Linus Vanas

Kvanttilaskenta ja salausmenetelmät

Tietotekniikan kandidaatintutkielma

7. kesäkuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Linus Vanas

Yhteystiedot: linus.j.o.vanas@student.jyu.fi

Työn nimi: Kvanttilaskenta ja salausmenetelmät

Title in English: Quantum computing and encryption methods

Työ: Kandidaatintutkielma

Sivumäärä: 21+0

Tiivistelmä: Kvanttilaskenta ja Shorin algoritmi rikkovat useita nykyisin yleisessä käytössä olevia julkisen avaimen salausmenetelmiä, kuten RSA-menetelmän. Tässä tutkielmassa tarkastellaan kvanttilaskennan vaikutusta salausmenetelmiin sekä erityisesti salausmenetelmiä, jotka ovat murtamattomia myös kvanttilaskennalla. Koodipohjainen McEliecen salausmenetelmä on turvallisuuden puolesta vakuuttavin vaihtoehto RSA-menetelmän korvaajaksi. NTRU-salausmenetelmä ja Lyubashevskyn allekirjoitusjärjestelmä käyttävät hiloihin liittyviä kvanttilaskennallakin vaikeita tehtäviä. Yksisuuntaisia funktiota, kuten hajautusfunktioita, voidaan käyttää kvanttilaskennan kestävänä allekirjoitusjärjestelmänä Lamportin kehittämällä ja Merklen parantamalla menetelmällä. Tällä hetkellä monet organisaatiot pyrkivät standardisoimaan kvanttilaskennalla murtumattomia salausmenetelmiä.

Avainsanat: kvanttilaskenta, salausmenetelmät, digitaaliset allekirjoitukset

Abstract: Quantum computing and Shor's algorithm break several encryption methods currently in use. In this thesis, the effect of quantum computing to encryption methods and encryption methods that are unbroken even with quantum computing are studied. McEliece's code-based encryption is the most confidence-inspiring alternative. The NTRU-encryption method and the Lyubashevsky signature system use lattice-related problems that are computationally difficult even for a quantum computer. One-way functions, like hash functions, can be used as a quantum-proof signature system by using a method developed by Lamport and improved by Merkle. Several organizations are currently in the process of standardizing quantum-resistant encryption methods.

Keywords: quantum computing, encryption methods, digital signatures

Sisältö

1 Johdanto

Salausmenetelmiä käytetään varmistamaan viestien luottamuksellisuus, aitous, eheys ja kiistämättömyys, kun viestejä välitetään epäluotettavilla kanavilla, kuten internetissä. Käytännölliset salausmenetelmät eivät ole teoriassa täysin murtamattomia. Ne on kuitenkin pyritty suunnittelemaan siten, että niiden murtaminen on laskennallisesti erittäin vaikeaa, ja veisi liian kauan tehokkaaltakin tietokoneelta.

Kvanttilaskennassa hyödynnetään kvanttimekaanisia ilmiöitä, mikä mahdollistaa joidenkin perinteisesti laskennallisesti vaikeiden ongelmien nopean ratkaisun. Kvanttilaskentaa hyödyntäviä kvanttitietokoneita on pyritty kehittämään, mutta kaikissa nykyisissä toteutuksissa on hyvin vähän kvanttibittejä, kubitteja. Suuri kvanttitietokone voisi toteutuessaan murtaa monia nykyään yleisessä käytössä olevia salausmenetelmiä.

Tässä tutkielmassa tarkastellaan kirjallisuuskatsauksen muodossa kvanttilaskennan vaikutusta salausmenetelmiin. Erityisesti keskitytään salausmenetelmiin, joita voi käyttää perinteisellä tietokoneella, mutta ei murtaa nopeasti hypoteettisella suurella kvanttitietokoneella. Englanniksi tutkimusalasta käytetään nimiä *Post-Quantum Cryptography* tai *Quantum-resistant Cryptography*.

Tutkimuskysymyksiä ovat

- Mitkä salausmenetelmät kvanttitietokone rikkoo ja miksi?
- Mitä kvanttilaskennan kestäviä salausmenetelmiä on olemassa?
- Mikä on esteenä kvanttilaskennallakin murtumattomien salaustekniikoiden yleiselle käyttöönotolle?

Tutkielman lähtökohdaksi on otettu aikaisemmat kirjallisuuskartoitukset, jotka Bernstein ja Lange (2017) ja Perlner ja Cooper (2009) ovat tehneet, sekä näiden lähdemateriaali. Tutkielmaan on valittu salaustekniikoita, joita käsitellään kummassakin päälähteessä. Niin uutta kuin vanhempaakin tietoa löytyy runsaasti myös näiden lähteiden ulkopuolelta. Kirjallisuuskartoituksia näyttää kuitenkin etenkin suomeksi olevan vähän, joten tutkielma voi vielä tuoda uusia näkökulmia aiheeseen.

Luvussa 2 esitellään salauksen perusteita ja nykyisiä salausmenetelmiä. Luvussa 3 käsitellään kvanttilaskennan perusteita sekä esitellään kaksi kvanttilaskentaa hyödyntävää algoritmia, joilla on merkitystä salauksen näkökulmasta. Luvussa 4 esitellään muutama salausmenetelmä, jotka näyttäisivät olevan murtamattomia kvanttitietokoneellakin. Luvussa 5 käsitellään kvanttilaskennan kestävien salausmenetelmien käyttöönoton ja standardisoinnin näkymiä. Lopuksi luvussa 6 esitetään tutkimuksen yhteenveto ja johtopäätöksiä.

2 Salausmenetelmät

Nykyisin käytössä olevat salausmenetelmät voidaan jakaa symmetrisiin ja epäsymmetrisiin salausmenetelmiin. Symmetrisessä salauksessa viesti salataan ja salattu viesti puretaan samalla avaimella. Viestin lähettäjän ja vastaanottajan pitää jotenkin sopia avaimesta ilman, että se vuotaa ulkopuoliselle. Perinteisesti tähän on tarvittu erillistä luotettavaa viestintäkanavaa, kuten kuriiria.

Symmetrisellä salausmenetelmällä turvataan viestinnän luottamuksellisuus. Vaikka salattu viesti siepattaisiin, on salauksen purkaminen ja viestin lukeminen ilman avainta vaikeaa. Symmetriset salausmenetelmät mahdollistavat myös viestin aitouden ja eheyden varmistamisen. Viestin vastaanottaja voi varmistua viestin aitoudesta, sillä viestin lähettäjällä on täytynyt olla käytössä sama avain kuin vastaanottajalla. Viestin eheys voidaan varmistaa tarkistussummalla. Hyökkäys sekä viestin että tarkistussumman muuttamiseksi vaatisi viestin purkamisen.

Epäsymmetrisissä salausmenetelmissä viestin salaamiseen ja purkamiseen käytetään eri avaimia. Diffie ja Hellman (1976) esittelivät julkisen avaimen salausmenetelmien perusperiaatteet. Julkisen avaimen salausmenetelmät ovat epäsymmetrisiä salausmenetelmiä, joissa lähettäjä salaa viestin vastaanottajan julkaisemalla julkisella avaimella. Viestin voi kuitenkin purkaa vain vastaanottajan salassa pitämällä yksityisellä avaimella. Julkinen avain muodostetaan yksityisestä avaimesta jollain helpolla operaatiolla, jonka käänteisoperaatio on vaikea.

Julkisen avaimen salausmenetelmät turvaavat viestin luottamuksen samalla tavalla kuin symmetrinenkin salaus. Käytännössä julkisen avaimen salausmenetelmillä sovitaan avain symmetriseen salaukseen, jota käytetään varsinaisen viestin salaamiseen. Viestin aitouden ja eheyden varmistamiseen voidaan puolestaan käyttää julkiseen avaimeen pohjautuvaa digitaalista allekirjoitusta.

Diffie ja Hellman (1976) esittelivät myös digitaalisten allekirjoitusten periaatteet. Allekirjoittaessa viesti, tai käytännössä tästä muodostettu tiiviste, salataan yksityisellä avaimella. Allekirjoitus tarkistetaan purkamalla sen salaus julkisella avaimella ja vertaamalla sitä alkuperäiseen viestiin tai tämän tiivisteeseen. Viesti on aito ja eheä, jos allekirjoitus vastaa

alkuperäistä viestiä. Allekirjoitus on lisäksi kiistämätön ainakin siltä osin, että sitä ei voi väärentää julkisella avaimella. Symmetriset salausmenetelmiä käytettäessä aitoutta ei pysty varmistamaan ilman avainta, jolla viestin voisi myös väärentää.

Yksi yleisimmistä julkisen avaimen salausmenetelmistä on RSA. Rivest, Shamir ja Adleman (1978) kehittivät menetelmän, jossa avainten muodostamiseen käytetään kahta satunnaista suurta alkulukua. Alkuperäiset luvut pidetään salaisena ja julkisessa avaimessa käytetään näiden tuloa. Käänteisoperaatiolle, kokonaisluvun jakamiselle alkulukutekijöihin, ei tunneta nopeaa ratkaisualgoritmia perinteisellä tietokoneella. RSA-menetelmää voidaan käyttää myös allekirjoitusjärjestelmänä.

Salausmenetelmien murtamista tutkivaa tieteenalaa kutsutaan kryptoanalyysiksi. Salausmenetelmää pidetään turvallisena, jos siitä ei ole löytynyt vakavia haavoittuvuuksia laajan kryptoanalyysin jälkeen. Kuitenkin esimerkiksi RSA-menetelmän kryptoanalyysi on alunperin tehty perinteisillä tietokoneilla ja laskennan malleilla. Kvanttitietokoneiden 1980-luvulla muotoutunutta teoriaa ei ole tällöin voitu ottaa huomioon.

3 Kvanttilaskennan vaikutus salausmenetelmiin

Jotkin ongelmat voidaan ratkaista kvanttilaskennalla nopeammin kuin perinteisteisillä laskennan malleilla ja tietokoneilla. Kvanttilaskenta tuo siten uuden ulottuvuuden myös salausmenetelmien kryptoanalyysiin. Tässä luvussa käsitellään kvanttilaskennan teoriaa sekä esitellään Shorin ja Groverin algoritmit, joilla on suuri vaikutus salausmenetelmiin.

3.1 Kvanttilaskenta

Kvanttilaskennan teoria on lähtöisin 1980-luvulta. Deutsch (1985) uskoo, että Churchin–Turingin teesiä voi pitää luonnonlakina, ja muotoilee fysikaalisen Churchin–Turingin periaatteen: ”Mitä tahansa äärellisesti toteuttavissa olevaa fysikaalista järjestelmää voi simuloida täydellisesti universaalin mallin mukaisella tietokoneella, joka operoi äärellisin keinoin” (Deutsch 1985, suomennos minun). Klassisen fysiikan jatkuvat lait ja perinteinen universaali Turingin kone eivät hänen mukaansa toteuta tätä määritelmää. Sen sijaan hän esittelee oman mallinsa universaalille kvanttitietokoneelle.

Deutschin (1985) mallin kvanttitietokoneella on äärellinen prosessori sekä ääretön muisti. Lisäksi koneen tilaan kuuluu tieto tämänhetkisestä sijainnista muistissa. Nämä osat ovat analogisia Turingin koneen tilarekisterille, nauhalle sekä lukupään sijainnille nauhalla. Kone suorittaa unitaarisia operaatioita yhdelle muistipaikalle kerrallaan. Operaatioiden kääntyvyys on yksi merkittävä ero klassiseen laskennan malliin.

Deutsch (1985) osoittaa, että hänen mallinsa mukainen kone pystyy simuloimaan mitä tahansa muuta kvanttitietokonetta mielivaltaisen suurella, mutta ei täydellisellä, tarkkuudella. Mallin laadinnassa ei kuitenkaan kiinnitetty huomiota simuloinnin aikavaativuuteen, vaan keskityttiin siihen, onko se yleensä mahdollista.

Bernstein ja Vazirani (1993) kutsuvat Deutschin (1985) mallin mukaista kvanttitietokonetta kvanttimekaaniseksi Turingin koneeksi (englanniksi *Quantum Turing Machine, QTM*). Deutsch (1985) itse ei tätä termiä käytä. Bernstein ja Vazirani (1993) osoittavat, että on olemassa universaali kvanttimekaaninen Turingin kone, jonka pystyy simuloimaan mitä ta-

hansa muuta kvanttitietokonetta polynomisella aikavaativuudella. Deutschin (1985) mallilta joidenkin koneiden simulointi veisi eksponentiaalisen ajan.

Kvanttitietokoneen tila voidaan käsittää usean tilan superpositiona, jota muokataan laskennan aikana. Jokaisella näistä alitiloista on kompleksinen amplitudi. Yksittäisen alitilan todennäköisyys olla lopullinen luettu tila on kyseisen alitilan amplitudin itseisarvon neliö. Tila voidaan lukea vasta laskennan lopuksi, koska tila muuttuu sitä luettaessa.

3.2 Shorin algoritmi

Shorin (1994) algoritmi mahdollistaa kokonaislukujen jaon alkulukutekijöihin sekä diskreetin logaritmin etsimisen nopeasti kvanttilaskentaa käyttäen. Shorin algoritmi murtaa RSA-menetelmän, jonka turvallisuus perustuu kokonaislukujen tekijöihin jaon vaikeuteen. Myös esimerkiksi ECC-salausmenetelmien turvallisuus perustuu Shorin algoritmin ratkaisemiin ongelmiin.

Parittoman luvun n jakamiseksi tekijöihin Shorin (1994) algoritmi etsii kvanttilaskentaa hyödyntäen satunnaisen luvun x kertaluvun r modulo n. Tällöin r on pienin positiivinen kokonaisluku, jolle pätee $x^r \equiv 1 \pmod{n}$. Tämän jälkeen suurin yhteinen tekijä $\text{syt}(x^{r/2}, n)$ on suurella todennäköisyydellä n:n alkulukutekijä.

Tekijöihin jaossa Shorin (1994) algoritmi kvanttilaskentaa käyttävä osuus on luvun x kertaluvun r modulo n etsintä. Sopivasti alustettuun kvanttitietokoneen tilaan tehdään Fourier'n muunnos, ja tuloksesta voidaan suurella todennäköisyydellä laskea r. Diskreetin logaritmin etsintäalgoritmi on samankaltainen kuin kertaluvun etsintäalgoritmi.

3.3 Groverin algoritmi

Groverin (1996) algoritmi hyödyntää kvanttimekaanisten järjestelmien aalto-ominaisuuksia alkioiden etsimiseen järjestämättömästä tietokannasta aikavaativuudella $O(\sqrt{n})$. Perinteisellä tietokoneella alkiot on käytävä läpi yksi kerrallaan vaatien lineaarisen ajan tietokannan koon suhteen. Toisin sanoen kvanttilaskenta mahdollistaa tietyt ehdot täyttävien alkioiden etsimisen mistä tahansa äärellisestä joukosta perinteistä laskentaa nopeammin.

Groverin (1996) ratkaisee hakutehtävän yleisessä muodossa ilman lisäoletuksia, joten sitä voidaan käyttää myös salausmenetelmien murtamiseen. Toisin kuin Shorin algoritmi, Groverin algoritmi vaikuttaa myös symmetristen salausmenetelmien turvallisuuteen. Neliöjuurellinen nopeutus on ei riitä rikkomaan salausmenetelmiä täysin, mutta se on kuitenkin huomioitava salausmenetelmien turvallisuustasoa arvioidessa. Esimerkiksi ennen 128-bittinen turvallisuustaso on Groverin algoritmi huomioiden vain 64-bittinen.

4 Vaihtoehtoiset salausmenetelmät

Shorin algoritmi murtaa useita yleisesti käytettyjä julkisen avaimen salausmenetelmiä. Shorin algoritmin ratkaisemat tehtävät eivät kuitenkaan ole ainoat julkisen avaimen salausmenetelmien perustaksi sopivat matemaattiset ongelmat. Tässä luvussa esitellään kaksi vaihtoehtoisiin ongelmiin perustuvaa salausmenetelmäluokkaa, koodi- ja hilapohjaiset salaustekniikat. Lisäksi esitellään yksisuuntaisiin funktioihin perustuvat allekirjoitukset, joilla ei ole vastaavaa salausmenetelmää.

4.1 Koodipohjaiset salaustekniikat

Virheenkorjauskoodeilla pystytään tallentamaan dataa niin, että tietty määrä esimerkiksi siirron yhteydessä siihen ilmestyneistä virheistä voidaan korjata. Virheenkorjaukseen käytetään koodeja, joiden purkamiseen tunnetaan nopea algoritmi. Yleiselle lineaariselle koodille ei vastaavaa nopeaa algoritmia tunneta. Koodeja voidaan käyttää julkisen avaimen salausmenetelmän pohjana naamioimalla helposti purettava koodi yleiseksi koodiksi.

McEliece (1978) käyttää salausmenetelmässään jaottomiin polynomeihin perustuvia Goppa-koodeja. Goppa-koodi voidaan purkaa nopeasti, ja se pystyy korjaamaan vastaavan polynomin asteen verran virheitä. McEliecen (1978) menetelmässä satunnaisesta jaottomasta polynomista luodaan generaattorimatriisi G. Goppa-koodin kätkemistä varten luodaan lisäksi satunnaiset epäsingulaarinen matriisi S ja permutaatiomatriisi P. Julkinen avain on näiden matriisien tulosta muodostettu generaattorimatriisi $G' = SGP$. Alkuperäiset matriisit jäävät yksityisiksi.

Viesti u salataan McEliecen (1978) menetelmässä muuttamalla se koodiksi julkisella generaattorimatriisilla ja lisäämällä siihen satunnaisia virheitä z, jolloin salattu viesti on $x = uG' + z$. Viestin vastaanottaja pystyy palauttamaan salatun viestin Goppa-koodiksi käyttäen matriisien S ja P käänteismatriiseja. Alkuperäinen viesti saadaan purkamalla Goppa-koodi.

Ilman yksityisavainta salattu viesti voidaan yrittää murtaa purkamalla se yleisenä lineaarisena koodina tai etsimällä alkuperäinen Goppa-koodi julkisesta generaatiomatriisista tun-

tematta kätkentään käytettyjä matriiseja. Kummallekaan hyökkäykselle ei tunneta nopeaa algoritmia sen paremmin perinteisellä kuin kvanttitietokoneellakaan.

Bernstein, Lange ja Peters (2008) pystyivät murtamaan McEliecen (1978) alunperin ehdottamat parametrit yleisen lineaarisen koodin purkamiseen perustuvalle menetelmällä. Hyökkäys vaati seitsemän päivää 200 prosessoria käyttäen. Bernstein, Lange ja Peters (2008) kuitenkin esittivät salausmenetelmälle myös uusia, hyökkäystä vastaan vahvempia parametreja, joilla saavutetaan nykyaikaiset turvallisuustasot.

McEliecen salausmenetelmässä on joitakin käytännöllisyyttä rajoittavia ongelmia. Yksityisavaimet ovat suuria, sillä niihin täytyy tallentaa kaksi satunnaismatriisia S ja P. McEliecen (1978) mukaan hänen menetelmäänsä ei myöskään sovellu allekirjoitusjärjestelmäksi, sillä purkualgoritmi ei toimi yleisellä syötteellä.

Salausmenetelmästä onkin kehitetty useita variaatioita ja parannuksia. Myös vaihtoehtoja Goppa-koodeille on tutkittu. Toisaalta monet salausmenetelmän variaatioista on myös rikottu ja näihin on luonnollisesti myös kohdistunut vähemmän kryptoanalyysia kuin alkuperäiseen menetelmään. Esimerkiksi Guo, Johansson ja Stankovski (2016) rikkoivat MDPC-koodeja käyttävän variaation, jonka Misoczki ym. (2013) olivat kehittäneet.

Li, Deng ja Wang (1994) osoittivat, että Niederreiterin (1986) salausmenetelmä on turvallisuuden kannalta ekvivalentti McEliecen menetelmän kanssa, jos molemmissa käytetään samoja koodeja ja parametreja. McEliecen ja Niederreiterin salausmenetelmiä käsitellään tämän vuoksi usein yhdessä. Courtois, Finiasz ja Sendrier (2001) ovat kehittäneet allekirjoitusmenetelmän, joka perustuu Niederreiterin salausmenetelmään. Allekirjoittaminen menetelmää käyttäen on kuitenkin hidasta.

4.2 Hilapohjaiset salaustekniikat ja allekirjoitukset

Vektorijoukon kokonaislukumonikertojen joukkoa kutsutaan hilaksi. Hilan virittävä vektorijoukkoa kutsutaan hilan kannaksi. Hiloihin liittyy laskennallisesti vaikeita tehtäviä, kuten lyhyimmän vektorin ongelma (engl. *shortest vector problem, SVP*) sekä lähimmän vektorin ongelma (engl. *closest vector problem, CVP*). Hiloihin liittyvien ongelmien pohjalta on

kehitetty monia julkisen avaimen salausmenetelmiä.

Hoffstein, Pipher ja Silverman (1998) käyttävät NTRU-salausmenetelmässään polynomirenkaita ja esittävät avaimet sekä salatun viestin polynomeina. NTRU-menetelmän turvallisuus perustuu kuitenkin hiloihin, sillä avainpolynomit vastaavat hilan kantoja. Yksityinen avain voidaan käsittää lyhyiden vektorien muodostamaksi kannaksi julkisen avaimen koostuessa pitkistä vektoreista. Lyhyiden vektorien löytämisen vaikeus estää yksityisavaimen laskemisen julkisesta.

Biasse ja Song (2016) ovat kvanttilaskentaa sekä Shorin algoritmia hyödyntäen kehittäneet ratkaisualgoritmeja joillekin polynomirenkaisiin ja siten hiloihin liittyviin ongelmiin. Nämä mahdollistavat joidenkin NTRU-menetelmän kaltaisten hilapohjaisten salausmenetelmien murtamisen. Vaikka itse NTRU-menetelmästä ei varsinaista haavoittuvuutta löytynytkään, Bernstein ym. (2018) ovat kehittäneet hyökkäystä vastaan suojatumman NTRU Prime -menetelmän.

Hilaongelmien sekä erityisesti NTRU-menetelmän muuntaminen allekirjoituskäyttöön on osoittautunut vaikeaksi. Gentry ym. (2001) mursivat NTRU-menetelmän pohjalta kehitetyn NSS-allekirjoitusjärjestelmän (Hoffstein, Pipher ja Silverman 2001). Nguyen ja Regev (2006) mursivat edelleen kehitetyn NTRUSIGN-allekirjoitusjärjestelmän (Hoffstein ym. 2003). Hiloihin perustuen on kehitetty kuitenkin muitakin allekirjoitusjärjestelmiä, kuten Lyubashevskyn (2012) allekirjoitusjärjestelmä.

4.3 Yksisuuntaisiin funktioihin perustuvat allekirjoitukset

Yksisuuntainen funktio on funktio, jonka kuvasta on laskennallisesti vaikeaa päätellä alkukuva. Yksisuuntaisia funktiota voidaan käyttää allekirjoitusjärjestelmien luomiseen ilman vastaavaa julkisen avaimen salausmenetelmää. Tähän soveltuvat esimerkiksi kryptografiset hajautusfunktiot. Hajautusfunktiot ovat allekirjoittamiseen erityisen käytännöllisiä, sillä niitä tarvitaan joka tapauksessa allekirjoitettavan tiivisteen luomiseen.

Lamportin (1979) allekirjoitusmenetelmässä allekirjoittaja arpoo jokaista salattavaa bittiä varten kaksi salaista avainta x_0 ja x_1. Kirjallisuudessa näihin on viitattu yksikertaisesti merk-

kijonona (Bernstein ja Lange 2017) tai sanalla *secret* (Perlner ja Cooper 2009). Julkinen avain muodostetaan julkisen yksisuuntaisen funktion h avulla ja koostuu salaisten avainten kuvista. Yhdelle bitille julkinen avain on $(h(x_0), h(x_1))$. Yksityisavaimen laskeminen julkisesta vaatisi yksisuuntaisen funktion alkukuvan löytämistä ja on siten vaikeaa.

Allekirjoitus tehdään Lamportin (1979) menetelmässä julkaisemalla toinen jokaisen bitin salaisista avaimista, riippuen siitä, onko allekirjoitettava bitti yksi vai nolla. Jos bitti on nolla, julkaistaan x_0 ja jos bitti on yksi, julkaistaan x_1. Allekirjoitus tarkistetaan laskemalla jokaisesta julkaistusta salaisesta avaimesta kuva julkisen funktion h avulla ja vertaamalla sitä julkiseen avaimeen. Jos kuva vastaa julkisessa avaimessa olevaa arvoa, on allekirjoitus aito.

Lamportin (1979) menetelmässä yhdellä allekirjoituskerralla yksityisavaimesta paljastetaan vain puolet, mikä ei vielä mahdollista muun kuin jo allekirjoitetun viestin allekirjoitusta. Avaimia voidaan kuitenkin käyttää turvallisesti vain kerran. Jos samoja avaimia käytetään useaan kertaan, paljastuu lopulta koko yksityisavain.

Lamportin menetelmään on useita parannuksia, joista monet ovat Merklen (1990) kehittämiä. Avaimia ja allekirjoituksia voi pienentää luomalla jokaista bittiä varten vain yksi avain. Tämä avain paljastetaan vain, jos bitin arvo on nolla. Allekirjoitettavaan viestiin täytyy lisätä allekirjoitettavien nollabittien määrä, jotta allekirjoitusta ei voi muuttaa poistamalla osa julkaistuista avaimista.

Keskeisin Merklen (1990) kehittämä parannus menetelmään mahdollistaa monen kertakäyttöisellä yksityisavaimella tehdyn allekirjoituksen tarkistamisen yhdellä julkisella avaimella. Yksityisavaimet yhdistetään binääripuuksi niin, että lehtisolmuissa on kunkin avaimen yksisuuntaisella funktiolla laskettu kuva. Yksityisavaimet yhdistetään pareittain ja yhdisteen kuvasta tehdään solmujen vanhempi. Solmujen yhdistämistä jatketaan, kunnes haluttu määrä yksityisavaimia on yhdistetty yhdeksi juurisolmuksi, joka julkaistaan.

Merklen (1990) menetelmässä allekirjoittaja paljastaa käyttämänsä yksityisavaimen lisäksi puusta ne solmut, joita tarvitaan julkisen avaimen laskemiseen. Allekirjoituksen tarkistaja laskee yksityisavaimen kuvan, sitten tämän yhdisteen allekirjoittajan paljastaman sisarsolmun avaimen kuvan kanssa ja niin edelleen kunnes pääsee juurisolmuun.

Buchmann, Dahmen ja Hülsing (2011) kehittivät XMSS-allekirjoitusjärjestelmän monien yksisuuntaisiin funktioihin perustuviin allekirjoituksiin tehtyjen parannusten pohjalta. XMSS muodostaa esiteltyyn tapaan julkisen avaimen monesta yhdistetystä yksityisavaimesta, mutta tallennustilan säästämiseksi yksityisavaimia ei tallenneta vaan ne luodaan vasta tarvittaessa. XMSS on myös mahdollista toteuttaa niin, että jo allekirjoitukseen käytetyn yksityisavaimen vuotaminen ei mahdollista uusien allekirjoitusten väärentämistä.

5 Standardisointi

Kvanttilaskennankestäviä salausmenetelmiä on kehitty paljon enemmän kuin tässä tutkielmassa on mahdollista käsitellä niin esitellyissä kolmessa luokassa kuin niiden ulkopuolella. Yleistä käyttöönottoa varten näiden joukosta olisi valittava muutama luotettava ja käytännöllinen menetelmä. Useat organisaatiot, kuten ETSI, IETF, ISO ja NIST (Bernstein ja Lange 2017), pyrkivätkin kehittämään kvanttilaskennankestävien salausmenetelmien standardia. Tässä luvussa käsitellään tarkemmin kahta kehityshanketta.

Euroopan Unionin rahoittama PQCRYPTO ei ole varsinainen standardisointihanke, vaan projekti pyrkii kehittämään kvanttilaskennankestäviä salausmenetelmiä yhdessä muiden organisaatioiden kanssa. Projekti on kuitenkin julkaissut joitain varhaisia suosituksia. Augot ym. (2015) suosittelevat raportissaan alkuperäisen kaltaista McEliecen salausmenetelmää julkisen avaimen salausmenetelmäksi. Lisäksi raportti suosittelee kahta hajautusfunktioihin pohjautuvaa allekirjoitusmenetelmää, joista toinen on XMSS.

Yhdysvaltain kauppaministeriön alainen *National Institute of Standards and Technology* (NIST) on yksi tahoista, joka pyrkii standardisoimaan kvanttilaskennankestäviä salausmenetelmiä. NIST:in 2010-luvun puolivälissä aloittaman standardisointiprosessin toiselle kierrokselle on valittu 17 julkisen avaimen salausmenetelmää ja yhdeksän allekirjoitusmenetelmää (Alagic ym. 2019). Näiden joukossa on niin koodi- kuin hilapohjaisia julkisen avaimen menetelmiä, mukaan lukien McEliecen menetelmään sekä NTRU-menetelmän perustuvia menetelmiä.

6 Yhteenveto

Kvanttilaskenta ja Shorin algoritmi rikkovat useita nykyisin yleisessä käytössä olevia julkisen avaimen salausmenetelmiä, kuten RSA-menetelmän. Kvanttilaskenta ja Groverin algoritmi heikentävät lisäksi symmetristen salausten turvallisuutta murtamatta niitä kuitenkaan täydellisesti. Groverin algoritmilta voidaan suojautua yksinkertaisesti nykyisten salausmenetelmien turvallisuustasoa nostamalla, mutta Shorin algoritmi vaatii vaihtoehtoisten salausmenetelmien etsimistä.

McEliecen salausmenetelmä on turvallisuuden puolesta vakuuttavin vaihtoehto RSA-menetelmän korvaajaksi, sillä se on yhtä vanha kuin RSA ja perusteiltaan yhä murtamaton. Menetelmä perustuu helposti purettavan Goppa-koodin naamioimiseen vaikeasti purettavaksi yleiseksi lineaariseksi koodiksi. McEliecen salausmenetelmän suurin ongelma on yksityisavaimen suuri koko. Menetelmällä ei myöskään ole vastaavaa käytännöllistä allekirjoitusmenetelmää.

Hiloihin liittyy laskennallisesti vaikeita tehtäviä, joita on käytetty niin julkisen avaimen salaus- kuin allekirjoitusmenetelmienkin luomiseen. Näitä ovat esimerkiksi NTRU-salausmenetelmä ja Lyubashevskyn allekirjoitusjärjestelmä. Monet hilapohjaiset salausmenetelmät ja etenkin allekirjoitusjärjestelmät ovat kuitenkin osoittautuneet haavoittuvaisiksi.

Allekirjoitettavan tiivisteen luomiseen käytettyjä hajautusfunktioita voi käyttää myös varsinaiseen allekirjoitukseen ilman julkisen avaimen salausmenetelmää. Lamportin kehittämässä menetelmässä jokaista allekirjoitusta varten tarvitaan oma avainpari, mutta Merklen kehittämä menetelmä mahdollistaa useaa yksityistä avainta vastaavan julkisen avaimen yhdistämisen yhdeksi hajautusfunktioiden avulla.

Tällä hetkellä monet organisaatiot pyrkivät standardisoimaan kvanttilaskennalla murtumattomia salausmenetelmiä. Standardisoinnin jälkeen vuorossa on menetelmien toteuttaminen käytännössä. Turvallisuuden takaamiseksi sekä menetelmien perusteisiin että käytännön toteutuksiin on jatkossakin kohdistettava turvallisuusanalyysia ja tutkimusta.

Lähteet

Alagic, Gorjan, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller ym. 2019. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process.* Tekninen raportti. US Department of Commerce, National Institute of Standards ja Technology.

Augot, Daniel, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman ym. 2015. *Initial recommendations of long-term secure post-quantum systems.* Tekninen raportti. PQCRYPTO. EU Horizon 2020.

Bernstein, Daniel J., Chitchanok Chuengsatiansup, Tanja Lange ja Christine van Vredendaal. 2018. "NTRU Prime: Reducing Attack Surface at Low Cost". Teoksessa *Selected Areas in Cryptography – SAC 2017,* toimittanut Carlisle Adams ja Jan Camenisch, 235–260. Cham: Springer International Publishing. ISBN: 978-3-319-72565-9.

Bernstein, Daniel J., ja Tanja Lange. 2017. "Post-quantum cryptography". *Nature* 549:188–194. doi:10.1038/nature23461.

Bernstein, Daniel J., Tanja Lange ja Christiane Peters. 2008. *Attacking and defending the McEliece cryptosystem.* Cryptology ePrint Archive, Report 2008/318. https://eprint.iacr.org/2008/318.

Bernstein, Ethan, ja Umesh Vazirani. 1993. "Quantum Complexity Theory". Teoksessa *Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing,* 11–20. STOC '93. San Diego, California, USA: ACM. ISBN: 0-89791-591-7. doi:10.1145/167088.167097.

Biasse, Jean-François, ja Fang Song. 2016. "Efficient Quantum Algorithms for Computing Class Groups and Solving the Principal Ideal Problem in Arbitrary Degree Number Fields". Teoksessa *Proceedings of the Twenty-seventh Annual ACM-SIAM Symposium on Discrete Algorithms,* 893–902. SODA '16. Arlington, Virginia: Society for Industrial / Applied Mathematics. ISBN: 978-1-611974-33-1. http://dl.acm.org/citation.cfm?id=2884435.2884499.

Buchmann, Johannes, Erik Dahmen ja Andreas Hülsing. 2011. “XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions”. Teoksessa *Post-Quantum Cryptography,* toimittanut Bo-Yin Yang, 117–129. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-25405-5.

Courtois, Nicolas T., Matthieu Finiasz ja Nicolas Sendrier. 2001. “How to Achieve a McEliece-Based Digital Signature Scheme”. Teoksessa *Advances in Cryptology — ASIACRYPT 2001,* toimittanut Colin Boyd, 157–174. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-45682-7.

Deutsch, David. 1985. “Quantum theory, the Church–Turing principle and the universal quantum computer”. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400 (1818): 97–117. doi:10.1098/rspa.1985.0070.

Diffie, W., ja M. Hellman. 1976. “New directions in cryptography”. *IEEE Transactions on Information Theory* 22, numero 6 (): 644–654. ISSN: 0018-9448. doi:10.1109/TIT.1976.1055638.

Gentry, Craig, Jakob Jonsson, Jacques Stern ja Michael Szydlo. 2001. “Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001”. Teoksessa *Advances in Cryptology — ASIACRYPT 2001,* toimittanut Colin Boyd, 1–20. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-45682-7.

Grover, Lov K. 1996. “A Fast Quantum Mechanical Algorithm for Database Search”. Teoksessa *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing,* 212–219. STOC ’96. Philadelphia, Pennsylvania, USA: ACM. ISBN: 0-89791-785-5. doi:10.1145/237814.237866.

Guo, Qian, Thomas Johansson ja Paul Stankovski. 2016. “A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors”. Teoksessa *Advances in Cryptology – ASIACRYPT 2016,* toimittanut Jung Hee Cheon ja Tsuyoshi Takagi, 789–815. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-662-53887-6.

Hoffstein, Jeffrey, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman ja William Whyte. 2003. “NTRUSign: Digital Signatures Using the NTRU Lattice”. Teoksessa *Topics in Cryptology — CT-RSA 2003,* toimittanut Marc Joye, 122–140. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-36563-1.

Hoffstein, Jeffrey, Jill Pipher ja Joseph H. Silverman. 1998. “NTRU: A ring-based public key cryptosystem”. Teoksessa *Algorithmic Number Theory,* toimittanut Joe P. Buhler, 267–288. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-69113-6.

———. 2001. “NSS: An NTRU Lattice-Based Signature Scheme”. Teoksessa *Advances in Cryptology — EUROCRYPT 2001,* toimittanut Birgit Pfitzmann, 211–228. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-44987-4.

Lamport, Leslie. 1979. *Constructing digital signatures from a one-way function.* Tekninen raportti. Technical Report CSL-98, SRI International Palo Alto.

Li, Yuan Xing, Robert H. Deng ja Xin Mei Wang. 1994. “On the equivalence of McEliece’s and Niederreiter’s public-key cryptosystems”. *IEEE Transactions on Information Theory* 40, numero 1 (): 271–273. ISSN: 0018-9448. doi:10.1109/18.272496.

Lyubashevsky, Vadim. 2012. “Lattice Signatures without Trapdoors”. Teoksessa *Advances in Cryptology – EUROCRYPT 2012,* toimittanut David Pointcheval ja Thomas Johansson, 738–755. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-29011-4.

McEliece, Robert J. 1978. “A public-key cryptosystem based on algebraic Coding Theory”. *Deep Space Network Progress Report* 42-44:114–116. https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

Merkle, Ralph C. 1990. “A Certified Digital Signature”. Teoksessa *Advances in Cryptology — CRYPTO’ 89 Proceedings,* toimittanut Gilles Brassard, 218–238. New York, NY: Springer New York. ISBN: 978-0-387-34805-6.

Misoczki, R., J. Tillich, N. Sendrier ja P. S. L. M. Barreto. 2013. “MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes”. Teoksessa *2013 IEEE International Symposium on Information Theory,* 2069–2073. doi:10.1109/ISIT.2013.6620590.

Nguyen, Phong Q., ja Oded Regev. 2006. “Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures”. Teoksessa *Advances in Cryptology - EUROCRYPT 2006,* toimittanut Serge Vaudenay, 271–288. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-34547-3.

Niederreiter, Harald. 1986. “Knapsack-type cryptosystems and algebraic coding theory”. *Problems in Control and Information Theory* 15 (2): 159–166.

Perlner, Ray A., ja David A. Cooper. 2009. “Quantum Resistant Public Key Cryptography: A Survey”. Teoksessa *Proceedings of the 8th Symposium on Identity and Trust on the Internet,* 85–93. IDtrust ’09. Gaithersburg, Maryland, USA: ACM. ISBN: 978-1-60558-474-4. doi:10.1145/1527017.1527028.

Rivest, R. L., A. Shamir ja L. Adleman. 1978. “A Method for Obtaining Digital Signatures and Public-key Cryptosystems”. *Commun. ACM* (New York, NY, USA) 21, numero 2 (): 120–126. ISSN: 0001-0782. doi:10.1145/359340.359342.

Shor, Peter W. 1994. “Algorithms for quantum computation: discrete logarithms and factoring”. Teoksessa *Proceedings 35th Annual Symposium on Foundations of Computer Science,* 124–134. doi:10.1109/SFCS.1994.365700.