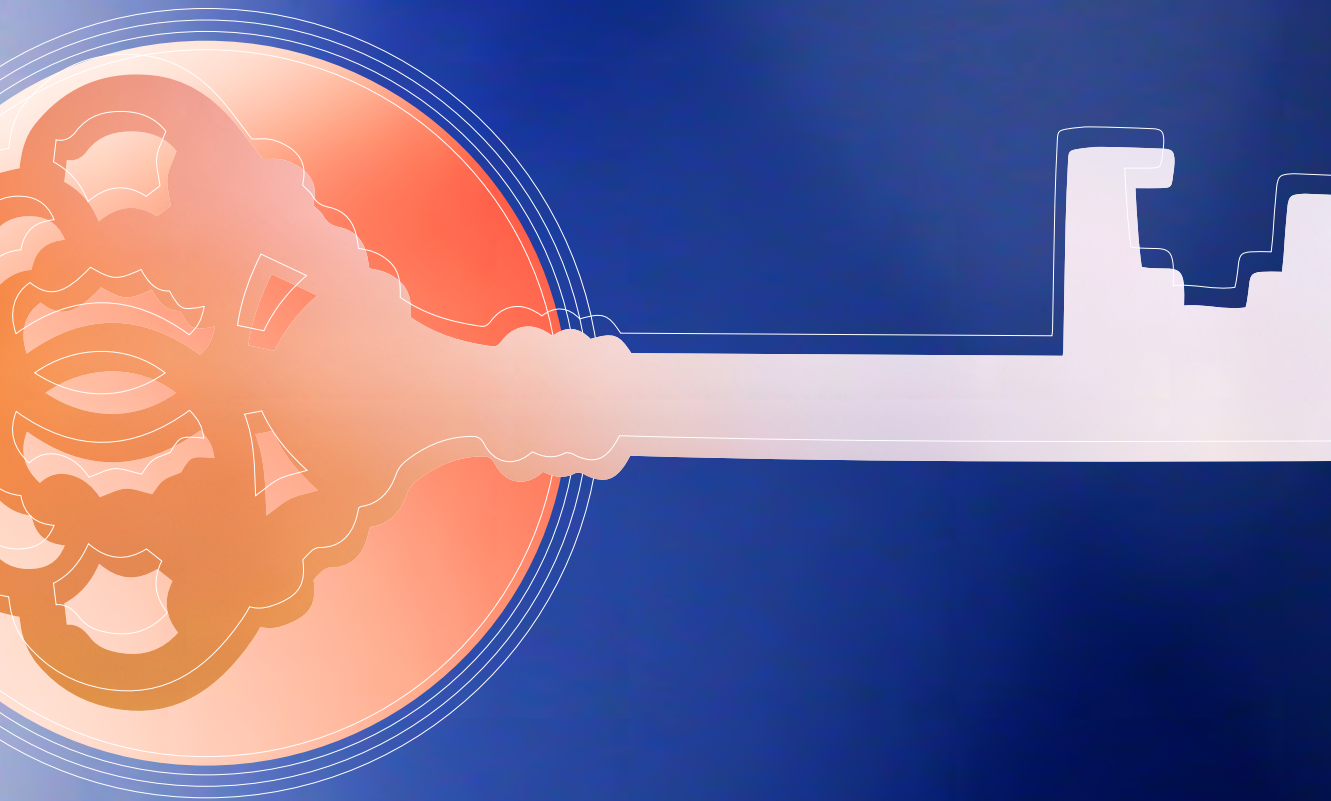
MIKAEL JOHANSSON
SABRINA MANISCALCO
SUVI LAMPILA

Kvanttiteknologian tulevaisuus ja kvantti-turvallinen internet



EDUSKUNNAN TULEVAISUUSVALIOKUNNAN JULKAISU 2 | 2025

EDUSKUNNAN TULEVAISUUSVALIOKUNNAN JULKAISU 2 | 2025

ISSN 2342-6594 (PAINETTU) ISBN 978-951-53-3830-3 (NID)
ISSN 2342-6608 (VERKKOJULKAISU) ISBN 978-951-53-3831-0 (PDF)

MIKAEL JOHANSSON
SABRINA MANISCALCO
SUVI LAMPILA

Kvanttiteknologian tulevaisuus ja kvantti-turvallinen internet

Sisällys

Esipuhe

Hyvä lukija,

Kädessäsi on kolmen artikkelin paketti, jonka eduskunnan tulevaisuusvaliokunnan teknologian ennakointi -ohjausryhmä tilasi tueksi kansanedustajille, virkamiehille ja muille aiheesta kiinnostuneille. Tarkoitus on kuvata kvanttiteknologian nykytila ja tulevat suuntaviivat tarkasti mutta ymmärrettävästi, ilman raskasta fysiikan kieltä.

Artikkeleista ensimmäinen avaa perustermit ja koko "kvantti-internetin" idean, toinen kartoittaa kvanttilaskennan kehityspolut ja kolmas syventyy siihen, miten verkkomme pysyvät turvassa kvanttikaudella. Ensin saat käsityksen perusasioista, sitten siirryt konkreettisiin sovelluksiin ja standardeihin.

Kvanttitietokoneet kiinnittivät valiokunnan huomion aikaisin

Kvanttilaitteet eivät ole valiokunnalle uusia. Jo vuoden 2018 "Suomen sata uutta mahdollisuutta 2018–2037" -raportti listasi kvanttitietokoneet ja kvanttikommunikaation yhdeksi radikaaleimmista tulevaisuusteknologioista. Jo tuolloin todettiin, että niiden vaikutus ulottuu sekä teolliseen kilpailukykyyn että tietoturvan perusteisiin. Jälkikäteen katsottuna ennuste osui nappiin: Kvanttitietokoneiden kehitys on kiihtynyt, ja nykyisin voimme ajaa kvanttilaskuja verkossa yli sadan kubitin laitteilla. Suurimmat koneet ylittävät jo tuhannen kubitin rajapyykin.

Suomi panostaa kvanttiteknologiaan

Poliittinen tuki kvanttiteknologialle on kasvanut samaan tahtiin tekniikan kehittyessä. Vuonna 2020 eduskunta myönsi 20,7 miljoonaa euroa VTT:lle ja IQM:lle Suomen ensimmäisen kvanttitietokoneen rakentamiseen. Onnistuneen prototyypin jälkeen rahoitusta kasvatettiin 70 miljoonaan euroon koneen laajentamiseksi 300 kubittiin. Vuonna 2024 Suomen Akatemia osoitti 13 miljoonaa euroa uudelle kvanttilippulaiva-ohjelmalle, ja huhtikuussa 2025 julkaistu kansallinen kvanttistrategia keskittyy tutkimukseen, teollisiin sovelluksiin, kvanttiturvalliseen infraan ja kansainväliseen yhteistyöhön.

Miksi kvanttiturvallisuus nousee nyt?

Edellä mainitut rahoitukset tukevat kvanttitietokoneiden kehittämistä sekä salausmenetelmien luomista. Kvanttitietokoneet voivat tulevaisuudessa murtaa nykyiset internetin salaukset. Teknologian ennakointi -ohjausryhmän tilaamat artikkelit pyrkivät vastaamaan siihen kysymykseen, miksi kvanttiturvallisuudesta huolehtiminen on jo tämän päivän kysymys.

Dosentti Mikael Johansson, joka on kvanttiteknologioiden päällikkö CSC – Tieteen tietotekniikan keskuksessa, avaa artikkelissaan kvantti-internetin perusteita ja näyttää, miten kvanttiteknologian yleistyessä perinteiset salausmenetelmät eivät enää riitä. Professori Sabrina Maniscalco kuvaa puolestaan sitä, kuinka kvanttilaskenta on jo siirtymässä laboratoriokokeiluista pilvialustoille ja kasvanut laskentateho tekee nykyisistä salaustekniikoista entistä haavoittuvampia. SSH Fellow Suvi Lampilan artikkeli selittää, miten nämä uuden sukupolven salausratkaisut syntyvät ja miksi on tärkeää jo nyt suunnitella järjestelmät niin, että ne voi myöhemmin helposti päivittää kvanttiturvallisiksi.

Suomalainen tietoliikenneala kvanttiturvallisen internetin kärkijoukoissa
Kvanttisiirtymä tarjoaa tietoliikennealalle mahdollisuuden, joka muistuttaa 1990-luvun GSM-ratkaisuja. Tutkimuslaitoksissa kehitetään jo kvanttiturvallisia salausratkaisuja ja avainhallintaa, ja viime vuosina on demonstroitu kvanttiturvallista mobiiliverkkoa sekä satelliittipohjaisia kvanttiavainjakelukokeiluja.

Yhdessä kotimaisen 6G-tutkimuksen, kansallisen kvanttilaskentainfrastruktuurin ja eurooppalaisen yhteistyön kanssa Suomella on edellytykset nousta johtavaksi kvanttiturvallisen internetin toimijaksi. Tässä tarvitaan rohkeita pilottiprojekteja niin kotimaassa kuin kansainvälisillä markkinoilla.

Miten lukea tätä julkaisua?
1. Johanssonin artikkeli esittelee kvantti-internetin perusteet, joten jos lomittuminen ja kubitit eivät vielä ole tuttuja, kannattaa aloittaa tästä.
2. Maniscalco esittelee artikkelissaan kvanttilaskennan kehityspolun, eri laitealustojen erot ja kaupallistumisen vaiheet, mikä tarjoaa vahvan pohjan investointien ja osaamistarpeiden arviointiin.
3. Lampila purkaa kryptografian murroksen ja antaa listan toimenpiteistä, joilla Suomi (ja jokainen organisaatio) voi varmistaa tietoturvansa myös päivänä, jolloin kvanttitietokoneet murtavat nykyiset salaukset.

Toivomme, että tämä kokoelma auttaa rakentamaan yhteistä käsitystä siitä, missä mennään, mihin olemme menossa ja mitä päätöksiä tarvitaan, jotta Suomi pysyy kvanttikehityksen eturivissä.

Helsingissä kesäkuussa 2025

Eduskunnan tulevaisuusvaliokunnan teknologian ennakointi -ohjausryhmä

VILLE VÄHÄMÄKI (ps.), ohjausryhmän puheenjohtaja

TIMO HARAKKA (sd.)
VILLE KAUNISTO (kok.)
SHEIKKI LAAKSO (ps.)
MIKA POUTALA (kd.)
SINUHE WALLINHEIMO (kok.)

Kvantti, internet ja kvantti-internet

SUOMEN DIGITAALINEN TULEVAISUUS KVANTTIAIKAKAUDELLA

MIKAEL JOHANSSON
FT, dos.
Kvanttiteknologioiden päällikkö, CSC – Tieteen tietotekniikan keskus

Johdanto

Tavallisessa internetissä siirretään paikasta toiseen bittejä eli nollia ja ykkösiä. Kvantti-internet käyttää kvanttibittejä.

Harva teknologinen innovaatio on muokannut nyky-yhteiskuntaa yhtä voimakkaasti kuin internet. Internet on nykyään talouden, turvallisuuden ja jokapäiväisen elämän perusta, joka yhdistää yritykset, viranomaiset ja yksityishenkilöt. Suomi on jo pitkään ollut teknologisen innovaation eturintamassa. Meillä alkoi 1980-luvun alussa digitaalinen vallankumous, joka teki Suomesta yhden maailman teknisesti edistyneimmistä yhteiskunnista. Tähän on useita syitä. Perustana voidaan pitää innovaatioon rohkaisevaa tiede- ja tutkimuspolitiikkaa, joka on kannustanut läpimurtoihin korkean teknologian aloilla.

Vuonna 1983 perustettiin Suomen yliopisto- ja tutkimusverkko Funet. Osana pohjoismaista NORDUnet-yhteistyötä se tasoitti tietä, kun Suomi halusi yhdistyä maailmanlaajuiseen internetverkkoon 1980-luvun lopulla. Kun digitaalinen aikakausi alkoi kypsyä, hyödynsimme tätä varhaista etumatkaamme ja nousimme johtavaksi toimijaksi matkaviestinnän alalla. Tästä olivat osoituksena Nokian maailmanlaajuinen menestys ja myöhempi johtajuus kyberturvallisuuden ja digitaalisten julkisten palvelujen alalla.

Internet on nyt uusien haasteiden ja mahdollisuuksien edessä, kun kvanttiteknologioiden läpimurto on käsillä. Kvanttilaskenta ja kvanttitietokoneet lupaavat mullistaa tietojenkäsittelyn siten, että ne mahdollistavat aikaisemmin käytännössä mahdottomien laskennallisten ongelmien ratkaisun. Mitä tulee tietoliikenteeseen, kvanttikoneet uhkaavat heikentää digitaalisen turvallisuuden takaavia salausjärjestelmiä ja täten Suomen kokonaisturvallisuutta.

Tällä hetkellä valtaosa internetissä kulkevasta liikenteestä – sähköpostista pankkipalvelujen kautta terveystietoihin – turvataan käyttäen niin kutsuttua julkisiin avaimiin perustuvaa salausta. Nykyiset salausmenetelmät pärjäävät käytännössä aina perinteisten tietokoneiden murtamiskyvylle, mutta ne eivät ole tarpeeksi vahvoja kehittyneiden kvanttitietokoneiden laskentakapasiteetille. Tämän takia, jotta internetistä ja tietoliikenteestä yleensä tulisi kvanttiturvallinen, on pakko siirtyä uusiin salausmenetelmiin mahdollisimman pian.

Samaan aikaan kvanttimekaniikkaan perustuva verkko, kvantti-internet, tarjoaa ennennäkemättömiä mahdollisuuksia turvalliseen viestintään sekä sellaiseen perustutkimukseen, jolla voidaan ymmärtää maailmankaikkeutta aiempaa syvemmin. Käyn tässä läpi sitä, miten kvanttiteknologia vaikuttaa internetiin ja tietoliikenteeseen, sekä laajemmin haasteita, joita digitaalinen maailma kohtaa seuraavien 25 vuoden aikana. Tarkastelen aihetta sekä kvanttiturvallisen internetin että itse kvantti-internetin näkökulmista. Kyberturvallisuusuhat, tekoälyyn perustuva dis-

informaatio, digitaaliseen infrastruktuuriin liittyvät kasvavat geopoliittiset jännitteet ja erilaiset ympäristönäkökohdat edellyttävät ennakoivaa politiikkaa. Kun Suomi pyrkii varmistamaan asemansa digitaalisen murroksen edelläkävijänä, on ratkaisevan tärkeää ymmärtää näitä muutoksia.

Perustat

VERKOT YHDISTÄVÄT IHMISET JA TIETOKONEET

Digitaalinen viestintä sai alkunsa sähköisistä lennättimistä 1800-luvun alkupuolella. Läpimurto tuli Samuel Morsen kehittämän järjestelmän kautta, jossa lennätinlinjoja pitkin lähetettiin viestejä, sähkeitä, käyttäen Morsen aakkosia, joissa viestin merkit kuvataan kahdella eripituisella pulssilla, lyhyellä ja pitkällä. Tunnetuin näistä on tietenkin SOS, kolme lyhyttä, kolme pitkää ja kolme lyhyttä pulssia: ··· --- ···.

Morsen aakkoset ovat mainio esimerkki siitä, miten tärkeitä standardit ovat viestinnässä. Lähettäjällä ja vastaanottajalla piti tietenkin olla yhteiskäsitys siitä, mitkä pulssijonot vastasivat mitäkin merkkiä. Sen lisäksi määriteltiin merkkien ja sanojen välinen tauko ja niin edelleen. Siirtonopeus kuitenkin toteutui käytännössä lähettäjän ja vastaanottajan kykyjen mukaan. Viestintästandardin määrittelyssä riittää töitä. Jo vuoden 1872 Rooman kansainvälinen lennätinkonventio on 98 sivua pitkä dokumentti, tosin kaksikielinen.

Ensimmäinen binäärilogiikkaa eli nollia ja ykkösiä käyttänyt tietokone oli Konrad Zusen Berliinissä 1930-luvun lopulla suunnittelema ja rakentama Z1. Kolme vuosikymmentä myöhemmin tuli ajankohtaiseksi yhdistää tietokoneita verkon yli. Suuret tietokoneet olivat harvinaisia, ja tutkijoille haluttiin tarjota helpommin laskentaresursseja etäkäytön kautta. 1960-luvun lopulla Yhdysvaltain puolustusministeriön Advanced Research Projects Agency (ARPA) käynnisti hankkeen, jolla yhdistettiin eri tutkimuslaitosten tietokoneita samaan verkkoon (ARPANET).

ARPANETissä lähetetiin heti Apollo 11 -kuulennon ja Woodstock-festivaalin jälkeen vuonna 1969 ensimmäinen viesti toiselle tietokoneelle. Välimatkaa oli 500 kilometriä. Viesti, jonka piti olla sana ”login”, lähetettiin Kalifornian yliopistosta Los Angelesista (UCLA) Stanfordin tutkimuslaitokseen (SRI). Vastaanottava kone kuitenkin kaatui kahden ensimmäisen merkin jälkeen, joten esi-internetverkon ensimmäiseksi viestiksi jäi ”lo”. Syy tähän oli, että tiedonsiirtonopeus oli liiankin korkea. Kone oli valmis vastaanottamaan noin 10 merkkiä sekunnissa, kun verkon nopeus oli jopa 5 000 merkkiä sekunnissa. Bill Duvall, joka operoi vastaanottavaa konetta, vertasi tilannetta elävästi yritykseen täyttää vesilasia paloruiskulla.

Sitä mukaa kun ARPANET kasvoi, kävivät sen rajoitukset yhä selkeämmiksi. Suurin puute liittyi tietoliikenteen protokolliin, jotka eivät olleet tarpeeksi kehittyneitä viestien reititykseen verkossa eri tietokoneiden välillä. Suuri muutos tuli niin kutsutun Transfer Control Protocol/Internetwork Protocol -standardin (TCP/IP) myötä, joka mahdollisti erilaisten tietokoneiden keskustelun toistensa kanssa. ARPANET siirtyi TCP/IP-protokollaan 1. tammikuuta 1983: internet oli syntynyt.

Vuonna 1983 perustettiin myös Suomen korkeakoulujen ja tutkimuksen tietoverkko Funet. Se oli merkittävässä roolissa Suomen nousussa telekommunikaation edelläkävijäksi maailmassa. Se toimi osana pohjoismaista NORDUnetiä ja liitti Suomen internetiin vuonna 1988. Tämä oli ensimmäinen kerta, kun korkeakoulujen ja tutkimusverkkojen käyttäjille Yhdysvaltojen ulkopuolella avattiin pääsy internetiin. Tässä voidaan mainita, että Suomen yhteys internetiin kuitenkin katkaistiin nopeasti, kun Teknillisen korkeakoulun TKK:n koneelta yritettiin murtautua Yhdysvaltojen avaruushallinnon NASAn ja Yhdysvaltain energiaministeriön Lawrence Livermore National Laboratoryn tietojärjestelmiin. Yhteys palautettiin melko nopeasti neuvottelujen jälkeen, mutta tapaus kuitenkin alleviivaa, miten tärkeitä turvallisuusnäkökulmat ovat tietoliikenteessä.

Tämän jälkeen internet valloitti maailman. Tim Berners-Lee kehitti World Wide Webin eli www-protokollan 1989. Maailmanlaajuiseen käyttöön tämä uusi tapa ”selata nettiä” avattiin vuonna 1991. Internetin käyttö kasvoi räjähdysmäisesti vuonna 1993, kun NCSA Mosaic -selain julkaistiin. Tämä tarjosi tavalliselle käyttäjälle helpon väylän nettiin, ja Yhdysvalloissa www:n käyttö kasvoi vuodessa yli 300 000 prosenttia. Samana vuonna internet tuli koko kansan ulottuville myös Suomessa Finnish Communication and Internet Exchange – FICIX ry:n, Euroopan vanhimman internetpalveluntarjoajien yhdysliikennepisteen, kautta.

Internetin runkoverkossa suuret datamäärät liikkuvat lankoja eli valokaapeleita pitkin. Yksittäiset käyttäjät kuitenkin käyttävät internetiä suureksi osaksi mobiililaitteiden kautta joko suoraan kännykästä tai jonkun langattoman wifi-verkon yli. Lähtölaukaus mobiililaitteiden tiedonsiirron vallankumoukselle oli GSM-verkon tulo vuonna 1991. Ensimmäisen sukupolven matkapuhelinverkot, kuten NMT, olivat analogisia; toisen sukupolven (2G) myötä siirryttiin digitaaliseen, salattuun matkapuhelinliikenteeseen, ja siinä GSM kasvoi johtavaksi. Suomen Pankin pääjohtaja Harri Holkeri soitti ensimmäisen laajasti julkisuutta saaneen GSM-puhelun Tampereen apulaiskaupunginjohtajalle Kaarina Suoniolle silloisen Radiolinjan verkon kautta. GSM:n myötä luotiin yhteentoimiva digitaalinen matkaviestintästandardi ja siirryttiin erillisistä kansallisista järjestelmistä yhtenäiseen maailmanlaajuiseen verkkoon. GSM vakiinnutti asemansa standardina, ja se on ollut perustana johtaville standardeille eli 3G:lle (UMTS), 4G:lle (LTE) ja 5G:lle sekä tulevalle 6G-verkolle.

Nokia oli alalla aktiivinen ja loi GSM-standardia, rakensi infrastruktuuria, kehitti matkapuhelimia ja vei teknologiaa maailmalle. Se, että yhtiö sitoutui strategisesti GSM-teknologiaan jo varhain, vaikutti suoraan sen nopeaan kasvuun ja teki siitä

maailmanlaajuisesti johtavan televiestintäteknologian yrityksen – *early adopter*, malliesimerkki varhaisen omaksumisen hyödystä.

GSM-verkon myötä maailma sai käyttöönsä myös tekstiviestit. Short Message Service (SMS) tuli osaksi GSM-standardia pitkälti Matti Makkosen vision kautta, ja Makkonen tunnustetaankin nykyään tekstiviestin isäksi. Läpimurron kätilöinä toimivat Nokia ja Radiolinja: vuonna 1993 Nokian kännykät toivat tekstiviestit kuluttajille ja Radiolinja avasi ensimmäisenä maailmassa kuluttajien välisen tekstiviestipalvelun. Tekstiviesteistä kasvoi vuosien mittaan merkittävä viestialusta. Vaikka nykyään kilpailevat pikaviestipalvelut ovatkin kammenneet ohi suosiossa, tavallinen tekstiviesti on edelleen kovassa käytössä. Koska se kuuluu matkapuhelinverkkojen standardiin, tekstiviestisovellus löytyy jokaisesta kännykästä ja on varmin tapa lähettää viesti käytännössä mihin matkapuhelimeen tahansa.

Internetin alkuaikoina tietoliikennettä ei juurikaan salattu. Viestit, tiedostot ja salasanat kulkivat verkossa selkotekstinä. Tilanne muuttui 1990-luvulla, kun kaupalliset tahot kiinnostuivat internetistä toden teolla. Erityisesti kaupankäynti verkossa kiihdytti salauksen käyttöönottoa, jotta verkossa liikkuva tieto saatiin suojattua. Kun internetin käytössä siirryttiin langattomiin mobiiliverkkoihin, korostui tarve suojata yhteyksiä, koska salakuuntelu helpottui. Suomalainen teknologia oli jälleen avainasemassa. Tatu Ylönen kehitti vuonna 1995 Secure Shell -salausprotokollan (SSH), jolla internetin tietoliikennettä voitiin salata. Nykyään käytännössä kaikki internetissä kulkeva tieto on salattu jollain salausprotokollalla, selailipa sitten ravintoloiden lounaslistoja tai tarkasteli pankkipalveluja tai OmaKanta-tietoja.

Salauksen ja yksityisyyden tarve on jo useimmille meistä itsestäänselvyys, vaikka salauksen tasosta käydäänkin vilkasta keskustelua. Kvanttitietokoneiden myötä nykyinen salaus on kuitenkin vaarassa murtua. Internetin on siirryttävä kvanttiturvalliseen muotoon.

KVANTTIMEKANIIKKA PÄHKINÄNKUORESSA

Kvanttiteknologiat hyödyntävät fysiikan perusperiaatteita, joihin maailmankaikkeutemme perustuu: kvanttimekaniikan lakeja. Jotta voimme hahmottaa kvanttiinternetin mullistavaa luonnetta, lyhyt oppimäärä kvanttimekaniikan perusteista tulee tarpeeseen. Vaikka vietämmekin vuonna 2025 YK:n julistamaa kvanttitieteen ja -teknologian vuotta ja juhlistamme samalla kvanttimekaniikan satavuotista taivalta, emme vieläkään täysin ymmärrä *miksi* kvanttimekaniikka toimii. Tiedämme kuitenkin melko hyvin, *miten* se toimii ja vaikuttaa.

Ympäröivä maailmamme seuraa klassisen fysiikan lakeja, joissa kaikki muuttuu täysin ennustettavalla tavalla. Kun meillä on riittävä tieto nykytilanteesta, voimme selvittää, mitä seuraavaksi tapahtuu – ainakin periaatteessa. Jos tarkastelemme maailmaa voimakkaan suurennuslasin läpi, saavumme kuitenkin atomitasolle, kvanttimekaniikan maailmaan, jossa kaikki on toisin. Kvanttimaailmassa todellisuus on sumea kuin haamumaailmassa, jossa muodot ovat epämääräisiä ja katoavaisia.

Maailmankaikkeuden arvaamaton sattumanvaraisuus tarkoittaa, että emme voi edes periaatteessa tietää, mitä seuraavalla hetkellä tapahtuu.

Kvanttimaailmaa ohjaavat tietyt kvanttimekaaniset ilmiöt. Tässä yhteydessä tärkeimmät ovat *superpositio* ja *lomittuminen*, jota kutsutaan myös kietoutumiseksi. Superpositio tarkoittaa, että joku kvanttijärjestelmä voi olla samanaikaisesti useassa eri tilassa. Esimerkiksi elektroni voi olla samanaikaisesti kahdessa paikassa tai fotoni, valopartikkeli, voi olla samanaikaisesti kahdessa eri polarisaatiotilassa, sekä vaakaan että pystyyn polarisoitunut. Polarisaatio on tuttu aurinkolaseista, joissa vaakasuoraan polarisoitunut valo, joka heijastuu vedenpinnasta tai märästä tienpinnasta, suodatetaan pois. Kahden tilan superpositio katoaa, kun tila mitataan.

Lomittuminen on superpositiotakin ihmeellisempi. Kaksi tai useampi hiukkanen voi olla kytköksissä toisiinsa niin, että niiden tilat ovat riippuvaisia toisistaan. Jos yhden lomittuneen hiukkasen tila mitataan, toisen hiukkasen tila määräytyy välittömästi. Lomittumisen löysi Albert Einstein sen jälkeen, kun hän oli perehtynyt kvanttimekaniikan kaavoihin. Hän kuitenkin tulkitsi tämän osoittavan, että kvanttimekaniikan määrittelyssä on jotain vialla, koska ilmiö näytti rikkovan maailmankaikkeuden nopeusrajoitusta eli valon nopeutta, lomittuminen kun mahdollistaa välittömän vaikutuksen kahden hiukkasen kesken riippumatta niiden välisestä etäisyydestä. Vaikka kvanttitilat olisivat valovuosien päässä toisistaan, lomittumisen kautta niillä on jonkintasoinen nolla-ajassa tapahtuva yhteys. Einstein oli epäileväinen kvanttimekaniikan suhteen loppuun saakka, ja kirjeessä vuodelta 1952 hän kirjoitti seuraavasti:

> *Tämä teoria muistuttaa minua hieman äärimmäisen älykkään vainoharhakin harhajärjestelmästä, joka on koostettu epäjohdonmukaisista ajatuselementeistä.*
>
> ALBERT EINSTEIN

Lomittuminen on kuitenkin todellinen ilmiö, jonka osoittamisesta jaettiin vuoden 2022 fysiikan Nobel-palkinto. Lomittumista käytetään hyväksi sekä kvanttilaskennassa että kvanttikommunikaatiossa, johon myös rakenteilla oleva kvantti-internet perustuu.

KVANTTILASKENTA

Perinteiset tietokoneet perustuvat ihmisen laatimaan binääriseen järjestelmään, jossa kaikki laskenta tapahtuu nollien ja ykkösten kautta. Tietokone suorittaa tehtäväänsä melko yksinkertaisella logiikalla niin, että muistissa nollista tulee ykkösiä ja ykkösistä nollia. Perusinformaatioyksikkö eli bitti voi siis olla joko nolla tai yksi, ja tietokoneohjelmat ohjaavat sitä, milloin joku bitti muuttaa arvoaan.

Kvanttitietokoneet puolestaan käyttävät laskennassa hyödykseen kvanttimekaniikan ilmiöitä, kuten yllä mainittuja superpositiota ja lomittumista. Kvanttitietokoneen perustana on kvanttibitti eli kubitti. Kubitti voi olla superpositiossa, jossa se

on osittain nolla ja osittain yksi samanaikaisesti. Kubitit voivat myös olla lomittuneita keskenään, jolloin yhtä kubittia ohjaamalla voidaan vaikuttaa useaan kubittiin samalla kertaa. Tämä mahdollistaa tiettyjen matemaattisten ongelmien ratkomisen huomattavasti tehokkaammin kuin yksinomaan perinteisellä tietokoneella tai edes supertietokoneella voidaan tehdä. Tässä on kuitenkin hyvä huomata, että kvanttitietokoneet soveltuvat ainoastaan rajatulle ongelmajoukolle. Ne eivät siis ole korvaamassa perinteisiä tietokoneita vaan tulevat näiden rinnalle. Yhdessä supertietokoneet ja kvanttikoneet voivat ratkoa tiettyjä suuria ja vaikeita ongelmia, jotka ovat liian raskaita yksinomaan klassisten supertietokoneiden ratkottaviksi.

Kvanttikiihdytetty suurteholaskenta voi kuitenkin mullistaa laskennallista tiedettä ja tuotekehitystä tulevaisuudessa ennennäkemättömällä tavalla. Lupaavimmat alueet ovat materiaalitiede, kemiallinen katalyysi ja biokemialliset sovellukset, kuten lääketiede, sekä erinäiset optimointiongelmat. Myös tekoälyn ja kvanttilaskennan yhdistämiseltä odotetaan paljon. Kvanttilaskennan mahdolliset hyödyt ovat siis valtavat, mutta kolikolla on myös toinen puoli: tarpeeksi tehokas kvanttitietokone pystyisi murtamaan nykyään laajasti käytössä olevat salausmenetelmät.

KVANTTITEKNOLOGIAN VAIKUTUS TIETOJEN SALAUKSEEN

Nykyinternetissä valtaosa tiedosta liikkuu salattuna eli viestit on kryptattu jollain menetelmällä. Kryptografiassa tiedot salataan virtuaalisilla avaimilla. Yksinkertaisin esimerkki tästä on Caesarin salakirjoitus, jossa jokainen kirjain korvataan säännönmukaisesti toisella kirjaimella. Avain määrittelee säännön, tässä tapauksessa sen, miten monella kirjaimella siirrytään aakkosissa eteenpäin. Jos avain on yksi, a:sta tulee b ja kissa on salattuna ljttb. Salausta purkaessa siirrytään puolestaan aakkosissa taaksepäin, jolloin b:stä tulee a, joten salakirjoitus joufsofu on selkotekstinä internet. Salauksen purku on triviaalia, jos avain on tiedossa, ja vaikka avainta ei tiedä, salauksen purkaminen on helppoa ihan kynällä ja paperilla, koska vaihtoehtoja on pieni määrä.

Nykyisin käytetyt salausmenetelmät ovat huomattavasti monimutkaisempia. Tarkoituksena on, että ilman salausavainta salausta ei pitäisi voida murtaa edes tehokkaimmilla supertietokoneilla. Esimerkiksi AES-256-salauksessa avain on 256 bitin pituinen jono nollia ja ykkösiä. Niiden kaikkien läpikäyminen vaatisi 2 256 vaihtoehdon kokeilemista, mikä vastaa tutummin lukua 1 077 eli 1 ja 77 nollaa. Tämä on täysin mahdotonta sekä klassisille että kvanttitietokoneille.

AES- ja Caesarin salaus ovat niin kutsuttuja symmetrisiä salausmenetelmiä, jotka vaativat, että sekä lähettäjä että vastaanottaja tietävät avaimen etukäteen. Tämä on epäkäytännöllistä internetissä, jossa lähetetään jatkuvasti salattuja viestejä uusien päätepisteiden välillä. Symmetrisiä avaimia, vaikka ne ovatkin erittäin turvallisia, ei tämän takia voida suoraan käyttää.

1970-luvulla keksittiin menetelmä, jolla osapuolet voivat jaella ja vaihtaa salausavaimia lennosta. Tämä asymmetrinen, julkisiin ja yksityisiin avaimiin perustuva

salausmenetelmä mullisti tietoliikenteen kyberturvallisuuden. Ideana on, että viesti salataan julkisella avaimella ja salauksen jälkeen se voidaan avata ainoastaan yksityisellä avaimella. Viestin vastaanottaja ikään kuin jakelee vapaasti ja ilmaiseksi avoimia riippulukkoja (julkinen avain), joita kuka tahansa voi käyttää lukitakseen viestin sisältävän lippaan. Kun virtuaalinen lipas on lukossa, lukon voi avata ainoastaan vastaanottaja yksityisellä avaimellaan. Käytännössä lippaan viesti on toisen, symmetrisen salauksen avain, kuten AES-256-avain, jota sitten käytetään viestiliikenteen kryptaukseen avainvaihdon jälkeen. Karkeistaen julkisen avaimen salaus perustuu johonkin matemaattiseen ongelmaan, joka on helppo selvittää yhteen suuntaan (lippaan lukitseminen lukolla) mutta joka on käänteisenä (lippaan lukon avaaminen) erittäin vaikea ratkaista ilman avainta.

Yksi suosituimmista julkisen avaimen salausalgoritmeista on RSA-menetelmä. RSA perustuu oletukselle, että siinä missä kahden alkuluvun kertominen on tietokoneelle triviaalia, käänteinen ongelma on käytännössä mahdoton, kun luvut ovat tarpeeksi suuria. $3 \times 5 = 15$ on helppo lasku, ja myös käänteisesti, jos aloittaa luvusta 15, vastaus $15 = 3 \times 5$ voidaan laskea päässä. Se, että $5\,723 = 59 \times 97$, on jo vaikeampi. RSA 2048 -menetelmä perustuu 2 048-bittisiin lukuihin eli noin 600 numeroa pitkiin desimaalilukuihin, jotka ovat kahden noin 300 numeroa pitkän alkeisluvun tulo. Turvallisuus tulee siitä, että siinä missä kahden 300-numeroisen luvun kertominen on helppoa, sen keksiminen, mitkä nuo kaksi lukua ovat, jos tiedetään ainoastaan niiden 600-numeroinen tulo, veisi jopa tulevaisuuden tehokkaimmilta supertietokoneilta miljardeja ja taas miljardeja vuosia. Nykyään käytetään myös laajasti elliptisiin käyriin perustuvaa Elliptic-Curve Cryptography -salausta (ECC). Siinä matemaattinen ongelma on eri mutta muutoin perusperiaate sama: helppo yhteen suuntaan, vaikea vastakkaiseen.

Peter Shor julkaisi vuonna 1994 kvanttialgoritmin eli menetelmän, joka hyödynsi käänteisessä ongelmassa kvanttitietokoneita, jotka olivat tuolloin julkaisuvuonna vielä ajatusasteella. Shorin algoritmi tehoaa sekä RSA- että ECC-salauksiin, salatun internetin perustuksiin, mikä tarkoitti, että tämä ”kvanttitiirikka” rikkoisi internetin salauksen ja sitä myötä koko nykyinternetin. Shorin algoritmi kiihdytti sekä kvanttitietokoneiden että uusien salausmenetelmien kehitystä, ja nyt molemmat teknologiat ovat valmistumassa.

Kvanttitietokoneiden uhka salaukselle on merkittävä, ja siihen on varauduttava jo nyt siten, että vaihdetaan kvanttilaskennalle haavoittuvaiset salausmenetelmät kvanttiturvallisiin vaihtoehtoihin. Kvanttitietokoneet eivät vielä pysty ajamaan Shorin algoritmia suurille kokonaisluvuille, emmekä tiedä, milloin ne siihen pystyvät. Tähän voi mennä 10, 20 tai 50 vuotta, ja on tietenkin myös mahdollista, että kvanttikoneet eivät edes pitkällä aikavälillä kehity niin paljon, että Shorin algoritmi olisi ajettavissa sellaisenaan. Useimpien arvioiden mukaan tarpeeksi tehokkaat kvanttilaskimet ovat kuitenkin tulossa.

Toukokuussa 2025 Craig Gidney Googlen kvantti-AI-ryhmästä alensi 95 prosentilla arviota siitä, paljonko Shorin algoritmin suorittamiseen tarvitaan kubitteja. Aikaisemman arvion mukaan RSA 2048 -salauksen murtamiseen tarvittaisiin noin 20 miljoonaa kubittia. Uudella toteutuksella Shorin algoritmi vaatisikin vain miljoona fyysistä kubittia. Tämä vastaa noin 1 600:aa virhesietoista niin kutsuttua loogista kubittia. Esimerkiksi Suomen vuoden 2025 kvanttistrategian tavoitteena on saavuttaa 1 000 loogisen kubitin kotimainen kvanttikone vuoteen 2035 mennessä, mikä antaa osviittaa kehityksen arvioidusta aikataulusta.

Vaikka internetin salausta purkavaa kvanttitietokonetta ei vielä ole, uhkan muodostaa niin kutsuttu *harvest now, decrypt later* -toimintamalli, jossa internetissä liikkuvaa tietoa kerätään jo nyt odottamaan sitä, että salauksen murtamiseen soveltuva tekniikka valmistuu. Verkossa liikkuu jatkuvasti tietoa, jonka ei haluta päätyvän vääriin käsiin, ei nyt, ei 10:n eikä 50 vuoden sisällä. Esimerkiksi kansalaisten terveystiedot, yritysten liikesalaisuudet ja valtioiden tiedustelutiedot ovat arkaluontoisia ja sensitiivistä dataa vielä vuosikymmeniä sen jälkeen, kun tiedot ovat liikkuneet verkossa paikasta toiseen.

Shorin algoritmi on myös vain ensimmäinen julkistettu menetelmä, joka soveltuu salauksen purkuun. Ei ole mitenkään poissuljettua, etteikö tehokkaampaa algoritmia voisi kehittää. Ehkä sellainen on jo kehitetty mutta julkisuudelta piilossa. On myös mahdollista, että on olemassa algoritmi, joka ei ole yhtä yleinen kuin Shorin algoritmi mutta joka vaatii huomattavasti pienempiä kvanttilaskentaresursseja. Jos tällainen ”Shoretten” algoritmi pystyisi murtamaan vain vaikkapa prosentin murto-osan salausavaimista, ei se olisi hyväksyttävää, sillä riski olisi liian suuri.

Toinen syy siirtyä pois kvanttiturvattomista salausmenetelmistä liittyy tietoliikenteeseen ainoastaan epäsuorasti. Myös digitaaliset allekirjoitukset perustuvat tällä hetkellä salausmenetelmiin, jotka ovat murrettavissa kvanttitietokoneilla. Tämä vaatii muutosta jopa tietoliikenteen salausta kiireellisemmin. Niin kauan kuin turvattomalla salauksella allekirjoitetut asiakirjat ovat laillisesti sitovia, ne muodostavat ongelman, joka jatkuu pitkälle tulevaisuuteen. Tehokkaan kvanttikoneen avulla voidaan luoda aidosta erottamaton, vapaasti valittavissa olevalla päivämäärällä allekirjoitettu asiakirja, esimerkkinä vaikkapa vuonna 2040 luotu väärennös mukamas vuonna 2025 tehdyistä maakaupoista, lainojen takauksista, perintökirjeistä ja niin edelleen. Jotta tämä uhka voidaan minimoida, on vietävä läpi mahdollisimman pian lakimuutos, joka vaatii, että kaikki sähköiset allekirjoitukset perustuvat kvanttiturvallisiin algoritmeihin. Tämä poistaisi mahdollisuuden luoda tekaistuja mutta aidoilta näyttäviä asiakirjoja, jotka olisi päivätty lakimuutoksen jälkeen.

Kvanttiturvallisen internetin toteuttamiseksi on olemassa kaksi pääasiallista menetelmää: toinen on vaihtaa turvattomat salausalgoritmit uusiin, kvanttiturvallisiin algoritmeihin (*Post-Quantum Cryptography*, PQC), ja toinen on siirtyä kvanttimekaniikkaan perustuvaan avainjakeluun (*Quantum Key Distribution*, QKD). Tarkastelen seuraavassa kappaleessa molempia erikseen sekä sen jälkeen yhdessä.

Kvanttiturvallinen internet

KVANTTITURVALLINEN KRYPTOGRAFIA ELI PQC – UUTTA VANHAN PÄÄLLE

Kvanttiturvallisella kryptografialla (*Post-Quantum Cryptography*, PQC) tarkoitetaan salausalgoritmeja, jotka on suunniteltu vastustamaan kvanttitietokoneiden hyökkäyksiä, jotka voivat murtaa perinteiset salausmenetelmät. PQC:n tavoitteena on suojata digitaalista tietoa tulevilta kvanttitietokoneiden uhkilta sellaisilla matemaattisilla ongelmilla, joiden uskotaan olevan vaikeita myös kvanttitietokoneille.

Asymmetrinen, julkisiin avaimiin perustuva salaus on lähes kaikkien digitaalisten palvelujen perustana, olipa kyse sitten verkkopankkitoiminnasta, sähköisistä viranomaispalveluista tai laitteiden välisestä turvallisesta viestinnästä. Jos kuitenkin rakennettaisiin riittävän tehokas kvanttitietokone, se voisi käyttää Shorin algoritmin kaltaisia algoritmeja RSA- ja ECC-salauksen murtamiseen murto-osassa klassisten tietokoneiden vaatimasta ajasta.

Tämä uhka on sinänsä jo tiedostettu, ja viranomaiset ympäri maailmaa ovat siirtymässä PQC-salausalgoritmeihin. Nämä uudet algoritmit on suunniteltu niin, että ne ovat turvallisia sekä klassisia että kvanttilaskennan hyökkäyksiä vastaan. Perusperiaate on sama kuin nykyisin käytössä olevissa avaintenvaihtoalgoritmeissa, mutta matemaattinen ongelma on myös kvanttikoneille vaikea. Yhdysvaltain standardisointi- ja teknologiainstituutti National Institute of Standards and Technology (NIST) viimeisteli vuonna 2024 useita PQC-standardeja, kuten CRYSTALS-Kyberin salausavainten jakelua varten ja CRYSTALS-Dilithiumin digitaalisia allekirjoituksia varten.

PQC:hen ei pääse siirtymään niin, että pelkästään asentaa ohjelmistopäivitykset. Yksi suurimmista haasteista on PQC-algoritmien integrointi olemassa olevaan laitteistoon. Monet laitteet, kuten reitittimet, VPN-laitteet ja IoT-laitteet, perustuvat sulautettuihin salausmoduuleihin, joita on vaikea tai mahdoton päivittää ilman laitteiston vaihtamista. Esimerkiksi vanhemmat reitittimet, joiden laiteohjelmisto sisältää kiinteästi kytkettyjä RSA- tai ECC-toteutuksia, eivät välttämättä tue uusia PQC-algoritmeja. Tämä edellyttää massiivista ponnistusta infrastruktuurin päivittämiseksi sekä julkisella että yksityisellä sektorilla.

PQC-algoritmit vaativat tyypillisesti suurempia avainkokoja ja laskentaresursseja kuin nykyiset algoritmit. Tämä voi johtaa suorituskyvyn pullonkauloihin erityisesti laitteissa, joissa on rajallinen laskentateho. Haasteena on varmistaa päästä päähän -turvallisuus. Jos yksikin viestintäketjun osa käyttää edelleen haavoittuvaista salausta, koko järjestelmä voi vaarantua. Testaus- ja sertifiointiprosessien on oltava tiukkoja.

NIST:n vuonna 2024 julkaisemat uudet PQC-standardit ovat herättäneet suurta kiinnostusta maailmanlaajuisesti. Keskustelu siitä, pitäisikö Euroopan luottaa pelkästään NIST:n standardeihin vai kehittää omia ratkaisuja, on kuitenkin käynnissä. Historialliset ennakkotapaukset korostavat riskejä, joita liittyy siihen, jos ulkopuolisia standardeja aletaan käyttää sellaisenaan. Esimerkiksi NSA lisäsi standardiinsa (Dual EC Deterministic Random Bit Generator) tarkoituksellisesti heikkouksia, mikä johti laajaan epäluottamukseen ja lopulta standardin hylkäämiseen.

PQC:hen siirtyminen vaatii huomattavaa panostusta. Yhdysvaltain hallituksen vuonna 2024 laatiman raportin mukaan liittovaltion virastot tarvitsevat noin 7,1 miljardia dollaria, jotta ne saavat siirrettyä tärkeimmät tietojärjestelmänsä PQC:hen vuoteen 2035 mennessä. Tähän sisältyvät ne kustannukset, joita syntyy, kun inventoidaan kattavasti nykyiset salausjärjestelmät, päivitetään tai korvataan sellaiset laitteistot, jotka eivät pysty tukemaan uusia algoritmeja, koulutetaan kyberturvallisuushenkilöstö sekä suoritetaan tiukka testaus ja sertifiointi.

Suomen kokonaiskustannukset ovat absoluuttisesti mitattuina pienemmät, mutta jos kustannus skaalataan suoraan asukasluvun mukaan, vaikutukset henkeä kohti voivat kuitenkin olla vertailukelpoisia – tämä tarkoittaisi Suomessa yli 100 miljoonan euron kustannusta.

KVANTTIAVAINJAKELU ELI QKD – PERINTEISTÄ SALAUSTA PIDEMMÄLLE

PQC:tä pidetään yleisesti yksinkertaisempana ratkaisuna internetin suojaamiseen, mutta kvanttiavainjakelulla (*Quantum Key Distribution*, QKD) on kuitenkin ainutlaatuisia etuja. QKD käyttää kvanttimekaniikan periaatteita, joilla se tuottaa ja jakelee luonnostaan turvallisia salausavaimia. QKD:n turvallisuus on taattu fysiikan laeilla: salakuunteluyritykset johtavat häiriöihin, jotka voi havaita välittömästi. Salausta ei periaatteessa voi purkaa edes rajattomalla laskentateholla.

Kvanttiavainvaihto tapahtuu yksittäisten fotonien, valohiukkasten, kautta. Käyn lyhyesti läpi, miten se toimii BB84-protokollassa, joka on yleisin menetelmä tällä hetkellä. Aarne ja Bertta vaihtavat tässä avaimia, ja Sale haluaisi salakuunnella heitä.

1. Aarne lähettää Bertalle fotonikubitteja. Jokainen bitti (0 tai 1) koodataan fotonin kvanttitilaan kahdessa eri kannassa, jotka Aarne valitsee sattumanvaraisesti.
2. Bertta mittaa saapuvat fotonikubitit. Hän valitsee jokaiselle kubitille mittauskannan sattumanvaraisesti. Jos hän sattuu valitsemaan saman kannan kuin Aarne, hän vastaanottaa oikean bitin (0 tai 1), muutoin tulos on satunnainen.

3. Aarne ja Bertta vertaavat kantojaan julkisen eli klassisen kanavan kautta mutta eivät vertaa sitä, mitä bittejä he lähettivät. Ne bitit, joille he sattuivat valitsemaan saman kannan, muodostavat raakaversion salausavaimesta.
4. Aarne ja Bertta tarkistavat, tapahtuiko salakuuntelua. He paljastavat pienen osan salausavaimen raakaversiosta ja vertaavat tuloksia toisiinsa. Jos liian monta bittiä eroaa toisistaan, he tietävät, että joku (Sale) on häirinnyt avaintenvaihtoa. Bittien eroavaisuus johtuu siitä, että fotonikubittien kvanttitilat häiriintyvät, jos joku ulkopuolinen mittaa niitä.

Yllä olevan menettelyn jälkeen Aarnella ja Bertalla on bittijono nollia ja ykkösiä ja he voivat olla periaatteessa varmoja, että kenelläkään muulla ei ole niistä tietoa. Toinen vaihtoehto on, että he huomaavat, että Sale on ollut salakuuntelemassa tai häiritsemässä avaimen lähetystä.

Koska bittijono on täysin sattumanvarainen eikä se perustu mihinkään matemaattiseen algoritmiin, ei sitä voida murtaa millään tietokoneella. Tällä bittijonolla voidaan nyt salata lähetyksiä. On hyvä huomata, että QKD-menetelmät soveltuvat ainoastaan salaisen avaimen määrittelyyn, eivät suoraan viestien lähetykseen. Niissä ei voida valita etukäteen, mitkä bitit ovat käyttökelpoisia lähetyksen jälkeen, koska tämä riippuu siitä, mille biteille Aarne ja Bertta sattuivat valitsemaan saman kvanttikannan.

Teoreettisista vahvuuksistaan huolimatta QKD:llä on useita käytännön haasteita. Sen käyttöönotto edellyttää erikoislaitteistoja, kuten yhden fotonin ilmaisimia ja sellaisia lähettimiä, joiden asennus ja ylläpito on vielä kallista. Lisäksi QKD:n tehokas toimintaetäisyys on rajattu: tällä hetkellä käytännössä noin 100 kilometrin luokkaa. Tätä pidemmät yhteydet vaativat joko satelliittilinkkejä tai kvanttitoistimia, *quantum repeaters*, joita ei vielä ole saatavilla.

QKD-yhteyksiä voidaan rakentaa kaukana toisistaan olevien päätepisteiden välille satelliittien ja lasersäteiden avulla. Satelliitti-QKD:lla on kuitenkin omat ongelmansa. Satelliittien lisäksi tarvitaan maa-asemia, jotka toimivat vastaanottimina. Sen lisäksi, että maa-asemat maksavat paljon, ne ovat kooltaan suuria, tyypillisesti pienen talon kokoisia. Liikkuviakin maa-asemia kehitetään, mutta tällöinkin kyse on ajoneuvoilla liikuteltavista laitteistoista. Esimerkiksi langaton QKD-yhteys mobiililaitteissa kuuluu näin ollen vielä science fiction -kategoriaan. Koska satelliitti-QKD vaati ”näköyhteyden” satelliitin ja maa-aseman välillä, kirkas sää haittaa yhteyttä, kun aurinko häikäisee maa-asemaa, ja pilvinen sää estää yhteyden kokonaan.

PQC JA QKD KÄYTÄNNÖSSÄ

Kvanttitietokoneiden uhka tietoturvallisuudelle on tunnistettu laajasti ympäri maailman. Valtiolliset ja muut julkiset toimijat ovat julkaisseet kannanottoja ja suositelleet siirtymään erityisesti PQC:hen. Suomen kyberturvallisuusstrategia 2024–2035 painottaa: ”Suomen yhtenä strategisena tavoitteena on olla kriittisten salaustekno-

logioiden osalta omavarainen ja kvanttiuhkaan varautunut valtio 2030-luvun alkuun mennessä." Suomi (Traficom) on 17 muun EU-maan kanssa julkaissut lausuman, jossa suositellaan ottamaan PQC käyttöön hybridimuotoisena eli yhdistämään jo käytössä olevat salausmenetelmät PQC:hen. Yhdistelmä on täten ainakin yhtä turvallinen kuin nykyiset menetelmät, vaikka käytetystä PQC-menetelmästä löytyisikin tulevaisuudessa haavoittuvuuksia.

Myös Suomen kvanttiteknologiastrategia 2025–2035 asettaa välitavoitteeksi vuodelle 2030, että Suomen kriittiset tietovarannot ja tietoliikenneyhteydet on suojattu kvanttilaskennan kestäviksi PQC:n avulla. Tämä tavoite on kunnianhimoinen. EU:n tasolla tullaan todennäköisesti suosittelemaan vastaavaa siirtymää vuoteen 2035 mennessä. Tässä pienen maan ketteryys voi olla merkittävä kilpailuetu. Kun olemme etunenässä laajamittaisen kvanttiturvallisen tiedonsiirron käyttöönotossa, kasvanee esimerkiksi houkutus käsitellä luottamuksellista dataa Suomeen sijoitetuissa datakeskuksissa verrattuna sellaisiin maihin, joissa siirtymä seuraa hitaampaa aikataulua.

Myös kaupalliset toimijat ovat siirtymässä PQC:hen kiihtyvällä vauhdilla. Esimerkkeinä mainittakoon Applen iMessage, Zoomin videoneuvottelutyökalu sekä Metan Facebook ja WhatsApp. OpenSSH, laajalti käytetty avoimen lähdekoodin työkalupaketti SSH-protokollalle, siirtyi huhtikuussa 2025 käyttämään versiosta 10.0 lähtien oletusarvoisesti klassista ja kvanttiturvallista salausta yhdessä.

Myös QKD:tä edistetään voimakkaasti ympäri maailman. Euroopassa on käynnistetty EuroQCI-ohjelman puitteissa kaikissa EU:n jäsenvaltioissa pilottikokeilut, joissa QKD-verkon toimivuutta testataan kansallisesti. Suomessa toimii kansallisen kvanttikommunikaatioinfrastruktuurin hanke NaQCI.fi, jonka puitteissa VTT ja CSC ovat testanneet QKD:n toimivuutta julkisessa verkossa sekä Cinia ja Erillisverkot vastaavasti viranomaisverkossa. EuroQCI-ohjelma jatkuu seuraavaksi valtionrajat ylittävien QKD-verkkojen piloteilla, ja Suomi on ensimmäisessä vaiheessa varautunut yhdistymään Viron ja Ruotsin QKD-infrastruktuureihin. Pitkille välimatkoille suunnitellaan myös satelliittien kautta kulkevaa QKD:tä. Tässä Kiina on edelläkävijä, sillä se lähetti Micius-kvanttisatelliitin kiertämään maata jo 2016. Tänä vuonna raportoitiin mikrosatelliittien avulla tehdystä kvanttiavainvaihdosta Kiinan ja Etelä-Afrikan välillä 12 900 kilometrin välimatkalla. Myös Euroopassa on suunnitteilla useita QKD-satelliittien laukaisuja lähitulevaisuudessa. Nokia julkisti kesäkuussa 2025 suunnitelmansa pilotoida matalalla kiertoradalla olevien satelliittien käyttöä kattamaan erittäin pitkiä QKD-etäisyyksiä. Pilotti toteutetaan yhdessä Colt Technology Servicesin ja Honeywellin kanssa.

Lupaavista QKD-kenttätesteistä huolimatta eurooppalaiset virastot – Ranskan ANSSI, Saksan BSI, Alankomaiden NLNCSA ja Ruotsin puolustusvoimat – ovat julkaisseet yhteisen kannanoton siitä, että QKD:n ei pitäisi korvata klassista salausta, vaikka se periaatteessa tarjoaakin korkeaa turvallisuutta, ja että PQC on välttämä-

tön, jotta salausta voidaan käyttää laajamittaisesti. Myös USA:n kansallinen turvallisuusvirasto NSA on julkaissut yhteneviä lausumia.

QKD on kehittyvää teknologiaa. Laitteet eivät toimi vielä kovin hyvin, standardointi puuttuu ja toimintamatka kuituverkkoja pitkin on rajattu niin, että se vaatii useita niin kutsuttuja luotettuja solmupisteitä, *trusted nodes*, matkan varrella. Mobiililaitevalmiutta ei ole. Jotta kvanttiturvalliseen tietoliikenteeseen voidaan siirtyä mahdollisimman nopeasti, on PQC tällä hetkellä ehdottomasti ensimmäinen vaihtoehto.

QKD:hen on kuitenkin viisasta sijoittaa pitkällä tähtäimellä. Sen avulla voidaan luoda erittäin turvallinen runkoverkko kriittiselle viestinnälle. Päinvastoin kuin PQC, QKD-salaus ei ole riippuvainen siitä uskosta, että salausalgoritmien perustana oleville matemaattisille tehtäville ei tulla löytämään tehokasta ratkaisumenetelmää tulevaisuudessa. Vaikka QKD:n fysiikan lakeihin perustuva turvallisuus periaatteessa onkin murtamaton, käytännössä näin ei kuitenkaan ole. Menetelmä perustuu QKD-laitteisiin, joiden toimintaan täytyy pystyä luottamaan. Yhtenä EuroQCI-hankkeen tavoitteena on tukea eurooppalaisten QKD-laitteiden kehitystä. Vaikka *made in EU* -laitteisiin varmasti voidaan luottaa enemmän kuin *made in China* -versioihin, on täysin luotettava toimitusketju käytännössä mahdoton varmistaa.

Jos Suomi ottaisi QKD:n käyttöön strategisissa paikoissa, esimerkiksi valtion tietokeskusten välillä, se voisi saada arvokasta kokemusta ja edistää kvanttiverkkoteknologian innovointia. Toiseksi QKD voi luoda uusia liiketoiminta-aloja kvanttioptiikkaa hyödyntävien laitteiden valmistuksesta kvanttiturvallisen viestinnän palvelujen tarjoamiseen, mikä edistäisi talouskasvua ja loisi uusia työpaikkoja. QKD voidaan myös nähdä kvantti-internetin esiasteena.

Kvantti-internet

Kvantti-internet on kvanttitietokoneiden verkko, joka jonain päivänä lähettää ja vastaanottaa kvanttitiloihin koodattua tietoa kvanttimekaniikan ilmiöitä hyödyntäen. Nykyisessä klassisessa internetissä tieto siirtyy lähettäjältä vastaanottajalle bitteinä eli nollina ja ykkösinä lankoja ja langattomia verkkoja pitkin useiden välikäsien kautta. Kvanttimekaniikkaan perustuva kvantti-internet mahdollistaa uudenlaisen viestinnän, jossa hyödynnetään lomittumisen ja superposition periaatteita ja tiedonsiirtoon käytetään kvanttibittejä eli kubitteja.

Heti alkuun on hyvä huomata, että kvantti-internet ei tule korvaamaan tavallista internetiä vaan toimii sen rinnalla niin, että se mahdollistaa uusia sovelluksia sekä tiedonsiirtoon että tieteen tekemiseen. Siellä käytettäisiin lomittumiseen perustuvaa kvanttiavainjakelua, jolla saataisiin pystyyn erittäin turvallinen tietoverkko. On myös visioitu, että kvantti-internetissä voitaisiin käyttää hajautettua kvanttilaskentaa ja erittäin herkkiä kvanttianturiverkkoja. Vaikka kvantti-internet on vielä

kehitteillä, sillä on potentiaalia mullistaa kyberturvallisuutta ja tutkimusta tavoilla, joihin klassinen teknologia ei pysty vastaamaan. Seuraavaksi tarkastelemme sen tärkeimpiä sovelluskohteita.

YKSITTÄISESTÄ QKD-YHTEYDESTÄ KOKONAISEEN VERKKOON

Kävin edellä lyhyesti läpi QKD:n perusteet ja nykytilan. Perinteisessä QKD:ssä suojatut avaimet jaetaan suoraan kahden osapuolen välillä erityistä kvanttikanavaa pitkin, mikä rajoittaa verkon ulottuvuutta ja joustavuutta. Yhdistämällä yksittäiset kahden pisteen väliset QKD-linkit päästään maailmanlaajuiseen kvantti-internetiin tai ainakin sellaiseen, joka kattaa maapallon osittain.

Kun aletaan kehittää kvantti-internetin protokollia ja arkkitehtuuria, pitää ensi sijassa keskittyä kvanttitoistimien ja lomittumisen vaihdon tekniikkaan, jotta sillä kyetään jakamaan lomittuneita tiloja useiden solmujen välillä pitkien etäisyyksien päähän. Tämä mahdollistaa laajan käytön ja kvanttitiedon dynaamisen reitityksen aivan kuten klassisessa internetissä. Suurin muutos on siirtyä yksinkertaisista, lineaarisista QKD-protokollista monimutkaisiin, kietoutumiseen perustuviin verkkoprotokolliin, jotka edellyttävät synkronointia, kvanttimuistia ja reaaliaikaista koordinointia useiden kvanttisolmujen välillä.

Jos laaja kvantti-internet toteutuisi, myös arkipäiväisestä tietoliikenteestä tulisi erittäin hyvin suojattua, ainakin osittain. Esimerkiksi mobiililaitteisiin ei ole mahdollista luoda luotettavaa QKD-yhteyttä edes pitkällä aikavälillä. Aivan kuten tavallisessa internetissä myös kvantti-internetissä turvallisuus määrittyy heikoimman linkin kautta. Vaikka itse kvanttikanava kahden pisteen välillä olisi turvattu, voidaan esimerkiksi päätepisteiden laitteisiin edelleen kohdistaa tietomurtoja joko fyysisesti tai ohjelmistojen ja ohjelmistopäivitysten kautta. Kvantti-internet ei siis kokonaan poista salakuuntelun mahdollisuutta, vaikka tekeekin siitä entistä vaikeampaa.

KVANTTITIETOKONEIDEN YHDISTÄMINEN VERKON YLI

Kvantti-internet voisi yhdistää kvanttitietokoneita ympäri maailman ja muodostaa hajautetun kvanttilaskentaverkon. Tällöin kvanttitietokoneet voisivat jakaa resursseja ja laskentakuormaa, mikä lisäisi kokonaislaskentatehoa.

Vaikka hajautetun kvanttilaskennan teoreettiset edut ovat huomattavat, tekniset haasteet tämän toteuttamiseksi ovat kuitenkin valtavat. Jotta laskentatehon lisä olisi merkittävä, tulisi useiden kubittien pysyä lomittuneina kvanttitietokoneiden välillä. Usealla kvanttikoneella tehtävät laskutoimitukset pitäisi myös synkronoida hyvin tarkasti koneiden ja yksittäisten kubittien kesken.

Nykyiset kvanttilaitteistot ovat yhä monien läpimurtojen päässä siitä, että niiden varaan voisi luotettavasti pystyttää tällaisen verkoston. Kvanttikoneita ei pystytä yhdistämään toisiinsa vielä pitkään aikaan kovin pitkien välimatkojen päästä. Edes perinteisiä supertietokoneita ei ole koskaan yhdistetty niin, että eri paikoissa sijaitsevat prosessorit ratkoisivat samaa ongelmaa rinnakkain. On huomattavasti

helpompaa ja tehokkaampaa yhdistää suorittimia, sekä klassisia että kvantti-sellaisia, saman paikallisen erikoistuneen verkon kautta kuin internetin yli.

KVANTTI-INTERNET TUTKIMUSLAITTEISTONA

Ehkä mielenkiintoisin sovelluskohde kvantti-internetille on käyttää sitä hajautettuna, valtavana tieteellisenä tutkimuslaitteistona. Viestinnän ja laskennan lisäksi kvantti-internet voi tukea kvanttianturien verkkoja. Kvanttianturit voivat olla tietyissä käyttökohteissa klassisia antureita tarkempia. Niitä voidaan käyttää geologian, ilmaston seurannan ja biolääketieteellisen diagnostiikan sovelluksissa. Kvantti-internet mahdollistaisi sen, että tällaiset anturit voisivat jakaa lomittuneita tiloja ja korreloida mittauksia suurella tarkkuudella suurten etäisyyksien päähän.

Yksi lupaavimmista sovelluksista on kvanttikellojen synkronointi. Yhdistämällä atomikelloja toisiinsa lomittuneiden fotonien avulla voidaan saavuttaa ennennäkemätön tarkkuus ajanmittauksessa. Tämä parantaisi maailmanlaajuisia satelliittinavigointijärjestelmiä (GNSS) sekä mahdollistaisi erinäisiä fysiikan kokeita, kuten yleisen suhteellisuusteorian testaamisen aiempaa suuremmalla tarkkuudella. Kvanttiverkko voisi synkronoida eri mantereilla sijaitsevien laboratorioiden kelloja, jolloin havaittaisiin pienimmätkin ajanvaihtelut, jotka saattaisivat viitata uusiin fysikaalisiin ilmiöihin.

Kvantti-internet voi edistää hajautettujen kvanttianturiverkkojen luontia. Nämä koostuisivat kvanttikanavien kautta toisiinsa liitetyistä antureista, jotka jakaisivat lomittuneita tiloja, jotta saavutettaisiin klassisen rajan ylittävä herkkyys. Tällainen maapallon kokoinen tutkimuslaitteisto on todennäköisesti helpompi pystyttää kuin kvanttitietokoneita yhdistävä verkko, koska keskinäistä lomittumista vaativien kubittien määrä on pienempi. Esimerkiksi kvanttimagneettimittareiden verkostoa voitaisiin käyttää maapallon magneettikentän pienen pienten muutosten seurantaan, mikä hyödyttäisi geofysikaalisia tutkimuksia tai jopa seismisen toiminnan ennustuksia.

Kvanttiantureiden verkko voisi myös muodostaa erittäin herkän interferometrin, jolla voitaisiin havaita painovoima-aaltoja ja tutkia gravitaatiokentän vaihteluita suurilla etäisyyksillä. Eri kvanttianturiverkkojen myötä havainnoitaisiin entistä tarkemmin myös muita ilmiöitä, kuten kosmista säteilyä tai kaikkein pienimpiä vaihteluita aika-avaruudessa. Tällaiset havainnot voisivat antaa uutta tietoa pimeästä aineesta, tarjota uusia koeasetelmia kvanttigravitaatioteorioille tai johtaa jopa siihen, että löydettäisiin aiemmin tuntemattomia kosmisia tapahtumia. Yleisesti ottaen kvantti-internetin kautta kytketyt kvanttianturit tarjoaisivat työkaluja ymmärtää maailmankaikkeuden saloja aiempaa syvemmin.

MAAN ULKOPUOLINEN KVANTTI-INTERNET

Kvantti-internet Kuun kamaralla voi kuulostaa tieteiskirjallisuudelta mutta voi olla todellisuutta nopeammalla aikataululla kuin ensin ajateltuna voisi kuvitella. Nokia kokeili pystyttää 4G-mobiiliverkon ensimmäistä kertaa Kuuhun aikaisemmin tänä

vuonna eli 2025. Vaikka koe ei täysimääräisesti onnistunutkaan, osoitti se kuitenkin toteuttamiskelpoisuutensa. Jos kvantti-internet pystytettäisiin Kuuhun, se voisi joiltain osilta johtaa jopa toimintavarmempaan verkkoon kuin maapallolla.

Kvantti-internet hyötyy Maassa olevasta valokuitu- ja satelliitti-infrastruktuurista, mutta ilmakehän häiriöt, kuitusignaalihäviöt pitkillä etäisyyksillä ja kaupunkien sähkömagneettinen kohina voivat heikentää kvanttisignaaleja. Kuussa tyhjiöympäristö voisi turvata häiriöttömämmän kvanttilähetyksen, jolloin tietyt kokeet olisi mahdollisesti helpompi toteuttaa. Vakaa näköyhteys ja mahdollisuus perustaa omia maa-asemia ilman Maan sähkömagneettista ruuhkaa tarjoavat Kuulle lisäetuja. Kuun kvanttiverkon rakennukseen liittyy kuitenkin huomattavia esteitä erityisesti logistiikan puolella. Sinne on kuitenkin suunnitteilla pysyviä kuuasemia, jolloin osa haasteista lieventyy selvästi.

Kvanttiverkko, joka ulottuisi maapallolta Kuuhun, voisi mahdollistaa vieläkin tarkempia tieteellisiä kokeita kvanttiturvallisen QKD-verkon lisäksi. Muun muassa Yhdysvaltain avaruushallinto NASA on tarkastellut tätä mahdollisuutta erillisessä hankkeessaan (Deep Space Quantum Link). Vieläkin pidemmän matkan kvanttilinkkejä on mietitty esimerkiksi Maan ja avaruusalusten tai Maan ja Marsin välille.

Pidemmän aikavälin uhkia internetille

Kvanttitietokoneiden tuoma uhka on ainoastaan yksi monista haasteista tulevaisuuden internetille ja kokonaisturvallisuudelle. Suomen tietoliikenneyhteyksiin vaikuttavat lukuisat tekijät, jotka ulottuvat ympäristön, yhteiskunnan, ilmakehän ja tähtitieteen alueille. On ratkaisevan tärkeää ymmärtää näitä vaikutuksia, jotta voidaan kehittää kestävää digitaalista infrastruktuuria.

Ympäristön osalta auringon aktiivisuus, kuten auringonpurkaukset, voi aiheuttaa geomagneettisia myrskyjä, jotka häiritsevät sähköverkkoja ja satelliittiviestintää. Suomen pohjoinen sijainti tekee meistä erityisen alttiita tällaisille häiriöille, jotka voivat vaikuttaa tietoliikenneyhteyksiin.

Ilmastonmuutos lisää sään ääri-ilmiöitä. Jos voimakkaat sateet ja myrskyt lisääntyvät, se voi pahentaa jokien tulvia sisämaassa sekä rannikkotulvia erityisesti Suomenlahden satamakaupunkien ympäristössä. Tulvat voivat vahingoittaa maanpäällisiä valokuitukaapeleita, tietoliikennekeskuksia ja voimalaitoksia, jotka ovat kriittisiä internetpalvelujen jatkuvuudelle. Merikaapeleiden laskeutumispaikat puolestaan sijaitsevat usein alavilla rannikkoalueilla, ja kun myrskytulvat yleistyvät ja voimistuvat, ovat laskemispaikat aiempaa suuremmassa vaarassa joutua tulvan alle. Jopa tilapäinen tulva voi tuhota kriittisen elektroniikan tai vaatia kalliita korjauksia ja jälkiasennuksia.

Yhä kehittyneemmät kyberhyökkäykset aiheuttavat merkittäviä riskejä Suomen tietoinfrastruktuurille. Valtioiden tukemat toimijat ja järjestäytyneet tietoverkkorikolliset voivat kohdistaa hyökkäyksiä kriittisiin järjestelmiin, mikä voi johtaa tietomurtoihin tai palveluhäiriöihin. Suomen kyberturvallisuusstrategiassa 2024–2035 näihin haasteisiin vastataan parantamalla kansallisia kyberpuolustuskykyjä. Kasvavat geopoliittiset jännitteet voivat myös johtaa merenalaisten kaapeleiden ja muiden kriittisten infrastruktuurien sabotointiin. Viimeaikaiset tapahtumat Itämerellä ja Suomenlahdella ovat tietenkin lisänneet huolta tällaisista haavoittuvuuksista. Suomi liittyikin vuonna 2024 New Yorkin julkilausumaan merikaapeliturvallisuudesta. Siinä sovittiin yhteisistä tavoitteista ja keinoista vahvistaa merikaapeleiden turvallisuutta ja toimintakykyä.

Internet voi myös vähitellen pirstaloitua geopoliittisten linjojen mukaan, jolloin siitä tulee niin kutsuttu *splinternet*. Jos erimielisyydet internetin hallinnasta jatkuvat demokratioiden ja autoritaaristen hallintojen välillä, voimme nähdä erillisiä teknisiä standardeja tai jopa täysin erillisiä verkkoja. Tämä on pulma Suomelle, joka on tiukasti mukana avoimen internetin ja oikeusvaltioperiaatteen leirissä. Toisaalta suomalaiset käyttäjät ja yritykset hyötyvät maailmanlaajuisesta internetistä, mutta toisaalta Suomen on varauduttava siihen, että osa maailmaa rajoittaa yhteyksiä tai sisältöjä. Venäjä on jo viime vuosina kokeillut eristää internetinsä (Runet) maailmanlaajuisesta verkosta.

Internet ei ole vain tekninen vaan myös taloudellinen verkko. Suomen talous digitalisoituu entisestään. Etätyö, verkkopalvelut ja tekoälypohjainen teollisuus vaativat nopeaa ja luotettavaa verkkoa, joten internetin luotettavuus on taloudellinen prioriteetti. Mitä tulee kriittisiin palveluihin, yksi haaste on riippuvuus ulkomaisista teknologiajäteistä. Pakotteiden ja kauppasotien myötä joidenkin alustojen tai laitteistojen käyttöä saatetaan rajoittaa. Suomi sai maistiaisen tästä ongelmasta 5G-infrastruktuurin kanssa. Monet maat joutuivat punnitsemaan, miten riippuvainen kannattaa olla edullisista kiinalaisista laitteista, kun on mietittävä samalla turvallisuusnäkökulmaa. Omat teknologiset valmiudet vähentävät riippuvuusriskejä. Vapaan ja samalla turvallisen internetin ylläpito edellyttää järkevää politiikkaa. Suomi panee EU:n kautta täytäntöön uusia säädöksiä, kuten NIS2-direktiivin, joka nostaa kyberturvallisuusvaatimuksia infrastruktuurin ylläpitäjille.

Kaikki tarvittavat päivitykset fyysisestä kaapelin suojauksesta kvanttiturvallisuuteen maksavat sen verran paljon, että se ei ole taloudellisesti lainkaan vähäpätöistä. Investoinnit jättimäisiin hankkeisiin, kuten arktisiin kaapeleihin tai kansallisiin kvanttiverkkoihin, edellyttävät väkiluvultaan pienessä maassa joko valtion rahoitusta tai kansainvälistä kustannusten jakoa. Tähän mennessä Suomi on osoittanut halukkuutta investoida digitaaliseen infrastruktuuriin, koska sitä pidetään strategisena voimavarana. Poliittinen tahto on ratkaisevan tärkeää: johtajien on tunnustettava, että menot kyberpuolustukseen tai varajärjestelmiin ovat ikään kuin vakuutus maan taloudelle ja turvallisuudelle. Varautumisen käsite on Suomessa perinteisesti syvälle juurtunut. Jatkakaamme tätä myös tietoliikenteen osalta.

TIEDONSIIRRON UUDET TEHOKKUUSVAATIMUKSET

Vaikka telekommunikaation infrastruktuuri on Suomessa perinteisesti ollut vahva, olemme jäämässä jälkeen kiinteän nettiyhteyden nopeudessa. Suomi oli mediaaninopeudella 155 Mb/s sijalla 40, kun internetyhteyksien suorituskykyä testaava Ookla vertaili 155:tä maata keskenään huhtikuussa 2025. Esimerkiksi kaikki Pohjoismaat ovat tilastossa Suomea edellä. Vertailun vuoksi: top 10 -joukkoon pääsy vaatisi siirtonopeutta 252 Mb/s. Mobiililaajakaistan kohdalla tilanne on parempi. Siinä Suomi on 104 maan vertailussa nopeudella 146 Mb/s sijalla 20. Tämänhetkinen top 10 -sijoitus, vähintään 198 Mb/s, vaatisi vain hieman nopeammat yhteydet.

Tällä hetkellä valtaosa kuluttajien internetkäytöstä ei vaadikaan juuri suurempaa nopeutta. Mobiililaajakaistalla käyttää sujuvasti esimerkiksi suoratoistopalveluja. Tulevaisuudessa tarvittava yhteysnopeus voi kuitenkin kasvaa räjähdysmäisesti. Immersiivisten metaversumien eli virtuaalitodellisuuden (*virtual reality*, VR) tai lisätyn todellisuuden (*augmented reality*, AR) massiivinen käyttöönotto voi nostaa datan kulutuksen ennennäkemättömiin mittoihin, mikä haastaa Suomen verkot.

Reaaliaikainen etäkäyttö ja etärobotiikka, kuten kirurgisten toimenpiteiden suoritus etänä tai teollisuusrobottien tai lennokkien käyttö etänä vaarallisissa ympäristöissä, onnistuvat teräväpiirtovideon ja anturitietojen avulla. Tällöin reaaliaikainen multisensorinen data (video, haptinen palaute, ympäristöanturit) on siirrettävä luotettavasti ja mahdollisimman pienellä viiveellä, jotta pystytään varmistamaan tarkka ohjaus. Tämä vaatii myös suurta siirtonopeutta, jotta voidaan käsitellä samanaikaisia HD- tai 4K-videosyötteitä useista eri kuvakulmista. Hätätilanteissa verkon luotettavuus ja alhainen viive voivat kirjaimellisesti pelastaa hengen. Esimerkiksi ambulanssista voidaan lähettää potilaan telemetriaa matkalla sairaalaan tai voidaan käyttää lisättyä todellisuutta, jonka avulla etälääkäri voi avustaa kenttäleikkauksissa. Luotettavan etälääketieteen käyttöönotto Suomen kaltaisessa harvaan asutussa maassa voi parantaa palveluiden saatavuutta haja-asutusalueilla, joilta on pitkä matka lähimpään suureen sairaalaan. Tällaiset lääketieteelliset sovellukset vaativat nopeuden lisäksi myös verkon priorisointia, jotta muu liikenne ei hidasta kriittisten terveystietojen kulkua.

Massiivisesti hajautettu tekoäly ja reunalaskenta, *edge computing*, voivat myös nostaa datansiirtotarvetta. Kotitalouksissa tekoälymallien käyttö kasvanee tulevaisuudessa esimerkiksi kehittyneen puheenkäsittelyn, reaaliaikaisen kääntämisen ja immersiivisen pelaamisen myötä. Automatisoidut kodit, ajoneuvot ja työpaikat voivat tuottaa teratavuja dataa päivässä, jolloin reaaliaikainen synkronointi ja varmuuskopiointi edellyttävät tehokasta laajakaistaa.
Myös aivokäyttöliittymät (*Brain-Computer Inteface*, BCI) eli laitteet, jotka tallentavat ja välittävät yksityiskohtaisia hermosignaaleja joko lääketieteelliseen käyttöön tai kehittyneeseen ihmisen ja tietokoneen vuorovaikutukseen, tuottavat paljon dataa. Aivosignaalien näytteenottotaajuus voi olla suuri. Reaaliaikaiset sovellukset, kuten robottiraajat tai kehittyneet virtuaaliset avatarit, edellyttävät vakaita ja nopeita laajakaistayhteyksiä.

Tulevaisuudessa kaistaleveyden tarve kasvaa Suomessa huomattavasti. Suomen internetin runkoverkko on erittäin hyvin kytketty muuhun maailmaan siirtonopeuden osalta. Toukokuussa 2025 CSC – Tieteen tietotekniikan keskus, Nokia ja hollantilainen SURF testasivat ennätysnopeaa kvanttiturvallista valokuituyhteyttä CSC:n Kajaanin datakeskuksen ja Amsterdamin välillä. Data kulki 3 500 kilometrin matkan yli 1,2 Tb/s:n nopeudella. Kuluttaja- ja yrityskäytön puolella pitää kuitenkin panostaa laajakaistan infrastruktuurin päivitykseen ja erityisesti kiinteisiin valokuituyhteyksiin.

Nopeat verkkoyhteydet mahdollistavat uusia toimialoja kuten sovelluskehitystä, verkkopalveluita ja digitaalista mediaa sekä tehostaa nykyisiä toimialoja. Nopeat kuituverkot ja laaja 5G/6G-kattavuus tarjoavat yrittäjille hedelmällisen maaperän rakentaa ja testata uusia suuren kaistanleveyden ja matalan viiveen palveluja. Yritys, joka haluaa esimerkiksi pilotoida holografista oppimisalustaa tai etälääkärirobottia, tekee sen todennäköisesti maassa, jossa verkko voi tukea sitä laajamittaisesti – mailla, joilla on verkoissaan kapasiteettivaraa voivat ottaa käyttöön uusia teknologioita muita nopeammin. Tämä voi luoda itseään vahvistavan kehityksen, jossa vankka infrastruktuuri houkuttelee teknologiainvestointeja, jotka puolestaan lisäävät innovointia ja taloudellista toimintaa.

Kansainvälisen yhteistyön tuomat mahdollisuudet

Suomella on hyvät mahdollisuudet hyötyä kansainvälisestä yhteistyöstä ja globaaleista markkinoista, kun kehitetään kvanttiturvallista kommunikaatiota. Erityisesti kannattaa sitoutua yhteistyöhön Pohjoismaiden, Euroopan unionin ja NATOn kanssa mutta myös laajempien kansainvälisten organisaatioiden kanssa. Hyvä esimerkki maamme tunnustetusta asemasta kvanttiteknologioiden saralla on se, että Suomi johtaa EU:n puolustukseen liittyvää kvanttiteknologiahanketta Quantum Enablers for Strategic Advantage (QUEST). Hankkeen tavoitteena on hyödyntää kvanttiteknologiaa puolustusvalmiuksien parantamiseksi ja samalla edistää Euroopan autonomiaa, joustavuutta ja turvallisuutta. Samalla kun hyödynnämme kansainvälisesti tunnustettua asiantuntemustamme kvanttiteknologian, kyberturvallisuuden ja digitaalisen infrastruktuurin alalla, voimme edelleen vakiinnuttaa asemaamme keskeisenä toimijana kehittyvässä kvanttiturvallisen viestinnän ekosysteemissä.

Pohjoinen sijainti on haaste erityisesti langattomien verkkojen ja satelliittiyhteyksien kannalta. Samalla maantieteellinen sijaintimme on strategisesti merkittävä: turvallisten kvanttiviestintävalmiuksien luominen arktisen alueen läheisyyteen auttaa vahvistamaan Pohjois-Euroopan ja arktisen alueen toiminta- ja puolustuskykyä. Arktisen alueen kaupallinen ja sotilaallinen merkitys kasvaa tulevaisuudessa

huomattavasti. Tässä meillä on mahdollisuus vahvistaa rooliamme Pohjois-Euroopan turvallisuuden ja teknologisten innovaatioiden tarjoajana. Voimme edistää NATOn toimintavarmuutta siten, että tarjoamme arktiselle alueelle kestäviä, kvanttiturvallisia viestintäratkaisuja. Jos Suomi esimerkiksi isännöisi kvanttiviestinnän testausympäristöä, se asettaisi meidät eturintamaan sekä EU:n että NATOn pyrkimyksissä varmistaa kvanttiturvallinen viestintäkyky.

Suomelle olisi eduksi lisätä kansainvälistä yhteistyötä myös muissa verkostoissa, kuten eurooppalaisessa Quantum Internet Alliancessa (QIA). QIA on asettanut tavoitteekseen rakentaa maailman ensimmäinen globaali kvantti-internet, *made in Europe*. Keskeisenä osana tätä pyrkimystä on kehittää eurooppalaisten yritysten ekosysteemiä, joka muun muassa toimittaisi komponentteja kvantti-internetin tarpeisiin. Kun suomalaiset yritykset ovat aktiivisesti mukana toiminnassa, voi niille avautua laaja uuden teknologian markkina-alue.

Kun olemme varhaisessa vaiheessa mukana kehittämässä ratkaisuja uusilla aloilla, kuten arktisissa kvanttiverkoissa ja kvanttikestävässä kyberturvallisuudessa, Suomelle avautuu mahdollisuus vallata arvokkaita markkinasegmenttejä globaalissa kvanttitaloudessa, jonka ennustetaan kasvavan nopeasti 2030-luvulta alkaen. Lisäksi kansainvälisellä yhteistyöllä varmistetaan, että suomalaiset tutkimuslaitokset ja yritykset saavat käyttöönsä johtavia osaajia, yhteistä infrastruktuuria ja yhteistoiminnallista innovointia, mikä nopeuttaa kotimaisten valmiuksien kehittämistä. Strategiselta kannalta, kun Suomi sitoutuu asiaan ennakoivasti, pystymme paitsi turvaamaan oman kriittisen viestintämme myös osallistumaan aktiivisesti maailmanlaajuisten normien, standardien ja käytäntöjen määrittämiseen kvanttiverkkojen osalta.

Yhteenveto

Kvanttiteknologiat vaikuttavat jo nyt internetiin. Näkyvin käynnissä oleva muutos liittyy kvanttiturvallisten salausmenetelmien, PQC:n, käyttöönottoon. Tämä on kiireellisin toimenpide, jotta yhteiskunnan kokonaisturvallisuutta voidaan suojata tulevilta kvanttitietokoneilta. Siirtymään on sitouduttu Suomen ja EU:n tasolla – nyt on tärkeintä toimeenpano.

Kvanttiavainjakelu, QKD, on myös saamassa tulta alleen. Suomi osallistuu EU:n laajuiseen hankkeeseen kytkeä Eurooppa yhtenäiseen verkkoon, joka on suojattu salakuuntelulta fysiikan lakeihin perustuvalla tekniikalla. QKD-teknologia on vielä melko varhaisessa kehitysvaiheessa, eikä se tulevaisuudessakaan sovellu tiedonsiirron turvaamiseen yleisesti. Kriittisille kiinteille yhteyksille QKD:n ja PQC:n yhteiskäyttö tarjoaa kuitenkin ennennäkemätöntä tietoturvaa.

Kasvanut tietoturva on myönteistä yksittäisen käyttäjän, järjestön tai yrityksen kannalta. Yhteiskunnallisella tasolla on keskusteltu jo pitkään siitä, pitäisikö salauksen vahvuutta rajoittaa. Jo olemassa olevat salausmenetelmät pystyvät käytännössä täysin estämään sen, että salauksen voisi purkaa, ainakin ennen kvanttitietokoneiden läpimurtoa. Tämä voi kasvattaa houkutusta sisällyttää hyväksytyille salausstandardeille takaportteja eli piilotettuja menetelmiä purkaa salaus. Takaportteja on kuitenkin käytännössä mahdotonta tehdä turvallisesti eli niin, että salauksen kiertävä menetelmä pysyisi varmasti ainoastaan keksijävaltion tai -viraston tiedossa. Riski esimerkiksi arkaluontoisten henkilötietojen tai arvokkaiden yrityssalaisuuksien vuodolle olisi korkea. Tästä huolimatta jotkut tahot voivat yrittää heikentää salauksen tasoa näennäistä tasoa alemmaksi. Tarkkaavaisuus on paikallaan erityisesti silloin, kun otetaan käyttöön uusia standardeja. Kryptoketteryys, mahdollisuus pienellä vaivalla vaihtaa heikoksi tai epäilyttäväksi todettu salausalgoritmi toiseen, tulee huomioida tarkasti.

QKD-verkko on tosiasiallisen kvantti-internetin esiaste. Kvantti-internet ei korvaa tavallista internetiä, aivan kuten kvanttitietokoneet eivät korvaa perinteisiä tietokoneita eikä kvanttigravimetri keittiövaakaa. Sen sijaan kvanttiteknologia laajentaa olemassa olevan tekniikan sovellusalueita merkittävällä tavalla. Kvantti-internet mahdollistaa huipputurvallisen tiedonsiirron lisäksi aivan uutta tiedettä ja tutkimusta. Se voidaan nähdä myös massiivisen kokoisena tutkimuslaitteistona, joka antaa työkalut selvittää maailmankaikkeuden mysteerejä uudella tavalla.

Kvanttikommunikaation kokonaismarkkinoiden on ennustettu kasvavan voimakkaasti lähivuosina. Konsulttiyhtiö McKinsey arvioi, että globaali kokonaismarkkinapotentiaali kasvaa noin 9–13 miljardiin euroon vuoteen 2035 mennessä. Kun kysyntä kasvaa maailmanlaajuisesti, Suomi voi vahvalla panostuksella luoda merkittävää vientiteollisuutta.

Internetiä ei keksitty Suomessa, mutta Suomesta nousi telekommunikaation suurvalta, koska useat tahot ymmärsivät aikaisessa vaiheessa, miten tärkeää uusi teknologia on. Kvanttiteknologioiden vaikutus internetiin kasvaa ja myös näkyy yhä enemmän. Suomella olisi erinomainen mahdollisuus profiloitua huippuosaamiskeskuksena myös tällä saralla. Alan tutkimus-, kehitys- ja innovaatiotoiminta on maassamme melko aktiivista, oli sitten kyse perustutkimuksesta tai tuote- ja palvelukehityksestä.

Jotta johtaisimme kehitystä telekommunikaatiossa myös kvanttipäivityksen jälkeen, Suomen olisi kuitenkin panostettava teknologiaan vieläkin enemmän. Niin perustutkimus, tutkimuksesta tuotteeksi -vaihe kuin kaupallinen tuotekehityskin voisivat olla nykyistä vankemmalla pohjalla. Orastava teknologia vaatii julkista rahoitusta ja kannusteita yritysinvestointien rinnalle. Kvantti-internet tulee – pysykäämme kehityksen kärjessä!

KIITOKSET

Haluan kiittää seuraavia henkilöitä keskusteluista: Harri Salminen, Jani Myyry, Katja Mankinen, Jussi Auvinen, Toni Härkönen ja Billy Braithwaite.
Teitte kokonaisuudesta paremman.

LÄHTEET

Ahonen, P. (2008) *Funet – Suomen tie internetiin*. CSC – Tieteen tietotekniikan keskus Oy.

CSC – Tieteen tietotekniikan keskus (2025).
CSC, SURF ja Nokia saavuttivat 1,2 Tbit/s datansiirtonopeuden.
https://csc.fi/uutinen/csc-surf-ja-nokia-saavuttivat-12-tbit-s-datansiirtonopeuden/.

Delle Donne, C. et al. (2025) An operating system for executing applications on quantum network nodes. *Nature* 639, 321–328. https://doi.org/10.1038/s41586-025-08704-w.

Euroopan Komissio (2025) NIS2 Directive:
new rules on cybersecurity of network and information systems.
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

The International Telegraph Convention – Revised at Rome (1872).
http://handle.itu.int/11.1004/020.1000/5.3.61.en.100.

Johansson, M. (2024) *Kvantdatorer*. Svenska Litteratursällskapet.
https://www.sls.fi/publications/kvantdatorer/.

Juurus, K. (2002) Kuka sen keksi? *Helsingin Sanomat Kuukausiliite* 6/2002.
https://www.hs.fi/kuukausiliite/art-2000002747830.html.

Kimble, H. (2008) The quantum internet. *Nature* 453, 1023–1030.
https://doi.org/10.1038/nature07127.

Kyberturvallisuuskeskus (2024) Kvanttiturvalliset algoritmit ja niihin siirtyminen.
https://www.kyberturvallisuuskeskus.fi/fi/kvanttiturvalliset-algoritmit-ja-niihin-siirtyminen.

Liikenne- ja viestintäministeriö (2024) Suomi mukaan New Yorkin julkilausumaan merikaapeliturvallisuudesta. https://valtioneuvosto.fi/-/1410829/suomi-mukaan-new-yorkin-julkilausumaan-merikaapeliturvallisuudesta.

Li, Y. et al. (2025) Microsatellite-based real-time quantum key distribution.
Nature 640, 47–54. https://doi.org/10.1038/s41586-025-08739-z.

McKinsey Digital (2025) Quantum communication: Trends and outlook.
https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-communication-growth-drivers-cybersecurity-and-quantum-computing/.

National Institute of Standards and Technology (NIST) (2024)
NIST Releases First 3 Finalized Post-Quantum Encryption Standards.
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

National Institute of Standards and Technology (NIST) (2024)
Post-Quantum Cryptography: Additional Digital Signature Schemes.
https://csrc.nist.gov/projects/pqc-dig-sig.

Nover, S. (2024) 'We were just trying to get it to work':
The failure that started the internet. *BBC*.
https://www.bbc.com/future/article/20241028-the-failure-that-started-the-internet.

Ookla, Speedtest Global Index, huhtikuu 2025.
https://www.speedtest.net/global-index.

Puolustusministeriö (2025) Suomi johtamaan puolustuksen kvanttiteknologiahanketta EU:ssa. https://www.defmin.fi/ajankohtaista/tiedotteet_ja_uutiset/suomi_johtamaan_puolustuksen_kvanttiteknologiahanketta_eu_ssa.15056.news.

Ranskan kyberturvallisuusvirasto (ANSSI), Saksan liittovaltion tietoturvavirasto (BSI), Alankomaiden kansallinen viestintäturvallisuusvirasto (NLNCSA), Ruotsin kansallinen viestintäturvallisuusviranomainen, Ruotsin puolustusvoimat (2024).
Position Paper on Quantum Key Distribution.
https://cyber.gouv.fr/actualites/uses-and-limits-quantum-key-distribution.

Suomen kansallinen kvanttikommunikaatioinfrastruktuuri
– National Quantum Communications Infrastructure Finland NaQCI.fi.
https://www.naqci.fi/.

Shannon, C. E. (1948) *A mathematical theory of communication*.
The Bell System *Technical Journal* 27, 379–423.
https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

Steinbock, D. (2001) *The Nokia Revolution – The Story of an Extraordinary Company That Transformed an Industry*. Amacom.

Työ- ja elinkeinoministeriö (2025) *Suomen kvanttiteknologiastrategia 2025–2035: Suomen uusi kasvun moottori ja kestävän tulevaisuuden rakentaja*.
https://urn.fi/URN:ISBN:978-952-327-628-4.

USA:n kansallinen turvallisuusvirasto (NSA) (2020) Quantum Key Distribution (QKD) and Quantum Cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

US Office of Management and Budget (2024) *Report on Post-Quantum Cryptography*.
https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf.

Valtioneuvosto (2025) *Yhteiskunnan turvallisuusstrategia*
– *Valtioneuvoston periaatepäätös.*
http://urn.fi/URN:ISBN:978-952-383-762-1.

Wehner, S et al. (2018) Quantum internet:
A vision for the road ahead. *Science* 362, eaam9288.
https://doi.org/10.1126/science.aam9288.

Ylönen, T. (1996) SSH – Secure Login Connections over the Internet.
Proceedings of the 6th USENIX Security Symposium (ss. 37–42). USENIX Association.
https://www.usenix.org/legacy/publications/library/proceedings/sec96/ylonen.html.

Kvanttilaskennan tulevaisuus

PERUSKÄSITTEET SEKÄ ODOTETTAVISSA OLEVIEN RATKAISUJEN JA NIIDEN PITKÄN AIKAVÄLIN VAIKUTUSTEN ANALYYSI

SABRINA MANISCALCO
Professori
Fysiikan osasto, Helsingin yliopisto

Johdanto

Kvanttilaskenta uudistaa lähitulevaisuudessa teknologisen toimintaympäristön. Kvanttilaskenta perustuu kvanttimekaniikan monimutkaisiin ja usein epäintuitiivisiin periaatteisiin, kuten superpositioon, lomittumiseen ja kvantti-interferenssiin. Tämä tuo täysin uusia ajattelutapoja tietojen prosessointiin ja käsittelyyn. Perinteiset tietokoneet perustuvat bitteihin, jotka ovat arvoltaan 0 tai 1. Kvanttitietokoneet taas hyödyntävät kvanttibittejä eli kubitteja, jotka voivat olla samanaikaisesti useammassa tilassa. Tämän perustavanlaatuisen eron ansiosta kvanttitietokoneet pystyvät käsittelemään ja analysoimaan valtavia määriä dataa täysin eri tavoin ja paljon tehokkaammin kuin perinteiset laskentatavat.

Kun teknologiayhteisö alkaa hyödyntää kvanttimekaniikan käytännön sovelluksia, siirrymme aikakaudelle, jolle on ominaista kvanttikeskeinen superlaskenta. Tämä nouseva paradigma yhdistää kehittyneellä tavalla kvanttiprosessorit, perinteisen suurteholaskennan ja tekoälyn. Tehokkaasti yhdistettyinä näillä jo itsessään tehokkailla teknologioilla saadaan aikaan ennennäkemätöntä suorituskykyä. Perinteiset suurteholaskentajärjestelmät ovat vakaita ja luotettavia alustoja dataintensiiviselle laskennalle ja simuloinnille. Kvanttiprosessorit taas ovat oivia ratkaisemaan tietyntyyppisiä ongelmia, jotka ovat perinteisille järjestelmille haastavia tai mahdottomia, kuten monimutkaisia kvanttikemian ja -materiaalien simulaatioita. Tekoäly puolestaan tehostaa näitä järjestelmiä hallitsemalla tehokkaasti monimutkaisuutta, ennakoimalla tuloksia ja automatisoimalla prosesseja. Kvanttilaskenta ei tule korvaamaan perinteistä tekoälyä, mutta sillä voidaan ratkaista kriittisiä pullonkauloja:

- **Datan saatavuus**: Kvanttisimulaatioilla voidaan tuottaa synteettistä tekoälyn koulutusdataa, kun kokeellista dataa on saatavilla rajallisesti (esim. harvinaiset kemialliset reaktiot, kemiallisten yhdisteiden mahdollisuuksien tunnistaminen ja niiden ominaisuuksien tutkimus uusien lääkkeiden löytämiseksi).
- **Tarkkuusvaatimukset**: Kvanttijärjestelmät suoriutuvat paremmin äärimmäistä tarkkuutta vaativissa skenaarioissa, kuten proteiinien laskostumisen tai lääkemolekyylin proteiiniin sitoutumisen ennustamisessa.

Kvanttilaskennan yhdistäminen perinteiseen suurteholaskentaan ja tekoälyyn tarjoaa sekä akateemisille että teollisuudessa toimiville tutkijoille mahdollisuuden ratkoa monimutkaisia haasteita, joita on pitkään pidetty laskennallisesti hankalina. Eri toimialat, kuten lääketeollisuus, materiaalitiede, logistiikan optimointi ja rahoitusala voivat hyötyä suuresti tällaisesta kvanttipohjaisesta laskentatehosta. Kvanttikeskeinen superlaskenta voi esimerkiksi kiihdyttää merkittävästi lääkkeiden kehitysprosesseja: se voi simuloida täsmällisesti molekyylivaikutuksia kvanttitasolla ja vähentää siten huomattavasti uusien lääkkeiden markkinoille tuomiseen kuluvaa aikaa ja kustannuksia.

Tämän teknologisen murroksen kynnyksellä on selvää, että kvanttikeskeisen superlaskennan strateginen käyttöönotto ja integrointi nykyisiin teknisiin järjestelmiin enteilee merkittäviä kilpailuetuja niin toimialoille kuin valtioillekin. Tämän edistyksen saavuttaminen edellyttää kuitenkin yhteistyötä akateemisen yhteisön, toimialojen, valtionhallinnon ja kansainvälisten kumppanien kesken, jotta on mahdollista rakentaa yhtenäinen ja innovatiivinen kvanttiekosysteemi. Kun yhteiskunnat investoivat strategisesti osaamisen kehittämiseen, infrastruktuuriin, tutkimukseen ja maailmanlaajuiseen yhteistyöhön, ne voivat ottaa kaiken hyödyn irti kvanttilaskennan muutospotentiaalista. Näin voidaan ratkaista ihmiskunnan polttavimpia ja monimutkaisimpia haasteita. Myös julkiset hankinnat ovat keskeisiä kvanttiteknologia-alan kehittymisriskien vähentämisessä, sillä julkiset hankkijat ovat ensimmäisiä käyttöönottajia ja varmoja ostajia. Yhteys julkisiin hankintoihin vähentää startup-yritysten taloudellista epävarmuutta, nopeuttaa kaupallistamista ja edistää innovointia luomalla vakaita kysyntäsignaaleita, jotka tukevat markkinoiden kasvua.

Tässä asiakirjassa käydään läpi kvanttilaskennan perusperiaatteet, tarkastellaan keskeisiä teknologisia virstanpylväitä kolmella eri aikajänteellä (5, 15 ja 25 vuotta) ja arvioidaan ennakoituja vaikutuksia toimialoihin, yhteiskuntaan ja maailmanlaajuiseen kilpailukykyyn. Tarjoamme tiekartan tämän mullistavan teknologian mahdolliseen kehityskulkuun. Esitys pohjautuu 2024 GESDA Science Breakthrough Radar -työkaluun ja tosielämän esimerkkeihin ekosysteemiyhteistyöstä.

Kvanttilaskennan peruskäsitteet

Toisin kuin perinteiset tietokoneet, kvanttitietokoneet käyttävät kvanttimekaniikan periaatteita – *superpositiota ja lomittumista* – tietojen käsittelyyn tavoilla, joihin perinteiset järjestelmät eivät kykene.

MITEN KVANTTILASKENTA EROAA PERINTEISESTÄ LASKENNASTA?

1. **Kubitit: bittien kvanttiversio**
   Perinteisessä laskennassa tieto tallennetaan bitteinä, joiden arvo voi olla joko 0 tai 1. Kvanttitietokoneet sen sijaan käyttävät *kubitteja*, jotka voivat olla samanaikaisesti arvoltaan sekä 0 että 1. Tämä perustuu *superpositioksi* kutsuttuun ominaisuuteen. Kvanttitietokoneiden on näin ollen mahdollista käsitellä useita eri mahdollisuuksia samaan aikaan. Siksi ne ovat valtavan tehokkaita tietyissä tehtävissä.
2. **Superpositio: rinnakkaisuuden mahdollistaminen**
   Superpositioperiaatteen ansiosta kvanttilaitteet pystyvät tutkimaan useita ratkaisuja samaan aikaan. Tähän periaatteeseen pohjautuu myös kvanttiinterferenssi eli ilmiö, joka voi asianmukaisesti hallittuna vahvistaa tai sulkea pois oikeita tai vääriä ratkaisuja ja siten merkittävästi nopeuttaa tietyntyyppisten ongelmien ratkaisemista.

3. **Lomittuminen: ainutlaatuinen kvanttiyhteys**
   Toinen kvanttilaskennan keskeinen ominaisuus on *lomittuminen,* jossa kubitit kytkeytyvät toisiinsa siten, että yhden kubitin tila voi suoraan vaikuttaa toisen kubitin tilaan, vaikka ne olisivat kaukana toisistaan. Lomittuminen mahdollistaa hyvin koordinoidut operaatiot ja on edellytyksenä monille kvanttialgoritmeille.
4. **Kvanttitietokoneiden toiminta**
   Kvanttitietokoneet suorittavat laskentaa käyttäen *kvanttiportteja*, jotka ohjaavat kubitteja suorittamaan tiettyjä tehtäviä. Kvanttiportit yhdistyvät *kvanttipiireiksi* kutsutuiksi sarjoiksi, jotka on suunniteltu ratkaisemaan tiettyjä ongelmia. Tämä voi kuulostaa monimutkaiselta, mutta se on verrattavissa tietokoneen ohjelmointiin – johon kuitenkin liittyy uusia kvanttifysiikkaan perustuvia sääntöjä.
5. **Nykyiset haasteet**
   Nykyiset kvanttitietokoneet ovat kehityksessään yhä varhaisessa vaiheessa, josta käytetään usein nimitystä *NISQ-aikakausi* (*Noisy Intermediate-Scale Quantum*). Ne ovat toisin sanoen kubittimäärältään pieniä ja alttiita kohinan ja epävakauden (jota kutsutaan *dekoherenssiksi*) aiheuttamille virheille. Tutkijat tekevät ahkerasti töitä näiden haasteiden voittamiseksi: he kehittävät tekniikoita, jotta voidaan vähentää ja korjata virheitä, ja rakentavat luotettavampia systeemejä.

KESKEISET TERMIT TIIVISTETTYNÄ

Kubitti: Kvanttitiedon perusyksikkö; ikään kuin bitti, jolla on ainutlaatuisia kvanttiominaisuuksia.

Superpositio: Kubitin kyky olla useammassa tilassa yhtä aikaa ikään kuin pyörivä kolikko, joka ei ole pysähtynyt kruunaksi tai klaavaksi.

Lomittuminen: Kubittien välinen erityinen korrelaatio, joka mahdollistaa koordinoidut operaatiot ja kvanttialgoritmit.

Kvanttipiiri: Ohjeistus (tai tietty sarja kvanttiportteja), joka kertoo kvanttitietokoneelle, mitä sen pitää tehdä.

NISQ *(Noisy Intermediate-Scale Quantum*): Epätäydellisten kvanttilaitteiden nykyinen sukupolvi.

Vikasietoinen kvanttilaskenta: Pitkän tähtäimen tavoite, jonka päämääränä on rakentaa virheitä automaattisesti korjaavia vakaita järjestelmiä. Virheitä korjaavat koodit ovat perusteknologiaa perinteisissä tietokoneissamme.

Kvanttilaskennan nykytila

Kvanttilaskenta on vuosikymmeniä kestäneen teoreettisen tutkimuksen ja alkuvaiheen kehityksen jälkeen siirtynyt aktiiviseen muutosvaiheeseen. Johtavat kvanttilaskennan yritykset ovat saavuttaneet *kvanttihyödyn aikakauden*, jolla kvanttitietokoneet alkavat haastaa perinteisiä menetelmiä ratkaista tietyntyyppisiä ongelmia. Tämä on merkittävä virstanpylväs, sillä nyt kvanttijärjestelmät eivät ole enää puhtaasti kokeellisia, vaan niillä alkaa olla käytännön sovellettavuutta, jolla on aluksi tieteellistä ja myöhemmin kaupallista arvoa.

Sekä *kvanttilaitteistot että -ohjelmistot* kehittyvät nopeasti. Laitteistokehitys keskittyy kubittien lukumäärän lisäämiseen, niiden tarkkuuden (eli vikasietoisuuden) parantamiseen ja niiden toiminnan nopeuttamiseen. Lisäksi tällä hetkellä on olemassa useita erilaisia fyysisiä toteutuksia kvanttitietokoneista, joissa kubitit on toteutettu erilaisilla fyysisillä menetelmillä tai alustoilla. Näitä alustoja ovat muun muassa suprajohtavat kubitit (tällä hetkellä kehittynein teknologia), neutraalit atomit, ioniloukut, fotoniikka ja puolijohdekubitit. Vielä ei ole varmaa, mikä näistä alustoista lopulta osoittautuu voittavaksi teknologiaksi tulevaisuuden skaalautuvissa kvanttitietokoneissa, mutta toistaiseksi jokaisen erityyppisen kvanttitietokoneen kehitys edellyttää suuria investointeja. Tähän liittyy riski, että jotkut valituista teknologioista saattavat osoittautua tarpeettomiksi.

Kvanttiohjelmistoista on samaan aikaan tulossa yhä tärkeämpiä. Ne ovat yleensä riippumattomia laitteistoista ja siten vähemmän riskialttiita kuin kvanttilaitteistot, koska niitä voidaan käyttää erilaisilla fyysisillä kvanttilaskenta-alustoilla ja optimoida niille. Lisäksi kvanttiohjelmistot toimivat kvanttilaitteistoja ja tosielämän sovelluksia yhdistävänä siltana. Niiden avulla kehittäjien on mahdollista suunnitella algoritmeja ja ratkaisuja, joissa hyödynnetään kvanttilaskennan ainutlaatuista kykyä ratkaista haasteita esimerkiksi optimoinnissa, salaustekniikoissa, tekoälyssä ja materiaalitieteessä.

Painopiste on siirtymässä sellaisten *kvanttiohjelmistojen, -ratkaisujen* ja *-sovellusten* kehittämiseen, joilla on *konkreettisia vaikutuksia tosielämässä*. Ohjelmistokehitys perustuu luontaisesti siihen, että kehitetään sovelluksia tiettyihin käyttötapauksiin, joilla voidaan luoda kaupallista arvoa. Tärkeydestään huolimatta kvanttiohjelmistojen kehitys saa usein osakseen vähemmän strategista huomiota kuin laitteistojen kehitys. Tämän aliedustuksen riskinä on, että se voi hidastaa kvanttilaskentakapasiteetin muuntamista käytännön hyödyiksi. Jotta kvanttilaskennan täysi potentiaali voidaan hyödyntää, on olennaista priorisoida investointeja ohjelmistokehitykseen laitteistokehityksen rinnalla.

Kun siirrytään kvanttihyödyn aikakauteen, korostuu tarve tasapainoiselle lähestymistavalle, jolla edistetään sekä laitteistojen skaalautuvuutta että ohjelmistopohjaisia ratkaisuja yhteiskunnan ja eri toimialojen polttaviin haasteisiin. Näin kvant-

tilaskenta voi kehittyä uraauurtavasta tieteellisestä pyrkimyksestä muutoksia aikaansaavaksi teknologiaksi, jolla on laajoja taloudellisia ja yhteiskunnallisia vaikutuksia.

Lyhyen aikavälin näkymät (0–5 vuotta): NISQ-aikakausi ja hybridijärjestelmät

Seuraavien viiden vuoden aikana kvanttilaskentaa määrittää pitkälti NISQ (Noisy Intermediate-Scale Quantum) -aikakausi. NISQ viittaa kvanttitietokoneisiin, joissa on rajallinen määrä kubitteja – tyypillisesti kymmenistä muutamaan sataan – ja joissa edelleen ilmenee virheitä, koska ne reagoivat herkästi ympäristön häiriötekijöihin. Tulevaisuuden vikasietoiset kvanttitietokoneet pystyvät korjaamaan virheet, mutta NISQ-aikakauden järjestelmistä puuttuu vielä luotettava virheiden korjaustoiminto, eli ne eivät kykene suorittamaan pitkiä tai monimutkaisia laskentatehtäviä luotettavasti ja virheittä.

Siitä huolimatta NISQ-aikakauden laitteet ovat erittäin lupaavia erityisesti tietyntyyppisissä monimutkaisissa ongelmissa, joita on haastavaa tai mahdotonta ratkaista tehokkaasti perinteisillä tietokoneilla. *Kvanttiedun* käsite kuvaa tilannetta, jossa kvanttitietokone pystyy ratkaisemaan tieteellisesti olennaisen käytännön ongelman merkittävästi paremmin kuin yksikään perinteinen supertietokone. Ensimmäisiä osoituksia kvanttiedusta tieteellisesti merkityksellisissä käytännön sovelluksissa, erityisesti kemiallisten prosessien ja materiaalien simuloinnissa, odotetaan jo tällä lyhyellä 0–5 vuoden aikavälillä.

TEKNISET ODOTUKSET

Kubittien lukumäärän odotetaan lisääntyvän ja niiden laadun odotetaan paranevan tasaisesti seuraavien viiden vuoden aikana. Kvanttiprosessorien ennakoidaan kasvavan maltillisesti satoihin kubitteihin ja kehittyvän huomattavasti luotettavammiksi ja tarkemmiksi perustoiminnoissaan. Kehitystä tapahtuu myös virheenlievennystekniikoissa eli keinoissa vähentää kohinan vaikutusta sitä kokonaan poistamatta. Nämä parannukset lisäävät kvanttilaskennan käytännöllisyyttä ja vaikuttavuutta.

Yksi keskeinen kehitysaskel tulee olemaan kvanttilaskentaa ja perinteistä laskentaa yhdistävien hybridialgoritmien käytön lisääntyminen. Näissä algoritmeissa yhdistyvät strategisesti kvanttilaskennan ja perinteisen laskennan parhaat ominaisuudet-. Tämän ansiosta kvanttitietokoneet voivat keskittyä vahvuuksiensa mukaisiin tehtäviin, kun taas perinteiset järjestelmät hoitavat muun laskennan. Tällaiset hybridiratkaisut tulevat todennäköisesti tuottamaan ensimmäiset vakuuttavat näytöt kvanttiedusta tosielämän skenaarioissa.

Myös pilvipalveluiden välityksellä käytettävä kvanttilaskenta jatkaa kasvuaan ja tulee saataville myös erikoistuneiden laboratorioiden ulkopuolisille tahoille. Suuret teknodlogiayhtiöt, kuten IBM, Amazon ja Microsoft, tarjoavat jo nyt pilvipohjaista kvanttilaskentaa ja mahdollistavat sen kautta laajemman kokeellisen toiminnan ja yhteistyön tutkijoiden, startup-yritysten ja muiden yritysten välillä ympäri maailmaa.

SOVELLUKSET

Lyhyellä aikavälillä kvanttilaskennan vaikutus näkyy eniten toimialoilla, joilla kvanttivaikutukset ovat luonnollisesti hallitsevassa asemassa, erityisesti kvanttikemian ja materiaalitieteen aloilla. Yksi merkittävä esimerkki on molekyylivuorovaikutusten simulointi, joka on ratkaisevan tärkeää lääketeollisuuden yrityksissä, kun kehitetään uusia lääkkeitä. Kvanttilaskenta mahdollistaa perinteisiin tietokoneisiin verrattuna tarkemmat ja tehokkaammat monimutkaisten molekyylien ja kemiallisten reaktioiden mallinnukset. Varhaisia kvanttisimulaatioita käytetään esimerkiksi fotodynaamisten syöpähoitojen tutkimuksessa. Kvanttimallit auttavat tutkijoita ymmärtämään, miten valolla aktivoituvat lääkeaineet vaikuttavat toisiinsa molekyylitasolla, jotta lääkeaine voidaan kohdistaa tarkasti syöpäsoluihin tervettä kudosta vahingoittamatta.

Kvanttisimulaatiot tulevat olemaan ratkaisevan tärkeässä asemassa myös materiaalitieteessä: ne tarjoavat näkymiä suprajohteiden tai innovatiivisten akkuyhdisteiden kaltaisten uusien materiaalien ominaisuuksiin ja käyttäytymiseen, mikä voi nopeuttaa niiden kehitystä ja kaupallista soveltamista.

Myös kvanttitehostettu koneoppiminen ja optimointi ovat kehittymässä tehokkaiksi välineiksi. Varhaiset sovellukset talouden, logistiikan ja toimitusketjujen hallinnassa tulevat osoittamaan kvanttialgoritmien potentiaalin ratkaista tehokkaasti monimutkaisia ongelmia, jotka liittyvät resurssien kohdentamiseen, aikataulutukseen ja riskianalyysiin.

HAASTEET

Nykyisistä haasteista huolimatta kvanttilaskennan tulevaisuuden näkymät ovat erittäin optimistiset erityisesti siksi, että nykyisten rajoitteiden käsittelyyn kehitetään innovatiivisia strategioita. Vaikka NISQ-aikakauden kvanttitietokoneet tekevät ympäristövuorovaikutuksista johtuvia virheitä, joita usein kutsutaan ”kohinaksi” (noise), tämä ei poista kvanttitietokoneiden käytännön hyödyllisyyttä. Ala on päinvastoin hyväksynyt nämä rajoitteet ja alkanut kehittää räätälöityjä kvanttialgoritmeja ja -ratkaisuja, joiden on nimenomaan tarkoitus toimia tehokkaasti nykyisten teknologisten edellytysten rajoissa.

Yksi keskeinen tekijä kvanttilaskennan investointien riskien vähentämisessä on kvanttiohjelmistoyritysten strateginen rooli. Nämä organisaatiot toimivat ensiarvoisen tärkeinä välikäsinä laitteistojen toimittajien ja loppukäyttäjien välillä, koska ne mahdollistavat kvanttialgoritmien ja -ratkaisujen yhteissuunnittelun. Ohjelmistokehittäjät voivat merkittävästi parantaa kvanttiratkaisujen käytännön soveltuvuutta

ja suorituskykyä, kun he ymmärtävät nykyisten kvanttilaitteistojen rajoitteet ja sisällyttävät ne suunnitelmiinsa.

Lisäksi kvanttilaskennan onnistunut käyttöönotto nojaa yhä enemmän kokonaisvaltaiseen yhteissuunnitteluun – ei pelkästään laitteistojen ja ohjelmistojen välillä vaan myös sovellusalustoissa ja taustalla toimivissa infrastruktuuriohjelmistoissa. Tämä kokonaisvaltainen lähestymistapa takaa, että kvanttialgoritmit on kohdistettu operoimaan nykyisten kvanttilaitteiden toiminnallisuuksien ja rajoitteiden kanssa. Siten ne maksimoivat laitteiden välittömän potentiaalin ja luovat pohjan nopealle kehitykselle.

Kvanttilaskenta voi tämän integrointiin ja yhteistyöhön perustuvan lähestymistavan kautta tuottaa konkreettisia hyötyjä jo NISQ-aikakaudella. Nykyisistä rajoitteista huolimatta kvanttiekosysteemi muuttaakin haasteita aktiivisesti mahdollisuuksiksi innovoida, saada aikaan varhaisia käytännön vaikutuksia ja ylläpitää teknistä kehitystä.

VAIKUTUKSET

Kvanttilaskennan vaikutus lyhyellä aikavälillä tulee olemaan merkittävä. Kvanttiedun osoittaminen onnistuneesti tietyissä tieteellisissä ja toimialakohtaisissa ongelmissa – kuten kemiallisten vuorovaikutusten simuloinnissa ja kehittyneiden materiaalien kehityksessä – tulee olemaan keskeinen virstanpylväs, joka todistaa kvanttilaskennan konkreettisen arvon. Näiden varhaisten onnistumisten odotetaan herättävän lisää kiinnostusta ja houkuttelevan investointeja niin eri toimialojen johtavilta yrityksiltä, valtioilta kuin yksityisiltä sijoittajiltakin.

Lisäksi kvanttiteknologian tarjoajien ja toimialojen väliset pilotit ja kumppanuudet ovat jo nyt yleistymässä. Tällainen yhteistyö auttaa toimialoja tunnistamaan kvanttilaskennan käytännön käyttökohteita, jotka puolestaan ohjaavat strategista päätöksentekoa ja investointeja.

On tärkeää huomata, että kvanttiteknologian laajeneminen tuo mukanaan merkittävää kysyntää erikoisosaamiselle. Kvanttiohjelmistojen kehittäjät, insinöörit ja tutkijat ovat ratkaisevan tärkeitä kvanttilaskennan potentiaalin toteutumisessa. Yliopistot ja teknilliset oppilaitokset ympäri maailmaa lisäävät jo nyt koulutusaloitteiden kautta kvanttilukutaitoa opetussuunnitelmiinsa varmistaakseen, että työntekijät valmistautuvat tulevaisuuteen, jossa kvanttilaskenta on keskeisessä asemassa.

Keskipitkän aikavälin näkymät (5–15 vuotta): vikasietoisuus ja kvanttietu

TEKNISET ODOTUKSET

Loogisilla kubiteilla varustettuja vikasietoisia kvanttijärjestelmiä odotetaan valmistuvan seuraavan 5–15 vuoden kuluessa, mikä tulee olemaan merkittävä virstanpylväs kvanttilaskentakyvyn kehityksessä. Toimialan laitteistot vakiintuvat todennäköisesti sellaisten arkkitehtuurien ympärille, jotka ovat erityisen lupaavia ja pitkälle kehittyneitä, kuten suprajohtavat piirit, ioniloukut ja fotoniikka-alustat. Kvanttivirheiden korjausmenetelmät, erityisesti pintakoodit ja LDPC-koodit (Low-Density Parity-Check), kehittyvät myös merkittävästi. Lisäksi tällä aikajaksolla integroidaan kvanttilaskentaa yhä enemmän olemassa oleviin suurteholaskentakeskuksiin ja yhdistetään näin perinteisen laskennan ja kvanttilaskennan vahvuudet.

SOVELLUKSET

Odotettavissa olevan teknisen kehityksen myötä otetaan useissa kriittisissä toimintaympäristöissä käyttöön mullistavia sovelluksia. Kvanttilaskenta mahdollistaa monimutkaisten molekyylijärjestelmien tarkan simuloinnin ennennäkemättömässä laajuudessa, mistä on suurta hyötyä eri toimialoille, kuten lääketeollisuudelle, kemikaaliteollisuudelle ja materiaalitieteelle. Ennakoidaan, että laaja-alainen kvanttikoneoppiminen tulee mullistamaan yksilöllisen lääketieteellisen hoidon tarjoamalla kohdennettua diagnostiikkaa ja potilaille räätälöityjä yksilöllisiä hoitosuunnitelmia. Lisäksi kvanttilaskenta mahdollistaa reaaliaikaisen optimoinnin, joka lisää logistiikan, energian jakelun ja rahoitusjärjestelmien tehokkuutta ja parantaa siten konkreettisesti toiminnan vaikuttavuutta.

HAASTEET

Vaikka lupaavaa kehitystä on tapahtunut, on myös useita merkittäviä haasteita, jotka on ratkaistava. Kvanttilaskennan suorituskyvyn arvioimisen mittarit on välttämätöntä standardoida, ja koko toimialalla on otettava käyttöön selkeät vertailukäytännöt. Lisäksi on tärkeää eri sovellusten yhteissuunnittelu, jossa kvanttilaitteistot ja algoritmit kohdennetaan tarkasti tiettyjen käyttötapausten kanssa. Siten voidaan tarjota käytännön kvanttietua ja kvanttiarvoa eri toimialoille. Myös tietoturvallisuus on merkittävä huolenaihe erityisesti sellaisten Shorin algoritmin kaltaisten kvanttialgoritmien osalta, joilla on mahdollista murtaa perinteiset salausjärjestelmät. Tässä korostuu kvanttiturvallisten tietoturvaratkaisujen tarve.

VAIKUTUKSET

Odotettavissa olevat edistysaskeleet kvanttiteknologiassa johtavat siihen, että kvanttilaskennan nopeuttamat sovellukset tuottavat mitattavaa liiketoiminnallista arvoa, mikä luo kilpailuetua kaikilla toimialoilla. Tämän johdosta kvanttiosastot yleistyvät suurissa yrityksissä, mikä kuvastaa kvanttilaskennan strategista tärkeyttä. Lisäksi valtiot ympäri maailmaa ottavat todennäköisesti käyttöön kvanttiturvallisia

viestintäratkaisuja ja investoivat kvanttikestävään infrastruktuuriin valmistautuakseen vakaasti tulevaisuuteen, jossa kvanttilaskentaa käytetään laajasti.

Pitkän aikavälin näkymät (15–25+ vuotta): skaalautuva ja yleiskäyttöinen kvanttilaskenta

TEKNISET ODOTUKSET

Kvanttilaskennan ennakoidaan 15–25 vuodessa ja sitä pitemmällä aikavälillä kehittyvän pisteeseen, jossa tarjolla on skaalautuvia miljoonan kubitin prosessoreita ja laajasti saatavilla olevia kaupallisia kvanttipilvialustoja. Kvanttiteknologia tulee integroitumaan tiiviisti toimialojen vakiotyönkulkuihin ja mahdollistamaan siten kvanttilaskentaa ja tekoälyä yhdistävät saumattomat hybridijärjestelmät, joilla automatisoidaan kehittämisen ja innovoinnin prosessit sekä monimutkaiset ongelmanratkaisuprosessit. Lisäksi kvanttiteknologian kehityksen odotetaan tuottavan kansainvälisten viitekehysten ohjaamia, pitkälle kehittyneitä ja monialaisia ekosysteemeitä, jotka tukevat kvanttikyvykkyyden koordinoitua kasvua ja vastuullista käyttöä maailmanlaajuisesti.

SOVELLUKSET

Kvanttilaskentateknologian kehittyessä laajasti skaalautuvaksi ja integroituessa valtavirtasovelluksiin on odotettavissa perustavanlaatuisia muutoksia useilla eri toimialoilla. Yksilöllinen lääketieteellinen hoito kehittyy uudelle tasolle kvanttilaskennan tehostaman biologisen mallinnuksen avulla ja mahdollistaa siten läpimurtoja diagnostiikassa, täsmähoidoissa ja terveydenhuollon toteuttamisessa. Kvanttilaskenta edistää merkittävästi syvällistä ilmastosimulointia ja parantaa näin ilmastonmuutoksen hillitsemis- ja sopeutumistoimien täsmällisyyttä. Kyberturvallisuuden alalla pitkälle kehittynyt kvanttisalaus mahdollistaa tietoturvallisen viestinnän ja pilvilaskennan, joka pystyy torjumaan perinteiset uhat ja kvanttiuhat. Kvanttiteknologiat kiihdyttävät myös seuraavan sukupolven puhtaan energian järjestelmien ja kehittyneiden materiaalien kehitystä, joten ne ovat ratkaisevan tärkeitä maailmanlaajuisessa kestävässä kehityksessä.

Lisäksi on odotettavissa, että kehitetään erilaisia uusia ja vielä ennennäkemättömiä kvanttilaskentaan pohjautuvia sovelluksia ja teknologioita, jotka tulevat valtavirtaistumaan. Tällaisia uusia kehitysaskeleita on tällä hetkellä haastavaa ennakoida täsmällisesti. Kuitenkin yleisesti tunnustetaan, että merkittävimmät pitkän aikavälin vaikutukset syntyvät täysin uusista toimialoista ja sovelluksista, joita kvanttiteknologia mahdollistaa.

HAASTEET

Lupaavista kehitysaskeleista huolimatta jäljellä on myös merkittäviä haasteita. Kvanttijärjestelmät kuluttavat energiaa ja edellyttävät resurssien hallintaa, erityisesti jäähdytystä. Tästä aiheutuu huomattavia teknisiä ja taloudellisia esteitä. Eettiset näkökohdat on huomioitava ja sääntelykehyksiä on kehitettävä ennakoivasti, jotta voidaan hallita yhteiskunnallisia vaikutuksia ja varmistaa teknologian vastuullinen ja tasapuolinen käyttöönotto. Lisäksi tulee yhä tärkeämmäksi ratkaista mahdollinen eriarvoistuminen pitkälle kehittyneen kvantti-infrastruktuurin maailmanlaajuisessa saatavuudessa, jotta voidaan estää teknologisen kuilun syntyminen valtioiden ja yhteisöjen välille.

VAIKUTUKSET

Skaalautuvan ja yleiskäyttöisen kvanttilaskennan käyttöönoton odotetaan aiheuttavan rakenteellisia muutoksia tutkimusmenetelmissä, innovaatiosykleissä ja laajemmin taloudellisessa toimintaympäristössä. Maailmanlaajuinen kilpailu kvanttiteknologiassa kiristyy, minkä johdosta teknologisesta suvereniteetista tulee tärkeä prioriteetti niin valtioille kuin toimialoillekin. Lopulta kvanttiteknologiat kehittyvät erikoistyökaluista laajasti saatavilla oleviksi yleiskäyttöisiksi työkaluiksi ja juurtuvat syvälle yhteiskuntien, toimialojen ja valtionhallinnon toimintoihin. Siten ne uudistavat tapoja, joilla monimutkaisia maailmanlaajuisia haasteita ratkaistaan.

Vaikutukset eri toimialoilla

Kvanttilaskenta tulee aiheuttamaan perustavanlaatuisia muutoksia useilla eri toimialoilla ja mahdollistamaan läpimurtoja, jotka tukevat suoraan kriittisiä maailmanlaajuisia tavoitteita, kuten YK:n kestävän kehityksen tavoitteita. Alla on esitetty joitakin esimerkkejä siitä, miten kvanttiteknologia voi uudistaa keskeisiä toimialoja:

- **Terveydenhuolto**: Kvanttilaskenta nopeuttaa merkittävästi lääkkeiden kehitysprosesseja, optimoi genomianalyysejä, mahdollistaa täsmälääkkeet yksilöllisten potilassimulaatioiden avulla ja edistää ehkäisevää terveydenhuoltoa, mikä viime kädessä auttaa ihmisiä elämään pidempään ja terveemmin.
- **Energia**: Kvanttilaskentaan pohjautuva simulointi mahdollistaa katalyysiinnovaatiot, joilla saadaan aikaan puhtaampia teollisia prosesseja. Lisäksi se parantaa energian varastoinnissa käytettäviä akkumateriaaleja, nopeuttaa fuusioenergian tutkimusta, parantaa hiilidioksidin talteenottoteknologioita ja optimoi lannoitteiden tuotantoa. Näin se tukee kestäviä energiajärjestelmiä ja ruokaturvaa.
- **Talous**: Kvanttialgoritmit tehostavat taloudellista mallintamista, mikä tekee portfolioiden optimoinnista nopeampaa ja täsmällisempää. Se myös parantaa merkittävästi petosten havaitsemista sekä hioo riskien mallintamisstrategioita ja edistää näin turvallisempaa ja tehokkaampaa taloudellista toimintaympäristöä.

- **Ilmasto**: Kvanttisimulointi parantaa merkittävästi ilmastomallien täsmällisyyttä: se simuloi realistisesti ilmakehän ja valtamerten järjestelmiä sekä ekologisia järjestelmiä ja mahdollistaa siten täsmälliset ilmastoennusteet ja vaikuttavat lieventämis- ja sopeutumisstrategiat.
- **Tietoturva**: Kvanttisalauksesta ja kvanttiturvallisesta salauksesta tulee tehokkaan kvanttilaskennan aikakaudella kriittisen tärkeitä ja pakollisia välineitä tietoturvallisen viestinnän ja tietosuojan ylläpitämisessä.
- **Materiaaliteollisuus**: Kvanttilaskenta mullistaa uusien materiaalien löytämisen ja suunnittelun. Näillä uusilla materiaaleilla tulee olemaan räätälöityjä ominaisuuksia, mikä mahdollistaa vahvempien, kevyempien ja kestävämpien materiaalien kehittämisen valmistusteollisuuden, liikenteen, elektroniikan ja infrastruktuurin eri sovelluksiin. Kvanttilaskentaan pohjautuvat materiaali-innovaatiot vähentävät merkittävästi aikaa ja kustannuksia, mitä pitkälle kehittyneiden ja tehokkaiden materiaalien asettaminen markkinoille edellyttää.

Pitkällä aikavälillä kvanttilaskennan merkittävimmät vaikutukset aiheutuvat todennäköisesti täysin uusista ja vielä ennennäkemättömistä sovelluksista ja toimialoista, jotka uudistavat yhteiskunnan tapoja ratkaista monimutkaisia maailmanlaajuisia haasteita.

Johtopäätökset: kvanttitulevaisuuden mahdollistaminen

Kvanttilaskenta ei ole enää kaukainen lupaus vaan nouseva muutosvoima, jolla on perustavanlaatuisia vaikutuksia kyberturvallisuuteen, terveydenhuoltoon, ilmastotoimiin, taloudelliseen kilpailukykyyn ja moniin muihin asioihin. Tämän ennennäkemättömän potentiaalin valjastaminen on nykyisten poliittisten päättäjien käsissä, sillä heidän strategiset päätöksensä muovaavat yhteiskunnallista ja taloudellista toimintaympäristöämme vuosikymmeniä eteenpäin.

Poliittisten päättäjien tulisi erityisesti keskittyä seuraaviin kuuteen kriittiseen osa-alueeseen, jotta he tukisivat tehokkaasti kvanttilaskentaan liittyvää innovointia:

1. **Osaamisen kehittäminen**: Perustetaan kansallisia kvanttilaskennan koulutuskeskuksia ja laaditaan elinikäisen oppimisen ohjelmia kvanttiteknologioille. Tämä mahdollistaa keskeisen osaavan työvoiman kouluttamisen.

2. **Investoinnit infrastruktuuriin**: Varmistetaan helppo ja tasapuolinen pääsy ja strategiset investoinnit kvanttilaskentaa ja perinteistä laskentaa yhdistäviin hybridimuotoisiin suurteholaskentalaitteisto- ja ohjelmistoinfrastruktuureihin. Tällä varmistetaan kriittisten laskentaresurssien luotettava saatavuus.
3. **Startup-yritysten tukeminen**: Mahdollistetaan markkinaehtoiset hankintakäytännöt ja kärsivälliset pääomasijoitukset, jotta kvanttilaskentaa hyödyntävät startup-yritykset pystyvät kehittämään kvanttiratkaisuja ja tuomaan niitä nopeammin markkinoille.
4. **Kvanttiohjelmistojen ja -sovellusten strateginen kehittäminen**: Asetetaan etusijalle sellaisten kvanttiohjelmistojen ja käytännön kvanttiratkaisujen strateginen kehittäminen, jotka mahdollistavat nopean käyttöönoton eri toimialoilla, maksimoivat sovelluspotentiaalin ja nopeuttavat teknologian skaalautumista eri toimialoilla.
5. **Kansainväliset kumppanuudet**: Osallistutaan aktiivisesti kansainvälisiin kvanttiyhteistyöprojekteihin – mukaan lukien EU:n, NATOn ja maailmanlaajuisten yhteenliittymien puitteissa tapahtuvat kumppanuudet – jotta voidaan nopeuttaa teknologian kehitystä ja taata sen tehokas maailmanlaajuinen hallinta.
6. **Standardointi ja ennakointi**: Johdetaan kvanttiteknologian standardien ja ennakointivalmiuksien luomista, jotta pystytään ennakoimaan teknologista kehitystä ja uusia sovelluksia.

Kriittisen tärkeitä ovat myös tasapainoiset kansalliset kvanttistrategiat, joissa painotetaan sekä laitteistoja että ohjelmistoja. Erityisesti kvanttiohjelmistot ovat keskeinen komponentti, joka muuntaa kvanttilaskennan tutkimuksen skaalautuviksi tosielämän sovelluksiksi ja parantaa siten pitkän aikavälin yhteiskunnallisia ja taloudellisia vaikutuksia.

Omaksumalla tämän kvanttikeskeisen vision – jossa kvanttilaskenta yhdistetään tekoälyyn ja perinteiseen superlaskentaan – voimme hyödyntää ennennäkemätöntä laskentatehoa. Näin voimme ratkaista ihmiskunnan suurimpia haasteita hiilidioksidin talteenoton ja uusien materiaalien kaltaisten kestävien ratkaisujen edistämisestä aina lääkekehityksen ja yksilöllisen lääketieteellisen hoidon nopeuttamiseen. Kvanttilaskennan aikakausi on jo alkanut. Seuraavien viiden vuoden aikana tehtävät poliittiset päätökset muovaavat kvanttilaskentavetoista tulevaisuutta ratkaisevasti neljännesvuosisadaksi eteenpäin. Ne määrittävät, ottavatko yhteiskunnat johtavan aseman vai jäävätkö ne jälkeen tulevaisuuden maailmanlaajuisessa innovaatiotaloudessa.

VIITTEET

GESDA Science Breakthrough Radar (2024)
https://radar.gesda.global/ Viitattu 14.5.2025.

WEF Embracing the Quantum Economy: A Pathway for Business Leaders (2025)
https://www.weforum.org/publications/embracing-the-quantum-economy-a-pathway-for-business-leaders/
Viitattu 14.5.2025.

Kvanttiturvallinen internet

KVANTTITURVALLINEN SIIRTYMÄ

SUVI LAMPILA
SSH Fellow
SSH Communications Security Oyj

Kryptografian muutokset 2025–2030

Yksi merkittävimpiä muutoksia tietoturvassa tällä vuosikymmenellä on siirtyminen kvanttiturvalliseen kryptografiaan (*post-quantum cryptography*, PQC). Salauksen osalta siirtyminen on jo alkanut. Kvanttiturvallisten sovellusten ja laitteiden käyttöönotto etenee riippumatta siitä, missä aikataulussa itse kvanttiteknologia etenee. Tämä on erityisen tärkeää siksi, että osa tulevaisuuden kvanttikoneella avustetuista hyökkäyksistä koskee tällä hetkellä suojattua tietoa.

- Kvanttiuhalta voi suojautua ainoastaan etukäteen, jotta salassa pidettävän tiedon luottamuksellisuus säilyy.
- Kaikki organisaatiot ja kansalaiset tulevat siirtymään kvanttiturvalliseen kryptografiaan, joka toimii tavallisella tietokoneella eikä vaadi kvanttiteknologiaa.
- Se, tapahtuuko siirtyminen hallitusti ja kustannustehokkaasti vai pakon edessä ja jälkijunassa, riippuu siitä, miten tehokkaasti ohjeistus saadaan vietyä käytäntöön kansallisella tasolla sekä Euroopan unionissa.

Kvanttiturvallista siirtymää on verrattu vuosituhannen vaihteen *Year 2000* (Y2K) -tietokoneongelman korjaukseen, jossa suuri määrä ohjelmistoja ja järjestelmiä täytyi päivittää. Year to Quantum (Y2Q) -vertaus kuitenkin ontuu, koska nyt korjaus ei koske vain yhtä järjestelmävirhettä, vaan päivitettävää on huomattavasti enemmän sekä järjestelmien ja ohjelmistojen määrässä että niiden käyttämissä useissa kryptografisissa toiminnoissa. Y2Q on se päivä, kun kvanttikoneiden kyvykkyys riittää murtamaan nykyisin laajassa käytössä olevan julkisen avaimen kryptografian. Kukaan ei pysty varmuudella sanomaan, koska tuo päivä koittaa. Siirtymisen kuitenkin täytyy tapahtua vahvasti etunojassa, jotta salassa pidettävän tiedon luottamuksellisuus säilyy.

Julkisen avaimen kryptografiaa käytetään salauksen suojauksen lisäksi myös muun muassa järjestelmien ja käyttäjien tunnistamisessa. Kvanttihaavoittuvat luotetut varmenteet ja autentikointiavaimet täytyy korvata kvanttiturvallisilla viimeistään silloin, kun on syytä olettaa, että kriittinen kvanttikyvykkyys on saavutettu. Käytännössä sähköiset kvanttiturvalliset allekirjoitukset tulee ottaa nekin hyvissä ajoin käyttöön, koska emme saa ajautua tilanteeseen, jossa digitaalisia allekirjoituksia esimerkiksi varmenteissa kyseenalaistettaisiin jälkikäteen.

Yhteiskuntamme on hyvin pitkälle digitalisoitunut vuosituhannen alusta, eikä PQC-siirtymässä ole varaa epäonnistua, sillä yhteiskuntamme ei enää toimi ilman digiympäristöä. Jos päivityksiä ei olisi saatu tehtyä ajoissa Y2K:n kohdalla, uuden vuoden jälkeen olisimme voineet lukea paperilehdistä onnettomuuksista, käteisellä olisi silti voinut maksaa kaupassa ja virastoon olisi voinut kävellä asiakaspalvelutiskille. Maailma on kuitenkin muuttunut. Julkisen avaimen kryptografia mahdol-

listaa jokapäiväisten digitaalisten palveluiden turvallisen tuottamisen internetissä. Onnistuessaan kvanttiturvallinen siirtymä ei näy tavallisille kansalaisille mitenkään. Esimerkiksi selaimessa tutun lukon kuvan osoittama salattu ja autentikoitu yhteys on vaihdettu kvanttiturvalliseen palveluiden ylläpitäjien, kyberteknologiatoimijoiden ja -yritysten sekä poliittisten päättäjien yhteisen ponnistuksen tuloksena.

Ideaalitilanteessa kvanttiturvallinen salaus olisi käytössä jo vuosikymmeniä ennen kryptografisesti merkittävää kvanttikonetta ja kvanttiturvalliseen salaukseen ja tunnistautumiseen voitaisiin siirtyä ketterästi. On mahdollista, että pitkään salassa pidettävien tietojen turvaamisessa olemme jo auttamattomasti myöhässä, sillä toteutuessaan kvanttiuhka on takautuva. Internetissä salattu verkkoliikenne voidaan kaapata talteen ja perinteinen salaus purkaa myöhemmin kvanttikoneella. Tällaiselta ”haali nyt, pura myöhemmin” -hyökkäykseltä voi suojautua ainoastaan etukäteen varmistamalla, että salauksen suojaukseen käytetään kvanttiturvallista avaimenvaihtoa, kuten ML-KEM-kapselointia. Myös suojattavan lohkosalaimen tulee olla kvanttikestävä, esimerkiksi riittävän pitkä AES-avain.

Demokratia ja yhteiskuntarauha perustuvat kansalaisten luottamukseen siihen, että julkiset digitaaliset palvelut ovat luotettavia ja tunnistettavissa. Pelkästään epäilys siitä, että jokin valtio tai vihamielinen taho on saavuttanut kyvykkyyden rakentaa kryptografisesti merkittävän kvanttikoneen, riittää aiheuttamaan merkittävää vahinkoa. Jos luotetun varmenteen myöntäjän avain murretaan, silloin pankit ja finanssialan toimijat eivät voi luottaa rahaliikenteen oikeellisuuteen. Myöskään aitoja web-palveluita ei pysty erottamaan vihamielisen tahon kopiosta. Digitaalisen yhteiskunnan toimimisen edellytykset murenevat, mikäli sähköisiin allekirjoituksiin ja tunnistautumiseen ei enää luoteta.

KVANTTIHAAVOITTUVA KRYPTOGRAFIA TULEE TIENSÄ PÄÄHÄN

Yhdysvaltojen ja eurooppalaisten maiden lainsäädäntö ja suositukset sanelevat pitkälti yleisesti saatavilla olevien palveluiden ja ohjelmistotuotteiden ominaisuuksia. Siksi on todennäköistä, että kvanttihaavoittuva kryptografia ainoana suojauksena tulee tiensä päähän julkisessa internetissä asteittain vuoteen 2035 mennessä. Kaupallisten tuotteiden elinkaari seuraa hyvin todennäköisesti isoimmilla markkinoilla kvanttiturvallisen siirtymän aikataulua siten, että useat vanhat tuotteet korvataan jo vuoteen 2030 mennessä. Ohjelmisto- ja laitepäivityksiin täytyy varautua niidenkin, joiden riskiarviossa kvanttiuhka ei ole kriittinen.

Useimmissa kansallisissa siirtymäaikatauluissa on niputettu eri käyttökohteet samaan koriin ja annettu aikarajoja siirtymän toteuttamiselle. Siirtymän aikataulut länsimaissa ovat pääosin yhteneväisiä Yhdysvaltojen lainsäädännön kanssa. Euroopan unionin maiden kyberturvavirastojen kehotus on suojautua ”haali nyt, pura myöhemmin” -hyökkäykseltä mahdollisimman pian, kuitenkin viimeistään vuoteen 2030 mennessä. Iso-Britannia tavoittelee priorisoitujen järjestelmien kvanttiturvallisuutta vuoteen 2031 mennessä. Yhdysvaltojen priorisoitu kvanttisiirtymä tapah-

tuu vuoteen 2030 mennessä, kuitenkin poikkeukset ovat sallittuja vuoteen 2035 asti. Kiina aikoo olla kvanttiturvallinen jo vuonna 2027.

Selkeät aikataulut suosituksissa ja lainsäädännössä ovat tarpeellisia tienviittoja, mutta on hyvä tiedostaa, että kvanttihyökkäyksen kannalta merkityksellistä on huolehtia mahdollisimman pian luottamuksellisuuden varmistamisesta ja sitten todentamisesta, koska todentamisen kohdalla hyökkäys ei ole samalla tavalla takautuva. Myös käytännön toimet sanelevat aikatauluja: esimerkiksi julkisessa internetissä on käytössä juurivarmenteita, jotka täytyy päivittää joka tapauksessa vuonna 2029, joten on toivottavaa, että ne päivitetään samalla kvanttiturvallisiksi. Kvanttiturvallista siirtymää ei tule viivyttää sillä perusteella, että kaikki siirtymäpäivitykset haluttaisiin tehdä samalla kertaa. Kuten kyberturvassa yleensäkin ketterät tietoturvapäivitykset ovat osa normaalia toiminnan ylläpitoa, ja kvanttiturvallinen siirtymä tulisi sekä budjetoida että suunnitella matkana kvanttiturvallisuuteen sen sijaan, että varauduttaisiin yksittäiseen päivitysprojektiin.

KVANTTITURVALLISET VAATIMUKSET JA YLEISET STANDARDIT

Suomessa Liikenne- ja viestintävirasto Traficom julkaisi vuonna 2024 kryptografiset vahvuusvaatimukset, joissa määritellään yleiskäyttöisten *National Institute of Standards and Technologyn (NIST) PQC-algoritmistandardien käyttö*

- ML-KEM, avaintenvaihdon suojaukseen lähtökohtaisesti hybridimoodissa vaaditun klassisen menetelmän kanssa
- ML-DSA, allekirjoituksiin lähtökohtaisesti hybridimoodissa vaaditun klassisen menetelmän kanssa.

Turvaluokitellun tiedon suojaamiseen on määritelty tarkasti vähimmäisvaatimukset ja aikataulusta annettu Traficomin ohjeistus: ”Hyväksyntäviranomainen suosittelee siirtymistä kvanttiturvallisten algoritmien käyttöön mahdollisuuksien mukaan mahdollisimman pian.”

Kvanttiturvallinen siirtymä koskee kuitenkin koko yhteiskuntaa ja internetiä laajemmin, ei ainoastaan kansallisia turvaluokiteltuja järjestelmiä, joita tämän hetken suositukset pääsääntöisesti kattavat. Siellä, missä tarve kvanttiturvalliselle salaukselle on jo nyt suuri, esimerkiksi salassa pidettävät henkilö- tai potilastiedot, ei välttämättä ole priorisoitu kvanttiturvallista siirtymää, koska velvoittava lainsäädäntö ja ohjeistus ovat puutteellisia. Vaikka riskit tiedostettaisiin, lasketaan sen varaan, että kvanttiuhan realisoituminen ei osu omalle kohdalle vaan nyt tehdyt laiminlyönnit tulevat eteen vasta vuosien päästä. Huoltovarmuuskeskuksen *Kvanttilaskennan tietoturvavaikutukset – suositus varautua* -tilannekatsauksesta (2024) suomalaisten huoltovarmuuskriittisten yritysten varautumisesta kvanttiuhkaan käy ilmi, että vain harva yritys oli tehnyt konkreettisia toimenpiteitä kvanttiuhkien huomioimiseksi.

NIST:n standardeista on usein tullut kaupallisissa ohjelmistoissa käytössä olevia yleisstandardeja, joita käytetään niin Euroopassa kuin Aasiassakin. On hyvin todennäköistä, että näin tapahtuu myös PQC-algoritmien kohdalla, vaikka osassa Euroopan kansallisista suosituksista on eroavaisuuksia. Esimerkiksi Saksan liittovaltion tietoturvavirasto BSI suosittelee kvanttiturvalliseen avaintenvaihtoon NIST:n kisasta 2022 tippunutta konservatiivista FrodoKEM-algoritmia, mutta sallii myös nopeamman ML-KEM:n käytön hybridimoodissa. Classic McEliece -algoritmia pidettiin vielä maaliskuuhun 2025 asti ultrakonservatiivisena kvanttiturvallisena vaihtoehtona, mutta Ranskan kyberturvavirasto ANSSI ei enää suosittele sen käyttöä uuden kryptoanalyysin valossa.

Avoin prosessi uusien algoritmien valikoimiseksi NIST:n standardiksi on kuitenkin luonteeltaan sellainen, etteivät NIST:n standardit ole yksin pohjoisamerikkalaisia, vaan useimmissa on laaja pohja asiantuntijoita ympäri maailmaa, erityisesti Euroopasta. Yleismaailmallisesti hyväksytty ja jo pitkään käytössä ollut NIST:n lohkosalainstandardi *Advanced Encryption Standard* (AES) on kvanttikestävä ja Euroopasta lähtöisin. Myös Kyber on taustaltaan osin eurooppalainen. NIST standardoi sen variantista ensisijaisen kvanttiturvallisen avaimenkapselointialgoritmin ML-KEM:n elokuussa 2024. Kyberin kehityksessä oli mukana kaupallisia toimijoita, kuten IBM, sekä akateemisia toimijoita – kryptografeja ja matemaatikkoja – Alankomaista, Belgiasta, Kanadasta, Ranskasta, Saksasta, Sveitsistä ja Yhdysvalloista. ML-KEM on jonkin verran kolmannen kierroksen Kyberiä nopeampi, koska sitä optimoitiin vielä entisestään standardoinnin aikana. NIST:n PQC-kilpailuun osallistuneista algoritmeista Kyber oli jo lähtökohtaisesti nopea. Myös suomalainen kyberturvapioneeri SSH Communications Security suositteli sitä *PQC Finland* -projektin (2022) aikaisten testien perusteella soveltuvaksi internetin verkkoprotokollien, kuten In*ternet Protocol Security* (IPsec), *Transport Layer Security* (TLS) ja *Secure Shell* (SSH), käyttöön.

Nykyisin laajassa käytössä oleva kvanttihaavoittuva RSA-salaus- ja allekirjoitusalgoritmi tullaan korvaamaan useammalla eri PQC-algoritmilla käyttökohteen mukaan. Tarvittavien algoritmien kirjoa lisäävät erilaiset vaatimukset sekä turvatasoissa että käyttöympäristöjen kyvykkyyksissä. Osa PQC-algoritmeista on tietoturvan näkökulmasta konservatiivisempia vaihtoehtoja kuin toiset. Ne kuitenkin jättävät toivomisen varaa tehokkuuden suhteen tai eivät muiden ominaisuuksiensa puolesta ole käytännöllisiä internetissä tarvittavaan viestintään.

PQC-SIIRTYMÄN PROSESSI

PQC-siirtymä on prosessina huomattavan laaja ja muodostuu pääpiirteissään seuraavista osatekijöistä:

- Menetelmät eli algoritmit: näiden arviointi ja valinta käyttökohteen mukaan. NIST:n PQC-kilpailu, kansalliset kriteerit.
- Menetelmien vaatimusten heijastaminen tiedostomuotoihin ja yhteyskäytäntöihin eli protokolliin. Standardointielimet: IETF, IEEE, ISO/IEC.

- Yhteyskäytäntöjen ja menetelmien toteutus uusiin ja tuettuihin laitteistoihin ja ohjelmistoihin. Kaupallisten tuotteiden elinkaari määräytyy pitkälle suurimpien markkinoiden mukaan, ja päivityksiä vanhaa salausta tukeviin järjestelmiin ei ole saatavissa rajattoman kauaa. Ohjelmistojen ja laitteistojen valmistajat.
- Toteutusten turva-arviointi ja viranomaiskäyttöön ja kriittiseen käyttöön hyväksyminen.
- Kansalliset viranomaiset ja näiden valtuuttamat laboratoriot.
- Järjestelmätason muutostarpeiden kartoittaminen ja siirtymän vaiheiden toteutuksen suunnittelu.
- Laitteistoja ja ohjelmistoja käyttävät organisaatiot ja järjestelmätoimittajat, asiaan liittyvät kolmannet osapuolet.
- Toteutussuunnitelman mukainen järjestelmien vaiheittainen lisäsuojaus, päivitys, käyttöönotto, koulutus, operointi ja käytöstäpoisto. Järjestelmäoperaattorit ja -toimittajat.
- Muutokset pitkäaikaisiin avaimiin – varmenteet, toimikortit – sekä levossa salatun datan uudelleensalaus uusilla menetelmillä. Laitteistotoimittajat, varmentajat, operaattorit.

Kvanttiturvallinen toteutus

Kvanttiturvallisuus vaatii tarkoituksenmukaisen kryptografian lisäksi huolellista toteutusta. Suositeltavaa on yhdistää PQC-avaimenkapselointimekanismi (KEM) ja klassinen elliptisten käyrien Diffie-Hellman (ECDH) hybridiavaimenvaihdoksi, jotta siirtyminen voidaan tehdä hallitusti ja turvallisesti olemassa olevissa järjestelmissä. Täysin uusi sovellus, jonka ei tarvitse siirtymän aikana tukea myös olemassa olevia klassista avaimenvaihtoa käyttäviä sovelluksia, voitaisiin toteuttaa ainoastaan PQC-KEM-avaimenkapselointimekanismia hyödyntäen. Hybridiavaimenvaihdossa on kuitenkin se etu, että jos nyt valittu PQC-KEM osoittautuu tulevaisuudessa heikoksi, hyökkääjän täytyy murtaa sekä PQC-KEM että klassinen ECDH, mikä lisää hyökkäyksen kustannuksia ja protokollasta riippuen myös hyökkäykseen kuluvaa aikaa. Esimerkiksi internetin alemman tason verkkoliikenteen IPsec-salausprotokollassa *Internet Key Exchange* (IKE) -hybridiavaimenvaihto ketjuttuu siten, että hyökkääjä joutuu murtamaan avaimenvaihdon yksi kerrallaan, mikä lisää hyökkäykseen kuluvaa aikaa. Internetin sovellustason *Transport Layer Security* (TLS)- ja *Secure Shell* (SSH) -salausprotokollissa puolestaan hyökkäyksen voi aloittaa samaan aikaan molempia eli ECDH:ta ja PQC-KEM:ää vastaan, mutta tärkeää kaikissa on se, että salaisuus on purettavissa ainoastaan, jos molemmat avaimenvaihdot on murrettu.

Tämän lisäksi *kvanttiärsyttävä* toteutus hyödyntää lyhyitä kryptoperiodeja siten, että uusi avaintenvaihto, *rekey*, tehdään riittävän usein saman yhteyden aikana. Näin session alussa salaukseen käytettävän kertakäyttöisen avaimenvaihdon murtamisella ei voida murtaa myöhemmin samassa sessiossa salattua tietoliikennettä. Kvanttiärsyttävä toteutus tekee hyökkäyksestä käytännössä kalliimpaa ja vaikeampaa hyökkääjälle, mikä toivottavasti johtaa siihen, että kvanttikoneen resursseja tulevaisuudessa käytetään ratkaisemaan yhteiskunnalle hyödyllisiä ongelmia.

Kryptoketteryydellä tarkoitetaan tuotteiden salausalgoritmien ja todentamisalgoritmien päivittämisen ja käyttöönoton helppoutta, kun standardit ja vaatimukset muuttuvat tulevaisuudessa. Kryptoketteryys tulee ottaa huomioon jo nyt. Käytännössä järjestelmät tullaan päivittämään iteratiivisesti siten, että internetissä on yhtä aikaa käytössä sekä kvanttiturvallisia että kvanttiturvattomia järjestelmiä. Kvanttiturvallisen määritelmä myös muuttuu ajan kuluessa. Esimerkiksi Yhdysvaltojen valtionhallinto vahvisti vuonna 2022 lain, jonka mukaan 2030 mennessä tulee suosia kvanttiturvallisia algoritmeja, mutta yhteydet sallitaan vanhoilla klassisilla algoritmeilla vuoteen 2035 asti, minkä jälkeen kvanttiturvattomia algoritmeja ei enää saa käyttää. Yhdysvaltojen *Commercial National Security Algorithm Suite* (CNSA) 2.0:ssa kvanttiturvallisen kryptografian käyttöönottovuodet on porrastettu käyttökohteiden mukaan. Esimerkiksi kvanttiturvallisten algoritmien tulee olla tuettuja ja ensisijaisesti käytössä selaimissa jo vuonna 2025.

KVANTTITURVALLINEN SIIRTYMÄ INTERNETISSÄ

Tammi–maaliskuun 2025 mittausten perusteella kvanttiturvallinen hybridiavaimenvaihto on ollut mahdollista Suomessa yli 40 prosentille selainten käyttäjistä, kun taas maailmanlaajuisesti osuus oli noin 34 prosenttia (Cloudflare Radar 2025). Kattavuus laajenee nopeasti, kun selaimia ja käyttöjärjestelmiä päivitetään uusiin versioihin. Tällä on kvanttiturvan kannalta merkitystä kuitenkin vasta, kun palvelinpää, kuten selaimella käytettävän sovelluksen web-sivusto ja kuormantasaajat, on myös päivitetty kvanttiturvalliseksi.

Internetin yli käytettävä sovellus ei ole kvanttiturvallinen, elleivät palvelun, kuten vero.fi tai kanta.fi, käyttämät yhteydet ole kvanttiturvallisia.

Huomionarvoista on, että kansalaisen yhteys julkiseen palveluun tai verkkopankkiin on kuitenkin vain jäävuoren huippu päivitystarpeesta matkalla kokonaisuudessaan kvanttiturvallisiin palveluihin. Yksittäisen käyttäjälle näkyvän palvelun taustalla on usein valtava määrä päivitettävää, esimerkiksi tietokantayhteyksiä, varmuuskopiointiyhteyksiä, erilaisia järjestelmien välisiä integraatioita, kuten auditointi- ja ylläpitoseurannan yhteyksiä, käyttöjärjestelmiä sekä etä- ja pääsynhallintajärjestelmiä.

Huhtikuussa 2025 julkaistiin avoimen lähdekoodin OpenSSL:n kvanttiturvallinen versio 3.5 TLS-toteutukseen. Se tulee vauhdittamaan kvanttiturvallista siirtymää erityisesti web-sovelluksissa. Huhtikuussa julkaistiin myös OpenSSH:n uusin

kvanttiturvallinen versio 10, jossa on ensisijaisena kvanttiturvallinen hybridiavaimenvaihto ML-KEM-algoritmilla. Ensimmäisiin kaupallisiin ratkaisuihin ML-KEM-algoritmi päivitettiin jo loppuvuodesta 2024.

KVANTTITURVALLINEN TUNNELOINTI

Olemassa olevan sovelluksen yhteydet voidaan ohjata kvanttiturvalliseen tunneliin, joka suojaa kvanttihaavoittuvaa järjestelmää turvattomassa verkossa kuten internetissä. Se on suositeltavaa erityisesti suojaustarpeessa oleville sovelluksille, joita on vaikea päivittää kvanttiturvalliseksi, tai käytössä oleviin järjestelmiin, joihin ei haluta tehdä muutoksia vielä kvanttiturvallisen siirtymän alkuvaiheessa. Samankaltaista ratkaisua on käytetty jo vuosikymmeniä kokonaan salaamattomien protokollien suojelemiseksi, mutta myös kvanttihaavoittuvaa kryptografiaa käyttävä sovellus voidaan suojata tunneloimalla.

Ison-Britannian kansallinen kyberturvakeskus *National Cyber Security Centre* (NCSC) julkaisi maaliskuussa 2025 migraatioaikatauluohjeistuksen, jossa olemassa olevien järjestelmien kohdalla vaihtoehdoksi on mainittu riskin hyväksyminen. Toimenpiteet tulisi mieluummin valita ensisijaisesti salattavan tiedon luottamuksellisuuden näkökulmasta. Edelleen käytössä olevat vanhat kriittiset järjestelmät tulee suojata, vaikka itse järjestelmän käyttämää kryptografiaa ei päivitettäisi kvanttiturvalliseksi. Tässä asiassa riskin hyväksymisen sijaan Suomen tulisi ottaa mallia Kanadasta, missä kvanttiturvalliseen kryptografiaan perustuva tunnelointi on sallittu vaihtoehto kvanttiuhan ratkaisemiseksi.

Suositeltavat vaihtoehdot:

- kvanttiturvallinen tunnelointi joko väliaikaisesti tai järjestelmän elinkaaren loppuun
- vanhan kryptografian päivitys kriittisiltä osin
- järjestelmän kokonaispäivitys modernimpaan teknologiaan, joka käyttää lähtökohtaisesti kvanttiturvallista kryptografiaa.

Kvanttiteknologia kryptografian lisänä

Tulevaisuuden ratkaisuksi kvanttiuhkaan on tarjottu kvanttiteknologiaa ja erityisesti quantum key distribution (QKD, kvanttiavaintenvaihto) -menetelmiä. Kvanttiturvallinen kryptografia PQC on jo kuitenkin käytännössä ratkaissut internetin laajuisen avaimenvaihdon, kun QKD-menetelmiä vasta kehitetään. Toisin kuin mitään olemassa olevaa kvanttiavaimenvaihtoa kvanttiturvallista kryptografiaa voi käyttää sekä verkon että myös sovellustason salauksen suojaamiseen kvanttiuhalta.

Laajamittainen QKD-menetelmien käyttöönotto vaatii internetin tasolla skaalaltaan valtavia laite- ja verkkoinfrastruktuurin muutoksia, mikä tekee ratkaisusta kalliin. QKD vaatii toimiakseen pitkillä välimatkoilla toisintajia, mikä käytännössä tarkoittaa luotettua kolmatta osapuolta – jolla käytetystä QKD-teknologiasta riippuen on hallussaan joko salaista avainmateriaalia tai mahdollisuus sabotoida yhteys.

Päästä päähän -salauksella varmistetaan, että mikään ulkoinen osapuoli ei pääse käsiksi tietoon. Se on toisintajien takia lähes mahdotonta toteuttaa laajassa QKD-verkossa kustannustehokkaasti. Vaikka QKD:tä käytettäisiin vain osana hybridiavaimenvaihtoa tuomaan teoreettista lisäsuojaa pääosin PQC-avaimenkapselointimekanismilla suojattuun yhteyteen, QKD vaatii toimiakseen valokuituyhteyden tai suoran näköyhteyden. Tämä rajaa sen käyttömahdollisuuksia, ja esimerkiksi radiosiirtotien käyttö on poissuljettua.

QKD:n toteuttamiseen voidaan valokuidun sijasta käyttää satelliittiteknologiaa, mutta erityisesti Suomen oloissa siinä on ilmeisiä heikkouksia, kuten toimintavarmuus erilaisten sääilmiöiden aikana. Häiriötä aiheuttavat auringonvalo, pilvipeite, lumi-, räntä- ja vesisade ja ilmankosteus. Suomeen soveltuvan tulevaisuuden kyberturvateknologian tulee olla toimintavarmaa ja sopeutuvaa myös pohjoisen olosuhteisiin, mitä QKD ja satelliittijärjestelmät eivät näillä leveysasteilla ole.

Sääolosuhteita voidaan kompensoida siirtämällä QKD-salausavaimiin materiaalia etukäteen ja varautumalla useamman viikon katveaikoihin. Tällöin tulisi kuitenkin ennustaa tarvittavan salausavainmateriaalin määrä, eli käytännössä sen datan määrä, joka tulee salata katveajan aikana. Sen kylkiäisenä syntyy uusi vaikeammin ratkottava ongelma: Miten ennakkosalausavainmateriaali turvataan päätelaitteilla ja toisintajissa? Missä laitteissa avainmateriaalin tulee olla käytettävissä?

Kvanttiturvallisen kryptografian selkeä etu on salausavainten laatiminen, kun niitä tarvitaan ja niin usein kuin niitä tarvitaan. Lisäksi etukäteissuunnittelua ei tarvitse tehdä sääennusteiden perusteella ja nopeisiin muutoksiin salattavan datan määrässä voidaan reagoida automaattisesti ja välittömästi.

QKD-menetelmät varmistavat kvanttimekaniikan keinoin, ettei siirtotiellä ole salakuuntelijoita. Tämä QKD:n ilmeinen hyöty on samalla sen akilleenkantapää. Jos kvanttiavaimenvaihdossa väliin pääsee valokuidussa tai satelliittiyhteydessä kolmas osapuoli – tässä tapauksessa tarkoitetaan ulkopuolista MITM:ää (man in the middle), ei QKD:n toisintajaa – tai siihen tulee ulkopuolista häiriötä esimerkiksi valokuidun dataliikenteestä, QKD itsessään paljastaa, että näin on tapahtunut ja avainmateriaali jätetään käyttämättä. Tämä turvallisuutta korostava ominaisuus mahdollistaa samalla myös palvelunestohyökkäyksen, ja järjestelmä on haavoittuvainen sabotaasille ja häirinnälle.

Kvanttiturvalliseen kryptografiaan perustuvissa järjestelmissä pelkkä salatun liikenteen seuraaminen ei aiheuta palvelunestohyökkäystä. Verkkoprotokollat, joita

kryptografiaa käyttävät tietoturvasovellukset hyödyntävät, on suunniteltu lähtökohtaisesti niin, että niitä voidaan käyttää turvattomassa verkossa kuten internetissä ja liikenne reitittyy automaattisesti uudestaan ja mahdolliset ulkopuolisen yritykset muokata salattua liikennettä havaitaan itse tietoturvasovellusprotokollassa.

Hyökkääjällä on aina etulyöntiasema, kun sabotointi- tai palvelunestohyökkäyksen voi ajoittaa hyökkääjälle sopivasti silloin, kun sääolosuhteet tai poliittiset olosuhteet ovat satelliittiteknologiaa hyödyntävälle QKD:lle epäsuotuisat.

Yhteenvetona: QKD-menetelmissä on ylitsepääsemättömiä käytännön ongelmia:

- Toisintaja (repeater) on luotettu kolmas osapuoli.
- Palvelunestohyökkäyspotentiaali.
- PQC:tä tarvitaan joka tapauksessa autentikointiin sekä valokuiduttomiin yhteyksiin.

Kvanttiavaintenvaihto on kallis, tutkimusvaiheessa oleva ratkaisu, jota ei pysty hyödyntämään turvallisesti olemassa olevalla internetin infrastruktuurilla. Siinäkin tilanteessa, että meillä olisi Suomessa satelliitti-QKD:n kannalta ideaali-ilmasto, sijaitsisimme lähempänä päiväntasaajaa ja meillä olisi tiheästi linkittyvä kaupunkiverkosto, jotta noin 50–100 kilometrin välein olisi mahdollisuus luotettuihin tulevaisuuden toisintajiin, sekä rajattomasti resursseja uuteen teknologiaan ja erillisiin datavalokuitu- ja pimeävalokuituinvestointeihin, QKD ratkaisisi salauksen avaintenvaihdon internetissä vain osittain ja kvanttiturvallista tunnistautumista ei laisinkaan. QKD on tutkimuskohde, josta saattaa pitkällä aikavälillä tulla hyödyllisiä ratkaisuja mahdollisesti johonkin muuhun kuin mihin sitä on testiympäristöissä tähän mennessä maailmalla käytetty. Kvanttiturvallisen internetin osana sillä on kapea käyttökohde ja siten marginaalinen hyöty.

Tietoturvan muutokset tulevaisuudessa

Tietoturvassa, erityisesti kryptografiassa, noudatetaan yleensä konservatiivisia periaatteita. Muutoksia tehdään harkiten ja vain kun niihin on perusteltu tarve, sillä aina on riski, että parannusten mukana tulee uusia haavoittuvuuksia ja epäyhteentoimivuutta.

Historiallisesti uuteen kryptografiseen algoritmiin on siirrytty, kun edellisen standardin turvallisuus on kyseenalaistettu tai se on osoitettu käytännössä haavoittuvaksi. Toisinaan uusi algoritmi tuo merkittävän parannuksen käyttönopeuteen tai tehokkuuteen, kuten siirtyminen äärellisen kentän Galois Field Diffie-Hellman (DH) -avaimenvaihdosta elliptisten käyrien avaimenvaihtoon (ECDH). Kvanttiturvallisessa siirtymässä osassa käyttötapauksista päästään myös käyttönopeuden

parannukseen klassisiin avaimenvaihtomekanismeihin verrattuna, mutta suurin motivaatio on klassisten metodien mureneminen kvanttiuhan paineen alla.

TIIVISTEALGORITMIT

Joskus uudet standardit tulevat käyttöön hyvin hitaasti, esimerkkinä Secure Hash Algorithm -tiivistealgoritmien SHA-2 ja SHA-3 tilanne. SHA-3 on ollut standardi jo vuosia, mutta sitä ei ole otettu laajaan yleiskäyttöön osin siksi, että SHA-2 on näkyvissä olevat uhat kestävä, kvanttiturvallinen, laajassa käytössä oleva ja nykyisillä laitteilla tehokkaasti toteutettavissa. Edellinen siirtymä SHA-1:stä SHA-2:een on ollut haastava prosessi, joka alkoi jo 2000-luvun alussa ja kiihtyi, kun SHA-1:n törmäyskestävyydestä löytyi haavoittuvuuksia. Yli kaksi vuosikymmentä myöhemmin SHA-1 on edelleen käytössä monissa järjestelmissä. Salausalgoritmien ongelmakenttää kuvaa, että rikkonaisella SHA-1-tiivistefunktiolla on käyttökohteita, kuten tiivistepohjainen viestien todennuskoodi (HMAC), joissa se on edelleen käyttökelpoinen. HMAC:n turvallisuus ei perustu tiivistefunktion törmäyskestävyyteen toisin kuin esimerkiksi varmenteiden allekirjoituksissa. Kvanttiturvallisen siirtymän yhteydessä on kuitenkin hyvä tilaisuus tehdä salausjärjestelmien suurempi määräaikaishuolto ja päästä eroon vanhentuneesta painolastista. Jos SHA-1 sallitaan sille edelleen soveltuvissa käyttökohteissa, riski on iso sille, että sitä käytettäisiin vahingossa sellaisissa käyttökohteissa, joissa se on haavoittuva.

Yhdysvaltojen valtionhallinnon Commercial National Security Algorithm Suite (CNSA) 2.0:ssa määritellään menetelmät, joita valtionhallinnon tietojärjestelmissä käytettävissä kaupallisissa ohjelmistoissa tulee toteuttaa. CNSA 2.0:ssa edellytetään NIST:n PQC-algoritmien käyttöä, AES-salausta ja SHA-2-tiivistefunktiota. Uudempi SHA-3-tiivistefunktio ja sen SHAKE on sallittu vain osana ML-KEM-algoritmia, mutta yleiskäyttöisenä tiivistefunktiona sitä ei sallita. SHA-3:n suunnittelussa sivukanavahyökkäykset on huomioitu paremmin kuin SHA-2:ssa, mutta tämä ei ole ollut riittävä peruste tehdä siirtymää SHA-2:sta SHA-3:een. Molemmista on 128-bittistä, 192-bittistä ja 256-bittistä turvatasoa vastaavat variantit. Todennäköisesti SHA-3:een tullaan kuitenkin siirtymään jollakin aikavälillä, koska ei ole kustannustehokasta toteuttaa rautakiihdytystä sekä SHA-2:lle että SHA-3:lle. Kvanttiuhan kannalta siirtymään ei kuitenkaan ole tarvetta, ja siksi hyvin todennäköisesti siirtyminen SHA-3:een yleiskäyttöisenä tulee tapahtumaan Yhdysvalloissa vasta myöhemmin tulevaisuudessa.

VAIHTOEHTOISET KVANTTITURVALLISET ALGORITMIT

Kvanttiturvalliseen todentamiseen ja tunnistamiseen siirtyminen tulee olemaan haastavaa ratkaista maailmanlaajuisesti. NIST julkaisi elokuussa 2024 yhtä aikaa ML-KEM-standardin kanssa yleiskäyttöisen digitaalisen ML-DSA-allekirjoitusalgoritmin sekä SLH-DSA-allekirjoitusalgoritmin. Hilapohjainen ML-DSA ei valitettavasti sovellu suurempien avainten ja allekirjoituksen takia yleiskäyttöisesti korvaamaan kaikkia kvanttihaavoittuvia RSA- ja elliptisten käyrien allekirjoitusmenetelmiä. Toiveet paremmin sopivasta menetelmästä kohdistuvatkin NIST:n PQC-jatkokilpailun allekirjoitusalgoritmeihin. Näistä odotetaan löytyvän hilame-

netelmille vaihtoehtoinen ja profiililtaan ML-DSA:ta pienempi menetelmä. Uusien todentamis- ja tunnistamisalgoritmien standardointi kestää vielä vuosia. Niitä ei todennäköisesti oteta käyttöön ML-DSA:n rinnalle ennen vuotta 2030 tai edes 2035 mennessä, ellei vaihtoehtoisten allekirjoitusalgoritmien tehokkuus ole merkittävästi parempi. Pitkään työn alla on ollut Falcon, joka myös valittiin standardoitavaksi vaihtoehtoiseksi allekirjoitusalgoritmiksi samaan aikaan kuin Dilithium vuonna 2022. Vaikka FN-DSA:ksi kaavailtu Falcon-algoritmi standardoitaisiinkin pian, se ei välttämättä tule aktiiviseen käyttöön, koska sillä ei ole juurikaan etuja verrattuna ML-DSA:han. Falcon-algoritmin turvalliset toteutukset ovat haastavia, ja senkin vuoksi sen käyttö jää todennäköisesti vähäiseksi.

NIST:n PQC-kilpailun neljänneltä kierrokselta valittiin maaliskuussa 2025 vaihtoehtoinen avaimenkapselointimekanismi HQC standardoitavaksi siltä varalta, että joskus tulevaisuudessa hilapohjaisista PQC-algoritmeista löydetään klassinen tai kvanttiheikkous ja on tarve siirtyä ML-KEM:stä toisenlaiseen matematiikkaan perustuvaan PQC-algoritmiin. Standardoinnin odotetaan kestävän ainakin vuoteen 2027 asti. Sen jälkeen menee todennäköisesti useampia vuosia, että HQC tulee osaksi standardoituja tietoliikenneyhteyskäytäntöjä ja sitä kautta mahdollisesti vaihtoehdoksi yleiseen käyttöön.

NIST kehittää myös kevytsalausstandardia (Light Weight Encryption, LWE), joka on Ascon-algoritmiin perustuva kvanttiturvallinen symmetrinen salausalgoritmi. Se on tarkoitettu energiarajoitteisiin, muun muassa akkukäyttöisiin, laitteisiin, joihin AES-lohkosalain ei niin hyvin sovellu. Internet of (Industrial) Things -laitteiden määrä jatkaa räjähdysmäistä kasvuaan, ja vähäenergisissä ympäristöissä kevytsalaukselle on käyttöä.

On tarpeen huomioida kansallisessa tietoturvakriteeristössä myös nämä uudet käyttötapaukset.

DATAKESKEINEN TURVALLISUUS JA TRENDIT

Kvanttiturvallisen siirtymän rinnalla pidemmällä aikajänteellä on odotettavissa siirtymä datakeskeiseen turvallisuuteen (data-centric security). Nykyisissä järjestelmissä pääsynhallinta on usein erotettu datasta. Kontrollit ovat tiedonkäsittelyympäristön, -laitteen tai -sovelluksen tasolla, mutta eivät tietoalkioiden ja dokumenttien tasolla. Datakeskeisyydessä suojausmääritykset ja pääsynvalvonta on määritelty dokumenttitasolla ja ne salataan kunkin käyttäjän rooli- tai henkilöavaimille erikseen. Lisäksi dokumentteja ja muuta dataa tullaan säilyttämään enenevässä määrin salattuna myös silloin, kun data ei ole käytössä.

Nollaluottamusfilosofia (zero trust) ja erityisesti sen näkyvyys- ja analytiikkapilareiden tarve kyberpuolustuksen tukena kasvattaa merkitystään, kun rikollisuus siirtyy tekoälyavusteisiin hyökkäyksiin, joiden havainnointiin ja torjumiseen ihmisoperaattoreiden suorituskyky ei riitä.

Kaupallisia ratkaisuja pyritään maailmalla käyttämään kasvavassa määrin valtionhallinnon tarpeisiin commercial for national security -ajattelun mukaisesti. Kaupalliset tuotteet ovat kustannuksiltaan huomattavasti räätälöityjä ratkaisuja edullisempia.

Euroopan unionin kyberkestävyyssäädös vaatii ohjelmistotuotteilta CE-merkin. Jotta vaadittavat sertifioinnit on mahdollista saada tärkeille ja kriittisille järjestelmille ja samalla voidaan säilyttää suomalaisen laitteisto- ja ohjelmistoteollisuuden kilpailukyky, on panostettava myöntämiskyvykkyyden kehittämiseen.

Termistö

Suomennokset, lyhenteet ja artikkelissa käytetyt termit aakkosjärjestyksessä.

- AES *Advanced Encryption Standard,* lohkosalainalgoritmi. NIST standardoi Rijndaelin variantin AES:ksi vuonna 2001. Kvanttikestävä, kunhan avain on tarpeeksi pitkä. Esimerkiksi Isossa-Britanniassa vaaditaan vähintään 128-bittinen avain ja Yhdysvalloissa 256-bittinen avain.
- CNSA 2.0 *Commercial National Security Algorithm Suite*. Yhdysvaltojen kvanttikestävät algoritmivaatimukset kaupallisille ratkaisuille kansallisen turvallisuuden järjestelmissä.
- Diffie-Hellman (DH). Klassinen kvanttihaavoittuva avaimenvaihtomekanismi, jota käytetään esimerkiksi IPsec- ja SSH-yhteyksissä.
- ECC. Elliptisten käyrien kryptografia, joka on kvanttihaavoittuvaa ja tulee korvata kvanttiturvallisilla algoritmeilla tai jota tulee vahvistaa esimerkiksi kvanttiturvallisella ML-KEM-metodilla hybridimoodissa. Käytetään esimerkiksi TLS- ja SSH-yhteyksissä.
- FIPS *Federal Information Processing Standards*. Yhdysvaltojen liittovaltion informaationkäsittelystandardit, joita jokaisen valtionviraston tulee käyttää.
- ”Haali nyt, pura myöhemmin” -hyökkäys
  Harvest now, decrypt later attack
  Kerätään talteen kiinnostavista lähteistä tulevaa kommunikaatiota purettavaksi myöhemmin, kun riittävän tehokas menetelmä tai laitteisto on saatavilla.
- HQC *Hamming Quasi-Cyclic*. Vaihtoehtoinen kvanttikestävä julkisen avaimen kryptografian algoritmi, jonka NIST valitsi vuonna 2025 standardoitavaksi varalle, jos nykyisestä hilapohjaisesta kvanttikestävästä julkisen avaimen kryptografiasta löydetään tulevaisuudessa haavoittuvuus ja ensisijainen ML-KEM täytyy korvata.

- Kvanttiturvallinen kryptografia
  Post-quantum cryptography (PQC)
  Kvanttiuhkaa sietävää matematiikkaan perustuvaa kryptografiaa pohjautuen ongelmiin, joihin ei tunneta perinteisellä tietokoneella eikä kvanttitietokoneella toimivaa tehokasta ratkaisua.
- Kvanttihaavoittuva kryptografia
  Quantum-vulnerable cryptography
  Matematiikkaan perustuvaa julkisen avaimen kryptografiaa, jonka perustana olevaan ongelmaan tunnetaan tehokas kvanttialgoritmi. Haavoittuvia algoritmeja esimerkiksi RSA, ECC, Diffie-Helman (DH) ja ECDH.
- Kvanttikestävä
  Quantum-resilient
  Synonyymi kvanttiturvalliselle algoritmille tai toteutukselle, joka kestää sekä tulevaisuuden kvanttikoneella että supertietokoneella avustetun hyökkäyksen.
- Kvanttiärsyttävä
  Quantum-annoying
- LWE *Light Weight Encryptio*n. Tuleva NIST-standardi Ascon-algoritmista. Kevytsalain AES:n vaihtoehdoksi laitteisiin, joihin AES ei sovellu.
- ML-DSA *Module Lattice (-based) Digital Signature Algorithm*. Hilapohjainen kvanttikestävä FIPS 204 -standardi, jonka NIST standardoi Chrystals-Dilithium-variantista vuonna 2024.
- ML-KEM *Module Lattice (-based) Key-Encapsulation Mechanism*.
  Hilapohjainen kvanttikestävä FIPS 203 -avaimenkapselointistandardi, jonka NIST standardoi Chrystals-Kyber-variantista vuonna 2024.
- NIST *National Institute of Standards and Technology*.
  Yhdysvaltalainen valtionvirasto, jonka tehtävänä on esimerkiksi valita julkisella kilpailulla kryptografiset algoritmit, joista kehitetään ja julkaistaan FIPS-standardit.
- Nollaluottamus
  Zero trust
  Kyberturvan tavoitetila, jossa esimerkiksi käyttäjien ja järjestelmien identiteetti ja valtuudet tarkistetaan automaattisesti joka kerta riippumatta siitä, ovatko yhteydet sisäverkossa vai internetissä.
- QKD *Quantum key distribution*. Kvanttiavaintenvaihto, tutkimusvaiheessa oleva kvantti-ilmiöön perustuva teknologia, jolla voidaan siirtää avainmateriaalia valokuidun tai satelliitin avulla. Ei suositella missään Pohjois-Amerikassa tai Euroopassa valtiollisen tahon toimesta, eikä sallita missään ainoana mekanismina.
- RSA. Kvanttihaavoittuva julkisen avaimen kryptografian algoritmi, joka on ollut käytössä vuosikymmeniä ja joka täytyy korvata erilaisilla kvanttiturvallisilla algoritmeilla eri käyttökohteissa.

- SLH-DSA *Stateless Hash-Based Digital Signature Algorithm*. Tilaton tiivistepohjainen kvanttikestävä FIPS 205 -standardi, jonka NIST standardoi SPHINCS+-variantista vuonna 2024.

Lähteet

PQC Finland (2022) *Kvanttiturvalliset salausmenetelmät Suomessa.* https://publications.vtt.fi/julkaisut/muut/2022/Kvanttiturvalliset-salausmenetelm%c3%a4t-Suomessa.pdf (viitattu 3.2.2025)

BSI (2024) *Position Paper on Quantum Key Distribution*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html?nn=916626 (viitattu 3.2.2025).

Traficom (2024) *Kvanttiturvalliset algoritmit ja niihin siirtyminen*. https://www.kyberturvallisuuskeskus.fi/fi/kvanttiturvalliset-algoritmit-ja-niihin-siirtyminen (viitattu 10.2.2025).

Traficom (2024) Kvanttiturvallisia algoritmeja lisätty kansalliseen kriteeristöön. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kvanttiturvallisia-algoritmeja-lisatty-kansalliseen-kriteeristoon (viitattu 10.2.2025).

Huoltovarmuuskeskus (2024) *Kvanttilaskennan tietoturvavaikutukset – suositus varautua.* https://www.huoltovarmuuskeskus.fi/files/f373b420acf314b4e6d5e70c24393593c3ad27c8/hvk-kvanttilaskennan-tietoturvavaikutukset-raportti-2024.pdf (viitattu 12.3.2025).

EU PQC joint statement (2024) *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography.* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf (viitattu 12.3.2025).

NIST (2024) Post-Quantum Cryptography: Additional Digital Signature Schemes. https://csrc.nist.gov/projects/pqc-dig-sig (viitattu 8.4.2025).

NIST (2025) HQC Announced as a 4th Round Selection. https://www.nist.gov/news-events/news/2025/03/nist-pqc-standardization-process-hqc-announced-4th-round-selection (viitattu 8.4.2025).

UK NCSC (2025) *Timelines for migration to post-quantum cryptography.* https://www.ncsc.gov.uk/guidance/pqc-migration-timelines (viitattu 8.4.2025).

Cloudflare Radar (2025) Post-Quantum encrypted share of HTTPS request traffic. https://radar.cloudflare.com/adoption-and-usage#post-quantum-encryption-adoption (viitattu 31.3.2025).

EDUSKUNTA
RIKSDAGEN