Puolustusvoimien tutkimuslaitos
Tutkimuskatsaus 01 – 2017

16.01.2017

Kvanttilaskenta ja kyberturvallisuus

Mika Helsingius
Informaatiotekniikkaosasto

Kvanttilaskenta kehittyy tällä hetkellä nopeasti. Kvanttitietokoneet, kvanttiverkot ja kvanttiturvalliset salausmenetelmät ovat laajan tutkimuksen kohteena eri puolilla maailmaa. Kehittyvä kvanttiteknologia voi aiheuttaa uusia uhkia kyberturvallisuudelle, mutta toisaalta se voi parantaa tiedonvälityksen turvallisuutta. Tässä artikkelissa esitellään kansainvälisten asiantuntijoiden näkemyksiä kvanttiteknologian tilasta ja kehitysnäkemyksistä.

Kvanttilaskennan ja kyberturvallisuuden suhde

Sveitsiläinen ID Quantique järjesti vuonna 2016 sarjassaan kahdeksannen tutkijoille, jatko-opiskelijoille ja liike-elämän edustajille tarkoitetun ”8th Winter School on Quantum Cyber Security” talvikoulun. Kurssin luennoitsijoina oli tutkijoita alan yrityksistä, tutkimuslaitoksista ja yliopistoista. Heistä moni on tehnyt merkittävää kvanttilaskennan ja kvanttimekaniikan perustutkimusta. Itse tapahtuman järjestäjän IDQ:n juuret ovat Geneven yliopistossa, sen sovelletun fysiikan laitoksella (Group of Applied Physics, GAP).

Quantum Cyber Security voidaan kääntää kvanttikyberturvallisuudeksi, kyse on kvanttimekaniikan ilmiöiden vaikutuksista kyberturvallisuuteen. Tämän termin alle on sisällytetty useita erilaisia teknologioita sekä teoreettisista lähestymistapoja. Yksi usein käytetty kolmijako on: kvanttiturvalliset verkot, kvanttilaskennan käyttö salausten murtamiseen ja kvanttiturvalliset salausalgoritmit. Monien ilmiöiden rajat ovat häilyviä eikä termistö ole vakiintunutta, esimerkiksi termejä ”quantum safe” (kvanttiturvallinen) ja ”post quantum” (kvanttien jälkeinen) ei ole määritelty yksiselitteisesti ja eri tahot ymmärtävät ne hieman eri tavoilla.

IDQ keskittyy omassa toiminnassaan kvanttiturvallisiin tietoliikenneverkkoihin. Turvallisuus perustuu fotonien kvanttiominaisuuksiin. Niiden avulla voidaan rakentaa kahden päätepisteen välinen tiedonsiirtolinkki, jonka salakuuntelu on teoriassa mahdotonta. Tiedonsiirron osapuolet havaitsevat, jos jokin ulkopuolinen taho yrittää seurata viestiliikennettä; samalla viestin sisältö muuttuu lukukelvottomaksi. Tämä on ehkä kehittynein kvanttiturvallisuuden sovellutus ja markkinoilla on jo kaupallisia tuotteita.

Kvanttilaskennan käyttö perinteisten salausjärjestelmien murtamiseen on myös kerännyt julkisuutta ja aiheuttanut huolia. Kyse on siitä, että monet nykyisistä salausmenetelmistä voitaneen murtaa siinä vaiheessa kun toimiva ja riittävän suuren bittimäärän omaava kvanttitietokone on saatu kehitettyä. Tämä uhka koskettaa mm. RSA-salausta, DSA-allekirjoitusta ja Diffien-Hellman avaintenvaihtoa. Tällaista kvanttikonetta ei vielä ole olemassa, mutta sellainen saattaa olla jo nurkan takana.

Kvanttiturvallisia salausalgoritmeja pyritään luomaan kvanttilaskennan uhkaa vastaan. Niiden tulisi olla sellaisia, etteivät tulevat kvanttitietokoneet pysty murtamaan niitä sen nopeammin kuin tavallisetkaan tietokoneet. Niitä voitaisiin käyttää korvaamaan nykyiset algoritmit eri laitteissa ja protokollissa. Merkittävä niihin liittyvä ongelma on se, ettei mitään algoritmia osata tällä hetkellä todistaa teoreettisesti kvanttiturvalliseksi.

Kvanttitietokone

Kvanttitietokoneista ja muista kvanttilaskennan sovellutuksista on keskusteltu yleisemmin ainakin 90-luvun alusta lähtien. Erilaisia teorioita, algoritmeja ja kokeellisia laitteistoja on esitelty tietotekniikan ja fysiikan konferensseissa ja julkaisuissa. Varsinkin tutkimustyön alkuaikoina näkemykset vaihtelivat äärimmäisyydestä toiseen; ensin joku esitti teoreettisia perusteita joiden mukaan kvanttilaskenta olisi laajemmassa mittakaavassa käytännössä mahdotonta, pian vastapuoli esitti kiertotien jonka avulla este saatiin kumottua. Tämän jälkeen palattiin taas alkuun, kun seuraava kvanttimekaniikan ominaisuus käytiin läpi. Kiistely jatkui pitkään ja monen kriitikon mukaan kvanttitietokone oli aina 20 vuoden päässä tulevaisuudessa.

Edistystä on kuitenkin tapahtunut, viime vuosina alan perustutkimus on lisääntynyt huomattavasti. Monet teoreettiset esteet on pystytty osoittamaan vääriksi ja toimivien kvanttitietokoneiden rakentamiseksi on löydetty uusia oikoteitä. Uudet edistysaskeleet ovat liittyneet mm. virheiden korjaamiseen ja laskentatulosten tarkastelemiseen romahduttamatta herkkää kvanttitilaa. Erittäin merkittävää on se, että monet ideat on myös todennettu kokeellisesti.

Optimismi on lisääntynyt ja aikatauluja on ryhdytty korjaamaan alaspäin. Talvikoulun asiantuntijat olivat yksimielisiä siitä, että universaali kvanttitietokone on rakennettavissa. Heidän mukaansa kaikki kvanttitietokoneeseen tarvittavat osat ovat jo periaatteessa olemassa, mutta kaikki erityisvaatimukset eivät täyty vielä samaan aikaan samassa järjestelmässä. Kyse on enemmänkin insinööriteknisestä ongelmasta, mitään uusia teoreettisia läpimurtoja ei tarvita. Asiantuntijoiden mukaan olisi melko optimistista uskoa, että universaali kvanttitietokone olisi käytettävissä 5 vuoden päästä, mutta 10 vuoden aikana se on hyvinkin mahdollista ja 20 vuoden sisällä lähes varmaa.

Tutkijoiden mukaan me elämme tällä hetkellä kvanttikivikautta. Teoreettinen ymmärryksemme on hyvin vajavaista ja kvanttimekaniikka on täynnä toistaiseksi kartoittamattomia alueita. Uudet löydöt näyttävät kuitenkin ennemminkin avaavan uusia polkuja kuin kasaavan uudenlaisia esteitä. Kvanttikoneiden algoritmien kehitys on käytännössä lähtöpisteessä. Tilanne vastaa tietokoneiden kehitystasoa hetkellä, jolloin ensimmäinen transistori oli saatu kehitettyä (1947). Releisiin sekä elektroniputkiin perustuvien koneiden ohjelmointi oli käsityötä, korkeamman tason ohjelmointikielet ja käyttöjärjestelmät olivat vielä epämääräisten visioiden asteella. Tällä hetkellä ei osata kunnolla edes kuvitella, millaisia algoritmeja tulevaisuuden kvanttikoneille voidaan kehittää. Kehityssykli lähtee todella käyntiin siinä vaiheessa, kun tutkijat saavat käyttönsä ensimmäiset kvanttikoneiden prototyypit ja he pääsevät kokeilemaan erilaisia lähestymistapoja.

Monet yritykset ja yliopistot työskentelevät aktiivisesti kvanttikoneiden kehittämiseksi, nyt on jo siirrytty marginaalialueesta suuriin tutkimusohjelmiin. Mukana ovat mm. IBM, Microsoft, Google ja D-Wave. Ongelmaa lähestytään useilla eri tavoilla, puhutaan porttimallisista, yhdensuuntaisista, topologisista sekä adiabaattisista kvanttikoneista. Tähän asti kvantti-ilmiöiden tutkimukseen on käytetty ioniloukkuja, lasereita ja mikroaaltoja,

Puolustusvoimien tutkimuslaitos on Pääesikunnan alainen sotilaslaitos, joka tuottaa monialaisesti puolustusvoimien tarvitsemia vaativia tutkimus-, kehittämis-, testaus- ja evaluaatiopalveluja. Tutkimuslaitoksessa yhdistyvät strategian ja operaatiotaidon, eri teknologia-alueiden ja ihmisen toimintakyvyn tutkimus. Tutkimuskatsaukset sisältävät yleistajuisia ja ajankohtaisia näkökulmia laitoksen osaamisalueilla.

mutta tulevaisuuden kannalta lupaavimpia ovat integroidut kvanttipiirit. Kvanttipiirien kehitystyö vaatii suuria voimavaroja, siksi yritysten mukaantulo on kehityksen kannalta välttämätöntä. Toiveena on että jossain vaiheessa kvanttipiireistä tulee samaan tapaan skaalattavia kuin nykyisistä digitaalipiireistä, tällöin Mooren laki voisi toistaa itseään kvanttimekaniikassa.

Microsoft uskoo kehityksen kulkevan hybridikoneiden kautta, niissä kvanttikoneen osia on yhdistetty perinteiseen tietokoneeseen. Käytännössä kaikki lähitulevaisuuden koneet tulevat olemaan jonkinlaisia hybrideitä, koska ongelmien kuvaaminen ja siirto kvanttikoneille sekä vastausten suodattaminen vaatii tavallisilla koneilla tehtäviä toimintoja.

Kirjavista lähestymistavoista huolimatta erilaiset kvanttikonetyypit on osoitettu teoreettisesti yhteensopiviksi. Jos algoritmi toimii yhdessä konetyypissä, se voidaan ainakin periaatteessa konvertoida toiselle konetyypille. Eri tekniikoilla on omat etunsa ja haittansa. Vaatimattomatkin muutaman kvantti- eli kubitin (engl. qubit) kokoiset ioniloukkoihin perustuvat laitteet voivat olla merkittäviä mm. synteettisessä kemiassa tai jossain muussa erityiskohteessa. Tutkijoiden mukaan on perusteltua, että eri tutkimusryhmät etenevät omaan tahtiinsa kokeillen omia ratkaisujaan. Kvanttilaskenta on toistaiseksi hyvin kokeellista tekniikkaa eikä yhtä oikeaa lähestymistapaa ole vielä olemassa. Emme edes tiedä, minne kehitys tulee tarkkaan ottaen johtamaan. Summittainen suunta on selvillä, mutta jokaisen kukkulan takaa paljastuu aina uusia päämääriä.

Kvanttikoneiden ohjelmoinnista ja algoritmeista ei voida sanoa vielä paljoakaan. Aluksi ratkaisut heijastelevat nykyisten tietokoneiden algoritmeja ja ohjelmointia, mutta todennäköisesti ennen pitkää siirrytään vielä täysin kartoittamattomille vesille. Kvanttialgoritmien ongelmana on se, ettei niille ole mitään selkeää vertailukohtaa normaalimaailmassa. Asiantuntijat uskovat, että siirtymä voi helposti viedä vuosikymmeniä, ovathan nykyisenkin tietotekniikan juuret 1950-luvulla.

Ihmisen kyky ymmärtää ja hahmottaa kvantti-ilmiöitä saattaa olla yksi pullonkaula, joka haittaa nykyisiä tutkijapolvia. Monet ilmiöt ovat arkitodellisuuden vastaisia, se häiritsee jatkuvasti jopa kokeneiden tutkijoiden ajatusprosessia. Vapaiden keskustelujen aikana monet heistä pohdiskelivat, joudummeko odottamaan uusien kvanttinatiivien sukupolvea? Jos kvanttilaskenta on heille tuttua jo lapsuudesta lähtien, niin ehkä he pystyisivät paremmin hahmottamaan kvanttimaailman ilmiöitä. Tällä hetkellä kukaan ei tiedä, vaatiiko tämä sukupolvien välisen kuilun ylittämistä tai laajempaa evolutionääristä harppausta. Mielenkiintoinen filosofinen kysymys liittyy myös tekoälyjen kehitykseen, voisivatko tulevaisuuden älykkäät järjestelmät vapauttaa itsensä helpommin inhimillisten ajattelutapojen kahleista ja hyödyntää kvanttilaskentaa aivan uusilla tavoilla.

Vaikka osa kysymyksistä on hyvin filosofisia, ne ovat kuitenkin relevantteja. Kvanttilaskenta on outoa ja tämän hetken parhaimmatkin tutkijat sanovat suoraan, etteivät he pysty kunnolla hahmottamaan kaikkia havaitsemiaan ilmiöitä. Tämän vuoksi he kehottavat myös varautumaan yllätyksiin, on todella vaikeaa tunnistaa mihin kaikkeen kehittyvä kvanttilaskenta tulee johtamaan. Mm. keskustelu kvanttiturvallisista algoritmeista ja kvanttilaskennan kehityksestä perustuu lähinnä arvauksiin, pitkällä tähtäimellä mitään kunnollista faktapohjaista tietoa tulevaisuuden järjestelmien mahdollisuuksista tai rajoitteista ei ole olemassa.

Hollannin hallituksen vuonna 2015 tekemän kartoituksen mukaan kvanttilaskentaan panostettiin eri puolilla maailmaa taulukon 1 mukaisesti. Tilastoista puuttuu mm. Venäjä, mutta useita lahjakkaita venäläistutkijoita on mukana muiden maiden tutkimusryhmissä. Venäjällä on paljon alan teoreettista osaamista, joten haluttessaan siitä voi tulla nopeasti merkittävä peluri tälle tutkimuskentälle. Myöskään Intian panostuksista ei ole tietoa. Luvut eivät kerro salassa tehtävästä tutkimuksesta, mutta esim. Wikileaks-vuotojen mukaan Yhdysvallat näkee itsensä melko tasavertaiseksi aiemmassa listassa mainittujen valtioiden kanssa. Koska asiantuntijoita on suhteellisen vähän ja tämän kehittyvän tutkimusalan edistyminen vaatii tutkimusryhmien välistä kanssakäymistä, on jossain määrin epätodennäköistä että jokin eristäytynyt ryhmä pystyisi tekemään merkittäviä tuloksia yksinään. Tuloksiin ei päästä myöskään ilman kunnollista panostusta. Talvikoulun osallistujissa merkillepantavaa oli Etelä-Korean ja Kiinan edustajien suuri määrä, nämä maat eivät aio jäädä jälkeen kehityksessä ja saattaa olla että ne tulevat olemaan kehityksen eturintamassa.

Maa tai alue	Henkeä
EU	2500
Kiina	2000
Yhdysvallat	1200
Kanada	350
Japani	300
Australia	250
Sveitsi	200
Singapore	130
Brasilia	100
Etelä-Korea	80

Taulukko 1. Kvanttilaskennan parissa työskentelevät tutkijat eri maissa.

Miten kvanttitietokone määritellään?

Professori Michele Moscan mukaan kvanttiteknologian kehitys on tällä hetkellä eksponentiaalista, vaikka useimmat tietoturvaihmiset ovat olettaneet kehityksen olevan paljon tasaisempaa. Tämä saattaa aiheuttaa jatkossa yllätyksiä, koska muutoksiin ei osata varautua ajoissa. Teoreettisella puolella on tapahtunut paljon edistystä ja usein fysikaalisia rajoitteita voidaan merkittävästi kiertää algoritmisilla menetelmillä. Keskustelua häiritsee myös se, ettei kvanttitietokoneen määritelmä ole mitenkään yksikäsitteinen.

Kanadalainen D-Wave väitti joitain vuosia sitten kehittäneensä toimivan adiabaattiseen laskentaan perustuvan kvanttitietokoneen. Tämä on synnyttänyt kiivasta keskustelua, jossa käydään suurinta kiistaa siitä onko kyseinen laite kvanttitietokone vai ei? Moscan mukaan tässä kohtaa keskustelussa on menty sivuraiteille. Hänen mukaansa eräs tapa jaotella tietokoneita on käyttää 5-portaista mallia.

Klassinen tietokone on tasolla 1, kaikki perustuu perinteiseen tietotekniikkaan.

Tason 2 koneessa tapahtuu joitain kvanttimekaanisia ilmiöitä (esim. transistorin sisällä), mutta sillä ei ole merkitystä loogisen tason toiminnoille.

Tason 3 koneessa joitain kvantti-ilmiöitä hyödynnetään koneen joissain osissa, ne vaikuttavat ainakin hieman laskennan tuloksiin.

Tason 4 kone hyödyntää kvantti-ilmiöitä laajasti ja skaalautuvasti osana laskentaa, kyse ei ole vain yhtä käyttötarkoitusta varten tehdystä laitteesta.

Tason 5 kone on täysi kvanttitietokone jolla voidaan ajaa kaikkia teoreetiselle kvanttikoneelle suunniteltuja algoritmeja (tietysti koneen bittimäärän puitteissa).

Moscan mukaan D-Wave:n kvanttikone on jossain tasojen 2-4 välillä. Sen sisällä tapahtuu jotain kvantti-ilmiöitä ja niillä on jotain vaikutuksia lopputuloksiin. Hänen mukaansa laite on kiinnostava ja sen myötä opimme ainakin jotain uutta käytännön teknologian kehittämisestä.

D-WAVE

D-WAVE:n edustajat ovat itse todenneet, että heidän koneensa ei ole ohjelmoitava yleiskäyttöinen kvanttitietokone. Se pystyy laskemaan suoraan ns. Ising Hamiltonian ongelmia, yksinkertaistettuna se löytää matalimman kohdan energiavalleista menemällä vuorten läpi. Laskettavat ongelmat pitää muuttaa tähän muotoon ja tarvittavat kytkennät pitää ohjelmoida heidän sirulleen. Alussa ongelmien koodaus oli hankalaa käsityötä, mutta nykyisin heillä on siihen valmiita työkaluja.

Itse piiri on pienikokoinen, mutta se sijaitsee n. 3 metrin levyisen kuution sisällä. Suurin osa laitteen tilasta menee jäähdytykseen ja signaalien läpivienteihin, ympäristön häiriövaikutukset on saatava eliminoitua. 1000-qubitin Washington-piiri on jaettu 12x12 yksikön lohkoihin, jokaisessa lohkossa on 8 kubittia jotka on kvanttimekaanisesti kytketty toisiinsa tietyn topologian mukaan. Uudemmissa 2000-kubitin malleissa topologiaa on uudistettu ja kubittien välisiä vaikutuksia on lisätty. On hyvä muistaa että nämä ovat nimenomaan ns. adiabaattisia kubitteja, eivät sellaisia universaaleja kubitteja joita on saatu aikaan esim. ioniloukkuteknologialla. D-WAVE:n tekniikan etuna on teknologian kehittyminen, tähän saakka he ovat pystyneet aina kaksinkertaistamaan bittimäärän n. kahden vuoden välein eikä tämän trendin jatkumiselle ole näkyvissä esteitä.

Kriitikot ovat kysyneet, miksi D-WAVE olisi onnistunut siinä missä muut ovat epäonnistuneet. Yhtiön edustaja Colin Williams esitti tähän joitain syitä. Yhtiön palkkalistoilla on suuri joukko kvanttiteknologioiden tutkijoita, joilla on takanaan yli 100 patenttia ja 80 tieteellistä artikkelia. Itse menetelmä ei ole mitenkään vallankumouksellinen, tosin ympäristön häiriöiden eliminoiminen vaatii paljon valmistusteknisen osaamisen kehittämistä ja heiltäkin kului siihen useita vuosia. Läpimurron kannalta ensiarvoista oli miljardiluokan puolijohdetehtaan suostumus prototyyppipiirien valmistukseen. Piireissä käytettävien Josephson-liitosten valmistaminen perustuu niobiumin käyttöön ja 6-kerroksiseen CMOS-litografiaan. Tämä teknologia ja käytetyt materiaaliyhdistelmät eivät ole triviaaleja ja se sisältää valmistuslinjojen kannalta monia riskejä. Epäonnistuessaan uusi prosessi olisi voinut saastuttaa käytetyn valmistuslinjan, tällöin puhdistus ja linjan pitkä käyttökatko olisivat aiheuttaneet tuotantolaitokselle valtavia tappioita. Muut vastaavia järjestelmiä tutkineet ryhmät ovat pystyneet ainoastaan teoreettiseen työhön, mutta D-WAVE pääsi testaamaan ja kehittämään niitä myös käytännössä. Nykyisin heillä on käytössään työhön tarvittavat valmistuslinjat ja tämä muodostaa korkean esteen kilpailulle.

Pidemmän ajan sisällä D-WAVE uskoo että heidän osaamisensa auttaa myös universaalisen kvanttikoneen rakentamisessa. Tällä hetkellä se ei ole heille prioriteettilistan kärjessä, koska liiketoiminnallisesti on kannattavampaa poimia ensin matalammalla riippuvat hedelmät. He uskovat että heidän tekniikkansa on käyttökelpoinen mm. optimoinnissa, tekoälyssä ja syväoppimisessa. Heidän tutkijansa ovat tehneet monia kokeiluja mm. hahmontunnistuksessa, konenäössä ja synteettisessä kemiassa. Google tutkii heidän kanssaan uusia algoritmeja ja tiedonhakumenetelmiä massiivisia tietovarantoja silmälläpitäen.

D-WAVE:n koneella ei pystytä ajamaan suoraan jaottomiin lukuihin perustuvan salauksen murtamiseen tarkoitettua Shorin algoritmia. Yhtiön mukaan ongelma voidaan kuitenkin kuvata heidän koneelleen, he ovat kokeilleet mm. luvun 10877 jakamista tekijöihin 149 ja 73. Algoritmeja voidaan kuitenkin kehittää, lisäksi toisenlaiset topologiat muuttaisivat tarvittavien kvanttibittien määrää. Tämän hetkisellä topologialla esim. RSA768 vaatisi 113390 kubittia joka olisi saavutettavissa 6 vuoden aikana nykyisellä kehitystahdilla. Noin 100 M€:n panostuksella he voisivat kehittää laite ja algoritmiyhdistelmän, joka olisi tarkoitettu erityisesti lukujen tekijöihin jakamiseen. Tällä hetkellä he eivät kuitenkaan näe sitä liiketaloudellisesti kannattavaksi, koska markkinat sellaiselle olisivat pienet ja tällä hetkellä adiabaattiselle laskennalle on muita kaupallisesti paljon merkittävämpiä käyttökohteita.

Kvanttiturvalliset salausalgoritmit

Kvanttitietokoneiden nopea kehittyminen ja sen aiheuttama uhka nykyisille salausjärjestelmille on ollut Yhdysvalloissa kuuma keskustelunaihe syksystä 2015 lähtien. Aiemmin se oli vain teoreettinen mahdollisuus, mutta nyt näyttää siltä että perinteiset salausjärjestelmät ovat kriisissä aiemmin kuin on uskottu. Eurooppassa yritykset eivät ole vielä kunnolla heränneet, Yhdysvalloissa ainakin suuremmat yritykset ottavat jo salauksen kvanttiturvallisuuden puheeksi keskusteltaessa uusista hankinnoista.

Talvikoulun osanottajien mielestä nykyiset epäsymmetriset salaukset tulevat murtumaan, todennäköisesti ennemmin kuin myöhemmin. Yksityisten henkilöiden ulottuville tällainen teknologia ei tule niin nopeasti, mutta valtiollisille toimijoille ja mahdollisesti varakkaimmille rikollisorganisaatioille hinta ei tule olemaan esteenä. Klassisen salausparadigman mukaan salaaminen oli helppoa, mutta salauksen murtaminen oli vaikeaa. Kvanttiparadigman mukaan salaaminen on helppoa ja myöskin klassisilla menetelmillä salattujen tiedostojen murtaminen on helppoa.

Tilanne on erityisen vakava salaisen ja pitkään sellaisena säilyvän tiedon kannalta, tämä koskettaa mm. valtioita ja asevoimia. Salaiset tiedot puolustusjärjestelmistä tai vaikka ydinteknologiasta on nykyisin tehokkaasti suojattu eikä niitä saada välttämättä auki edes parhailla supertietokoneilla. Anastetut tiedostot voidaan kuitenkin tallettaa odottamaan myöhempää purkua, niiden sisältämä tieto voi olla arvokasta vielä 20 vuodenkin kuluttua. Tiedusteluorganisaatiot tallettavatkin kaiken haltuunsa saamansa informaation odottamaan sitä päivää kun sen purkaminen on mahdollista. Jos toimiva salausjärjestelmien purkuun soveltuva kvanttitietokone saadaan rakennettua kymmenen vuoden kuluttua, voidaan kaikki tähän asti varastoidut salatut tiedostot purkaa sen jälkeen hetkessä. Tämän vuoksi tärkeät tiedot pitäisi pystyä suojaamaan kvanttilaskentaa vastaan jo tänään.

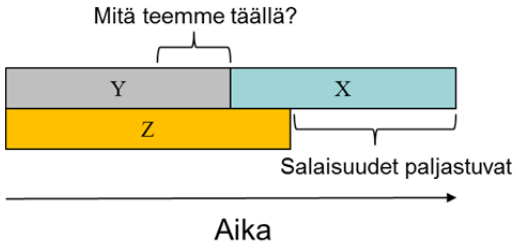
Tanja Lange Eindhovenin teknillisestä yliopistosta olettaa että universaali kvanttitietokone saadaan luultavasti rakennettua vuosien 2022 – 2027 välillä. Shor:in algoritmia käyttämällä kvanttikone voi laskea polynomisessa ajassa kokonaislukujen tekijöihin jaon (RSA on kuollut), diskreettien logaritmien ongelman äärellisissä kunnissa (DSA on kuollut), ja diskreettien logaritmien ongelman elliptisillä käyrillä (ECDHE on kuollut). Näiden seurauksena kaikki Internetin nykyiset julkisen avaimen salausmenetelmät menettävät merkityksensä. Toinen nk. Groverin algoritmi nopeuttaa brute-force etsintöjä; 2^64 kvanttioperaatiota riittää AES-128:lle ja 2^128 kvanttioperaatiota AES-256:lle.

Uusia kvanttiturvallisia algoritmeja pyritään kehittämään, mutta työ on vasta alussa. Ongelmaa pahentaa se, ettei meillä ole mitään matemaattisia tai muita teoreettisia menetelmiä joiden avulla jokin algoritmi voidaan osoittaa kvanttiturvalliseksi. Uudet algoritmit voivat olla pahimmillaan heikkoja jopa perinteisiä tietokoneita vastaan. Turvallisen salausalgoritmin kehittäminen on hidasta ja vaikeaa. Nykyisin käytössä olevia menetelmiä on tutkittu vuosia tai vuosikymmeniä ja samalla lukemattomat tutkijat ovat pyrkineet murtamaan niitä, silti niistäkin paljastuu ennen tuntemattomia haavoittuvuuksia. Kvanttialgoritmien kehitys on vielä alkutekijöissään, Shorin ja Groverin algoritmit tuskin ovat kehityksen viimeinen sana. Tanja Langen tutkimusryhmän sekä EU:n postquantum-kryptoprojektin verkkosivustot löytyvät osoitteista https://pqcrypto.org ja https://pqcrypto.eu.org.

Puolustusvoimien tutkimuslaitos on Pääesikunnan alainen sotilaslaitos, joka tuottaa monialaisesti puolustusvoimien tarvitsemia vaativia tutkimus-, kehittämis-, testaus- ja evaluaatiopalveluja. Tutkimuslaitoksessa yhdistyvät strategian ja operaatiotaidon, eri teknologia-alueiden ja ihmisen toimintakyvyn tutkimus. Tutkimuskatsaukset sisältävät yleistajuisia ja ajankohtaisia näkökulmia laitoksen osaamisalueilla.

Ongelmat eivät koske pelkästään tiedostoja. Salatut tiedonsiirtoyhteydet ovat tärkeä osa Internettiä, jonain päivänä niiden antama turva murtuu. Standardien ja infrastruktuurin muutos vie vuosia, emme voi heittää kerralla romukoppaan koko Internetin laitteisto- ja protokollavarantoa. Massiivisen työmäärän vuoksi korjausliike olisi pitänyt aloittaa jo eilen, ainakin se pitäisi aloittaa viimeistään tänään. ETSI:n[1] ja NIST:n[2] tapaiset organisaatiot ovat pyrkineet tunnistamaan uhkan suuruutta ja sitä kuinka helppoa olemassaolevien standardien muuttaminen on. Joissain tapauksissa uuden kvanttiturvallisen menetelmän lisääminen olemassa olevaan protokollaan on kohtuullisen helppoa, joissain tapauksissa muutos käytännössä romuttaa aikaisemman protokollan ja sellaiset sulautetut järjestelmät joissa kyseisiä protokollia käytetään.

Michele Mosca on esittänyt oman teoreemansa, jonka alkuarvot ovat seuraavat: X:llä ilmaisee sitä kuinka kauan salauksen pitää olla turvallinen, Y ilmaisee sen kuinka kauan olemassa olevan infrastruktuurin muuttaminen kvanttiturvalliseksi kestää ja Z kertoo koska salausten purkamiseen sopiva kvanttitietokone saadaan rakennettua. Teoreeman mukaan, jos X+Y > Z, huolestu. Jos X+Y > Z, silloin et voi taata vaadittua X vuoden turvallisuutta. Jos Y > Z, niin kyberjärjestelmät kaatuvat Z vuodessa ilman nopeaa korjausta asiaan.



Kuva 1. Moscan teoreema kuvana.

Kukaan ei osaa vielä sanoa kuinka suurien ongelmien edessä me olemme, mutta niin Yhdysvallat kuin Euroopan unionikin on sitä mieltä että uhkiin pitää alkaa reagoimaan.

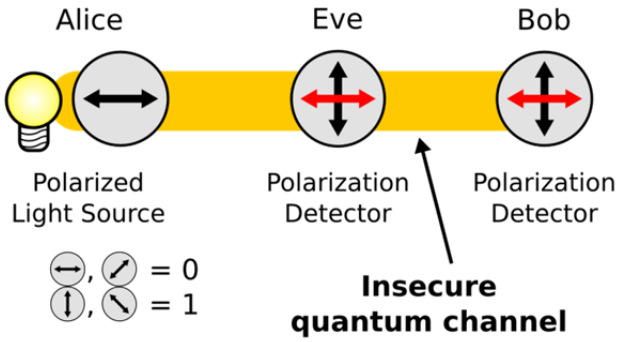
Kvanttiturvalliset verkot

Kvanttiturvallisista verkoista puhuttaessa on tärkeä ymmärtää joitain teoreettisia ja käytännöllisiä perusasioita. Kvanttimekaanisten ilmiöiden käyttöä viestien salaukseen tai väärennösten estämiseen on ideoitu jo aikaisemmin, mutta käyttökelpoisten tietoliikenteen salaukseen soveltuvien järjestelmien pohja luotiin Charles H. Bennetin ja Gilles Brassardin kehitettyä BB84 protokollan vuonna 1984. Sen jälkeen syntyneet Artur Ekertin E91 (1991) ja SARG04 (2004) ovat periaatteiltaan samantapaisia, niiden erot liittyvät käytännön toteutusten turvallisuuteen.

Kehitetyissä menetelmissä salattava tieto voidaan lähettää optista kuitua pitkin tai vapaassa tilassa, käyttämällä yksittäisiä fotoneja joiden polarisaatiot tai vaihe-erot vastaavat bittejä 0 ja 1. Fotoneilla voi olla kaksi toisistaan erotettavaa eli ortogonaalista polarisaatiotasoa, niiden vaihe-ero on 90 astetta. Kvanttisalauksessa käytetään kahta polarisaatioparia, yksi pari sisältää 0 ja 90 asteen polarisaatiot, toisessa parissa kulmat ovat 45 ja 135 astetta. Lähettäjä eli Alice valitsee kutakin lähetettävää bittiä kohden satunnaisesti yhden polarisaatioparin ja lähettää sitten yhden bittiarvoa vastaavan fotonin vastaanottajalle eli Bobille. Bob valitsee satunnaisesti yhden polarisaatioparin ja mittaa saapuvan fotonin arvon. Jos sekä Alice ja Bob valitsivat saman polarisaatioparin, bitti välittyy oikein. Jos polarisaatioparit poikkesivat toisistaan, tulos on satunnainen koska parit eivät ole keskenään ortogonaalisia. Keskimäärin 50 % biteistä on virheellisiä.

Lähetettyään tarvittavan bittijoukon Alice ja Bob käyttävät klassista tiedonsiirtokanavaa ja sitä käyttäen he kertovat toisilleen mitä polarisaatiopareja he käyttivät lähetykseen ja vastaanottoon. Tämän tiedon avulla he voivat heittää menemään ne bitit, jotka perustuivat toisistaan eroaviin polarisaatiopareihin. Suurin osa jäljelle jääneistä biteistä on välittynyt oikein, mutta virheitäkin sattuu koska fyysisissä järjestelmissä on aina häiriöitä. Alice ja Bob valitsevat osan biteistä vertailua varten, niiden pitäisi olla pääosiltaan samoja. Jos bittivirheet ylittävät tietyn rajan, jossain on jotain vikaa ja on mahdollista että Eve on salakuunnellut liikennettä. Ns. non-cloning teoreeman mukaan kvanttitilaa ei voi mitata vaikuttamatta sen arvoon; Eve ei voi varastaa bittiä ja lähettää sen täydellistä kopioa eteenpäin koska hän ei tiedä kumpaa polarisaatioparia hänen olisi pitänyt käyttää kunkin bitin mittauksen tekemiseen.

Jos suuria häiriöitä ei havaita, voidaan loppuja bittejä käyttää jaetun salausavaimen välittämiseen. Jokin virheenkorjausalgoritmi tarvitaan, koska kaikki bitit eivät välity täysin virheettömästi. Korjattua avainta voidaan käyttää suoraan kertakäyttösalasanana, hyvin tärkeässä ja lyhyessä viestissä tämä on ok. Kvanttiverkko ei ole kuitenkaan täydellinen, etäisyyden kasvaessa virheiden määrä kasvaa ja bittinopeus laskee epäkäytännölliselle tasolle. Tämän vuoksi kvanttiverkkoa käytetään yleensä salausavainten välittämiseen, varsinainen data välitetään klassista kanavaa pitkin. Avainta vaihdetaan automaattisesti, vaihtoväli riippuu salaustarpeesta ja nopeusvaatimuksista. Tämä Quantum Key Distribution (QKD) eli kvanttiavaintenvälitys on yksi askel kohti turvallisempia yhteyksiä. Kaupallisia tuotteita on jo olemassa, mm. IDQ:n valmistamina. Kyse on normaaliin räkkiin asennettavasta laitteesta, osapuolten väliin tarvitaan yksityinen ”pimeä” kuitu kvanttidatan välitykseen sekä normaali verkkoyhteys. Laite voidaan myös kytkeä olemassa olevan salauslaitteen perään, esim. pankin järjestelmässä. Tällöin jo perinteisellä menetelmällä salattu yhteys salataan edelleen tekemällä XOR-operaatio sen ja kvanttisalaimen bittivirran läpi, hyökkääjän pitäisi kiertää molemmat salausmenetelmät.



Kuva 2. Alicen, Even ja Bobin käyttämät polarisaatioparit. Eve ei voi tietää etukäteen, onko Alice käyttänyt pysty ja vaakapolarisaatiota vai diagonaalipolarisaatiota. Eve ei voi tutkia ja kopioida välitettyä kvanttibittiä vaikuttamatta Bobin mittaamiin arvoihin.[3]

Kvanttihakkerointi

Fotoneihin pohjautuva kvanttisalaus pohjautuu todennäköisyyksiin. Teoreettinen laitteisto voidaan todistaa turvalliseksi kvanttimekaniikan lakien mukaan, turvataso voidaan laskea avaimen pituuden ja valittujen kynnysarvojen perusteella. On kuitenkin

[1] “Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges”, ETSI White Paper No. 8, 64 s., June 2015.
[2] “Report on Post-Quantum Cryptography”, NISTIR 8105, http://dx.doi.org/10.6028/NIST.IR.8105

[3] Tekijänoikeudet: By Andy Spencer - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=37393913

tärkeää ymmärtää, ettei fyysisen laitteiston turvallisuustaso ole vakio. Eri toteutusten todellinen turvataso voi vaihdella erinomaisen ja olemattoman välillä, laitteiston rakentajan ja suunnittelijan ammattitaidosta riippuen.

Kvanttihakkeri Vadim Makarov on murtanut monia nykyisiä kvanttiteknologiaan perustuvia tiedonsiirtojärjestelmiä ja mm. IDQ käyttää häntä laitteidensa testaamiseen ja paranteluun. Toistaiseksi hän ei ole tarvinnut kvanttimekaniikan tuntemusta laitteiden murtamiseen, klassinen tekniikka on ollut riittävää. Vaikka teoriassa jokin laite olisikin täydellinen, fyysiset järjestelmät sisältävät aina heikkouksia joita voidaan hyödyntää.

Kuten aiemmin mainittiin, kvanttisalaus perustuu yksittäisten fotonien käsittelyyn. Jollain tavalla yksittäinen lähetettävä bitti pitää muuttaa yksittäiseksi fotoniksi, mutta tätä ei voi tehdä suoraan lähtöpäässä. Välissä oleva optinen kuitu sisältää aina valmistusvirheitä ja vaimennuksia, jollain todennäköisyydellä kuidussa kiitävä fotoni törmää johonkin tai karkaa ulos kuidun pinnasta. Mitä pidempi kuitu on kyseessä, sitä useampi fotoni katoaa matkalla. Myös lämpötila ja käytetty kuitu vaikuttaa hävikkiin.

Koska fotoneja katoaa joka tapauksessa, ei ole järkevää käyttää kvanttikaivolaseria tai muita komponentteja joilla voitaisiin lähettää matkaan yksittäisiä fotoneita. Valonlähteenä käytetään yleensä jotain edullista puolijohdelaseria joka tuottaa yhtä bittiä kohden esimerkiksi 10 miljoonaa fotonia. Käytettävän kuidun pituus voi olla satoja metrejä tai kilometrejä, joten vaimennushävikkikin vaihtelee suuresti. Jollain tavalla pitää varmistaa, että vastaanottimen ilmaisimelle (detektorille) saapuu keskimäärin yksi fotoni bittiä kohden. Tämä onnistuu käyttämällä lähtöpäässä vaimenninta, jolla lähetettävää valoa himmennetään. Koska valo on kvantittunutta, tarkoittaa himmentäminen suoraan fotonien määrän vähentämistä. Jonkinlaista hienosäätöä tarvitaan jatkuvasti, koska laitteiden ja kuitujen lämpötila yms. seikat vaikuttavat fotonien hävikkiin.

Vaimennetut fotonit noudattavat tiettyä jakaumaa. Joskus fotoni jää kokonaan tulematta, välillä fotoneja tuleekin kaksi ja silloin tällöin useampia. Jos fotoneja tulee enemmän kuin yksi, voi Eve varastaa niistä yhden eikä kukaan havaitse mitään. Satunnaisilla ylimääräisillä fotoneilla ei vielä pääse pitkälle, mutta ylimäärää voidaan pyrkiä kasvattamaan. Jos yhteyden vaimennusta saadaan lisättyä väliaikaisesti, voidaan laitteistoa hämätä tuottamaan liian suuri määrä fotoneita. Kuidun suojaan voidaan tehdä ohut viilto, sitä kautta kuituun voidaan ampua laserpulsseja. Vastaanottimen sensoria voidaan sokaista tai vaurioittaa, tällöin järjestelmä skaalaa fotonien määrän väärin.

Lähettimen optroniikkaan kohdistetuilla pulsseilla on myös voitu saada tietoa lähetettyjen pulssien tilasta, koska pieni osa laservalosta heijastuu takaisin käytetystä optiikasta ja komponenteista ja niissä esiintyy erilaisia muisti-ilmiöitä. Erilaisia mahdollisuuksia on runsaasti, Makarov ja muut tutkijat ovat julkaisseet lukuisia kokeellisesti todistettuja tai teoreettisia hyökkäyksiä. Vastatoimina voidaan käyttää sensoreita, joilla pulssien tehoja valvotaan. Järjestelmän optista rakennetta voidaan muokata myös sellaiseksi, ettei eri polarisaatiotasojen tilaa voida tunnistaa epäsuorasti. Vaikka lähetintä ja vastaanotinta tarkastellaan usein mustina laatikoina, pystyvät kvanttihakkerit usein keräämään tietoa mustien laatikoiden sisältä; niitä voitaisiin ehkä kutsua harmaiksi laatikoiksi. Lähetyspään pulssilähteissä tai optiikassa voi myös olla eroja, tällöin pulssien ajastus tai muut erot voivat paljastaa lähetettävät bitit. Jos hyökkääjä pääsee riittävän lähelle lähetintä tai vastaanotinta, voi muu sähkömagneettinen hajasäteily paljastaa lähetettävän datan osittain tai kokonaan.

Käytetyt satunnaisluvut ovat toinen tärkeä virhelähde. Jos Alicen ja Bobin satunnaislukujen jakauma vinoutuu tai sisältää muuta ennustettavuutta, voi tämä auttaa Eveä salakuuntelussa. Tosielämässä on tapahtunut että itse satunnaislukugeneraattori toimi oikein, mutta sen perässä ollut FPGA-piiri muutti jakaumaa ennustettavampaan suuntaan. Laitteistoissa käytetyt komponentit muodostavat tunnistetun riskin, ainakin valtiolliset toimijat voivat piilottaa laitteisiin salaportteja joilla satunnaisuutta voitaisiin keventää halutulla ajanhetkellä. Satunnaislukujen tuottamiseksi IDQ on tuotteistanut kvantti-ilmiöihin perustuvan muutaman senttimetrin kokoisen satunnaislukugeneraattorin. Quantisperheen piirikortteja voidaan käyttää myös normaaleissa tietokoneissa, käyttökohteina kaikki laitteet jossa tarvitaan aitoa satunnaisuutta kertakäyttöavaimiin tai muihin tarkoituksiin.

Kvanttiverkot

Kuiduissa tapahtuvat häviöt rajoittavat QKD:n käytön maksimietäisyyttä. Alle sadan kilometrien etäisyydet ovat vielä käyttökelpoisia, mutta tietyn rajan jälkeen toimintakyky laskee merkittävästi. Luonnossa on saatu aikaan 2,5 bits/s yhteys 150km etäisyydelle, laboratorio-olosuhteissa on siirretty 3 bits/s 307km. Teoreettinen maksimi on jossain 500-1000km välillä, mutta tällöin on kyseessä kallis teknologiademonstraatio jolla ei ole käytännön merkitystä.

Non-cloning teoreema estää normaaleissa kuituverkoissa käytettävät vahvistimet, kvanttisalatun yhteyden Alicen ja Bobin välillä pitää olla suora. Yhteysetäisyyden kasvattaminen vaatii toistinasemia joissa viesti puretaan ja lähetetään uudelleen, toistinasemia pitäisi olla 100 - 200 km välein. Toistinasemissa viestintä on alttiina tavanomaisille tietoverkko-operaatioille. Jos toistinasemien määrä kasvaa, laskee koko QKD-verkkoa kohtaan osoitettu luottamus.

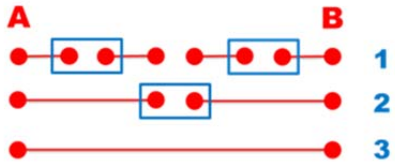
Etäisyyteen liittyvät ongelmat ovat kuitenkin kierrettävissä hyödyntämällä toista kvanttimekaniikan ilmiötä. Ratkaisuksi on esitetty kvanttiverkkoa, joka perustuu kvanttilomittumiseen ja teleportaatioon. Alicen ja Bobin käyttämät kvanttibitit lomitetaan, jolloin ne ovat samassa tilassa riippumatta siitä ovatko ne naapurissa tai galaksin toisella laidalla. Konseptin toimivuus on osoitettu teoreettisesti, käytännön työ on tällä hetkellä meneillään ja alan tutkijat uskovat että kvanttiverkkoa voitaisiin kokeilla muutaman vuoden kuluttua.

Kvanttiverkko on teoriassa helppo toteuttaa. Verkko kootaan lyhemmistä pätkistä, katkoskohdissa kvantit lomitetaan pätkä kerrallaan yhä pidemmiksi ketjuiksi. Lopulta ketjun päissä olevat kvantit on saatu lomitettua keskenään ja Alice ja Bob voivat hyödyntää niiden kvanttitiloja. Käytännössä fotonien lomittaminen vaatii kuitenkin niiden saamista vuorovaikutukseen toistensa kanssa tarkalleen oikeassa kohdassa oikeaan aikaan. Tämä on hyvin vaikeaa, koska se vaatii äärimmäisen tarkkoja ajoituksia saapuville fotoneille. Vaikka fotonit voitaisiin lähettää kuituihin tarkasti oikealla hetkellä, ei niiden kulkuaikaa pystytä kontrolloimaan. Lämpötilan muuttuminen asteen osilla pitkässä kuidussa vaikuttaa merkittävästi fotonien kulkuaikaan, lisäksi kulkuaika vaihtelee jatkuvasti. Vaikka yksittäiset fotoniparit yhdellä yhteysvälillä saadaan välillä lomittumaan, todennäköisyys pidempien ketjujen muodostamiselle lähestyy hyvin nopeasti nollaa.

Lomittumisen aikaansaamiseksi kontrolloidulla ja toistettavalla tavalla tarvitaan viivelinjoja, joilla fotonien tuloajat voidaan säätää täsmälleen kohdalleen. Viivelinjan toteuttamiseen tarvitaan kvanttimuisteja, joihin fotonin kvanttitila voidaan tallentaa häiriintymättä halutuksi ajanjaksoksi. Tämä on osoitettu teoreettisesti mahdolliseksi ja Geneven yliopiston tutkijaryhmä mm. Mikael Afzeliuksen ja Nicolas Gisinin johdolla työskentelee aktiivisesti

toimivan kvanttimuistin rakentamiseksi[4]. Työ perustuu sopiviin kidemateriaaleihin, joihin kvanttitila voidaan vangita lyhyeksi aikaa. Mikro- tai millisekuntien mittainen säädettävissä oleva viivelinja riittäisivät jo toimivan kvanttitoistimen (Quantum repeater) aikaansaamiseksi, tutkijat uskovat tähän päästävän vielä lähivuosien aikana.

On todennäköistä että kvanttimuistien tutkimus johtaa toimiviin kokeellisiin kvanttiverkkoihin muutaman vuoden sisällä, tällöin kvanttiturvallisesta avaintenvälityksestä tulee paljon käytännöllisempää ja kaupallisesti kiinnostavampaa. Klassiseen teknologiaan perustuvien välittimien poistuminen nostaa turvatasoa merkittävästi. Kuitujen lisäksi myös vapaassa ilmakehässä olevat kahden aseman väliset ratkaisut sekä maa-aseman ja satelliitin väliset yhteydet ovat aktiivisen tutkimuksen alla ja tuloksia voidaan odottaa lähivuosien aikana.



Kuva 3. Kvanttiverkko A:n ja B:n välille luodaan osissa. Siniset neliöt kuvaavat fotonien lomittamista yhteen. Lopulta A ja B ovat lomittuneet keskenään samaan kvanttitilaan. Jos yksikin välivaihe epäonnistuu, fotonin kvanttitila ei välity oikein. Kvanttitoistimet (quantum repeaters) vaativat toimiakseen kvanttimuisteja joiden avulla fotonien ajoitukset saadaan kohdalleen.

Kryptologia ja kvanttilaskenta

Gilles Brassard käsitteli esityksissään kvanttilaskennan[5] ja kryptologian[6] yhteistä historiaa. Brassard kehitti BB84-protokollan yhdessä Charles Bennettin kanssa ja he ovat käytännössä käynnistäneet koko nykyisen kvanttiturvallisten menetelmien kehityssyklin.

Bennettin 60-luvun opiskelutoveri Stephen Wiesner oli esittänyt varhaisia ajatuksia kvantti-informaation käyttämisestä informaation koodaamiseen jo vuonna 1968, mutta hän ei saanut niitä julkaistuksi koska IEEE:n lehtien referoijat eivät ymmärtäneet sitä (artikkeli julkaistiin lopulta 1983). Idea olisi saattanut hautautua vuosikymmeniksi, mutta vuonna 1979 Bennett tapasi Brassardin sattumalta uimarannalla Puerto Ricossa ja hän kertoi tälle Wiesnerin ajatuksista. Näiden keskustelujen tuloksena syntyi historian ensimmäinen kvanttikryptografiaa käsitellyt julkaisu vuonna 1983, se toimi lähtölaukauksena koko kvanttiavaintenvaihdon (QKD) ja kvanttikryptografian tutkimusalueelle.

Viime vuosien aikana Brassard ja Bennett ovat useita kertoja palanneet aiheeseen ja pyrkineet käsittelemään kvanttisalausta teoreettisista lähtökohdista, onko se todella turvallista vai voidaanko se murtaa joissain tilanteissa? Välillä BB84:stä ja muista variaatioista on löytynyt ongelmia, mutta ne on pystytty kiertämään tai osoittamaan vääriksi. Artur Ekert otti mukaan kvanttien lomittumisen sekä yhteydet Bell:in teoreemiin, niillä on ollut paljon merkitystä teorioiden kehitykselle. Manuel Blum kiinnitti huomiota QKD:n ja Einstein-Podolsky-Rosen (EPR) paradoksin yhteyksiin, on pohdittu voiko EPR mahdollistaa joitain hyökkäyksiä. Renato Renner tutki joitain mahdollisia haavoittuvuuksia, mutta lopulta ne onnistuttiin osoittamaan vääriksi. Myöhemmin Ekert ja Renner ovat tutkineet tarkemmin Bell:in teoreemojen vaikutuksia ja niiden perusteella turvallisuus näyttäisikin olevan taattu[7].

Kvanttisalaus liittyy myös suoraan Ralph Merklen työhön. Ollessaan opiskelija Berkleyssä vuonna 1974 hän keksi miten salaista tietoa voitiin välittää salaamatonta kanavaa pitkin. Hänen professorinsa ei ymmärtänyt ideaa ja Merkle putosi pois salaustekniikan kurssilta, mutta loppujen lopuksi hän sai julkaistua ajatuksensa vuonna 1978. Tällä välin naapurissa olevan Standfordin opiskelija Whitfield Diffie löysi enemmän vastakaikua ohjaajaltaan Martin Hellmanilta ja he saivat julkaistua vastaavat ajatuksensa julkisen avaimen menetelmistä ja sähköisistä allekirjoituksista. Ronald Rivest, Adi Shamir ja Leonard Adleman kehittivät ideoita hieman pidemmälle ja he loivat RSA kryptojärjestelmän.

Brassard ja muut ovat useita kertoja yhdistäneet Merklen alkuperäisiä ajatuksia muiden menetelmiin, he ovat osoittaneet että tietyt yhdistelmät saattavat vahvistaa salausjärjestelmiä kvanttilaskennan uhkia vastaan. Kaiken kaikkiaan tämä tutkimusalue on kuitenkin kaikkea muuta kuin selvää, monia asioita ei vielä tunneta riittävän tarkasti ja kokonaisia uusia salausjärjestelmä- ja salausten purkujärjestelmäperheitä saattaa vielä olla löytämättä.

Klassisen kryptologian suhde Shannonin informaatioteoriaan on selkeä. Shannonin teoriat pitävät selkeästi paikkansa klassisessa maailmassa, mutta kvanttimaailmassa se ei enää pidäkään kaikilta osin paikkaansa. Shannonin teorioita ei voida käyttää suoraan hyväksi kvantti-informaatiota sisältävien järjestelmien analysoinnissa ja teoreettisessa työssä, koska lomittuminen ja kloonaamattomuusteoria muuttavat joitain perusoletuksia.

Kryptologit voivat kehittää salausjärjestelmiä hyödyntämällä klassinen maailman tai kvanttimaailman ilmiöitä. Salauksia purkavat kryptoanalyytikot voivat puolestaan käyttää työkaluja, jotka perustuvat klassinen maailman tai kvanttimaailman ilmiöiden hyödyntämiseen. Salattu viesti voidaan lähettää klassista tai kvanttimaailman mukaista viestintäkanavaa pitkin. Jo tällä karkealla tasolla löytyy kahdeksan eri kombinaatiota, joissa klassisen ja kvanttimaailman menetelmät vaikuttavat eri tavoilla kokonaisuuteen. Kaikista ei ole vielä edes olemassa olevia esimerkkejä, meiltä puuttuvat mm. varsinaiset kvanttimekaniikkaan perustuvat salausalgoritmit. Nämä tutkimusalueet tarjoavat uusia tutkimuskysymyksiä vähintään vuosikymmeniksi. Tuloksena tulee olemaan lukuisia vielä tuntemattomia käytännön sovellutuksia ja teoreettisia lähestymistapoja. Niin salausmenetelmien kehittäjille kuin niiden purkajille riittää vielä paljon työsarkaa.

Onko kvanttimaailma siunaus vai kirous kryptologeille? Selkeää vastausta tähän ei ole olemassa. Tutkittaessa kvanttiteknologian vaikutuksia salaukselle joudumme nopeasti hyvin monimutkaisten asioiden eteen, läheskään kaikkia näkökulmia ei ole vielä tarkasteltu syvällisesti ja samanaikaisesti. Haluttaessa edes jonkinlaisia turvatakuita tarvitaan erilaisia ratkaisumalleja, joita voidaan käyttää rinnakkain. Pitää pyrkiä kehittämään klassista salausta, joka kestää kvanttilaskentaa. Viestintään tulisi käyttää kvanttiteknologiaan perustuvia langallisia ja langattomia verkkoja. Lopuksi tarvittaisiin vielä mahdollisesti olemassa olevia, mutta toistaiseksi tuntemattomia aitoja kvanttiteknologiaan pohjautuvia salausratkaisuja.

Jos kaikkia näitä keinoja käytetään samanaikaisesti, on epätodennäköisempää että ne kaikki pettäisivät samalla kertaa. Tämä on esimerkki syväpuolustuksen eli Defence in depth – konseptin hyödyntämisestä kvanttimaailmassa. Varsinaisia kvanttisalausal-

[4] Mikael Afzelius, Nicolas Gisin, and Hugues de Riedmatten, “Quantum memory for photons”, Physics Today 68(12), 42 (2015), http://dx.doi.org/10.1063/PT.3.3021.
[5] Gilles Brassard, “Brief History of Quantum Cryptography: A Personal Perspective”, http://arxiv.org/abs/quant-ph/0604072v1.
[6] Gilles Brassard, “Cryptography in a Quantum World”, http://arxiv.org/abs/1510.04256v1.
[7] Artur Ekert & Renato Renner, “The ultimate physical limits of privacy”, Nature, Vol 507, 2014, s. 443-447.

goritmeja ei ole vielä olemassa, mutta ns. kvanttiturvalliset klassiset algoritmit tarjoavat ainakin jonkinlaisen hidasteen.

Loppusanat

Kvanttilaskenta ja siihen liittyvät ilmiöt muodostavat laajan ja nopeasti kehittyvän kokonaisuuden, uusia havaintoja julkaistaan lähes viikoittain. Tämä raportti ei ole kattava yleiskatsaus kvanttilaskentaan vaan se pohjautuu hyvin tiiviisti talvikoulun esityksiin sekä vierailuihin IDQ:n Geneven toimipisteeseen ja Geneven yliopiston sovelletun fysiikan laitokselle. Kvanttilaskennan kehitys on tällä hetkellä nopeaa. Kvanttiturvallisista salausalgoritmeista puhutaan tällä hetkellä paljon Yhdysvalloissa ja muuallakin. Monet tutkimusryhmät suunnittelevat aktiivisesti erilaisia fysikaalisia kvanttikonearkkitehtuureja, mm. Googlella on prof. Martiniksen johdolla suunnitelma 6x7=42 kubittisen kvanttikoneen rakentamiseksi. Kiina hämmästytti maailmaa elokuussa 2016 laukaisemalla ensimmäisenä maana avaruuteen Micius-nimisen kvanttisatelliittinsa, jota tullaan käyttämään kvanttilomittumista hyödyntävien salattujen kommunikaatiokanavien testauksessa. Tämä ajatus oli alun perin lähtöisin Euroopasta, mutta Kiina oli se joka uskalsi lähteä tienraivaajaksi. Kiina ja Etelä-Korea ovat varmasti seuraamisen arvoisia maita kvanttiteknologiassa.

Tämän tutkimuskatsauksen lähdeviittaukset on rajattu muutamaan yleisesti saatavilla olevaan ja kiinnostaviksi nähtyyn julkaisuun.

Lisätietoja

TkT Mika Helsingius (p. 0299 800) on Puolustusvoimien tutkimuslaitoksen informaatiotekniikkaosaston vanhempi tutkija