Tampereen yliopisto

Taisto Tammilehto

KVANTTISALAUS

Turvaprotokollat ja käytännön sovellukset

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Elokuu 2024

TIIVISTELMÄ

Taisto Tammilehto: Kvanttisalaus – turvaprotokollat ja käytännön sovellukset
Kandidaattitutkielma
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaattiohjelma, tietotekniikka
Elokuu 2024

Tämän kandidaattitutkielman tavoitteena on antaa yleiskatsaus kvanttisalauksesta. Tutkielmasta tekee merkittävän suomenkielisen kirjallisuuden puute kvanttimekaniikan sovelluksista, kvanttilaskennasta ja etenkin kvanttisalauksesta. Kvanttilaskennan yleistyessä klassiset salausmenetelmät joutuvat kohtaamaan uudenlaisia hyökkäysriskejä. Tutkielma osoittaa lukijalle miksi klassiset kryptografiset menetelmät eivät ole tehokkaita kvanttilaskennallisia menetelmiä vastaan. Tutkielmassa korostuu kvanttisalauksen tärkeys yhteiskunnassa tulevaisuuden tietoturvan takaamiseksi. Tämä kirjallisuuskatsaus tutkii kvanttisalausta yleisestä näkökulmasta ja pyrkii antamaan lukijalle kattavan kuvauksen kvanttisalauksesta syventymättä aiheen matemaattiseen perustaan.

Kvanttisalaus on kansainvälisesti laajasti tutkittu aihe, josta on olemassa runsas englanninkielinen kirjallisuus. Tässä tutkielmassa kootaan yhteen kvanttisalausta käsittelevää kirjallisuutta ja vertaillaan kahta eri turvaprotokollaa. Tutkielmassa osoitetaan, kuinka kvanttimekaniikka on kytköksissä kvanttilaskentaan ja kvanttisalaukseen. Kvanttisalaukseen syvennytään tarkastelemalla kvanttikanavien toteutusta kvanttisalausjärjestelmässä. Turvaprotokollia vertaillaan keskenään ja lopuksi tarkastellaan BB84-turvaprotokollan implementointia kvanttisalausjärjestelmässä. Kvanttisalauksen toteutusta tutkimalla tämä kirjallisuuskatsaus antaa selkeän kuvan kvanttisalausjärjestelmistä ja niiden käytännön sovelluksista.

Kvanttilaskentaa on tutkittu pitkään ja useat läpimurrot kuten Shorin ja Groverin algoritmit julkaistiin jo 1900-luvun loppupuolella. Kirjallisuuskatsauksessa tutkitaan tämän vuoksi niin vanhoja kuin uusiakin julkaisuja. Tutkielman tulokset osoittavat kvanttisalauksen olevan lupaava teknologia, joka voi mullistaa kryptografian alan tulevaisuudessa. Kvanttitietokoneiden mahdollinen vaikutus nykyiseen kryptografiseen infrastruktuuriin on vakava huolenaihe, joka ansaitsee laajaa huomiota. Viimeaikaiset hyökkäykset kuten psykoterapiakeskus Vastaamoon ja Helsingin kaupunkiin kohdistuneet tietomurrot osoittavat, että vihamielisistä tekijöistä ei ole puutetta. Tutkielman tulokset ilmaisevat tarvetta luoda selkeä suunnitelma nykyisen yhteiskunnan tietoturvajärjestelmien vahvistamiseksi kvanttilaskennan mahdollistamia hyökkäyksiä vastaan.

Avainsanat: kvanttisalaus, kvanttikryptografia, kvanttitietoturva, kvanttitieto, kryptografia.

ALKUSANAT

Haluan ilmaista syvän kiitollisuuteni perheelleni heidän antamastaan tuesta.

Tampereella, 23.8.2024

Taisto Tammilehto

SISÄLLYSLUETTELO

1 Johdanto

Tässä kirjallisuuskatsauksessa analysoidaan kvanttisalauksen keskeisiä turvaprotokollia ja niiden toteutusta kvanttikanavien avulla. Kvanttisalauksen turvaprotokollia ja käytännön sovelluksia on vaikea ymmärtää ilman syvällistä käsitystä kvanttimekaniikan perusteista sekä kryptografiasta. Katsaus alkaa kvanttisalauksen perusteiden esittelyllä, jossa käsitellään sekä klassisen kryptografian että kvanttimekaniikan keskeisiä käsitteitä. Kvanttilaskenta uhkaa klassisia tietoturvajärjestelmiä, sillä kvanttilaskennan menetelmillä voidaan murtaa salauksia, joita ei klassisilla menetelmillä pysty murtamaan. Kvanttisalaus kehitettiin osittain tulevaisuuden turvaamiseksi, jotta olemassa olevia ja tulevia tietoturvajärjestelmiä voidaan suojata kvanttilaskennallisia menetelmiä vastaan. Tutkielman tutkimuskysymykset ovat:

1. Miten kvanttisalaus eroaa perinteisistä salausmenetelmistä?
2. Miten kvanttisalaus toimii käytännössä ja mitä haasteita kvanttisalauksen toteuttamisessa on?
3. Missä määrin kvanttikryptografia voi tarjota turvallisen ratkaisun arkaluonteisten tietojen suojaamiseen kvanttitietokoneiden aikakaudella, ja mitä rajoituksia ja mahdollisia kompromisseja sen käyttöönottoon liittyy?

1.1 Tutkielman rakenne

Tämä tutkielma tarjoaa yleiskatsauksen kvanttisalauksen perusteista ja sen soveltamisesta käytännön tietoturvajärjestelmissä. Tutkielmassa pohditaan, kuinka kvanttisalauksen avulla voidaan parantaa nykyisten kryptografisten menetelmien turvallisuutta ja vastata kasvaviin tietoturvahaasteisiin. Erojen selittäminen osoittaa, miksi kvanttimekaniikan perusteisiin pohjautuva kvanttisalaus tarjoaa vahvempaa tietoturvaa ja parempaa avaintenhallintaa kuin klassinen kryptografia, joka pohjautuu matemaattisiin laskelmiin. Kirjallisuuskatsaus tarjoaa myös historiallista viitekehystä kryptografiaan tarkastelemalla sen kehitystä muinaisista ajoista modernille aikakaudelle. Kvanttisalaukseen syvennytään tarkastelemalla kvanttikanavien perustamista ja siirtovälineitä, joita on käytetty kvanttisalausjärjestelmien käytännön toteutuksissa. Turvaprotokollia ja niiden sovelluksia käsitellään tarkasti tutkimalla niiden käytännön haasteita ja turvallisuutta. Johtopäätöksissä korostuu tarve siirtyä klassisesta salauksesta kohti kvanttisalausta uusien kvanttitekniikoiden kehittyessä ja yleistyessä. Tutkielman tarkoituksena on toimia apuvälineenä kvanttisalauksesta ja tietoturvan tulevaisuudesta kiinnostuneille.

Tutkielmassa on johdantoluvun lisäksi kahdeksan lukua, joissa käsitellään seuraavia aiheita:

- **Kryptografian perusteet ja CIA-malli:** Katsaus alkaa esittelemällä lukijalle kryptografian perusperiaatteet ja CIA-mallin (Confidentiality, Integrity, Availability). Lisäksi luvussa syvennytään kryptografian historiaan ja vanhoihin salausmenetelmiin.
- **Kvanttilaskenta ja periaatteiden yhteys:** Kolmannessa luvussa syvennytään kvanttilaskentaan ja osoitetaan, kuinka kvanttimekaniikan perusteet liittyvät kvanttilaskentaan. Luvussa yhdistetään aikaisemman luvun kvanttimekaniikan periaatteet kvanttilaskennan käsitteisiin.
- **Kvanttilaskennan ja kvanttisalauksen yhteys:** Neljännessä luvussa osoitetaan lukijalle kvanttilaskennan ja kvanttisalauksen yhteys. Luvussa vertaillaan klassisen kryptografian ja kvanttisalauksen eroja. Lisäksi siinä syvennytään kvanttisalaukseen ja klassiseen kryptografiaan.
- **Kvanttikanavien toteutus ja siirtovälineiden vertailu:** Viidennessä luvussa tutkitaan kvanttikanavien toteutusta ja vertaillaan kahden eri väliaineen ominaisuuksia.
- **Turvaprotokollat kvanttisalausjärjestelmissä:** Kuudennessa luvussa tutustutaan kvanttisalaukseen tarkemmin. Luvussa käsitellään kahta turvaprotokollaa, joita käytetään oikeissa kvanttisalausjärjestelmissä.
- **Turvaprotokollan implementointi:** Seitsemännessä luvussa tarkastellaan turvaprotokollan käytännön toteutusta kvanttisalausjärjestelmissä.
- **Tulevaisuus:** Kahdeksannessa luvussa arvioidaan kvanttilaskennan vaikutusta tulevaisuuden tietoturvaan.
- **Yhteenveto:** Viimeisessä luvussa kootaan yhteen tutkielman ydinviesti ja arvioidaan lähteiden luotettavuutta.

1.2 Esitietoa

Tutkielmassa selitetään useita kvanttisalauksen ja kvanttilaskennan periaatteita lomittumisen ja superposition avulla. Tässä on lyhyt selitys **superpositiolle** ja **lomittumiselle**, jotta lukijan on helpompi ymmärtää aihetta:

Superpositio: Kuvitellaan kolikko, joka heitetään ilmaan. Kolikko on samanaikaisesti sekä kruuna että klaava ennen kuin se laskeutuu. Vastaavasti kubitti voi olla sekä 0 että 1 samanaikaisesti, kunnes se mitataan. Superpositio on kvanttimekaniikan keskeinen ominaisuus, joka mahdollistaa kvanttilaskennan. Se tarkoittaa sitä, että kvanttibitti, eli kubitti, voi olla lineaarisena yhdistelmänä kahdesta perustilasta $|0\rangle$ ja $|1\rangle$. Tämä voidaan esittää matemaattisesti seuraavasti: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, missä α ja β ovat kompleksilukuja, jotka täyttävät ehdon $|\alpha|^2 + |\beta|^2 = 1$. (Nielsen & Chuang, 2000, s. 13–14)

Lomittuminen: Kuvittele kaksi hansikasta, jotka ovat aluksi eri laatikoissa. Tiedät, että toisessa laatikossa on oikea ja toisessa vasen hanska, mutta et tiedä, kummassa laatikossa kumpikin hanska on. Kun avaat yhden laatikon ja näet, että siinä on oikea hanska,

tiedät välittömästi, että toisessa laatikossa on vasen hanska. Lomittuminen on tähän verrattava ilmiö, mutta kvanttimaailmassa hiukkaset voivat olla samanaikaisesti useassa tilassa (superpositio), kunnes ne mitataan.

Tao (2024) selittää, että lomittuminen on kvanttimekaniikan erikoinen ilmiö, jossa kaksi tai useampi hiukkanen on niin tiiviisti yhteydessä toisiinsa, että niiden tila ei ole määriteltävissä yksittäin, vaan ainoastaan yhteisenä tilana. Tämä tarkoittaa, että kun mitataan yhden lomittuneen hiukkasen tila, myös toisen hiukkasen tila määrittyy välittömästi, riippumatta siitä, kuinka kaukana hiukkaset ovat toisistaan. Tätä ilmiötä ei voida selittää klassisen fysiikan avulla, sillä klassisessa maailmassa kahden objektin tila ei voi vaikuttaa toisiinsa välittömästi, jos ne ovat riittävän kaukana toisistaan. (Tao, 2024)

Lomittumista voidaan kuvata matemaattisesti käyttämällä tensorituloa. Jos kahden hiukkasen tila on lomittunut, sitä ei voida esittää kahden yksittäisen hiukkasen tilan yksinkertaisena tulona. Sen sijaan lomittuneen tilan täytyy kuvata yhtenä kokonaisuutena. Esimerkiksi Bell-parit ovat tyypillinen esimerkki lomittuneista hiukkasista, ja niiden tila voidaan esittää seuraavasti: $|\Psi\rangle = (|01\rangle + |10\rangle) / \sqrt{2}$. Tässä tilassa, jos ensimmäisen hiukkasen tila on 0, toisen hiukkasen tila on varmasti 1, ja päinvastoin. (Nielsen & Chuang, 2000)

2 Kryptografian perusteet

Panayiotis Kotzanikolau ja Christos Douligeris selittävät, että kryptografian alkuperäinen tarkoitus oli viestien luottamuksellisuuden takaaminen. Nykyaikainen kryptografia käsittelee kuitenkin laajempaa kirjoa aiheita. (Kotzanikolau & Douligeris, 2007, s. 459) Tässä luvussa tutustutaan kryptografian periaatteiseen ja historiaan.

2.1 Kryptografian periaatteet

Kryptografia on sidonnainen useaan tärkeään periaatteeseen. Tässä osiossa on esitelty kuusi kryptografialle olennaista periaatetta ja teoksia, jotka käsittelevät periaatteita.

1. Luottamuksellisuus: Tämä periaate takaa, ettei tietoon pääse käsiksi kukaan muu, kuin henkilö, joka on valtuutettu käsittelemään tietoa (Kotzanikolau & Douligeris, 2007, s. 459). Luottamuksellisuus on tärkeä osa CIA-mallin (Engl. Confidentiality, Integrity, Availability) eheyden takaamisessa. Tämä kolminaisuus tunnetaan tietoturvan kolmena päätavoitteena.

2. Todennus: Mike Just (2011) kertoo todennuksen takaavan viestin lähettäjän identiteetin, mikä varmentaa viestin todenperäisyyden. (Just, 2011)

3. Salaus: Tämä prosessi sisältää tiedon muuntamisen lukemattomaan muotoon salausalgoritmia hyödyntämällä. Levgeniia Kuzminykh, Bogdan Ghita ja Stavros Shiaeles (2021) selittävät, että salauksen avulla tiedon yksityisyyttä suojataan. (Kuzminykh et al., 2021, s. 1)

4. Tiedon eheys: Tämä periaate takaa kolmansien osapuolien häirinnän eston, jolloin datan johdonmukaisuus ja tarkkuus siirron aikana lähettäjältä vastaanottajalle säilyy. (Kotzanikolaou & Douligeris, 2007, s. 459; Martin, 2012)

5. Kiistämättömyys: Tämä periaate takaa, ettei lähettäjä pysty kieltämään allekirjoituksensa autenttisuutta. Kiistämättömyys tyypillisesti saavutetaan käyttämällä digitaalisia allekirjoituksia, jotka ovat lähettäjille ainutlaatuisia. (Just, 2011)

6. Avainhallinta: Kuzminykh ja muut (2021) kertovat avaintenhallinnan sisältää kryptografisten avainten ylläpidon, mihin kuuluu avainten jako, generointi, kierto ja muita tehtäviä. (Kuzminykh et al., 2021, s. 2–3)

Kotzanikolau ja Douligeris selittävät, että edellä mainittujen käytäntöjen lisäksi kryptografia voi myös saavuttaa useita muita turvallisuustavoitteita tietojärjestelmissä, kuten kulunvalvonnan, nimettömyyden, tai aikaleimauksen. (Kotzanikolau & Douligeris, 2007, s. 459–478) Kotzanikolaou ja Douligeris huomauttavat, että vaikka kryptografia on välttämätöntä tietoverkko- ja järjestelmäturvallisuudelle, ei se ole synonyymi turvallisuudelle (Kotzanikolaou & Douligeris, 2007). Travis Scholten ja kumppanit korostavat, että tavoiteltujen turvallisuuspäämäärien saavuttamiseksi on huomioitava myös organisatoriset menetelmät ja muut tekniset keinot (Scholten et al., 2024, s. 33–34).

2.2 Kryptografian historiaa

Kryptografia on ollut osa ihmiskunnan historiaa tuhansien vuosien ajan. Sen juuret ulottuvat noin 1900 eaa. muinaiseen Egyptiin, jossa hautamuistomerkkeihin kaiverrettuja hieroglyfejä on tulkittu salakirjoitukseksi. Myös Mesopotamiassa löydetyt savitaulut sisältävät salattuja tekstejä, joiden uskotaan olevan keramiikan lasitteen salaisia reseptejä. (Awasthi, 2024; Schneider, 2024). Antiikin Kreikassa 650 eaa. spartalaiset käyttivät scytale-nimistä välineistöä, jossa viesti kirjoitettiin puupalalle kiedotulle nahkarenkaalle. Vain oikean kokoinen puupala pystyi purkamaan viestin. Roomassa noin 100–40 eaa. Rooman armeija käytti keisarinsalausta, jossa jokainen kirjain korvattiin toisella kirjaimella, joka sijaitsi aakkosissa tietyn määrän paikkoja eteenpäin tai taaksepäin. (Kahn, 1996; Schneider, 2024) Esimerkiksi kirjaimesta A tulisi D ja kirjaimesta B tulisi E ja niin edelleen. (Andress, 2014; Schneider, 2024)

Keskiajalla 800-luvulla arabialaiset matemaatikot, kuten Al-Kindi, tekivät merkittäviä löytöjä kryptoanalyysin alalla. He kehittivät muun muassa frekvenssianalyysin, joka perustui kirjainten ja kirjainten yhdistelmien esiintymistiheyksien tutkimiseen. Frekvenssianalyysi oli kuitenkin vain yksi osa laajempaa kryptoanalyyttista työkalupakkia, jota kehitettiin eri kulttuureissa vuosisatojen ajan. Menetelmää käytettiin yksinkertaisen salauksen, kuten Caesarin salatekstin murtamiseen. (Kahn, 1996; Schneider, 2024) Frekvenssianalyysi perustuu siihen, että kielissä kirjaimet ja kirjainten yhdistelmät esiintyvät eri tiheyksillä.

Tässä on yksinkertaistettu selitys frekvenssisanalyysin toiminnasta:

1. Ensin katsotaan salattua viestiä ja lasketaan kirjaimien esiintyvyys, mikä antaa kunkin kirjaimen esiintyvyystiheyden.
2. Tämän jälkeen esiintyvyystiheyksiä verrataan tunnettuihin kirjainten esiintyvyystiheyksiin salatun viestin kielessä. Esimerkiksi kirjain ”E” on yleisin kirjain englannin kielessä ja sitä seuraa ”T”, ”A”, ”O”, ”I” ja ”N”.
3. Esiintyvyystiheyksiä vertailemalla voidaan tehdä valistuneita veikkauksia salatun viestin sisällöstä. Kirjaimen ”X” ollessa englanninkielisen kirjeen käytetyin kirjain, voidaan arvata hyvällä tarkkuudella kirjaimen ”X” vastaavan kirjainta ”E” tai ”T”.
4. Arvaukset voidaan sijoittaa salattuun viestiin, jolloin alkuperäiset sanat tai lauseet alkavat näkymään ja niiden avulla voidaan murtaa loput salatusta viestistä.

Frekvenssianalyysi ei toimi kaikentyyppisille salauksille. Esimerkiksi jos salausmenetelmässä on käytetty transpositiota (kirjainten järjestyksen sekoittamista), frekvenssianalyysi ei välttämättä paljasta alkuperäistä viestiä. Todellisuudessa frekvenssianalyysi on esimerkkiä monimutkaisempi menetelmä. Se hyödyntää myös kirjainten parien ja kolmikoiden esiintymistiheyksiä sekä kielen kielioppisääntöjä.

Nykyaikaisen kryptografian isänä pidetty Leon Battista Alberti tutki vuonna 1467 useita aakkosia yhdistävien salausmenetelmien, eli polyfonisten kryptosysteemien, käyttöä. Keskiajalla polyfoniset salaukset olivat vahvin tunnettu salausmuoto. Vaikka sen julkaisi Giovan Battista Bellaso, Vigenère-salaus liitettiin virheellisesti ranskalaiseen kryptologiin Blaise de Vigenèreen. Se tunnetaan 1500-luvun merkittävänä polyfonisena salauksena. Vaikka Vigenère ei itse keksinyt Vigenère-salausta, hän loi vahvemman autokey-salauksen vuonna 1586. (Schneider, 2024)

1800- ja 1900-luvulla salauksien rikkomiseen alettiin rakentamaan koneita. Yksi kuuluisa esimerkki on Enigma-salauslaite, jota Saksa käytti toisen maailmansodan aikaan. Koneet pystyivät käyttämään erittäin monimutkaisia menetelmiä suhteellisen nopeasti salauksien murtamiseen. (Banoth & Regar, 2023) Myöhemmin 1900-luvulla tietokoneiden kehittyessä pystyttiin soveltamaan jo niin monimutkaisia purkumetodeja, ettei niitä pystynyt suorittamaan ilman tietokonetta. (Banoth & Regar, 2023)

Nykyään tutkijat kehittävät salauksia, jotka pystyvät kestämään purkuyritykset tulevaisuuden tietokoneita vastaan. Salaukset perustuvat monimutkaisiin matemaattisiin ongelmiin ja jopa tehokkailla tietokoneilla on vaikeuksia näiden ongelmien ratkaisemissa. (Nimbe et al., 2022) Nykyiset salausmenetelmät pitävät kaikenlaista tietoa, kuten henkilökohtaisia viestejä, digitaalisia allekirjoituksia ja valtion salaisuuksia turvassa. (Kahn, 1996; Schneider, 2024)

1900-luvun loppupuolella suhteellisen uutena tieteenalana kvanttimekaniikkaa alettiin soveltamaan tiedon turvaamiseksi. Kvanttitietokoneiden esittämää uhkaa huomioitiin jo tällöin ja kvanttisalausta pidettiin tarpeellisena, sekä tulevaisuudenkestävänä. (Awasthi, 2024)

3 Yleiskatsaus kvanttilaskennasta

Kvanttilaskenta hyödyntää kvanttimekaniikan periaatteita ratkaisemaan ongelmia, joita ei pysty ratkaisemaan tehokkaasti klassisten tietokoneiden menetelmillä. Tämä luku esittelee kvanttilaskennan periaatteita, historiaa ja käytännön haasteita.

3.1 Kvanttilaskenta

Kvanttilaskenta eroaa klassisesta laskennasta, sillä kvanttilaskenta hyödyntää kvanttibittejä, eli kubitteja, jotka voivat olla olemassa useassa tilassa samanaikaisesti **superposition** ja **lomittumisen** ansiosta. Toisin kuin klassiset bitit, jotka rajoittuvat kahteen binääriseen tilaan (0 tai 1), kubitit hyödyntävät kvanttiominaisuuksia prosessoimaan suuria määriä tietoa rinnakkain. (Nielsen & Chuang, 2000, s. 13)

Daniel S. Abrams ja Seth Lloyd (1999) kertovat kvanttilaskennan teoreettisen alustan syntyneen Richard Feynmanin ehdotuksesta jo vuonna 1982. Feynman kuvitteli kvanttitietokoneiden olevan tehokkaita kvanttisysteemien simulaattoreita, mitkä käyttävät hyväkseen kvanttimekaniikan luonnollista rinnakkaisuutta. Nämä saavuttivat klassisia simulaatiometodeja parempia tuloksia. (Abrams & Lloyd, 1999)

Kvanttilaskennan merkitys on monitieteellistä ja se leviää useille alueille, kuten kryptografiaan, optimointiin, materiaalitutkimukseen ja lääkekehitykseen. Rinnakkaisuutta ja useiden ratkaisujen samanaikaista tutkimusta hyödyntämällä kvanttitietokoneilla on potentiaalia mullistaa laskennalliset tehtävät, mitkä ovat klassisille tietokoneille vaikeita.

Abramsin ja Lloydin artikkelissa osoitetaan, kuinka kvanttilaskennan käytännön sovelluksia on demonstroitu aikaisemmin kokonaislukujen tekijöihin jaossa Shorin algoritmia hyödyntämällä, sekä jäsentämättömässä haussa Groverin algoritmin avulla. (Grover, 1996) Kyseessä olevat algoritmit korostavat kvanttitietokoneiden kykyä ratkaista monimutkaisia ongelmia eksponentiaalisesti klassisia tietokoneita nopeammin.

Kvanttilaskennan historiallista kehitystä voidaan seurata tarkastelemalla merkityksellisiä kokeellisia sekä teoreettisia tapahtumia. Feynmanin varhaiset teoreettiset ehdotukset (Feynman, 1982), sekä läpimurrot kuten Peter Shorin algoritmi suurten lukujen tekijöihin jakamista varten polynomiajassa loivat perustan kvanttilaskennan tehokkuuden ymmärtämiselle. (Nielsen & Chuang, 2000, s. 6)

Kokeelliset vahvistukset kuten Shorin algoritmin implementaatio ydinmagneettista resonanssia (NMR) hyödyntämällä, tarjosivat konkreettista todistetta kvanttilaskennan mahdollisuuksista. (Vandersypen et al. 2001) Lisäksi viimeaikaiset saavutukset, kuten Googlen osoitus kvanttiylivoimasta Sycamore prosessorilla, korostavat nopeaa kehitystä kohti käytännöllistä kvanttilaskentaa. (Arute et al., 2019)

3.2 Kvanttilaskennan historiaa

Kvanttilaskennan kehityskululle tunnusomaista ovat uraauurtavat teoreettiset oivallukset ja merkittävät kokeelliset saavutukset, jotka ovat muovailleet sen kehitystä. Tämä alaluku tutkii kvanttilaskennan aikaisia teoreettisia ehdotuksia ja tärkeitä kokeellisia virstanpylväitä, jotka ovat puskeneet kvanttilaskennan ajatuksesta käytännön toteutukseksi.

Idea kvanttilaskennasta syntyi Richard Feynmanin kvanttimekaniikkaa ja tietotekniikkaa yhdistävistä näkemyksistä. Vuonna 1982 Feynman oletti klassisten tietokoneiden olevan

luonteeltaan tehottomia kvanttijärjestelmien simuloimisessa eksponentiaalisesti kasvavien laskennallisten resurssien tarpeen takia. Feynman kannatti kvanttitietokoneiden kehitystä kvantti-ilmiön tehokasta mallintamista varten ja väitteli klassisten systeemien olevan puutteellisia tehtävään. (Feynman, 1982)

Peter Shorin läpimurrot vuonna 1994 herättivät mielenkiintoa kvanttilaskentaa kohden demonstroimalla suurien kokonaislukujen tekijöihin jakoa polynomiajassa. Edellä mainittu perinteisesti pidettiin hankalana klassisilla tietokoneilla. Shorin algoritmi käytti hyväkseen kvanttirinnakkaisuutta ja kvantti Fourier-muunnosta (Engl. Quantum Fourier Transform, QFT) suurien lukujen tekijöiden jaossa eksponentiaalisesti klassisia algoritmeja nopeammin. Shorin algoritmi osoitti merkittävän uhan klassisia kryptografisia järjestelmiä kuten RSA:ta kohtaan. (Nielsen & Chuang, 2000)

Kvanttilaskennan siirtymää teoreettisista ehdotuksista käytännön toteutuksiin voi tarkastella useiden merkittävien kokeellisten saavutusten kautta. Kokeelliset saavutukset korostavat ja demonstroivat kvanttitietokäsittelyn käyttökelpoisuutta. Yksi aikaisimmista kokeellisista vahvistuksista tapahtui vuonna 2001, kun Vandersypen ja kumppanit onnistuneesti toteuttivat Shorin algoritmin hyödyntäen ydinmagneettista resonanssia. Koe toteutettiin seitsemän kubitin kvanttitietokoneella, ja tulokset tarjosivat todisteen kvanttialgoritmien käytöstä käytännön tilanteessa jakamalla luvun 15 alkulukuihin. (Vandersypen et al., 2001)

Vuonna 2019 Google saavutti merkittävän virstanpylvään demonstroimalla kvanttitietokoneiden ylivaltaa 54 kubittisella suprajohteisella Sycamore-prosessorilla. Sycamore-prosessori suoritti vaativan laskelman 200 sekunnissa, mikä vaatisi klassiselta supertietokoneelta noin 10 000 vuotta ratkaisuun. Demonstraatio osoitti, kuinka kvanttitietokoneet ovat ylivoimaisia laskennassa. (Arute et al., 2019)

Kvanttivirhekorjauksen kehitys on ollut olennaista kvanttilaskennan edistämisessä kohti käytännön sovelluksia. Virheenkorjausmenetelmät kuten pintaohjelmat korjaavat kvanttikoherenssin menetyksestä aiheutuvat virheet, mikä takaa luotettavuuden ja skaalautuvuuden kvanttilaskemissa. Mainitut edistysaskeleet ovat olleet merkittäviä tekijöitä kvanttilaskennan edistämisessä teoriasta käytännön toteutuksiin. (Fowler et al., 2012)

4 Kvanttisalaus

Kvanttisalauksen idean esittivät ensimmäisen kerran Stephen Wiesner 1970-luvulla sekä Charles H. Bennett IBM:ltä ja Gilles Brassard Montrealin yliopistosta vuosina 1984 ja 1985. (Gisin et al., 2002, s. 146) Klassinen kryptografia juurtuu matemaattisiin laskelmiin, mikä eroaa kvanttisalauksesta, joka operoi kvanttimekaniikan perusteilla. (Awasthi, 2024; Nimbe et al., 2022)

4.1 Erot klassisen kryptografian ja kvanttisalauksen välillä

Klassinen kryptografia hyödyntää perinteisiä matemaattisia menetelmiä kuten sijoitusta ja transpositiota tiedon suojaamiseksi. Klassisen kryptografian tarjoama suoja perustuu tiettyjen matemaattisten ongelmien, kuten suurten lukujen tekijöihin jaon monimutkaisuuteen. (Awasthi, 2024)

Toisin kuin klassinen kryptografia, kvanttisalaus perustuu kvanttimekaniikan lakeihin. Kvanttisalaus tuo uusia mahdollisuuksia turvallisuuteen, kuten salakuunteluyrityksien havaitsemisen ja niiden mitätöimisen. (Nimbe et al., 2022) Kvanttisalatut järjestelmät lupaavat vahvempaa turvaa ja parempaa avaintenhallintaa, mikä mahdollisesti ylittää klassisen kryptografian rajat. (Awasthi, 2024)

Pääerot

1. Turva: Kvanttisalaus tarjoaa klassista kryptografiaa vahvempaa suojausta. Kvanttisalauksella on kyky havaita ja vastustaa salakuuntelua. Edellä mainittua ominaisuutta ei ole olemassa klassisessa kryptografiassa. (Nimbe et al., 2022)
2. Avaimen jako: Kvanttisalaus on klassista kryptografiaa parempi avainten jaossa. Kvanttisalauksen etulyöntiasema perustuu kvanttimekaniikan ominaisuuksiin, kuten superpositioon ja lomittumiseen. (Awasthi, 2024)
3. Perusperiaatteet: Klassinen kryptografia perustuu matemaattisiin laskelmiin, kun taas kvanttisalaus toimii kvanttimekaniikan perusteiden mukaisesti. (Awasthi, 2024; Nimbe et al., 2022)
4. Tulevaisuudenkestävyys: Kvanttisalausta pidetään tulevaisuudenkestävänä kvanttitietokoneiden luomia uhkia vastaan. Klassiset kryptografiset algoritmit voidaan mahdollisesti murtaa kvanttitietokoneilla. (Awasthi, 2024)

4.2 Kvanttisalaus

Kvanttisalaus perustuu Heisenbergin epätarkkuusperiaatteeseen, jonka mukaan tiettyjen fyysisten ominaisuuksien pareja, kuten liikemäärää ja sijaintia, ei voida tarkasti mitata samanaikaisesti. Edeltävää periaatetta käytetään tunnetuissa kvanttisalauksen käytännön sovelluksissa, kuten kvanttiavaimen jakamisessa (Engl. Quantum Key Distribution), salakuuntelun tunnistamiseen. Protokollissa kolmannen osapuolen mitatessa siirrettävän fotonin kvanttitilaa syntyy tilassa häiriö, mikä paljastaa salakuunteluyrityksen. (Akter, 2023)

Kvanttisalaus tarjoaa myös ratkaisun kvanttitietokoneiden luomaan uhkaan. Kvanttitietokoneet kykenevät murtamaan useita nykypäivän salausalgoritmeja, mikä asettaa nykyisiä tietoturvajärjestelmiä haavoittuvaisiksi. Yllä mainitun vuoksi on kehittynyt kvanttiturvallisia salausmenetelmiä (Engl. Post-Quantum Cryptography, PQC). Kvanttiturvalliset salausalgoritmit ovat turvallisia niin klassisia, kuin myös kvanttitietokoneita vastaan, mikä

turvaa pitkäkestoisen tietoturvallisen viestinnän. (Mavroeidis et al., 2018) Kvanttisalauksen kehitystä on ajanut eteenpäin useat kvanttilaskennan edistysaskeleet. Kvanttitietokoneiden kehittyessä tehokkaammiksi, kasvaa tarve kvanttiturvallisille salausmenetelmille. Yllä mainittu johti uusien salausjärjestelmien kehitykseen, jotka pystyvät torjumaan myös kvanttitietokoneiden hyökkäyksiä. (Sharma et al., 2024)

4.3 Käyttötarkoituksia

Kvanttisalaus tarjoaa lukuisia mahdollisuuksia turvata arkaluontoista tietoa. Esimerkiksi pankkialalla sitä voidaan hyödyntää suojaamaan verkkomaksuja ja asiakastietoja. (Nielsen & Chuang, 2001, s. 57; Sharma, 2013) Myös useiden maiden armeijat (Krelina, 2021) ovat kiinnostuneita kvanttisalauksesta, sillä se mahdollistaa erittäin turvallisen tiedonsiirron. Lisäksi kvanttisalausta voidaan soveltaa esimerkiksi älykkäissä sähköverkoissa, joissa tietoturva on kriittistä. Kvanttisalauksen avulla voidaan varmistaa, että esimerkiksi älymittarit kommunikoivat turvallisesti keskenään ja energian siirto voidaan hallita luotettavasti. (Alshowkan et al., 2022)

Kvanttisalaus ei käsittele pelkästään kvanttiavaimen jakamista ja kvanttiturvallisia salausmenetelmiä. Kvanttitiedon suojaukselle on olemassa muutakin teoreettista käyttöä. Yksi teoreettisista käytöistä on kvanttiraha, missä kvanttitila toimii pankkisetelinä, jota ei voi väärentää (Nielsen & Chuang, 2001, s. 57). Toinen vastaava käyttö voisi olla kvanttisalaisuuksien jako, missä useat osapuolet voivat jakaa salaisuuden, joka voidaan vain koota usean osapuolen yhteistyöllä. Edellä mainitut teoreettiset esimerkit kvanttisalauksen käytöstä korostavat kvanttisalauksen joustavuutta toimia useissa tietoturvan osa-alueissa. (Broadbent & Schaffner, 2015)

Useista mahdollisista käyttökohteista huolimatta, on olemassa useita kvanttisalauksen haasteita. Kvanttisalauksessa kohina ja dekoherenssi ovat merkittäviä haasteita. (Grimes, 2019, 25–27). Kohina viittaa ympäristöstä tuleviin häiriötekijöihin, jotka voivat vaikuttaa kvanttibittien tilaan ja siten heikentää salauksen turvallisuutta (Pereira et al., 2022). Dekoherenssi puolestaan tarkoittaa kvanttitilan vuorovaikutusta ympäristön kanssa, mikä johtaa tilan rappeutumiseen klassisen tilan suuntaan (Brandt, 1998). Molemmat ilmiöt voivat aiheuttaa virheitä kvanttitiedon siirrossa ja vaikeuttaa luotettavan kvanttisalauksen toteuttamista. Tutkijat kehittävät jatkuvasti uusia menetelmiä kohinan ja dekoherensin vaikutusten vähentämiseksi, kuten esimerkiksi virheenkorjauskoodeja ja kvanttikanavien optimointia. (Nielsen & Chuang, 2010; Brandt, 1998)

Kvanttisalauksen käytännön sovelluksia on vaikea toteuttaa kohinan ja dekoherenssin johdosta. Kvanttisalauksen alalla on kasvava tarve jatkotutkimukselle, jotta kvanttiteknologioiden tietoturvaseuraamuksia voidaan ymmärtää. Lopuksi voidaan todeta, että kvanttisalauksen ala voi tarjota klassisia menetelmiä vahvempia turvaetuja. Kvanttisalauksen kehitys ja käyttöönotto on tärkeä askel kohti tiedon turvaamista kvanttiaikakaudella. Kuitenkin, niin kuin kaikkien kehittyvien teknologioiden kanssa, kvanttisalaus tuo esille uusia haasteita, joita on tärkeä huomioida jatkuvalla tutkimustyöllä. (Nielsen & Chuang, 2010; Brandt, 1998)

5 Kvanttikanavan luominen

Kokeellinen kvanttisalaus osoitettiin ensimmäisen kerran vuonna 1989. Sen jälkeen on tapahtunut valtavaa edistystä. Nykyään useat ryhmät ovat osoittaneet, että kvanttisalaus on mahdollista jopa laboratorion ulkopuolella. (Gisin et al., 2002, s. 21) Kvanttisalauksen toimimiseksi tarvitaan luotettava väliaine kubittien siirtämiseksi lähettäjän (Alice) ja vastaanottajan (Bob) välillä. Väliaine tunnetaan kvanttisalauksen yhteydessä kvanttikanavana ja se on välttämätön osa kvanttisalausjärjestelmää kvanttitiedon eheyden ja turvan takaamiseksi.

5.1 Kvanttikanavien tyypit

Kvanttikanavat voidaan jakaa kahteen tyyppiin: Valokuituun ja vapaatilaoptiseen datansiirtoon. Kvanttikanavaa perustaessa on harkittava molempien tyyppien etu- ja haittapuolia.

Valokuidut ovat ohuita säikeitä lasia tai muovia, jotka ohjaavat valosignaaleja pitkiä välimatkoja. Kvanttiviestinnässä valokuitu on yleisin välittäjäaine. Valokuidut tarjoavat korkeita tiedonsiirtonopeuksia ja ovat usein yhteensopivia olemassa olevan infrastruktuurin kanssa. Valokuidut ovat tarkasti tutkittuja ja niitä käytetään useissa käytännön sovelluksissa. Suurin ongelma valokuitujen kanssa on lähetyshäviön kasvu välimatkan kasvaessa. Lisäksi kubittien koherenssin hallinta voi olla haasteellista pitkillä välimatkoilla ympäristötekijöiden ja kuidun epätäydellisyyksien vuoksi. (Gisin et al., 2002, s. 14–16)

Vaapaatilaoptisessa datasiirrossa kubitteja siirretään ilman tai tyhjiön lävitse lasereilla. Vapaatilaoptinen datansiirto on hyödyllinen etenkin satelliittiviestinnässä ja tilanteissa, joissa valokuitukanavan rakentaminen on epäkäytännöllistä. Vapaatilaoptisen datasiirron avulla voidaan viestiä pitkiä välimatkoja ilman fyysistä infrastruktuuria, minkä vuoksi tämä kvanttikanavan tyyppi on soveltuva syrjäisille alueille ja avaruuteen. On kuitenkin huomioitava, että vapaatilaoptinen datansiirto on vaikutuksenalainen ilmakehän olosuhteille, kuten sumulle, sateelle ja turbulenssille. Lähettäjän ja vastaanottajan välillä on oltava selkeä näkölinja. (Gisin et al., 2002, s. 17)

5.2 Dekoherenssi kvanttikanavissa

Nielsen ja Chuang (2010) selittävät, että dekoherenssiä kvanttilaskennassa ja kvanttiinformaatiossa käytetään viittaamaan mihin tahansa kohinaan kvanttiprosessissa (Nielsen & Chuang, 2010, s. 398). Howard Brandt kertoo, että kubittien kytkökset sekä niiden sisäiseen että ulkoiseen ympäristöön johtavat väistämättä kvanttidekoherenssiin (Brandt, 1998, s. 260). Kun kvanttijärjestelmä vuorovaikuttaa ympäristönsä kanssa, kvanttikoherenssi - kvanttitilojen päällekkäisyys - tuhoutuu vähitellen, mikä johtaa tiedon menetykseen. Kvanttikanavien yhteydessä dekoherenssi on suuri haaste, sillä se voi vaarantaa kvanttiviestinnän turvallisuuden ja luotettavuuden. (Brandt, 1998)

Dekoherenssi kvanttikanavissa johtuu useista tekijöistä:

- **Ympäristön kanssa tapahtuva vuorovaikutus:** Kvanttijärjestelmät ovat erittäin herkkiä ympäristönsä kanssa tapahtuville vuorovaikutuksille. Värähtelyt, lämpövaihtelut (Brandt, 1998, s. 260) ja sähkömagneettiset kentät (Brandt, 1998, s. 279–280) voivat aiheuttaa kvanttitilojen romahtamisen.

- **Kvanttilaitteiden epätäydellisyydet:** Kvanttilaitteiden, kuten fotonilähteiden, detektorien ja optisten komponenttien, epätäydellisyydet voivat aiheuttaa kohinaa ja virheitä kvanttikanavaan. (Brandt, 1998, s. 283–287)
- **Kanavan häviöt:** Kvanttisignaalien heikentyminen absorption (Brandt, s. 320) tai sironnan vuoksi voi johtaa tiedon menetykseen. (Brandt, 1998, s. 342–343)
- **Kanavan dispersio:** Dispersio aiheuttaa kvanttisignaalin eri taajuuskomponenttien kulun eri nopeuksilla, mikä johtaa vääristymiin ja dekoherenssiin. (Granot, 2012)

5.3 Kvanttikanavan perustaminen

Kvanttikanavan perustamisessa on useita vaiheita, joihin kuuluu välittäjäaineen valinta, siirtolaitteiston valinta, dekoherenssin ja häviön minimointi, sekä kanavan testaus. Välittäjäaineen valinta perustuu kvanttisalausjärjestelmän vaatimuksiin. Vapaaoptinen kanava soveltuu etäseuduille ja avaruuteen (Gisin et al., 2002, s. 29–30), kun taas valokuitu on erinomainen valinta kaupunkimaisessa ympäristössä valmiin infrastruktuurin kanssa. (Gisin et al., 2002)

Valokuitusiirtolaitteistoa valmisteltaessa käytetään yksifotonisia lähteitä (Gisin et al., 2002, s. 12–14) ja tunnistimia, jotka ovat yhteensopivia valokuitujen aallonpituuden kanssa. Vapaatilaoptista kanavaa valmisteltaessa täytyy asettaa laserlähettimet ja vastaanottimet. On välttämätöntä varmistaa näköyhteys lähettäjien ja vastaanottimien välillä. Lopuksi tarkistetaan laitteiston vakaus ja kalibrointi. (Gisin et al., 2002)

Häviön ja dekoherenssin minimoiminen on välttämätön askel kvanttikanavan eheyden varmistamisessa. Valokuitukanavaa perustaessa on tärkeää valita pienihäviöiset valokuidut ja tarvittaessa käyttää vahvistimia signaalin vahvistamiseksi pitkillä välimatkoilla. Aallonpituusjakokanavointi (WDM) on tekniikka, jolla voidaan kasvattaa valokuitukanavan kapasiteettia (Townsend, 1997). Vapaatilaoptisen kanavan kanssa voidaan hyödyntää mukautuvia optiikkoja ilmakehästä johtuvien häiriöiden tasapainottamiseksi. Lisäksi vapaatilaoptiseen kanavaan voidaan implementoida virheenkorjausprotokollia signaalin häviön ja dekoherenssin vähentämiseksi. (Gisin et al., 2002)

Kvanttikanavan testaus sisältää alkutestausta häviön ja virhesuhteen mittaamiseksi. Laitteiston ja protokollien säätäminen on välttämätöntä kvanttikanavan optimoimiseksi. Valokuitukanavissa on tärkeää mitata vaimentuminen ja dispersion tuntomerkit (Gisin et al., s.15). Vapaatilaoptisessa kanavassa on tärkeää arvioida ympäristön vaikutukset signaalin laatuun. (Gisin et al., 2002)

Kvanttikanavan turvallisuuden tarkastaminen on tärkeää. Kvanttikanavat ovat luonnostaan turvallisia ei-kloonausteorian ja kvanttiepämääräisyyden takia. Kuitenkin käytännön sovelluksissa täytyy suojautua mahdollisia haavoittuvuuksia vastaan. Kvanttisalausjärjestelmät usein vaativat klassisia kanavia virheenkorjausta ja avainten seulontaa varten, minkä vuoksi on välttämätöntä varmistaa, että kvanttikanavat ja klassiset kanavat ovat hyvin yhtenäistetty ja synkronoitu. (Radanliev, 2024)

6 QKD-protokollien perusteet

Kvanttiavaimen jakaminen (Engl. Quantum Key Distribution, QKD) on tekniikka, joka mahdollistaa turvallisen viestinnän kahden tahon välillä jakamalla salaisen avaimen. QKD tarjoaa informaatioteoreettisturvallisen avaimen jaon (Engl. Information-Theoretic Secure Key Distribution), mikä tekee siitä keskeisen teknologian useilla teollisuusaloilla, kuten sotateollisuudessa, rahoitusalalla ja terveydenhuollossa. (Sharma et al., 2024) Kaksi tunnetuinta QKD-protokollaa ovat BB84- ja E91-protokolla.

6.1 Kvanttitilan romahdus

Kvanttitilan romahdus on yksi kvanttimekaniikan peruskäsitteistä, mutta samalla se on myös yksi alan suurimmista mysteereistä. Se kuvaa ilmiötä, jossa kvanttihiukkasen epävarma tila muuttuu tarkasti määritellyksi tilaksi, kun sitä mitataan. (Penrose, 1996)

Kun kvanttihiukkasta mitataan, sen superpositiotila "romahtaa" johonkin tarkkaan tilaan. Esimerkiksi elektronin pyöriminen voi romahtaa joko myötä- tai vastapäivään. (Penrose, 1996) Mitä tämä tarkoittaa käytännössä?

- **Epävarmuudesta varmuuteen:** Ennen mittausta emme voi tietää tarkasti, missä tilassa hiukkanen on. Mittaus kuitenkin pakottaa hiukkasen valitsemaan yhden tilan. (Grimes, 2019, s. 22–23)
- **Satunnaisuus:** Romahdus tapahtuu satunnaisesti. Emme voi ennustaa etukäteen, mihin tilaan hiukkanen romahtaa. (Grimes, 2019, s. 22–23)
- **Mittauksen rooli:** Mittaustoimenpide on se, joka aiheuttaa romahduksen. Ilman mittausta hiukkanen voi pysyä superpositiotilassa. (Grimes, 2019, s. 22–23)

Kvanttisalauksen turvallisuus perustuu olennaisesti siihen ilmiöön, että kvanttitila romahtaa mittauksessa. Tämä on yksi kvanttimekaniikan peruspilarista ja se onkin se ominaisuus, joka erottaa kvanttitietokoneet klassisista tietokoneista. Yrittäessä mitata kvanttitilaa, se muuttuu peruuttamattomasti, mikä paljastaa salakuuntelun yrityksen. Tämä tekee kvanttisalauksesta periaatteessa täysin turvallisen, sillä kaikki salakuunteluyritykset jättävät jälkiä. (Horodecki, 2009)

6.2 BB84-protokolla

Charles Bennetin ja Gilles Brassardin vuonna 1984 kehittämä BB84-protokolla on yksi tunnetuimmista QKD-protokollista. Protokollassa Alice ja Bob käyttävät kvanttitunnelia kubittien vaihdossa, mikä mahdollistaa salakuuntelulle resistentin jaetun avaimen generoinnin. BB84-protokolla on laajasti tutkittu ja sen käyttöä on sovellettu useissa tilanteissa. Useita kehityksiä ja päivityksiä on tehty protokollan toimintaan sen turvallisuuden ja käytännöllisyyden parantamiseksi. Näihin kehityksiin kuuluu muun muassa kehittyneen virheenkorjaustekniikan ja harhatilojen lisäys. (Abdullah et al., 2023)

BB84-protokollassa Alice valitsee satunnaisesti bitin arvon ja koodaa sen jommallekummalle kahdesta mahdollisesta kannasta. Tämän jälkeen Alice lähettää koodatun kubitin kvanttitunnelin läpi Bobille. Bob myös valitsee satunnaisesti kannan, jolla vastaanotettu kubitti mitataan. Bobin mitattua kubitit, Alice ja Bob julkisesti vertailevat heidän valitsemiaan kantoja. Kubiteissa, joissa he käyttivät samoja kantoja, Alicen koodaamien bittien arvot tulisivat vastata Bobin mittaamia arvoja, mistä muodostuu raaka-avain (Engl. raw

key). Kohinan ja mahdollisen salakuuntelun vuoksi virheenkorjaus ja yksityisyydenvahvistus suoritetaan lopullisen avaimen saamiseksi. (Abdullah et al., 2023)

6.3 E91-protokolla

Artur Ekertin vuonna 1991 esittämä E91-protokolla on toinen merkittävä QKD-protokolla. E91-protokolla perustuu lomittumiseen ja Bellin teoreeman rikkomiseen, mikä tarjoaa vahvemman turvatodistuksen BB84-protokollaan verrattuna. E91-protokolla käyttää lomittunutta fotoniparia, mitkä lähetetään molemmille osapuolille, eli Alicelle ja Bobille. Alicen ja Bobin fotoneihin tekemien mittausten korrelaatio mahdollistaa jaetun salaisen avaimen generoinnin. (Fujiwara et al., 2015)

E91-protokollassa lähde luo parin lomittuneita fotoneja ja lähettää yhden fotonin kummastakin parista Alicelle ja toisen Bobille. Alice ja Bob molemmat valitsevat satunnaisesti yhden kolmesta mahdollisesta kannasta, missä fotonit mitataan. Kaikkien fotonien mitattua Alice ja Bob julkisesti vertailevat valitsemiaan kantoja ja pitävät tulokset kierroksilta, joissa he valitsivat saman kannan. Tämän jälkeen he valitsevat satunnaisesti osajoukon tuloksista ja testaavat sen salakuuntelun varalta tarkistamalla rikkooko mittausten välinen korrelaatio Bellin teoreemaa (Fujiwara et al., 2015). Mikäli salakuuntelua ei havaita, he käyttävät jäljelle jääneitä tuloksia raaka-avaimen muodostamiseen. Myös kuten BB94-protokollassa, virheenkorjaus- ja yksityisyyden vahvistusaskeleet suoritetaan lopullisen avaimen saamiseksi. (Fujiwara et al., 2015)

6.4 Erot protokollien välillä

Vaikka molemmat protokollat ovat QKD-protokollia, niin ne eroavat useilla tavoilla. BB84-protokolla on valmista ja mittaa -protokolla (Engl. prepare and measure protocol), mikä tarkoittaa, että Alice valmistaa kvanttitilat ja Bob mittaa ne. Toisin kuin BB84-protokolla, E91-protokolla on lomittumiseen perustuva protokolla, missä lähde valmistelee lomittuneet tilat, jotka Alice ja Bob mittaavat. Edellä mainittu ero johtaa erilaisiin turvatodistuksiin E91- ja BB84-protokollille. BB84-protokollan turva perustuu ei-kloonauslauseeseen (Engl. no-cloning theorem), kun taas E91-protokollan turva perustuu Bellin epäyhtälön rikkeisiin. (Sharma et al., 2024)

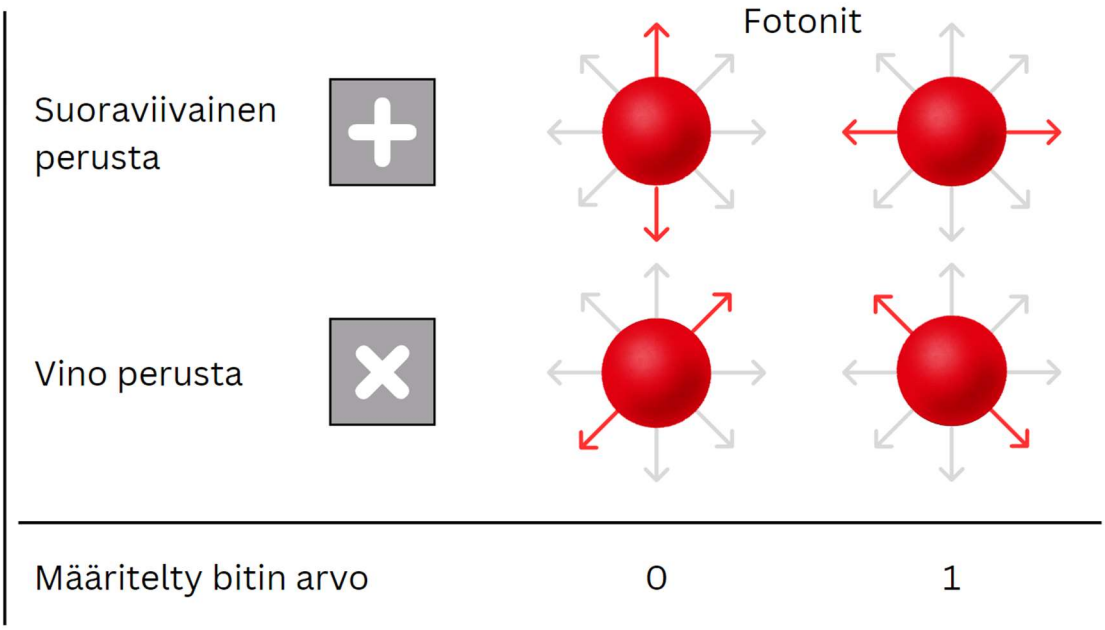
BB84- ja E91-protokollat molemmat tarjoavat turvallisen tavan avainten jaolle hyödyntämällä kvanttimekaniikan periaatteita. Mainitut protokollat muodostavat kvanttisalauksen kannan ja ovat luoneet reitin kehittyneempien ja turvallisempien kvanttiviestinnän protokollien kehittämiselle.

7 BB84-protokollan implementointi

Charles Bennetin vuonna 1984 esittämä BB84-protokolla on eniten implementoitu QKD-skeema. BB84-protokolla mahdollistaa salaisen jaetun avaimen generoinnin kahden osapuolen välillä, mitä voidaan käyttää tietoturvalliseen viestintään. Tämä luku selittää kuinka BB84-protokolla voidaan toteuttaa kvanttisalausjärjestelmässä.

7.1 Lähetys ja mittaus

Alice valmistelee satunnaisesti polarisoituja fotoneja, jotka edustavat kubitteja. Jokainen fotoni voi olla polarisoitunut joko vaakasuoraan tai pystysuoraan (suoraviivainen kanta), tai 45 asteen kulmassa näihin suoriin nähden (vino kanta). (Bennet & Brassard, 1984) Kannan valinta on merkittävää, sillä se määrittää mittausten tulokset ja avainten jaon tietoturvan. Tämä valinta on analoginen klassisen optiikan polarisaatiosuodattimien valitsemiseen. Kuvassa 1 on esitetty kannan valinta:

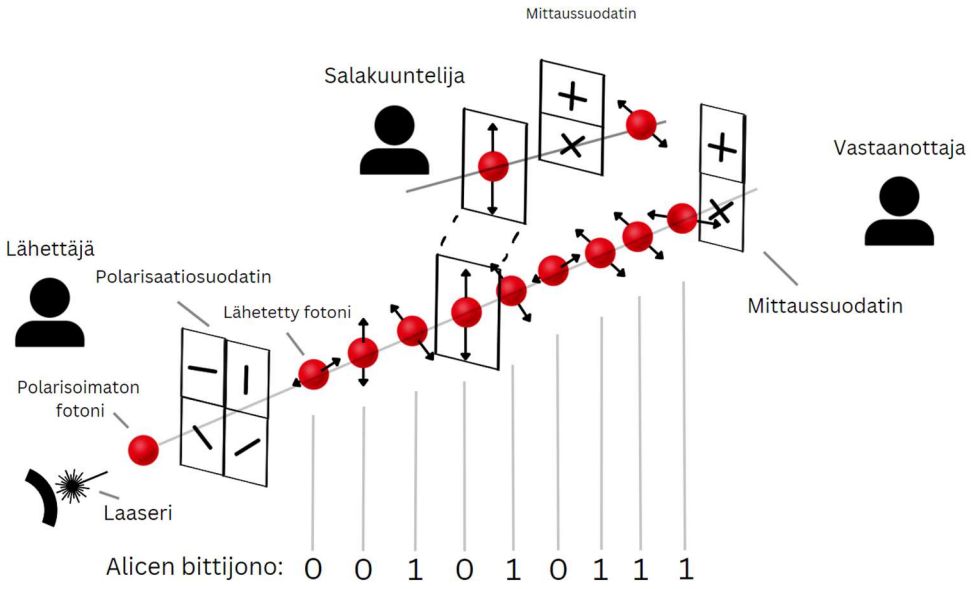


Kuva 1. *Nuolet osoittavat fotonien polarisaatiotilat. Vaakasuora viiva, jossa on arvot 0 ja 1, osoittaa, miten nämä polarisaatiotilat vastaavat bittiarvoja. BB84-protokollassa lähettäjä (Alice) valitsee satunnaisesti kannan (suoraviivainen tai vino) ja polarisaatiotilan (0 tai 1) jokaiselle fotonille. Kuva on mukailtu lähteestä (Lee ja muut, 2016).*

Voit ajatella kubittia pyörivänä kolikkona. Jos kolikko on pystyasennossa, se on superpositiotilassa, jossa se on sekä kruuna että klaava. Kun kolikko lasketaan, se voi osoittaa joko kruunaa tai klaavaa. Se, kumpaa näet, riippuu siitä, miten kolikko on käännetty ennen laskemista. Käännettävä suunta vastaa tässä kannan valintaa.

Alice lähettää kubitin Bobille kvanttikanavan kautta. Kvanttikanava voi olla valokuitua tai vapaatilaoptinen. Lähetyksen aikana on tärkeää ylläpitää kubittien koherenssi ja minimoida mahdolliset häviöt. (Gisin et al., 2002) Kvanttikanavan eheys suoraan vaikuttaa BB84-protokollan tietoturvaan ja tehokkuuteen.

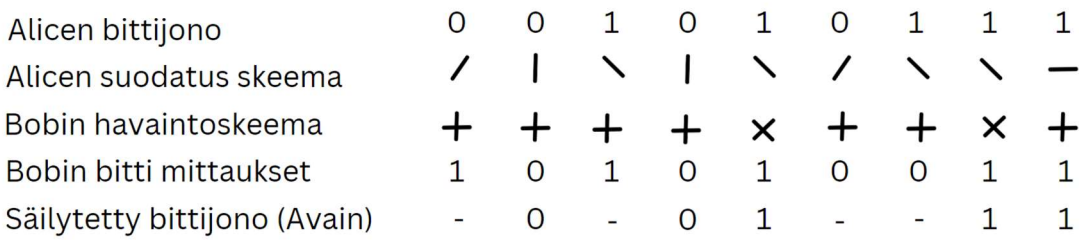
Kubitit vastaanottaessaan Bob satunnaisesti valitsee kannan (suoraviivainen tai vino) kunkin kubitin mittaamista varten. Bobin kannan valinta on satunnainen, joten tulee olemaan tilanteita, joissa Bobin kanta vastaa Alicen kantaa ja tilanteita, joissa ne eivät vastaa toisiaan. Kantojen vastatessa toisiaan Bobin mittatulos tarkasti vastaa Alicen lähettämän kubitin tilaa. Kun kannat eivät vastaa toisiaan mittatulos on satunnainen. (Bennet & Brassard, 1984) Satunnaisuus on perustavanlaatuinen olemus BB84-protokollassa, mikä varmistaa, että salakuunteluyritykset tuottavat huomattavia virheitä. Kuvassa 2 on havainnollistettu kvanttiavaimen jakamista.



Kuva 2. *Tämä kuva esittää kvanttiavaimen jakamisen periaatteen, jossa käytetään polarisoituja fotoneja turvalliseen viestintään kahden osapuolen, Alicen ja Bobin, välillä. Kuvan alareunassa näkyy Alicen lähettämä bittijono. Kuva havainnollistaa, miten kvanttimekaniikan lait mahdollistavat turvallisen tiedonsiirron, koska mahdollinen salakuuntelija muuttaa fotonien tilaa ja paljastuu näin. Kuva on mukailtu lähteestä (Lee ja muut, 2016).*

7.2 Virheenkorjaus ja yksityisyydenvahvistus

Lähetyksen ja mittauksen jälkeen Alice ja Bob julkisesti vertailevat heidän kantojaan kullakin kubitilla. He hylkäävät bitit, joissa kannat eivät vastaa toisiaan, säilyttäen vain bitit, joissa kannat ovat samat. Edellä mainittu prosessi tunnetaan avaimen seulomisena (Engl. key sifting). Jäljelle jäävät bitit muodostavat raa'an avaimen, joka on jaettu Alicen ja Bobin kesken. (Bennet & Brassard, 1984) Avaimen seulonta on välttämätöntä eroavaisuuksien poistamiseksi ja osapuolten avaimien identiteettisyyden varmistamiseksi. Kuva 3 näyttää, miten Alice ja Bob voivat luoda yhteisen salaisen avaimen käyttämällä kvanttifysiikan periaatteita, mikä tekee salakuuntelun havaitsemisesta mahdollista. Tämä on BB84-protokollan ydin.



Kuva 3. *Bobin mittaustulokset riippuvat siitä, osuivatko hänen valitsemansa kannat yhteen Alicen valintojen kanssa. Jos kannat ovat samat, Bob saa oikean bittiarvon; muuten mittaus on satunnainen. Lopuksi Alice ja Bob vertaavat kantavalintojaan julkisesti ja säilyttävät vain ne bitit, joissa heidän kantansa olivat samat. Näin he saavat yhteisen salaisen avaimen. Kuva on mukailtu lähteestä (Lee ja muut, 2016).*

Raaka avain voi sisältää virheitä kvanttikanavan kohinan tai salakuuntelun takia. Alice ja Bob suorittavat virheenkorjauksen virheiden tunnistamiseksi ja korjaamiseksi. Useita virheenkorjaustekniikoita voidaan käyttää, kuten pariteetin tarkastusta ja itsekorjaavaa koodia. (Shor & Preskill, 2000) Virheenkorjaus takaa lopullisen avaimen identiteettisyyden molempien osapuolien välillä myös lähetystenaikaisten virheiden läsnäolleessa.

Virheenkorjauksen jälkeen Alice ja Bob suorittavat yksityisyydenvahvistuksen vähentääkseen tietoa, mitä salakuuntelija on saattanut kerätä. Prosessi sisältää avaimen lyhentämistä siten, että mikä tahansa osittainen tieto mitä salakuuntelijalla voi olla hallussa, muuttuu merkityksettömäksi. Tekniikat kuten tiivistysfunktiot ovat usein käytettyjä yksityisyydenvahvistuksessa. (Short & Preskill, 2000) Yksityisyydenvahvistus parantaa lopullisen avaimen tietoturvallisuutta tehden siitä resistentin salakuuntelulle.

7.3 Turvallisuus

BB84-protokollan turvallisuus perustuu kvanttimekaniikan periaatteisiin. Salakuuntelijan yrityksen siepata ja mitata kubitteja tuo esille tunnistettavia virheitä, mikä varoittaa Alicea ja Bobia salakuuntelun olemassaolosta. Ei-kloonauslause toteaa, että on mahdotonta luoda kaksi identtistä kopiota tuntemattomasta kvanttitilasta, mikä varmistaa BB84-protokollan turvallisuuden. (Bennet & Brassard, 1984) BB84-protokollan edistysaskeleet, kuten harhatilojen käyttö ja kehittyneet virheenkorjaustekniikat ovat edelleen edistäneet protokollan turvallisuutta ja käytännöllisyyttä. (Pereira et al., 2023)

BB84-protokollan implementointi käytännön tilanteisiin sisältää käytännön haasteiden kuten lähteen epätäydellisyyden ja ympäristötekijöiden huomioimisen. Viimeaikaiset tutkimukset ovat osoittaneet BB84-protokollan vankkuuden useiden epätäydellisyyksien, kuten tilan valmistelun virheiden ja sivukanavien, läsnäolleessa. (Pereira et al., 2023)

8 Kvanttisalaukseen siirtyminen organisaatiossa

Mavroeidis ja kumppanit toteaa, että vuosi vuodelta näyttää siltä, että lähestyy hetki, jolloin voimme luoda täysin toimivan yleiskäyttöisen kvanttitietokoneen, joka pystyy hyödyntämään vahvoja kvanttialgoritmeja, kuten Shorin ja Groverin algoritmia. (Mavroeidis et al., 2018, s. 8) Scholten ja kollegat vastaavasti korostavat, että kvanttitietokoneiden kehittyminen aiheuttaa merkittäviä haasteita nykyisille tietoturvaratkaisuille, mikä edellyttää uusien, kvanttikestävien menetelmien kehittämistä. (Scholten et al., 2024) Tässä luvussa arvioidaan missä määrin kvanttikryptografia voi tarjota turvallisen ratkaisun arkaluonteisten tietojen suojaamiseen kvanttitietokoneiden aikakaudella, ja mitä rajoituksia ja mahdollisia kompromisseja sen käyttöönottoon liittyy.

8.1 Tietoturvan merkitys organisaatiossa

NISTin mukaan kvanttitietokoneet tulevat vaarantamaan nykyisten julkisen avaimen salausjärjestelmien turvallisuuden (Mavroeidis et al., 2018, s. 4). Scholten ja kollegat toteavat, että jokainen organisaatio riippuu digitaalisesta infrastruktuuriviestinnästä. Tässä mielessä organisaatiot pitävät salausmenetelmiä viimeisenä puolustuslinjana. Sekä luottamus että suojaus ovat vaarassa, kun epäsymmetrinen salaus todennäköisesti rikkoutuu, kun salausmerkityksellinen kvanttitietokone tulee saataville. (Scholten et al., 2024, s. 33) Mavroeidis ja kumppanit huomauttavat, että kaikki nykyään käytetyt julkisen avaimen algoritmit perustuvat kahteen matemaattiseen ongelmaan: suurten lukujen tekijöihin jakamiseen ja diskreettien logaritmien laskemiseen. Molemmilla on samanlainen matemaattinen rakenne, ja ne voidaan murtaa nopeasti Shorin algoritmilla. (Mavroeidis et al., 2018, s. 4)

8.2 Kvanttiturvallisuuden saavuttaminen

Ensimmäinen askel kohti kvanttiturvallisuutta on kartoittaa organisaation nykyiset salauskäytännöt. Tärkeimmät tiedot ja järjestelmät on tunnistettava ja suojattava sekä teknisestä että liiketoiminnallisesta näkökulmasta. Sen jälkeen on laadittava vaiheittainen suunnitelma siirtymään kvanttiturvalliseen ympäristöön. Scholtenin ja kumppanien mukaan inkrementaalinen eli vähitellen tapahtuva muutos on tässä avainasemassa. Pienillä kokeiluilla, oppimalla virheistä ja hyödyntämällä onnistuneita ratkaisuja voidaan rakentaa kestävä ja turvallinen kvanttiturvallinen infrastruktuuri. (Scholten et al., 2024, s. 33) Vastaus kvanttitietokoneiden luomaan uhkaan on kvanttitietokoneille vastustuskykyisten salausjärjestelmien käyttöönotto. Mavroeidisin ja kumppanien mukaan tällaisia järjestelmiä ovat esimerkiksi kvanttiavaimen jakamisjärjestelmät kuten BB84-protokolla sekä mate-

maattisiin perusteisiin perustuvat ratkaisut kuten ristikkorakenteinen kryptografia, hajautusfunktioihin perustuvat signatuurit ja koodipohjainen kryptografia. (Mavroeidis et al., 2018, s. 8)

8.3 Siirtymävaihe

Siirtyessä kvanttiturvalliseen salaukseen on tärkeää huolehtia siitä, että organisaation kyky mukautua uusiin teknologioihin säilyy. Tulevaisuudessa joudutaan mahdollisesti päivittämään salausmenetelmiä, mutta nämä muutokset eivät saa häiritä organisaation keskeisiä toimintoja. On tärkeä ymmärtää, että siirtymä kvanttiturvalliseen salaukseen on enemmän kuin pelkkä vanhan menetelmän vaihtaminen uuteen. Esimerkiksi sovelluksen tai järjestelmän muuntamiseen käytettävien valmiiksi määriteltyjen korjausmenetelmien tai -mallien tunnistaminen ja niiden hyödyntäminen nykyaikaisissa käyttöönottomenetelmissä on tärkeää. On hyvin todennäköistä, että organisaatiot, joilla on paljon sovelluksia, voivat tyypillisesti luoda ja käyttää useita uusia salauskäyttöönottomalleja toistuvasti. (Scholten et al., 2024, s. 34)

8.4 Käyttöönotto

Siirtymän jälkeen on tärkeää perustaa luotettavan tasoinen osaaminen kvanttiturvallisen salauksen käyttöönotossa ja käytössä. Syvä ymmärrys kvanttialgoritmien suorituskykyprofiilista ja resurssikäytöstä on tärkeää. Organisaation täytyy tunnistaa kykeneviä salaus- ja tietoverkkoinsinöörejä, turvallisuusarkkitehteja ja projektinjohtohenkilöstöä, sekä tarjota heille ympäristö ja mahdollisuus oppia, sekä tehdä kokeita. (Scholten et al., 2024, s. 34) Jatkossa organisaatioiden tulisi kehittää ja toteuttaa strategioita kvanttitietokoneiden hyödyntämiseksi niiden kehittyessä. Tällainen strategia riippuu luonnollisesti yksittäisestä organisaatiosta, sen yleisemmistä teknologiastrategioista ja sen kiinnostuksesta edistyneiden laskentamahdollisuuksien käyttöön. (Scholten et al., 2024, s. 36)

9 Yhteenveto

Tämä tutkielma tarkasteli kvanttisalauksen tieteenalaa vertailemalla klassista kryptografiaa kvanttisalaukseen. Vertailu osoittaa kvanttisalauksen tarjoavan ylivoimaista tietoturvaa klassiseen kryptografiaan verrattuna. Tutkielmassa korostuu tarve siirtyä klassisesta kryptografiasta kohti kvanttisalausta kvanttiteknologioiden kehittyessä. Kryptografian tieteenalan tutkimukset tarjoavat historiallista taustaa salausmenetelmiin, jota tutkittiin tässä kirjallisuuskatsauksessa seuraamalla kryptografisten menetelmien kehitystä muinaisista ajoista nykypäivään. Tarkastelemalla kvanttikanavien perustamista ja QKD-protokollien implementaatiota tämä tutkielma esitteli kvanttisalaukseen liittyviä käytännön haasteita.

Lopuksi tutkielma korosti kvanttitietokoneiden merkittävää uhkaa nykyisille salausmenetelmille, mikä asettaa organisaatioiden tietoturvan vaakalaudalle. Ratkaisuksi esitetään siirtyminen kvanttikestäviin salausmenetelmiin, kuten kvanttiavaimenjakamiseen ja matemaattisiin perusteisiin perustuviin menetelmiin.

Tutkielma painottaa, että siirtymä on suositeltavaa toteuttaa vaiheittain, aloittaen organisaation arkaluonteisimmista tiedoista ja järjestelmistä. Organisaatioiden tulee kartoittaa nykyiset salauskäytännöt, laatia siirtymäsuunnitelma ja investoida osaamisen kehittämiseen kvanttiturvallisen salauksen hallinnassa.

Tutkielman luotettavuutta on pyritty parantamaan runsaalla lähteiden käytöllä. Monet lähteistä ovat julkaistu tunnetuissa tieteellisissä lehdissä, kuten Physical Review Letters, Nature ja Reviews of Modern Physics. Nämä lehdet ovat vertaisarvioituja ja tunnettuja korkeista julkaisustandardeistaan, mikä lisää niiden luotettavuutta. Esimerkiksi Abramsin ja Lloydin (1999) sekä Aruten et al. (2019) artikkelit ovat julkaistu näissä arvostetuissa lehdissä. Lisäksi useat lähteet ovat kirjoittaneet alansa johtavat asiantuntijat, kuten Richard Feynman ja Peter Shor, jotka ovat tunnettuja panoksistaan kvanttilaskennan ja kryptografian aloilla. Tämä lisää lähteiden uskottavuutta ja luotettavuutta.

Kirjat ja oppikirjat, kuten Andressin (2014) ja Nielsenin ja Chuangin (2000) teokset, tarjoavat kattavan ja perusteellisen käsityksen aiheista ja ovat usein käytettyjä akateemisessa opetuksessa. Ne ovat myös vertaisarvioituja ja julkaistu tunnetuilla kustantajilla, kuten Elsevier ja Cambridge University Press. Joissakin lähteissä, kuten Akterin (2023) ja Awasthin (2024) artikkeleissa, on käytetty arXiv-alustaa, joka on tunnettu tieteellisten esipainosten arkisto. Vaikka arXiv-lähteet eivät ole aina vertaisarvioituja, ne tarjoavat ajankohtaista tutkimustietoa ja ovat usein ensimmäinen askel kohti virallista julkaisua.

Tiivistettynä tämän tutkielman löydöt korostavat tarvetta kvanttisalauksen tutkimiselle ja jatkuvalle kehitykselle tulevaisuuden tietoturvan takaamiseksi. Tutkielman tarkoituksena on toimia lähteenä kvanttisalauksesta ja kryptografiasta kiinnostuneille.

Tekoälyn käyttö

Opinnäytteessäni käytetyt tekoälytyökalut ja niiden käyttötarkoitukset on kuvailtu alla:

Työkalun nimi (ja versio): Gemini 1.5.

Käyttötarkoitus ja osio, jossa työkalua käytettiin: Tekoälyä on käytetty kaikissa luvuissa. Tutkielman sisältö ja ideat ovat omaperäisiä tai perustuvat käytettyihin lähteisiin. Gemini-kielimallia **on käytetty tekstin kieliasun hiomiseen ja rakenteen selkeyttämiseen, sekä tekstin luomiseen.** Tämän ansiosta olen voinut keskittyä sisällön kehittämiseen ja varmistaa, että tutkimukseni on mahdollisimman ymmärrettävää lukijalle.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien tekoälyllä tuotetut osat, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

Lähdeluettelo

Abdullah, A. A., & Jassem, Y. H. (2019). *Enhancement of quantum key distribution protocol BB84*. Journal of Computational and Theoretical Nanoscience, 16(3), 1138-1154. doi:10.1166/jctn.2019.8009.

Abrams, D. S., & Lloyd, S. (1999). *Quantum algorithms for factoring and searching*. Physical Review Letters, 83(24), 5162-5165. Noudettu osoitteesta https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.83.5162

Alshowkan, M., Evans, P.G., Starke, M., Earl, D., Peters, N. (2022*). Authentication of smart grid communications using quantum key distribution*. Sci Rep 12, 1273. https://doi.org/10.1038/s41598-022-16090-w

Andress, J. (2014). Cryptography. *In The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice* (2nd ed., pp. 69-88). Elsevier. Noudettu osoitteesta https://doi.org/10.1016/B978-0-12-800744-0.00005-1

Akter, M. S. (2023). *Quantum cryptography for enhanced network security: A comprehensive review*. Noudettu osoitteesta https://doi.org/10.48550/arXiv.2306.09248

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.

Awasthi, P. (2024). *Post Quantum Cryptography & its Comparison with Classical Cryptography*. Journal of Cryptographic Research, 12(1), 45-67.

Banoth, R., & Regar, S. (2023). *Classical and Modern Cryptography for Beginners*. Springer Cham.

Bennett, C. H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.

Brandt, H. E. (1998). *Qubit devices and the issue of quantum decoherence*. Progress in Quantum Electronics, 22, 257-370.

Broadbent, A., & Schaffner, C. (2015). *Quantum cryptography beyond quantum key distribution*. Designs, Codes and Cryptography, 78(2), 351-382.

Feynman, R. P. (1982). *Simulating physics with computers*. International Journal of Theoretical Physics, 21(6-7), 467-488.

Fowler, A. G., Mariantoni, M., Martinis, J. M., & Cleland, A. N. (2012). *Surface codes: Towards practical large-scale quantum computation*. Physical Review A, 86(3), 032324.

Fujiwara, M., Yoshino, K.-i., Nambu, Y., Yamashita, T., Miki, S., Terai, H., ... & Sasaki, M. (2015). *Modified E91 protocol demonstration with hybrid entanglement photon source*. Optics Express, 18(20), 20080-20085.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). *Quantum cryptography*. Reviews of Modern Physics, 74(1), 145-195.

Granot, E. (2012). *Fundamental dispersion limit for spectrally bounded On-Off-Keying communication channels and its implications to Quantum Mechanics and the Paraxial Approximation*. Europhysics Letters, 100(4), 44004. doi:10.1209/0295-5075/100/44004

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.

Grover, L. K. (1996). *A fast quantum mechanical algorithm for database search*. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212-219.

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). *Quantum entanglement*. Reviews of Modern Physics, 81(2), 865–942. https://doi.org/10.1103/RevModPhys.81.865

Jozsa, R., & Linden, N. (2002). *On the role of entanglement in quantum computational speed-up* [quant-ph/0201143v2]. arXiv preprint arXiv:quant-ph/0201143.

Just, M. (2011). *Nonrepudiation of Digital Signatures*. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_88

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (Uudistettu painos). Scribner.

Kotzanikolaou, P., & Douligeris, C. (2007). *Cryptography Primer: Introduction to Cryptographic Principles and Algorithms*. Liite A, 459–479.

Krelina, M. *Quantum technology for military applications. EPJ Quantum Technol*. 8, 24 (2021). https://doi.org/10.1140/epjqt/s40507-021-00113-y

Lee, J., Kim, S., & Kim, K. (2016). *Is Quantum State in BB84 Protocol Really Unclonable?* Kuva 1. Noudettu osoitteesta: https://www.semanticscholar.org/paper/Is-Quantum-State-in-BB84-Protocol-Really-Unclonable-Lee-Kim/1d0e2facfd2c79db6f100c4b2c8a81153475a940?utm_source=direct_link

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). *The impact of quantum computing on present cryptography*. International Journal of Advanced Computer Science and Applications (IJACSA), 9(3), 405-414.

Martin, K. M. (2012*). Everyday cryptography: Fundamental principles and applications*. Oxford University Press.

Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.

Nimbe, P., Weyori, B. A., & Adekoya, A. F. (2022). *A novel classical and quantum cryptographic scheme for data encryption*.

Kuzminykh, L., Ghita, B., & Shiaeles, S. (2021). *Comparative Analysis of Cryptographic Key Management Systems*. arXiv.org. https://doi.org/10.48550/arXiv.2109.09905.

Penrose, R. *On Gravity's role in Quantum State Reduction*. Gen Relat Gravit 28, 581–600 (1996). https://doi.org/10.1007/BF02105068

Pereira, M., Currás-Lorenzo, G., Navarrete, Á., Mizutani, A., Kato, G., Curty, M., & Tamaki, K. (2023). *Modified BB84 quantum key distribution protocol robust to source imperfections*. Physical Review Research, 5(2), 023065.

Radanliev, P. (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15, Article number: 4.

Schneider, J. (2024). *A brief history of cryptography: Sending secret messages throughout time.* IBM. Noudettu osoitteesta https://www.ibm.com/blog/cryptography-history/

Scholten, T. L., Williams, C. J., Moody, D., Mosca, M., Hurley, W. ("whurley"), Zeng, W. J., Troyer, M., & Gambetta, J. M. (2024). *Assessing the Benefits and Risks of Quantum Computers*. arXiv:2401.16317 [quant-ph]. Noudettu osoitteesta https://arxiv.org/abs/2401.16317.

Sharma, A. (2013). *Authentication in Online Banking Systems through Quantum Cryptography*. International Journal of Engineering and Technology, 1 5(3), 2696-2700. doi:10.54254/2753-8818/30/20241130.

Sharma, P., Gupta, V., & Sood, S. K. (2024). *Evolution of quantum cryptography in response to the computational power of quantum computers*: An archival view. Archives of Computational Methods in Engineering, doi:10.1007/s11831-024-10122-6

Shor, P. W., & Preskill, J. (2000). *Simple proof of security of the BB84 quantum key distribution protocol*. Physical Review Letters, 85(2), 441-444.

Tao, Y. (2024). *Quantum entanglement: Principles and research progress in quantum information processing*. Theoretical and Natural Science, 30(1), 263-274. doi:10.54254/2753-8818/30/20241130

Tarawneh, M. (2023). *Recent advances in cryptography*. Journal of Cryptographic Research, 11(1), 45-67.

Townsend, P., (1997). *Simultaneous Quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM*, Elect. Lett. 33, 188-190.

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.