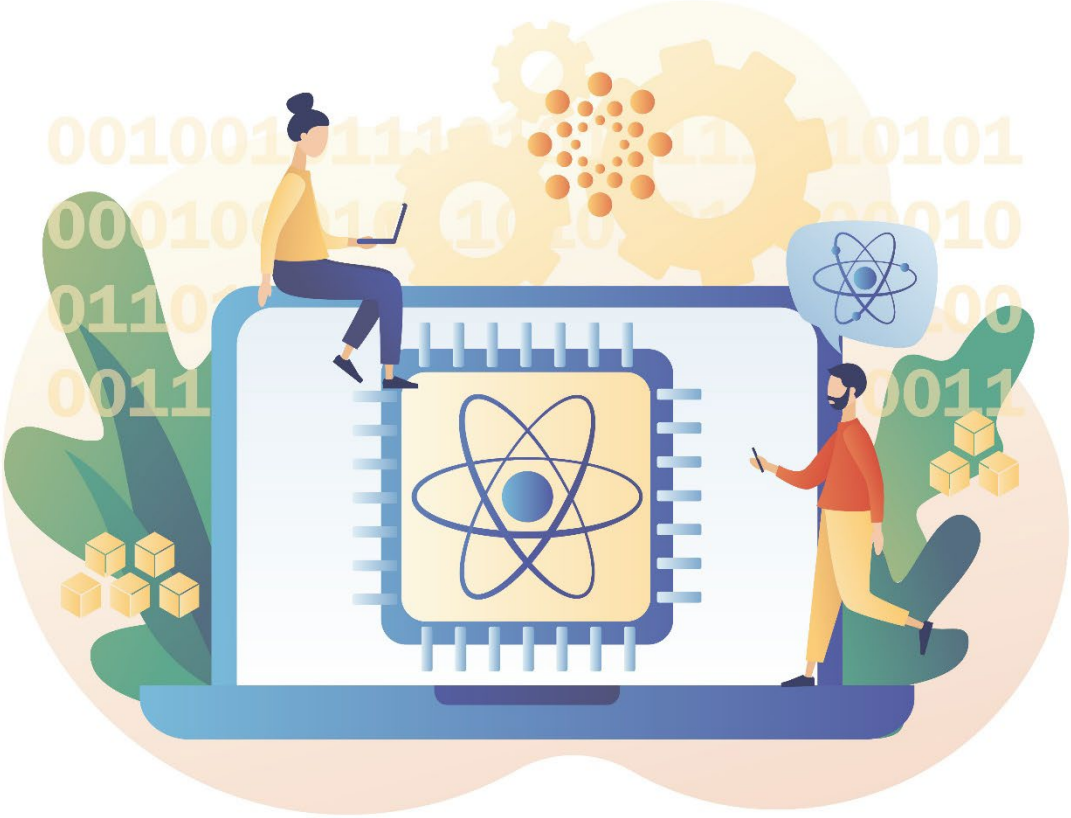
VTT

Policy brief

Kvanttikoneiden nopea kehitys aiheuttaa mullistuksia myös nyky-yhteiskuntaa suojaavalle kryptografialle. Haasteeseen vastaaminen edellyttää sekä tutkimus- että käytännön osaamisen kehittämistä.

Kvanttiturvalliset salausmenetelmät Suomessa



Tiivistelmä

Nykyaikainen digitaalinen yhteiskunta on vahvasti riippuvainen kryptografiasta. Sen avulla suojataan sekä valtionsalaisuuksia että kansalaisten pankkiasiointia. Meillä on käytössä sekä salaisen avaimen että julkisen avaimen kryptografiaa. Salaisen avaimen kryptografia on tehokasta ja soveltuu esimerkiksi suurten datamäärien salaamiseen. Kun kommunikoivien osapuolien lukumäärä kasvaa, on järkevämpi käyttää julkisen avaimen kryptografiaa, jossa lähettää salaa viestin vastaanottajan julkisella avaimella, ja vastaanottaja purkaa sen omalla yksityisellä avaimellaan. Viestien salauksen lisäksi julkisen avaimen kryptografialla voidaan toteuttaa myös digitaalinen allekirjoittaminen.

Kvanttikoneiden kehitys heittää varjon olemassa olevien kryptogafisten ratkaisujen päälle. Niille on jo keksitty algoritmeja, joiden avulla voidaan ratkaista julkisen avaimen kryptografiassa taustalla käytettyjä matemaattisia ongelmia. Sen vuoksi meidän on otettava käyttöön erilaisille matemaattisille rakenteille perustuvia algoritmeja, joita vastaan kvanttikoneella ei ole tehokasta hyökätä. Yhdysvalloissa NIST on käynnistänyt kilpailun uusien PQC-algoritmien standardoimiseksi. Ensimmäiset standardoitavat algoritmit on jo valittu, ja kilpailu jatkunee vielä vuoteen 2024.

Uudet algoritmit vaativat vielä tutkimusta, ja muutamista onkin jo löydetty vakavia heikkouksia. PQC-algoritmit ovat myös teknisiltä ominaisuuksiltaan erilaisia, joten niitä ei voida suoraan liittää olemassaoleviin järjestelmiin. Tässä projektissa olemme kehittäneet suomalaista kryptografian osaamista, verkostoitumista ja varautumista kvanttikoneiden ajalle. Tutkimme myös PQC-algoritmien rajapintoja ja optimointimahdollisuuksia. Suomi on tällä hetkellä eturintamassa niin kvanttiturvallisen kryprografian kuin myös varsinaisten kvanttiteknologioiden suhteen. Aseman säilyttämiseksi tarvitsemme hyvin koulutettua väkeä sekä tutkimukseen ja tuotekehitykseen että uusien teknologioiden toteuttamiseen. Lisäksi meidän on lisättävä tietoisuutta kvanttikoneiden aiheuttamasta uhasta digitaaliselle nyky-yhteiskunnalle. Vanhojen järjestelmien päivittämien tulee olemaan valtava ja aikaavievä urakka. Niin julkisten kuin yksityistenkin organisaatioiden on varaututtava siirtymään PQC-aikaan huolehtimalla järjestelmiensä ketteryydestä ja avainhenkilöidensä koulutuksesta.

Kvanttikoneiden nousun uhka nykyaikaiselle kryptografialle

Melkein kaikki digitaalinen kanssakäyminen nyky-yhteiskunnassa on suojattu kryptografian avulla. Esimerkiksi jokaisen kansalaisen arkinen kommunikointi pankin kanssa hyödyntää erilaisia kryptografisia algoritmeja, joilla sekä salataan tiedonvaihtoa että varmennetaan keskustelukumppanin identiteetti. Osalle salattavasta tiedosta riittää pysyä salaisena sen lyhyen hetken ajan, kun kommunikaatio tapahtuu, mutta yhteiskunnassa on paljon informaatiota, jonka pitää pysyä luottamuksellisena vuosikymmeniä.

Moderni kryptografia voidaan jakaa kahteen kategoriaan: symmetrisen eli salaisen avaimen kryptografiaan sekä asymmetriseen eli julkisen avaimen kryptografiaan. Symmetrisen avaimen kryptografiassa sekä lähettäjällä että vastaanottajalla on identtinen avain, jolla voi sekä salata että purkaa dataa. Algoritmit, kuten AES, ovat nopeita ja tehokkaita, joten symmetrinen salaus soveltuu suurten datamäärien suojaamiseen. Avainten hallinta ja vaihtaminen kommunikoivien osapuolten välillä on tämän kategorian heikkous. Sen vuoksi internetin aikakaudella äärimmäisen tärkeäksi on muodostunut julkisen avaimen kryptografia, jossa lähettää salaa viestin vastaanottajan julkisella avaimella, ja vastaanottaja purkaa sen omalla yksityisellä avaimellaan. Viestien salauksen lisäksi julkisen avaimen kryptografialla voidaan toteuttaa myös digitaalinen allekirjoittaminen.

Julkisen avaimen salaus ei ole yhtä tehokasta kuin symmetrinen salaus, joten on tavanomaista yhdistää eri metodeja. Esimerkiksi TLS-protokollassa, jonka avulla salataan verkkoliikennettä ja joka on käytössä muun muassa HTTPS-yhteyksissä, käytetään julkisen avaimen metodeja yhteyden avaamiseen ja symmetristen avainten vaihtamiseen. Tämän alun kättelyvaiheen jälkeen osapuolet jatkavat kommunikointia käyttäen nopeampaa symmetristä salausta.

Nykyiset julkisen avaimen salausalgoritmit perustuvat pariin erilaiseen matemaattiseen ongelmaan: tekijöihin jakoon, sekä diskreetteihin logaritmeihin ja elliptisiin käyriin. Ne saadaan murrettua tehokkaalla kvanttitietokoneella ja Shorin algoritmilla. Myös symmetrinen salaus heikkenee, mutta ei yhtä vakavasti, sillä niitä vastaan käytettävä Groverin algoritmi antaa vain pienen nopeutuksen symmetristen salausmenetelmien murtamiseen.

Kvanttiturvallisissa salausmenetelmissä hyödynnetään toisenlaisia matemaattisia rakenteita ja ongelmia: hiloja, monimuuttujia, isogeenejä ja koodiluokkia. Uusilla algoritmeilla tulee olemaan totutusta poikkeavia käytännön ominaisuuksia, kuten suurempia avaimia, allekirjoituksia tai salatekstejä. Sen vuoksi niitä ei voi suoraan liittää nykyisiin järjestelmiin, protokoliin ja tietoverkkoihin, vaan tarvitaan järjestelmien uudelleen arviointia ja suunnittelua.

Yhdysvalloissa NIST on aloittanut PQC-standardisointiprosessin vuonna 2016, ja se päättynee 2022–2024. Standardiin on etsitty algoritmeja kilpailun avulla, jossa käynnistyi kesällä 2022 jo neljäs kierros. Kolmannelta kierrokselta valittiin jo muutamia algoritmeja standardoitavaksi, ja neljännelle kierrokselle lähetettiin matemaattisesti erilaisia algoritmeja jatkoanalyysiä varten. Eri ratkaisuilla on hyötynsä ja heikkoutensa, eikä uusia salausalgoritmeja ei ole vielä tutkittu riittävästi, joten standardiin joudutaan valitsemaan useita algoritmeja.

Muutamassa isossa Euroopan maassa on jo tehty päätöksiä siirtyä kvanttiturvallisiin ratkaisuihin, kuten Saksassa on valittu Classic McEliece sekä Frodo. Myös Ranskassa, Kiinassa, Venäjällä ja Alankomaissa on jo kansallisia suosituksia asiasta. Monissa muissa maissa on prosessi käynnistetty, kuten Ruotsissa ja Norjassa, ja vähintään uhka on tunnistettu myös Virossa ja Tanskassa. Lisäksi esimerkiksi ENISA:n raportissa[1] on esitetty kaksi keinoa kvanttiuhan lieventämiseen ennen kuin uudet PQC-standardit ovat kypsyneet: Hybridimallissa

[1] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

käytetään yhdistelmää perinteisestä ja PQC-algoritmista turvallisuuden lisäämiseksi. Toinen vaihtoehto on jakaa etukäteen kommunikoiville laitteille tai muille osapuolille pareittain symmetrisiä avaimia. Tämä strategia soveltuu vain pienille ja stabiileille ympäristöille, sillä avaintenhallinnasta tulee muuten liian raskasta.

Seuraavassa taulukossa on esitetty vertailu Suomessa käytössä olevien turvallisuusluokkien (TL) ja NIST:in kilpailussa käytettyjen turvatasojen välillä. Suomalaisessa ohjeessa[2] on määritelty kryptografinen vahvuus bitteinä kullekin tasolle, ja lueteltu esimerkkejä algoritmeista ja niiden avaimenpituuksista, jotka riittävät tason saavuttamiseen. Tässä katsauksessa mainitaan vain pari esimerkkiä, jotka vastaavat parhaiten NIST:in valitsemia turvallisuuskuvauksia. NIST ei kilpailussaan[3] asettanut tarkkoja kryptografisia bittivahvuuksia turvatasojensa pohjalle, koska kvanttikoneisiin ja kvanttialgoritmeihin liittyy niin suuria epävarmuuksia. Sen sijaan NIST määritteli tasot suhteellisen helposti analysoitavien referenssialgoritmien perusteella. Tämän referenssipisteen avulla NIST tavoitteli kykyä arvioida uusien algoritmien turvallisuutta ja tehokkuutta monipuolisesti ja joustavasti pitkin kilpailua.

Suomen kansalliset turvallisuusluokat			NIST:in kilpailun turvatasot	
TL	kryptografinen vahvuus bitteinä	esimerkiksi	turvataso	vertautuu hyökkääjän laskentatehoon, joka…
IV	128	lohkosalain AES-128, tiivistefunktio SHA-256	1	murtaisi 128-bittisen lohkosalaimen
			2	löytäisi törmäyksen 256-bittisestä tiivistefunktiosta
III	192	lohkosalain AES-192, tiivistefunktio SHA-384	3	murtaisi 192-bittisen lohkosalaimen
			4	löytäisi törmäyksen 384-bittisestä tiivistefunktiosta
II	256	lohkosalain AES-256, tiivistefunktio SHA-512	5	murtaisi 256-bittisen lohkosalaimen

Suurin osa projektin aikana tehdystä työstä on keskittynyt NIST:in kilpailun kolmannen kierroksen finalisteihin: Classic McEliece, CRYSTALS-KYBER, NTRU ja Saber avaimenkapsulointikategoriasta sekä CRYSTALS-DILITHIUM, FALCON ja Rainbow digitaalisten allekirjoitusten kategoriasta. Lisäksi kolmannella kierroksella oli joukko vaihtoehtoisia algoritmeja siltä varalta, että finalisteista löytyisi heikkouksia. Rainbown kohdalla näin kävikin. Heinäkuun alussa (2022) NIST julkaisi tiedotteen, jonka mukaan osa algoritmeista jatkaa vielä neljännelle kierrokselle jatkokehitykseen, ja CRYSTALS-KYBER sekä CRYSTALS-DILITHIUM, FALCON ja SPHINCS+ tullaan standardoimaan. SPHINCS+ oli yksi kolmannen kierroksen vaihtoehtoalgoritmeista, joka korvaa rikkoutuneen Rainbown. Valitettavasti myös SPHINCS+:sta löytyi pian standardointiuutisen jälkeen vakava heikkous. Myös neljännelle kierrokselle päässyt SIKE murrettiin kesällä. Alla olevassa taulukossa esitellään algoritmit, jotka on jo valittu standardoitavaksi tai jatkavat neljännelle kilpailukierrokselle. NIST tavoitteli valinnoilla suurempaa matemaattisen perustan vaihtelua, sillä kolmannella kierroksella hilapohjaiset ratkaisut olivat selkeässä enemmistössä; kaikkia munia ei haluttu laittaa samaan koriin. Neljänneltä kierrokselta valitaan ainakin yksi algoritmi lisää standardoitavaksi.

[2] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf
[3] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

Algoritmi	turvatasot	matemaattinen perusta	soveltuminen	valittu / 4. kierros
julkisen avaimen salaus / avaimenkapsulointi				
BIKE	1, 3, 5	QC-MDPC -koodi	Avaimet ja salatekstit ovat kooltaan vain hieman suurempia kuin hilapohjaisilla kilpailijoilla. Algoritmin tarvitsema kaistanleveys on pienehkö, joten kokonaistehokkuus on hyvä. Päivitetyssä versiossa on tavoiteltu parempia turvallisuustasoja.	4. kierros
Classic McEliece	1, 3, 5	binäärinen Goppa koodi	Pohjalla olevaa kryptosysteemiä on tutkittu 70-luvulta lähtien. Suuri julkinen avain vaikeuttaa sovittamista olemassa oleviin systeemeihin, toisaalta pieni salateksti voi olla etu tietyissä sovelluksissa.	4. kierros
CRYSTALS-KYBER	1, 3, 5	rakenteinen hila	Hyvä suorituskyky moniin erilaisiin sovelluksiin. Sama perusta kuin DILITHIUM-allekirjoitusalgoritmilla	valittu
HQC	1, 3, 5	QC-MDPC -koodi	Avaimet ja salatekstit ovat kohtuullisen kokoisia, joskin hilaratkaisut ovat selvästi pienempiä. Myös yleinen suorituskyky on kohtuullisella tasolla. Algoritmia on päivitetty välttämään aiemmin ongelmana olleita sivukanavahyökkäyksiä.	4. kierros
SIKE	1, 2, 3, 5	isogeeni	Kommunikaatio osapuolten välillä on tehokasta, mutta kumpikin osapuoli joutuu tekemään raskaita operaatiota tahollaan. Erityisesti pienitehoisilla laitteilla tämä voi olla ongelma. Algoritmi voi olla soveltuva hybridijärjestelmiin elliptisten käyrien rinnalle.	4. kierros (murrettu)
Digitaaliset allekirjoitukset				
CRYSTALS-DILITHIUM	2, 3, 5	rakenteinen hila	Suorituskyvyltään tasapainoinen, yksinkertaisempi toteuttaa kuin FALCON.	valittu
FALCON	1, 5	rakenteinen hila	Monimutkaisempi toteuttaa kuin DILITHIUM. Käyttää liukulukuja, joten laitteessa, jossa FALCON:ia käytetään, olisi hyvä olla niille kiihdytin. Pienehkö avaimen ja allekirjoituksen koko, sekä tehokas allekirjoitus ja varmennus ovat algoritmin vahvuuksia.	valittu
SPHINCS+	1, 3, 5	tilaton tiiviste	Algoritmi on monimutkainen toteuttaa ja allekirjoitukset ovat merkittävästi pidempiä kuin kilpailijoilla. Algoritmilla on useita erilaisia parametriyhdistelmiä, jotka vaikuttavat turvallisuuteen, suoritusnopeuteen ja allekirjoituksen kokoon.	valittu (murrettu)

Projektin tutkimustyön tuloksia

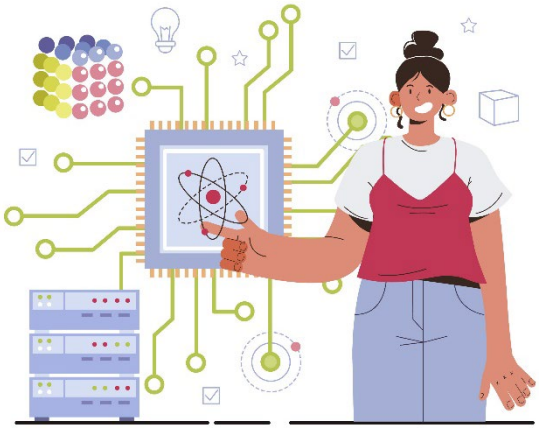
Tässä projektissa tavoitteena on ollut kehittää suomalaista kryptografian osaamista, verkostoitumista ja varautumista tulevalle kvanttitietokoneiden ajalle. Olemme kehittäneet myös rajapintoja uusille kvanttiturvallisille algoritmeille ja tutkineet mahdollisuuksia niiden optimointiin. Lisäksi projekti voitti Turvallisuus & Riskienhallinta -lehden ”Finnish Security Awards” tulevaisuuspalkinnon vuonna 2020.

Projektin ohjausryhmä päätti sivuuttaa kvanttiavainten vaihto –teknologian (Quantum Key Distribution, QKD) tutkimisen koska se ei ole salausalgoritmi eikä yksinään ole riittävä suoja Shor ja Grover -kvanttialgoritmejä vastaan. QKD vaatii kvanttikanavan salausavaimen siirtoon ja uutta teknologiaa sen toteuttamiseen, jolloin laajan mittakaavan kvanttisuojan rakentaminen on epäkäytännöllistä ja kustannuksiltaan huomattavaa verrattuna algoritmien implementoimisiin.

Tässä kappaleessa esitellään lyhyesti tutkimuksen tuloksia kvanttilaskentaan, PQC-algoritmeihin sekä niiden toteuttamiseen ja käyttämiseen liittyen. Lisätietoa niistä löytyy projektin nettisivuille kootuista seminaariesityksistä. Tutkimuksesta vedettävät johtopäätökset ja suositukset puolestaan löytyvät viimeisestä kappaleesta.

Yksi projektissa toteutetuista lopputöistä selvitti haastattelujen avulla kvanttikoneiden vaikutusta kryptografiaan. Haastattelujen perusteella lopputyössä arvioitiin muun muassa, että 2048-bittinen RSA-avain (arkisessa peruskäytössä tällä hetkellä) paljastuisi Shorin algoritmin ja noin 4000 loogisen kubitin avulla. Fyysisiä kubitteja tarvitaan kuitenkin paljon enemmän virheenkorjauksen vuoksi, joten yleiskäyttöinen kvanttikone, joka pystyy murtamaan 2048-bittisen RSA:n olisi luultavasti todellisuutta noin 10-20 vuoden päästä. Haastattelujen perusteella arvioitiin myös, että kvanttikoneiden kehitystyön motivaationa ei ole kryptografian murtaminen: kvanttikoneista odotetaan olevan suurta hyötyä esimerkiksi kvanttikemiaan, lääketutkimukseen sekä tekoälyn ja koneoppimisen kehittämiseen. Yleiskäyttöisen kvanttikoneen kehitystä ei näin ollen olisi tarvetta piilotella, ja tällaisen koneen kehittäjinä toimivat luultavasti yliopistot ja yritykset suurissa julkisissa projekteissa. On tietenkin mahdollista, että myös salaisia kehitysprojekteja on olemassa.

Kvanttilaskentatutkimusta



Suurten kokonaislukujen tekijöihin jako on yksi niistä kryptografiassa käytetyistä matemaattisista ongelmista, joka on liian vaikea klassiselle tietokoneelle, mutta mahdollinen kvanttikoneelle. Tässä projektissa tutkittiin kvanttikoneiden tarvitsemia resursseja ja suorituskykyä tekijöidenjako-ongelman ratkaisemisessa VQ-algoritmeja käyttäen (variational quantum algorithms). Näissä algoritmeissa osa tarvittavista parametreista optimoidaan etukäteen klassisella tietokoneella. Esimerkiksi saatavilla olevien kubittien määrä on merkittävä pullonkaula, joka on otettava huomioon sopivaa kvanttikoneella toimivaa algoritmia etsittäessä.

Tarkastelimme myös ennusteita kvanttilaskennan kehityksen aikajanasta: Shorin tekijöihinjakoalgoritmin tai diskreetin logaritmin ajaminen tarvittavine virheenkorjauksineen kryptografisesti merkittävän kokoisille luvuille (esim. 2048-bittinen RSA) vaatii nykyarvioiden mukaan useita miljoonia kubitteja. Tästä syystä näiden algoritmien kohdistama uhka nykyisille kryptografisille menetelmille ei hyvin todennäköisesti tule realisoitumaan ainakaan seuraavaan 10-20 vuoteen[4]. Kirjallisuudessa on hiljattain myös ehdotettu sovellettavan heuristisia kvanttioptimointialgoritmeja tekijöihin jaolle Shorin algoritmin sijaan. Nämä sietävät paremmin virheitä, ja vaativat vähemmän kubitteja, mutta niiden suorituskykyä on vaikeampi arvioida, joten nämä vaativat vielä lisätutkimusta.

Olemme myös kartoittaneet muita kryptografisiin ongelmiin (esim. hilaongelmat) liittyviä kvanttialgoritmeja. Näitä on löytynyt kirjallisuudesta niukasti, ja tiedossa olevat algoritmit eivät tarjoa eksponentiaalista nopeusetua klassisiin algoritmeihin nähden, joten nämä eivät näillä näkymin kohdista uhkaa kryptografialle. Toisaalta kvanttilaskennan nopeusedun syitä ja vaatimuksia ei vielä täysin tunneta, joten tällä hetkellä emme voi täysin poissulkea sitä mahdollisuutta, että tulevaisuudessa löytyisi vielä tehokkaampia algoritmeja joihinkin kryptografisesti merkittäviin ongelmiin.

Kvanttiturvalliset kryptografiset algoritmit

Kryptografisten järjestelmien keskinäinen vertailu voi olla hyvin monimutkaista. Tässä projektissa käytettiin kryptografisten metriikoiden taksonomiaa NISTin kilpailussa finaaliin päässeiden hilapohjaisten allekirjoitusalgoritmien (FALCON ja DILITHIUM) vertailuun. Vertailua vaikeutti se, että algoritmeja ja niiden parametreja on muutettu kilpailun edetessä, kun taas mittaristo on alun perin suunniteltu vertailemaan kypsempiä järjestelmiä. Tämän työkalun avulla pystyimme löytämään algoritmien välisiä eroja, esimerkiksi DILITHIUM on yleiskäyttöisempi, mutta FALCONia voi suosia, jos suorituskykyä on mahdollista optimoida tietyillä tavoilla. Samalla löysimme myös mittarin kehitysmahdollisuuksia. Jatkossa mittaristoa käytetään myös muiden finalistialgoritmien tarkasteluun.

Kahden kilpailualgoritmin, CRYSTALS-KYBERin ja FALCONin, teoreettiseen taustaan syvennyttiin kahdessa eri lopputyössä. KYBERin turvallisuus perustuu ns. häirityn oppimisen ongelmaan: hyökkääjän tulisi arvata salaisuus tuloksista, jotka ovat mahdollisesti väärin. KYBER koostuu kahdesta osasta, jotka molemmat sisältävät kolme algoritmia, avainten generoinnin, viestin salauksen sekä viestin avaamisen. Lopputyössä

[4] IBM:n tiekartasta voi tarkastella teollisuuden näkemystä kehitysnopeudesta https://www.ibm.com/quantum/roadmap

tarkasteltiin näitä algoritmeja ja todistettiin niiden oikeellisuus. Toisessa lopputyössä puolestaan käsiteltiin allekirjoitusalgoritmi FALCONin matemaattista perustaa. Varsinaisen tutkimusosuuden tavoite oli esittää matemaattiset todistukset FALCONin avainten generointiprosessissa toimiville algoritmeille. Tuloksena avainten generointiprosessin algoritmit on todistettu matemaattisesti oikeellisiksi ja päättyviksi.

Käytännön näkökulmasta on tärkeää tutkia myös algoritmien sovellettavuutta yhteiskunnan tietorakenteisiin. 5G verkoissa tietoturva perustuu pitkälti symmetrisen avaimen kryptografiaan, kuten AES tai SNOW 5G, mutta julkisen avaimen metodeja tarvitaan silti autentikointiprosesseihin. Nykyinen autentikointi ja avaintensopimisprotokolla (5G AKA) perustuu elliptisiin käyriin, joiden korvaamista kvanttiturvallisilla protokollilla tutkimme tässä projektissa. Työn tuloksena ehdotamme laajennettua protokollaa 5G AKA⊕, joka on standardiin yhteensopiva, kvanttiturvallinen ja lisäksi ratkaisee alkuperäisessä protokollassa olevia istuntoavaimiin ja linkitettävyys hyökkäykseen liittyviä ongelmia.

Lisäksi Kyberturvallisuuskeskuksen CAA-viranomainen perehtyi NIST PQC-valintaprosessin finalistialgoritmeihin tavoitteenaan tuoda sopivia algoritmeja myös kansalliseen kryptokriteeristöön salaustuotteiden tarkastustoimintaa varten. Valintaprosessi on vielä kesken eikä lopullisia kansallisia valintoja sen perusteella varmaankaan saada tämän projektin aikana tehtyä, mutta suuntaviivat alkavat selkiytyä. Hilamenetelmät edustavat enemmistöä ja luottamus niihin on korkealla tasolla. Toistaiseksi näyttää myös siltä, että ns. rakenteellisia hiloja käyttävät menetelmät, jotka ovat tehokkaampia, eivät jää jälkeen turvallisuuden osalta perinteisiä rakenteettomia hiloja käyttävistä algoritmeista. Usean muuttujan yhtälöryhmiin perustuvat allekirjoitusmenetelmät ovat viimeaikaisten tulosten perusteella menettäneet luotettavuuttaan eikä niitä todennäköisesti tulla valitsemaan. Koodausteoreettisten menetelmien osalta Classic McEliece-algoritmi nauttii suurinta luottamusta pitkän ja stabiilin historiansa takia, mutta sen käyttökohteet ovat rajoitettuja suurten avainpituuksien ja suorituskykyhaasteiden takia. Sikäli kun paine kansallisia kriteerejä kohtaan kasvaa teollisuuden puolelta, voidaan myös mahdollisesti hyväksyä suurinta luottamusta tällä hetkellä nauttivia algoritmeja määräaikaisesti kansalliseen käyttöön.

Algoritmien käytännöllisyys

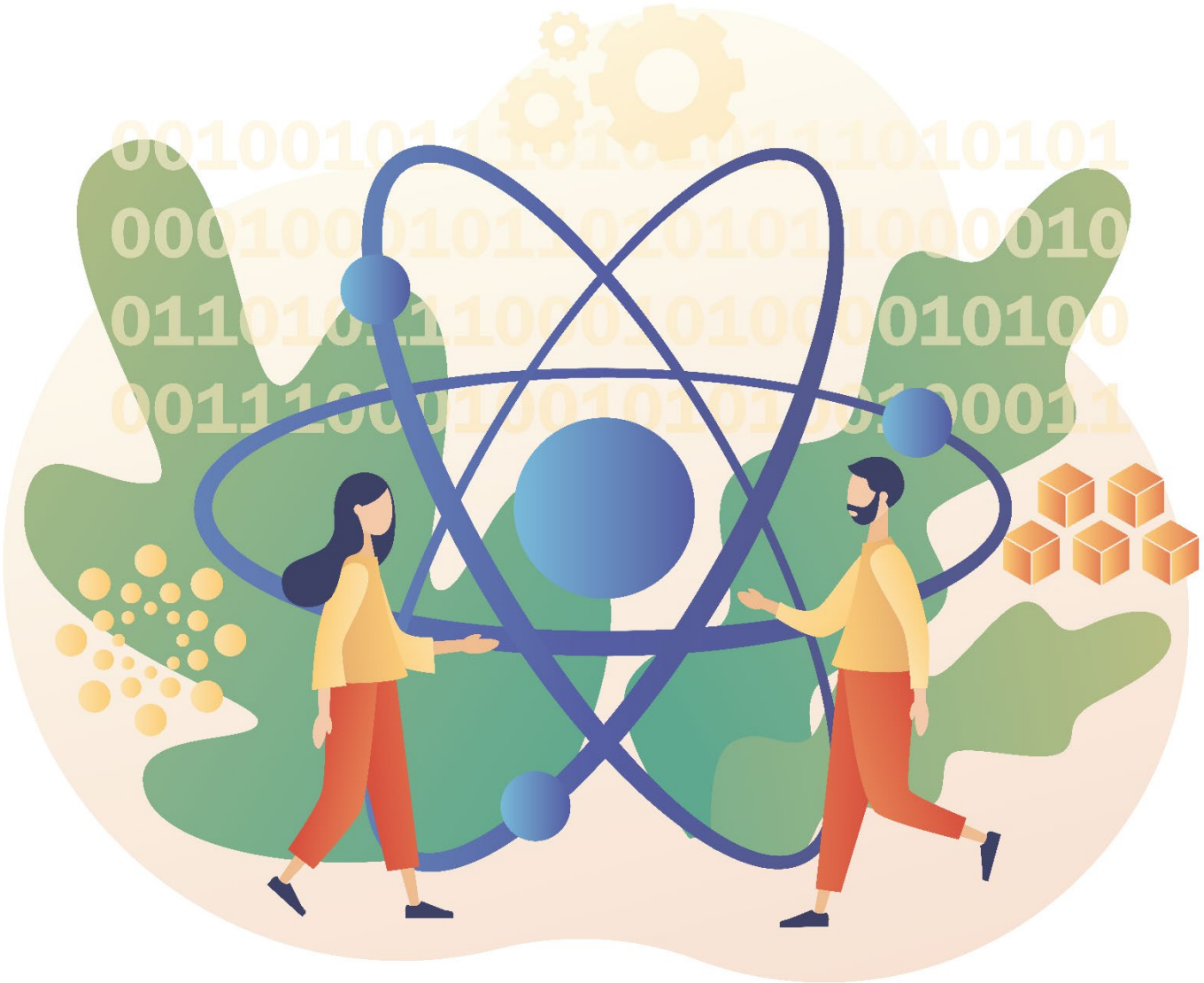
Ohjelmistokehityksessä on tavanomaista käyttää olemassa olevia kirjastoja monimutkaisempien tuotteiden rakentamiseen. Koska PQC algoritmit ovat vielä niin nuoria, niitä ei ole vielä laajasti saatavilla avoimen lähdekoodin kirjastoissa, joten yksi tämän projektin diplomitöistä keskittyi kvanttiturvallisten algoritmien (CRYSTALS-KYBER, SABER ja CRYSTALS-DILITHIUM) toteuttamiseen kryptografiseen ohjelmistokirjastoon (Crypto++:n erillinen haara). Tavoitteena oli saada käytettävyydeltään, suorituskyvyltään ja luotettavuudeltaan hyvä toteutus, joka olisi yhdenmukainen muun kirjaston kanssa ilman ylimääräisiä koodirivejä. Diplomityön puitteissa algoritmien suorituskyky saatiinkin tyydyttävälle tasolle ja alustava testaaminen ei vielä paljastanut esimerkiksi muistivuotoja. Käytettävyyttä voisi vielä parantaa esimerkiksi paremmalla poikkeusten käsittelyllä ja koodin rakenteen siistimisellä. Työn johtopäätöksenä voidaan sanoa, että koska algoritmien toteutus on haastavaa, niin jos jokin algoritmi on yksinkertaisempi kuin muut, esimerkiksi SABERin rakenne on yksinkertaisempi kuin KYBERin, sillä on suuri käytännön merkitys algoritmien kooditoteutuksille.

Tutkimme myös algoritmien soveltuvuutta erikoisempiin käyttökohteisiin: Älykkäässä liikenteessä autot lähettävät toisilleen tai tien varrella oleville asemille digitaalisesti allekirjoitettuja varoitusviestejä. Projektissa tehdyssä diplomityössä toteutettiin ohjelma, jossa ETSIn (European Telecommunications Standards Institute) dokumenteissa määritelty älykkään liikenteen varoitusviesti allekirjoitettiin joko CRYSTALS-DILITHIUMilla, FALCONilla, Rainbow'lla tai nykyisen standardin hyväksymillä elliptisillä käyrillä. Seuraavaksi vertailtiin eri algoritmeilla allekirjoitukseen ja varmennukseen kulunutta aikaa sekä allekirjoitetun viestin kokoa, ja vertailtiin kvanttiturvallisia vaihtoehtoja elliptisiin käyriin. Tulosten perusteella voidaan sanoa, että

jompikumpi hilapohjaisista vaihtoehdoista, CRYSTALS-DILITHIUM tai FALCON, voisi olla potentiaalinen vaihtoehto älykkään liikenteen käyttöön.

Useat projektipartnerit ovat tehneet toteutuksia PQC-algoritmeista omiin tuotteisiinsa. Kehitys myös jatkuu uusille tuotteille ja ominaisuuksille. Hybridiratkaisut, joissa uusia PQC-algoritmeja käytetään rinnakkain klassisten algoritmien kanssa, ovat olleet tyypillinen toteutusvalinta. Projektipartnerit tutkivat esimerkiksi CRYSTALS-KYBER ja -DILITHIUM algoritmien soveltuvuutta ja käyttöä IPSec/IKEv2 protokollan yhteydessä. Käytetyt avaintenvaihto- ja todennusalgoritmit sekä X509-varmenteet toteutettiin hybridimenetelmällä yhdistämällä PQC algoritmit klassiseen elliptisen käyrän systeemiin. Todellisen suorituskyvyn mittaamisen ja analysoinnin mahdollistamiseksi algoritmit myös toteutettiin VPN-tuotteeseen.

VPN:ää voi käyttää liikkeessä olevan datan suojaamiseen. Yksi projektin lopputöistä tutki, miten hyvin PQC-algoritmeilla (CRYSTALS-KYBER, SABER ja NTRUEncrypt osana hybriditoteutusta) toteutettu VPN pystyy suojaamaan datan sisällön passiiviselta tarkkailijalta. Työssä etsittiin verkkoliikenteestä ns. sormenjälkiä vierailluista sivustoista (Google vs. Facebook). Lopputuloksena oli, että vaikka PQC-algoritmeilla toteutettu VPN pystyy takaamaan viestinnän luottamuksellisuuden, verkkoliikenteessä on kuitenkin muotoja tai rakenteita, joita ei pysty peittämään ilman eri toiminnallisuutta.



Johtopäätökset ja suositukset

Tämän projektin aikana tutkimus keskittyi NIST:in kilpailun kolmannen kierroksen finalisteihin. Projektin ollessa päättymässä NIST julkaisi raportin, jonka mukaan neljä algoritmia siirtyy standardoitavaksi ja neljä muuta uudelle kilpailukierrokselle jatkokehitystä varten. Tässä vaiheessa hilapohjaiset ratkaisut ovat siis tulossa käyttöön, ja niiden rinnalle etsitään vähintään yhtä johonkin muuhun matemaattiseen ongelmaan perustuvaa algoritmia.

Suomi on tällä hetkellä eturintamassa niin kvanttiturvallisen kryprografian kuin myös varsinaisten kvanttiteknologioiden suhteen. Varsinaisen kvanttiteknologisen tutkimus- ja kehitystyön lisäksi Suomessa aletaan lähitulevaisuudessa tutkia myös kvanttipohjaisia kryptografisia avaimenvaihtoratkaisuja, jotka saattaisivat toimia vaihtoehtona PQC algoritmeille. Tämän projektin sisällä virisi uteliaisuus myös kvanttikryptografiasta mahdollisena uutena tutkimuskohteena.

Suomen liittyminen Pohjois-Atlantin puolustusliittoon, NATOon, avaa yleisestikin kotimaiselle salaustuoteteollisuudelle paljon isommat markkinat puhtaasti EU:n hyväksynnän alla olevien viranomaistuotteiden markkinoihin verrattuna. Toisaalta voidaan ajatella, että mahdollisissa NATO-hyväksytyissä korkean turvallisuuden tuotteissa Suomi lähtee liikkeelle takamatkalta, mutta kokonaan uusien teknologioiden kohdalla kaikki maat ovat liittoumista riippumatta samalla viivalla. Tämä tarkoittaa sitä, että hyvin toteutetut PQC-tuotteet voivat tarjota kotimaisille toimijoille kilpailuetua myös NATO-markkinoilla.

Niin NATOn kuin EU:nkin yhteydessä salaustuotteiden toteutusturvallisuus näyttelee isoa osaa hyväksynnän saamisessa. Tämän vuoksi algoritmien turvallista toteuttamista niin PQC-algoritmien kuin muidenkin perusteiden osalla tulee tutkia ja kehittää yhtäläisillä, todennäköisesti lisääntyvillä, panostuksilla jatkossakin.

Viranomaistuotteiden kehittäminen on hyvin suljettu ja suojeltukin markkina, ja siinä menestyminen vaatii tiivistä yhteistyötä kansallisten turvallisuusviranomaisten kanssa ja näiden ohjauksessa, koska iso osa informaatiosta ja luvituksesta kulkee pelkästään viranomaiselta toiselle.

Suomen kaiken kaikkiaan hyvän aseman säilyttämiseksi on tärkeää panostaa kvanttiturvallisen kryptografian osaamiseen. Suomi tarvitsee hyvin koulutettua väkeä sekä tutkimukseen ja tuotekehitykseen että uusien teknologioiden toteuttamiseen. Kolikon toinen puoli on myös huomioitava; tarvitsemme koulutusta kvanttikoneiden ohjelmointiin, optimointiin ja muuhun hyödyntämiseen. Tämän projektin puitteissa Aalto-yliopisto järjesti kahdesti yleissivistävän kvanttilaskennan erilliskurssin teollisuuspartnereille. Kurssi sai hyvää palautetta, ja kenties sille voisi olla kysyntää tulevaisuudessakin.

Meidän täytyy myös lisätä yleistä tietoisuutta kvanttikoneiden heittämästä varjosta digitaalisen yhteiskunnan ylle. Vaikka kvanttikoneita kehitetään nimenomaan hyödyllisiin tarkoituksiin, kuten lääketutkimuksen apuvälineeksi, niin yleiskäyttöistä kvanttikonetta voi käyttää myös rikollisiin ja vihamielisiin tarkoituksiin. Vanhojen kvanttikonehyökkäyksille alttiiden systeemien päivittäminen uusille algoritmeille ja protokollille tulee olemaan valtava insinöörityö, joka vie paljon aikaa. Siksi organisaatioiden — sekä julkisten että yksityisten — olisi hyvä alkaa selvittää omaa PQC-valmiuttaan, huolehtia järjestelmiensä ketteryydestä ja avainhenkilöiden koulutuksesta. Kansallisella tasolla olisi hyvä kehittää mittaristo seuraamaan organisaatioiden siirtymää kvanttiturvallisiin tietojärjestelmiin.

Joidenkin organisaatioiden velvollisuutena on suojella dataa kymmeniä vuosia. Tällä aikaskaalalla kvanttikoneet ovat jo nyt todellinen ongelma. Siksi näille organisaatioille voi olla tarpeellista käyttää hybridiratkaisuja ennen kuin standardiin lopulta valittavat PQC-algoritmit ovat riittävän käytettäviä ja kypsiä. Tässäkin projektissa tutkittiin hybridiratkaisujen toteuttamista, ja osa kilpailussa mukana olevista algoritmeista oletettavasti soveltuu tarkoitukseen paremmin kuin muut.

Kirjoittajat

Pääkirjoittaja:
Outi-Marja Latvala
outi-marja.latvala@vtt.fi

Projektipäällikkö:
Visa Vallivaara
visa.vallivaara@vtt.fi

Ohjausryhmän puheenjohtaja:
Jorma Mellin
jorma.mellin@ssh.fi

Projektin nettisivut: www.pqc.fi

ISBN: 978-951-38-8833-6

DOI: 10.32040/2022.978-951-38-8833-6