista on jo vuosia.

Kvanttitietokoneiden kehityksen lisäksi kvanttihehkutus kvanttilaskennan muotona tarjoaa lupaavia tuloksia ja saattaa viedä kvanttikryptoanalyysia harppauksella eteenpäin. Ainakaan toistaiseksi esimerkiksi Shorin algoritmista ei ole sellaista kvanttihehkutuksella toteutettua versiota, joka murtaisi nykyään käytössä olevia kryptografisia protokollia kuten RSA:n. Shorin algoritmi on universaalien kvanttitietokoneiden kvanttialgoritmi. Jääkin nähtäväksi saavutetaanko aikaisemmin tarpeeksi tehokas universaali kvanttitietokone Shorin algoritmia varten vai kehitetäänkö Shorin algoritmista sellainen versio, että se voitaisiin toteuttaa kvanttihehkutuksella. Toisin sanoen voidaanko esimerkiksi tekijöihin jako muuttaa optimointiongelmaksi, joka voitaisiin puolestaan ratkaista kvanttihehkutuksen avulla.

Tutkielman tekemisen aikana olen myös törmännyt sellaisiin väitteisiin, että koskaan ei saavutettaisi tarpeeksi tehokasta kvanttitietokonetta, joka kykenisi murtamaan nykyään käytössä olevia kryptografisia menetelmiä. Väite on varteenotettava siihen asti, kunnes jokin nykyisistä kryptografisista menetelmistä murtuu kvanttilaskennan avulla. Oli lopputulos kumpi tahansa, niin varmaa on, että turvallisuuden takaamiseksi on kvanttikryptoanalyysin mahdollisuuksiin varauduttava ja nykyisiä kryptografisia menetelmiä on parannettava niin, että ne ovat milloinkin tarpeeksi turvallisia kvanttihyökkäyksiä vastaan.

Kvanttiavaimen jako on hyvä esimerkki siitä, kuinka kvanttilaskenta mullistaa kryptologiaa. Klassinen kryptografia perustuu laskennan vaikeuteen eli kryptografista protokollaa voidaan pitää turvallisena, jos sen murtamiseen sen hetkisellä teknologialla kuluisi esimerkiksi miljoo-

nia vuosia. Klassisen kryptografian vitsaus on kuitenkin se, että teknologian kehittyessä murtamiseen kuluva aika voi tippua dramaattisesti, jolloin kryptografinen protokolla ei ole enää turvallinen. Kvanttiavaimen jako puolestaan ei ole riippuvainen laskentatehosta, sillä kvanttiavaimen jaossa yksittäinen kubitti voidaan mitata vain kerran, jonka jälkeen se menettää superposition. Kvanttiavaimen jaon turvallisuus perustuu siihen, kuinka paljon suoritetaan salakuuntelun tarkistamista. Esimerkiksi tarkistamalla 50 kubittia, niin salakuuntelija havaitaan 99,9999... % todennäköisyydellä. Turvallisuutta voidaan vielä kasvattaa vertaamalla enemmän kubitteja. Kvanttiavaimen jaossa on kuitenkin vielä parantamisen varaa sen käytännön toteutuksessa.

6 Yhteenveto

Kvanttilaskenta tarjoaa kryptologialle ennennäkemättömiä mahdollisuuksia klassiseen kryptologiaan nähden. Klassista kryptologiaa tarvitaan kuitenkin edelleen. Esimerkiksi kvanttiturvallisessa kryptografiassa kehitetään ja tutkitaan sellaisia menetelmiä, jotka eivät murru, vaikka kvanttikryptoanalyysissa koettaisiin läpimurto. Julkisen avaimen kryptografia on vaarassa murtua totaalisesti tarpeeksi tehokkaan kvanttitietokoneen kehittämisen myötä. Kvanttikryptografian menetelmiä saattaakin tulla laajasti käyttöön esimerkiksi julkisen avaimen kryptografian menetelmien korvaajina. Vaihtoehtoisesti ratkaisuja on etsitty kvanttiturvallisesta kryptografiasta.

Kvanttikryptologian tutkimus on tärkeää ja ajankohtaista. Salauksia voidaan purkaa jälkikäteen, joten esimerkiksi tänä päivänä tallennettu salattu viesti voidaan tulevaisuudessa teknologian mahdollistaessa murtaa. Varsinkin tehokkaiden sekä luotettavien ratkaisujen kehittäminen kestää vuosia, kuten myös kryptograafisen infrastruktuurin vaihtaminen.

Ainakaan vielä kvanttikryptoanalyysin kvanttialgoritmit eivät pysty murtamaan nykyään käytössä olevia kryptografisia protokollia kvanttilaskennan teknisen vaativuuden vuoksi. Monet teoriat ja kvanttialgoritmit odottavat tarpeeksi tehokkaan kvanttitietokoneen kehittämistä. Kvanttikryptografiassa on jo kuitenkin nähty protokollia, joita on saatu vietyä teoriasta aina kaupalliseen tuotantoon asti, esimerkkinä kvanttiavaimen jako.

Lähteet

Amer, O., Garg, V. ja Krawec, W. O. (2021). "An Introduction to Practical Quantum Key Distribution". *IEEE Aerospace and Electronic Systems Magazine* 36.3, s. 30–55. DOI: 10.1109/MAES.2020.3015571.

Anne Broadbent, C. S. (2015). "Quantum cryptography beyond quantum key distribution". *Designs, Codes and Cryptography* 78, s. 351–382. DOI: 10.1007/s10623-015-0157-4.

Bhatia, V. ja Ramkumar, K. (2020). "An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm". Teoksessa: *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, s. 89–94. DOI: 10.1109/ICCCA49541.2020.9250806.

Bozzio, M., Orieux, A., Vidarte, L. T., Zaquine, I., Kerenidis, I. ja Diamanti, E. (2018). "Experimental investigation of practical unforgeable quantum money". *npj Quantum Information* 4.1, s. 1–8.

Brassard, G., Høyer, P. ja Tapp, A. (kesäkuu 1997). "Quantum Cryptanalysis of Hash and Claw-Free Functions". *SIGACT News* 28.2, s. 14–19. ISSN: 0163-5700. DOI: 10.1145/261342.261346. URL: https://doi-org.libproxy.helsinki.fi/10.1145/261342.261346.

Chandra, S., Paira, S., Alam, S. S. ja Sanyal, G. (2014). "A comparative survey of Symmetric and Asymmetric Key Cryptography". Teoksessa: *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, s. 83–93. DOI: 10.1109/ICECCE.2014.7086640.

Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. ja Smith-Tone, D. (2016). *Report on post-quantum cryptography*. Vol. 12. US Department of Commerce, National Institute of Standards ja Technology.

D-Wave Systems (2021). *D-Wave Systems*. URL: https://www.dwavesys.com/ (viitattu 06. 12. 2021).

D-Wave Systems Documentation (2021). *What is Quantum Annealing?* URL: https://docs.dwavesys.com/docs/latest/c_gs_2.html (viitattu 04. 12. 2021).

Dam, W. van, Mosca, M. ja Vazirani, U. (2001). "How powerful is adiabatic quantum computation?" Teoksessa: *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, s. 279–287. DOI: 10.1109/SFCS.2001.959902.

Flajolet, P., Gardy, D. ja Thimonier, L. (1992). "Birthday paradox, coupon collectors, caching algorithms and self-organizing search". *Discrete Applied Mathematics* 39.3. cited By 229,

s. 207–229. DOI: 10.1016/0166-218X(92)90177-C. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-38249007777&doi=10.1016%2f0166-218X%2892%2990177-C&partnerID=40&md5=72df1003c1aa808efab04ff65b2b36ed.

Gheorghiu, V. ja Mosca, M. (2019). *Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes*. arXiv: 1902.02332 [quant-ph].

Gidney, C. ja Ekerå, M. (huhtikuu 2021). "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". *Quantum* 5, s. 433. ISSN: 2521-327X. DOI: 10.22331/q-2021-04-15-433. URL: http://dx.doi.org/10.22331/q-2021-04-15-433.

Grover, L. K. (1996). "A fast quantum mechanical algorithm for database search". Teoksessa: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, s. 212–219.

Hauke, P., Katzgraber, H. G., Lechner, W., Nishimori, H. ja Oliver, W. D. (2020). "Perspectives of quantum annealing: Methods and implementations". *Reports on Progress in Physics* 83.5, s. 054401.

IBM (2021). *Quantum Computing*. URL: https://www.ibm.com/quantum-computing/ (viitattu 29. 11. 2021).

Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S. ja Kais, S. (2018). "Quantum annealing for prime factorization". *Scientific reports* 8.1, s. 1–9.

Jordan, S. (2021). *Quantum Algorithm Zoo*. URL: https://quantumalgorithmzoo.org/ (viitattu 12. 12. 2021).

Jordan, S. P. ja Liu, Y.-K. (2018). "Quantum Cryptanalysis: Shor, Grover, and Beyond". *IEEE Security Privacy* 16.5, s. 14–21. DOI: 10.1109/MSP.2018.3761719.

Kadowaki, T. ja Nishimori, H. (1998). "Quantum annealing in the transverse Ising model". *Physical Review E* 58.5, s. 5355.

Kaplan, M., Leurent, G., Leverrier, A. ja Naya-Plasencia, M. (joulukuu 2016). "Quantum Differential and Linear Cryptanalysis". *IACR Transactions on Symmetric Cryptology*, s. 71–94. ISSN: 2519-173X. DOI: 10.46586/tosc.v2016.i1.71-94. URL: http://dx.doi.org/10.46586/tosc.v2016.i1.71-94.

Kelly, J. (2021). *A Preview of Bristlecone, Google's New Quantum Processor*. URL: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (viitattu 04. 12. 2021).

Kuznetsov, A., Svatovskij, I., Kiyan, N. ja Pushkar'ov, A. (2017). "Code-based public-key cryptosystems for the post-quantum period". Teoksessa: *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S T)*, s. 125–130. DOI: 10.1109/INFOCOMMST.2017.8246365.

Lapedus, M. (2021). *The Great Quantum Computing Race*. URL: https://semiengineering.com/the-great-quantum-computing-race/ (viitattu 06. 12. 2021).

Massey, J. (1988). "An introduction to contemporary cryptology". *Proceedings of the IEEE* 76.5, s. 533–549. DOI: 10.1109/5.4440.

Mavroeidis, V., Vishi, K., D., M. ja Jøsang, A. (2018). "The Impact of Quantum Computing on Present Cryptography". *International Journal of Advanced Computer Science and Applications* 9.3. ISSN: 2158-107X. DOI: 10.14569/ijacsa.2018.090354. URL: http://dx.doi.org/10.14569/IJACSA.2018.090354.

Nielsen, M. A. ja Chuang, I. (2002). *Quantum computation and quantum information*.

NIST, C. (heinäkuu 1992). "The Digital Signature Standard". *Commun. ACM* 35.7, s. 36–40. ISSN: 0001-0782. DOI: 10.1145/129902.129904. URL: https://doi-org.libproxy.helsinki.fi/10.1145/129902.129904.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. ja Wallden, P. (joulukuu 2020). "Advances in quantum cryptography". *Adv. Opt. Photon.* 12.4, s. 1012–1236. DOI: 10.1364/AOP.361502. URL: http://www.osapublishing.org/aop/abstract.cfm?URI=aop-12-4-1012.

Preneel, B. (1994). "Cryptographic hash functions". *European Transactions on Telecommunications* 5.4, s. 431–448.

Roetteler, M., Naehrig, M., Svore, K. M. ja Lauter, K. (2017). *Quantum resource estimates for computing elliptic curve discrete logarithms*. arXiv: 1706.06752 [quant-ph].

Shor, P. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". Teoksessa: *Proceedings 35th Annual Symposium on Foundations of Computer Science*, s. 124–134. DOI: 10.1109/SFCS.1994.365700.

Shor, P. W. (lokakuu 1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing* 26.5, s. 1484–1509. ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172.

Singh, S. (1999). *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. 1st. USA: Doubleday. ISBN: 0385495315.

Wallden, P. ja Kashefi, E. (maaliskuu 2019). "Cyber Security in the Quantum Era". *Commun. ACM* 62.4, s. 120. ISSN: 0001-0782. DOI: 10.1145/3241037. URL: https://doi-org.libproxy.helsinki.fi/10.1145/3241037.