Kvanttilaskennan aiheuttama kyberuhka ja siihen varautuminen

Perusteet, riskit, sääntely ja siirtymä kohti kvanttiturvallista salausta

Perusteet

Kyberuhka

Varautuminen

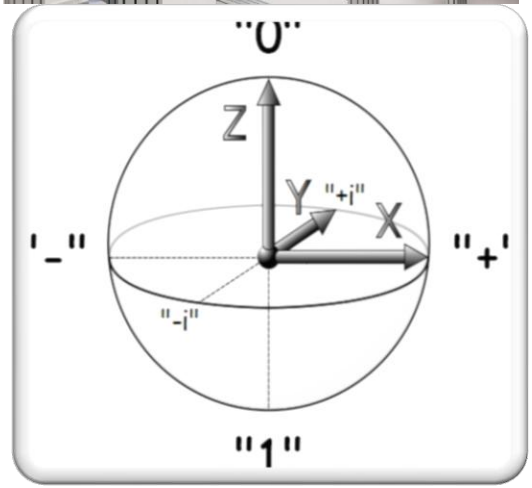
Ajankohtaista riskienhallinnasta: Kvanttilaskenta

02.06.2026

Visa Vallivaara, Research Team Leader visa.vallivaara@vtt.fi
Petri Puhakainen, Cybersecurity Lead petri.puhakainen@vtt.fi

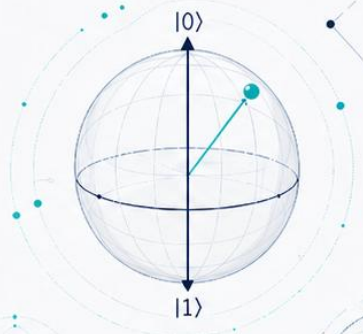
Bitti ja Kubitti

Character	ASCII code	Binary code
null character	0	0000000
a	97	1100001
b	98	1100010
c	99	1100011
A	65	1000001
B	66	1000010
C	67	1000011
%	37	0100101
+	43	0101011
0	48	0110000
1	49	0110001
Delete	127	1111111



Kvanttilaskennan neljä keskeistä käsitettä

Kvanttilaskenta on merkityksellistä kyberturvallisuuden kannalta, koska se hyödyntää luonnon ilmiöitä, jotka eroavat perustavanlaatuisesti klassisen laskennan ilmiöistä.



1 Kvantti

Kvantti on pienin mahdollinen energia- tai vuorovaikutusyksikkö.

Hyvin pieniiä mittakaavoilla luonto käyttäytyy tavalla, jota klassiset tietokoneet eivät voi tehokkaasti simuloida.

2 Kubitti

Kubitti on kvanttitietokoneen tiedon yksikkö.

Ennen mittausta se voi olla 0, 1 tai näiden yhdistelmä.

Mitä enemmän kubitteja, sitä enemmän laskentateho kasvaa eksponentiaalisesti.

3 Superpositio

Kubitti voi olla useassa tilassa samanaikaisesti, kunnes se mitataan.

Tämä mahdollistaa vaihtoehtojen käsittelyn rinnakkain.

4 Lomittuminen

Kubitit voivat lomittua niin, että toisen mittaaminen vaikuttaa välittömästi toiseen, riippumatta etäisyydestä.

Yhdessä superposition kanssa tämä tekee kvanttilaskennasta perustavanlaatuisesti erilaisen kuin klassinen laskenta.

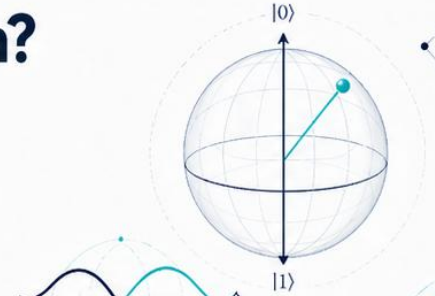
Ydinviesti

- Kvanttilaskenta hyödyntää kvantti-ilmiöitä, joita ei esiinny klassisen laskennan maailmassa.
- Kubitti, superpositio ja lomittuminen selittävät kvanttilaskennan potentiaalisen etulyöntiaseman.
- Nämä käsitteet auttavat ymmärtämään, miksi kyberuhka on olemassa.

Laskennalliset ongelmet

Miksi kvanttilaskenta aiheuttaa kyberuhan?

Nykyinen internetin tietoturva perustuu julkisen avaimen salaustekniikkaan, kuten RSA:han, Diffie–Hellmaniin ja ECC:hen. Peter Shor osoitti, että riittävän suuri kvanttitietokone voi ratkaista näiden algoritmien taustalla olevat ongelmat tehokkaasti.



1 Internetin peruspilarit

RSA, Diffie–Hellman ja ECC perustuvat matemaattisiin ongelmiin, jotka ovat klassiselle tietokoneelle käytännössä ratkaisematomia.

2 Shorin algoritmi

Riittävän suurella kvanttitietokoneella nämä ongelmat voidaan ratkaista polynomisessa ajassa.

3 Mikä murtuu?

Julkisen avaimen salaus on kriittinen riski TLS-avaintenvaihdossa, S/MIME-viesteissä, varmenteissa, ohjelmistojen allekirjoituksissa, VPN-yhteyksissä ja kryptolompakoissa.

4 Mikä kestää paremmin?

Symmetrinen salaus ja hash-funktiot kestävät kvanttihyökkäyksiä paremmin, mutta lyhyemmät avainpituudet menettävät turvamarginaalia. AES-256 on hyvä valinta pitkäikäisiin käyttötarkoituksiin.

5 Kerää nyt, pura myöhemmin + Moscan teoreema

Hyökkääjä voi kerätä tietoa salattuna jo tänään ja purkaa sen myöhemmin.

$$X + Y > Z$$

- X = tietojen luottamuksellisuuden elinkaari (vuosia)
- Y = siirtymän kesto (vuosia)
- Z = aika (vuosia) siihen, kunnes hyökkääjällä on riittävän tehokas kvanttitietokone

Ydinviesti

- Suurin kvanttiuhka kohdistuu julkisen avaimen salaustekniikkaan.
- Pitkäikäiset luottamukselliset tiedot ovat jo tänään vaarassa.
- Jos $X + Y > Z$, valmistautuminen on myöhässä.

Kvanttilaskennan kehitys

VTT

Resurssiarvioiden väheneneminen RSA:n murtamiseen:

[Submitted on 23 May 2019 (v1), last revised 13 Apr 2021 (this version, v3)]

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

[Submitted on 21 May 2025]

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

[Submitted on 12 Feb 2026]

The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes

Paul Webster, Lucas Berent, Omprakash Chandra, Evan T. Hockings, Nouédyn Baspin, Felix Thomsen, Samuel C. Smith, Lawrence Z. Cohen

[Submitted on 30 Mar 2026]

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain, Qian Xu, Robbie King, Lewis R. B. Picard, Harry Levine, Manuel Endres, John Preskill, Hsin-Yuan Huang, Dolev Bluvstein

Kaksi tutkimusta kvanttiuhkasta

Aiheet, tekijät ja miksi tulokset ovat tärkeitä

VTT

Tutkimus 1

Shor + atomikubitit

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Aihe

Kuinka pienellä neutraaliatomiarkkitehtuurilla Shorin algoritmia voisi ajaa kryptografisesti merkittävässä mittakaavassa.

Tekijät

Madelyn Cain, Qian Xu, Robbie King, Lewis R. B. Picard, Harry Levine, Manuel Endres, John Preskill, Hsin-Yuan Huang, Dolev Bluvstein

Keskeinen havainto

- **10 000** uudelleenjärjesteltävää atomikubittia
- **26 000** fyysistä kubittia: ECC/P-256 jopa päivissä
- **RSA-2048** selvistä hitaampi kuin ECC

Tutkimus 2

ECC + kryptovaluutat

Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations

Aihe

Elliptisen käyrän kryptografian ja kryptovaluuttojen kvanttihaavoittuvuudet sekä resurssiarviot ja lievennyskeinot.

Tekijät

Ryan Babbush, Adam Zalcman, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi, Justin Drake, Dan Boneh

Keskeinen havainto

- **1200–1450** loogista kubittia
- **< 500 000** fyysistä kubittia: secp256k1-riski
- **ECC** hyökkäysaika voi painua minuutteihin

Yhteinen viesti

Resurssiarviot pienenevät
Kvanttiuhka voi tulla lähemmäs aiempia arvioita nopeammin.

ECC korostuu riskinä
Julkisen avaimen järjestelmät, allekirjoitukset ja varmenteet vaativat huomiota.

Varautuminen alkaa nyt
Inventoi, priorisoi ja rakenna kryptoketteryys.

Lähteet: Cain et al. 2026; Babbush et al. 2026

Kriittinen tieto on osa huoltovarmuutta

Tieto + salaus + jatkuvuus

Kriittiset tiedot

Toiminnan jatkuvuus

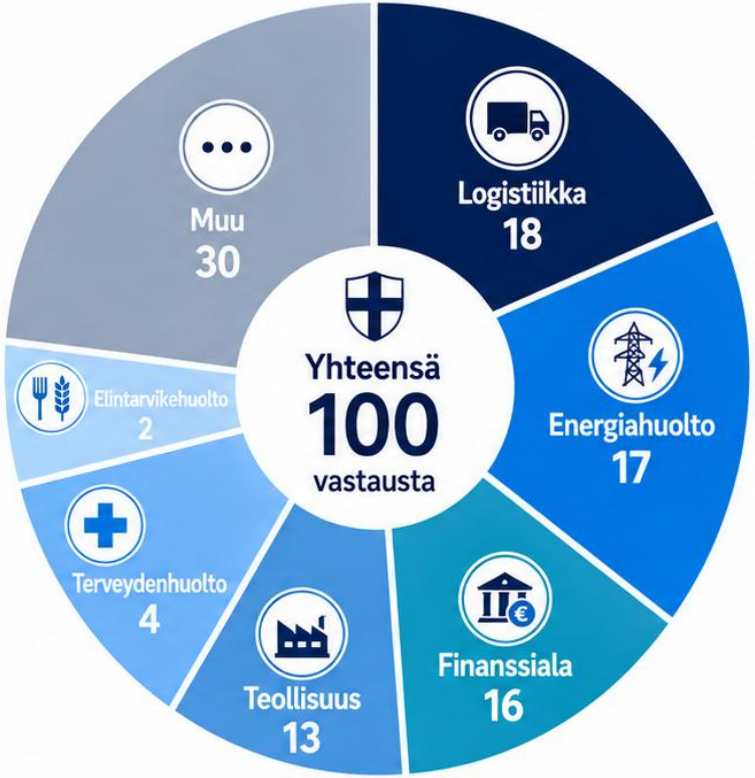
Kansallinen turvallisuus

Lähteet: HVK 2024; Cain et al. 2026; Babbush et al. 2026

Huoltovarmuustoimijoiden toimialat

Kerätyt vastaukset toimialoittain (n = 100)

- Muu 30
- Logistiikka 18
- Energiahuolto 17
- Finanssiala 16
- Teollisuus 13
- Terveydenhuolto 4
- Elintarvikehuolto 2



Muu sisältää mm.

media ja viestintä,
vesiteollisuus,
valtionhallinto,
ympäristönhuolto

Vastaajayritysten koko

44 %	38 %	17 %
suuria (>250 hlö)	keskikokoisia (50–249 hlö)	pieniä

Lähde: HVK 2024, Kuva 2

Mitä suojataan?

Kriittiset tiedot ja yhteydet

- Asiakas- ja henkilötiedot
- Luottamukselliset dokumentit
- Autentikaatio ja varmenteet
- Tietoliikenne
- Tietokannat
- Etäyhteydet

94 % käyttää salausta tiedonsiirtoon

55 %: lla yli 10 v suojattavaa

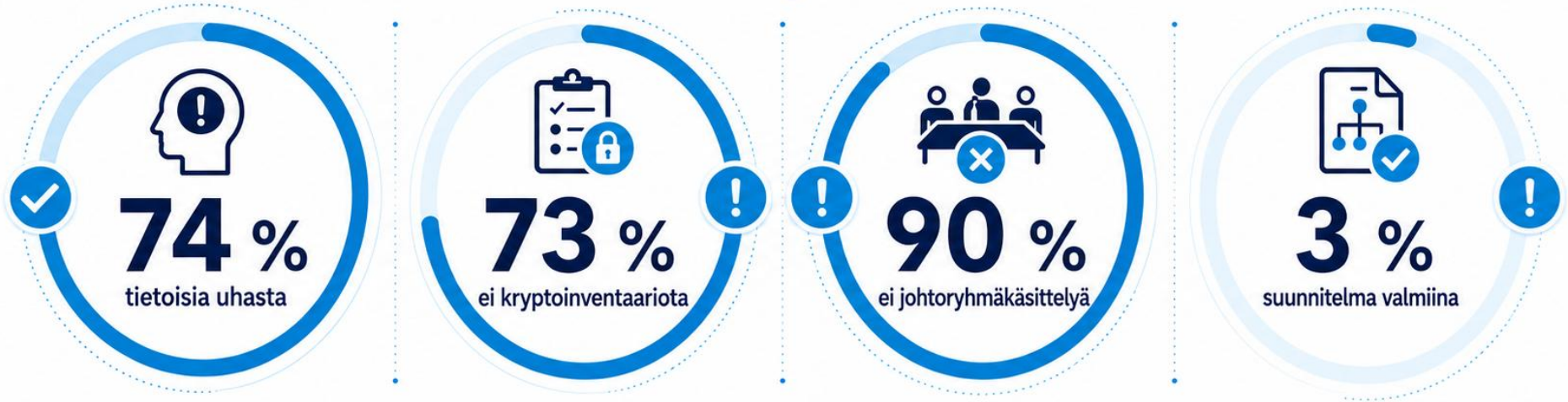
Lähteet: HVK 2024; Cain et al. 2026; Babbush et al. 2026

Pitkä salassapitoaika lisää riskiä

Tallenna nyt, pura myöhemmin

Lähteet: HVK 2024; Cain et al. 2026; Babbush et al. 2026

Tietoisuutta on – valmius puuttuu



Inventaario puuttuu

Osaaminen rajallista

Toimet vähäisiä

Lähteet: HVK 2024; Cain et al. 2026; Babbush et al. 2026

Kryptoinventaario

Et voi suojata sitä, mitä et tunne

Lähteet: HVK 2024; Cain et al. 2026; Babbush et al. 2026

Kryptoketteryys

Kyky vaihtaa algoritmit nopeasti ja hallitusti

Nykyiset algoritmit

- RSA
- ECC
- AES

Vaihdettavat algoritmit

- ML-KEM
- ML-DSA
- SLH-DSA

Algoritmit vaihdettavissa

Palvelu pysyy käynnissä

Älä sido turvallisuutta yhteen algoritmiin

Nopea reagointi
Heikot algoritmit voidaan vaihtaa nopeasti

Jatkuvuus
Muutokset ilman suurta käyttökatkoa

Hallittavuus
Yksi malli, monta algoritmia

Valmius kvanttiuhkaan
Siirtymä uusiin menetelmiin helpottuu

Ydinajatus

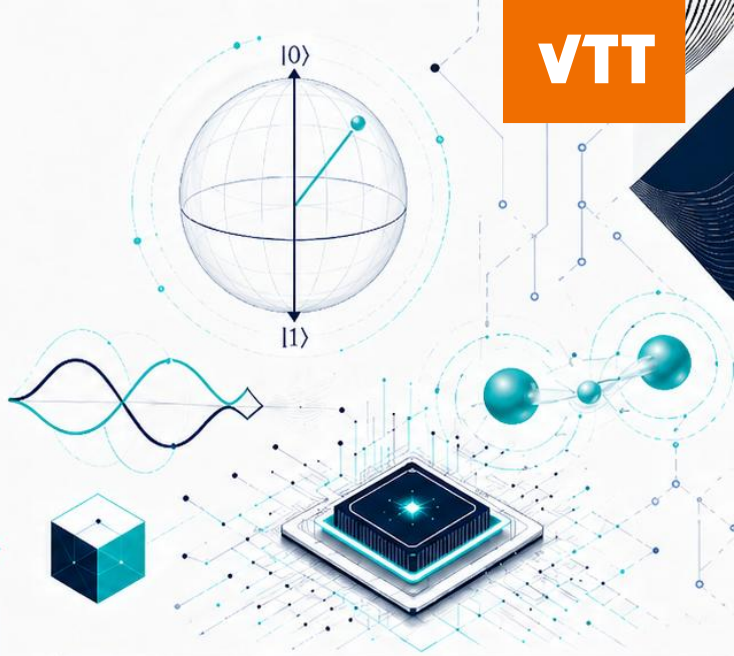
Inventoi → Suunnittele → Testaa → Vaihda

Siirtymän aikataulu

Käyttökelpoisen kvanttitietokoneen tarkka ajankohta on epävarma, mutta arviot siirtyvät yhä varhaisemmaksi – siksi käytännön suunnittelun aikahorisontti on tärkeämpi kuin tarkka vuosiarvaus.

KRIITTISIÄ JÄRJESTELMIÄ KOSKEVA MAALI: 2030

LAAJEMPI KOKONAISUUS MAHDOLLISIMMAN LAAJASTI: 2035



1

Ensimmäinen vuosi

Kryptoinventaario, riskinarviointi ja arkkitehtuurityö kryptojoustavuuden mahdollistamiseksi.

2

2027–2029

Pilotit ja kriittisten järjestelmien siirtymä.

3

2030–2033

Siirtymän päävaihe laajassa mittakaavassa koko organisaatiossa.

4

2034

Viimeisten OT/IoT-järjestelmien siirtymä.

Realistinen organisaatiotason siirtymä vie useita vuosia.

Ydinviesti

- Älä odota tarkkaa päivämäärää – aloita nyt.
- Kriittisten järjestelmien siirtymä vuoteen 2030 mennessä.
- Suunnittele laajempi siirtymä vuoteen 2035 mennessä.

Siirtymän suunnittelu

Siirtymä kvanttiresilienttiin salaukseen ei ole yksittäinen päivitys – se vaikuttaa sovelluksiin, infrastruktuuriin, hankintoihin, sopimuksiin ja toimittajiin, joten se alkaa nykytilan kartoituksesta ja suunnittelusta.

1 Vastuut

Nimetään omistaja. Toiminnallinen vastuu voi olla CISO:lla tai tietoturvajohtajalla, mutta ICT- ja teknologiajohdon tulee sitoutua vahvasti. Tarvitaan myös arkkitehtuurityötä, riskienhallintaa ja hankintoja. Suurissa organisaatioissa erillinen siirtymäohjelma, budjetti ja raportointi on hyvä käytäntö.

2 Kryptoinventaario

Laadi inventaario siitä, missä kaikkialla julkisen avaimen kryptografiaa käytetään organisaatiossa.

3 Mitä inventoidaan?

- TLS-varmenteet
- VPN- ja SSH-avaimet
- Ohjelmistojen allekirjoitussertifikaatit
- S/MIME ja digitaalinen allekirjoitus
- Tietokannat ja varmuuskopiot, jos ne perustuvat epäsymmetrisiin avaimiin
- Upotetut, teolliset ja verkottuneet laitteet
- Kolmansien osapuolten ohjelmistot ja pilvipalvelut

4 Riskiperusteinen priorisointi

Priorisoi luottamuksellisuuden keston ja liiketoiminnallisen kriittisyyden perusteella. Ensiksi kohteet, joilla on pitkä salassapitotarve tai korkea vaikutus, kuten terveys-, rahoitus- ja oikeudelliset tiedot, T&K-aineistot, juurivarmenteet, koodin allekirjoitus ja identiteetin hallinta.

5 Kryptoketteryys sekä toimittajat

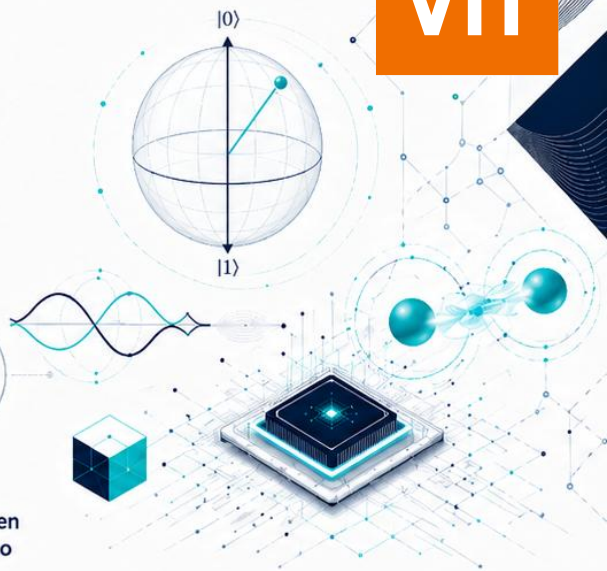
Rakenna kyvykkyys vaihtaa algoritmeja nopeasti abstraktiokerrosten, algoritmitunnisteiden ja keskitetyn avainhallinnan avulla. Lisää kvanttiresilientit vaatimukset sopimuksiin, vaadi toimittajien siirtymäsuunnitelmat ja edellytä NIST-tuki.

Ydinviesti

- Nimeä omistajuus ja ohjelman hallintamalli.
- Aloita kryptoinventaariolla ja priorisoinnilla.
- Toimittajat ja hankinnat ovat osa siirtymää.

Toteutus teoriasta käytäntöön

Siirtymä kvanttiresilienttiin suojaan perustuu NIST-standardeihin ja toteutetaan hallitusti vaiheittain käyttäen hybridiratkaisuja ennen täyttä siirtymää.



1 Pilotit testiympäristössä

Valitse yksi ei-kriittinen palvelu ja ota käyttöön hybridi-TLS. Mittaa suorituskyky, viive ja yhteensopivuus.

2 Pilotit tuotannossa

Laajenna käyttö rajatusti ja valitse kohde, jossa paluu vanhaan on helppoa.

3 Varmenneketju

Päivitä ensin sisäinen varmenne-infrastruktuuri tukemaan kvanttiturvallisia allekirjoituksia. Siirrä päätelaitteet vasta sen jälkeen.

4 Avainpituudet ja tiivisteet

Vaihda AES-128 AES-256:een siellä, missä se on perusteltua.

5 Korkean prioriteetin järjestelmät

Siirrä ensin pitkäikäistä tietoa käsittelevät järjestelmät sekä identiteetinhallinta, ohjelmistojen allekirjoitus ja kriittiset rajapinnat.

6 Laajamittainen käyttöönotto

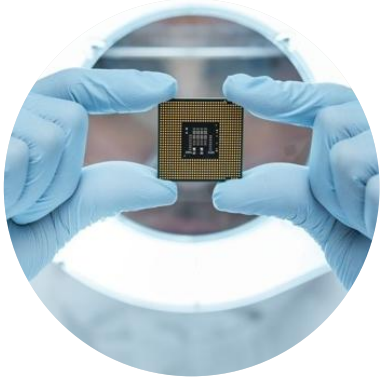
Kun työkalut, prosessit ja toimittajien tuki ovat kunnossa, siirrä loput järjestelmät hallitusti.

Siirtymän läpivienti vie suuressa organisaatiossa tyypillisesti useita vuosia.
Erityisen hankalia ovat pitkäikäiset OT/IOT-järjestelmät, koska niitä ei yleensä voi päivittää nopeasti.

Ydinviesti

- Standardit tarjoavat teknisen perustan siirtymälle.
- Hybridiratkaisut pienentävät siirtymän riskejä.
- Vaiheittainen käyttöönotto johtaa hallittuun ja onnistuneeseen siirtymään.

Käytännön rajoitukset



- Suuremmat avainkoot ja allekirjoitukset
  - ML-KEM vs. X25519: 800 bytes vs. 32 bytes (avaintenvaihto).
  - ML-DSA vs. Ed25519: 2420 bytes vs. 64 bytes (allekirjoitus).
  - Lisääntynyt viive TLS kättelyssä ja kaistanleveys kasvaa
  - Yhteensopimattomuus mikrokontrollerien kanssa muistivaatimusten vuoksi.
- Laskennan lisäkuorma
  - ML-KEM/DSA on paljon hitaampi avainten generoinnissa ja allekirjoituksissa verrattuna klassiseen.
  - Rasitus heikkotehoisille suorittimille.
  - Kuormitus paristokäyttöisille laitteille.
- Hybridijärjestelmän monimutkaisuus
  - PQC+klassinen hybridi menetelmä vaatii eniten resursseja

EU's Coordinated Implementation Roadmap for the Transition to PQC (23.6.2025)

VTT

European Commission

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

Sääntelyn vertailu USA:n ja EU:n välillä

VTT

YDINVIESTI

USA etenee toimeenpanon ja ohjeistuksen kautta.
EU etenee yhteisen tiekartan, ohjeistuksen ja sääntelyn kautta.

YHDYSVALLAT

LÄHTÖKOHTA
Liittovaltio ohjaa siirtymää,
yritykset seuraavat perässä.

OHJAUSKEINOT
Executive Order 14028,
NIST PQC -standardit ja ohjeet, CISA-ohjaus.

TAVOITE
Kriittisten järjestelmien kvanttiturvallisuus
2030-luvulle.

PÄÄVIESTI
Inventoi, priorisoi,
merkitse riskit ja päivitä.

EU

LÄHTÖKOHTA
EU rakentaa yhteistä tiekarttaa
ja lainsäädäntöä.

OHJAUSKEINOT
EU PQC Roadmap,
tulossa oleva Quantum Act,
ENISA ja jäsenvaltioiden ohjeistus.

TAVOITE
Laajamittainen kvanttiresilientti
infrastruktuuri 2030-luvulle.

PÄÄVIESTI
Vaiheittainen siirtymä,
hybridimallit ja kryptoketteryys.

YHTEINEN SUUNTA

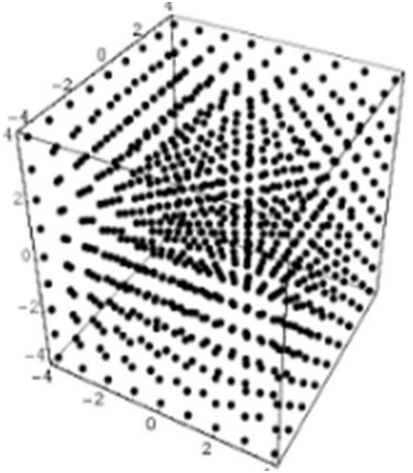
Molemmat korostavat varhaista valmistautumista,
kriittisten järjestelmien suojaamista ja vaiheittaista siirtymää
kvanttiresilienttiin kryptografiaan.

Lähteet: HVK 2024; Cain et al. 2026; Babbush et al. 2026

BLimPQC

- Beyond the Limits of Post-Quantum Cryptography
- A Co-Innovation project funded by Busines Finland
  - Part of Bittium's veturi ecosystem: "Seamless and Secure Connectivity"
- The project will answer to new challenges in PQC research and implementation
- Research: VTT, Aalto, Helsinki University and Oulu University
- Industry: Bittium, SSH, Xiphera, Jutel, Icareus, and Ericsson
- BLimPQC press release published 22.05.2025
- Webpage : www.pqc.fi

Project start date:	01. April 2025
Project end date:	31. March 2028
Budget:	6,5 M€
Coordinator:	VTT / Visa Vallivaara



BLimPQC Consortium

BLimPQC Work Packages:

- WP2: Quantum Computing and Quantum Key Distribution
  - What are the new developments in quantum computing?
  - Lead: Aalto University, Ilkka Tittonen & Matti Raasakka
- WP3: PQC Algorithms and Standardization
  - What are the implications of the NIST standards to the security of different applications?
  - Lead: University of Helsinki, Valtteri Niemi
- WP4: Regulation Impacts and Opportunities
  - How does regulation affect business landscape of different verticals, and what opportunities are subsequently emerging regionally and globally?
  - Lead: VTT, Outi-Marja Latvala
- WP5: PQC Implementations
  - What are the best ways to implement the standards in industrial use cases?
  - Lead: SSH, Tero Mononen
- WP6: Limits of PQC
  - Where are the gaps of current PQC and how do these gaps affect industry partners?
  - Lead: University of Oulu, Juha Partala

Mahdollisuus: Kvanttiturvalliset sairaalat - tutkimushanke

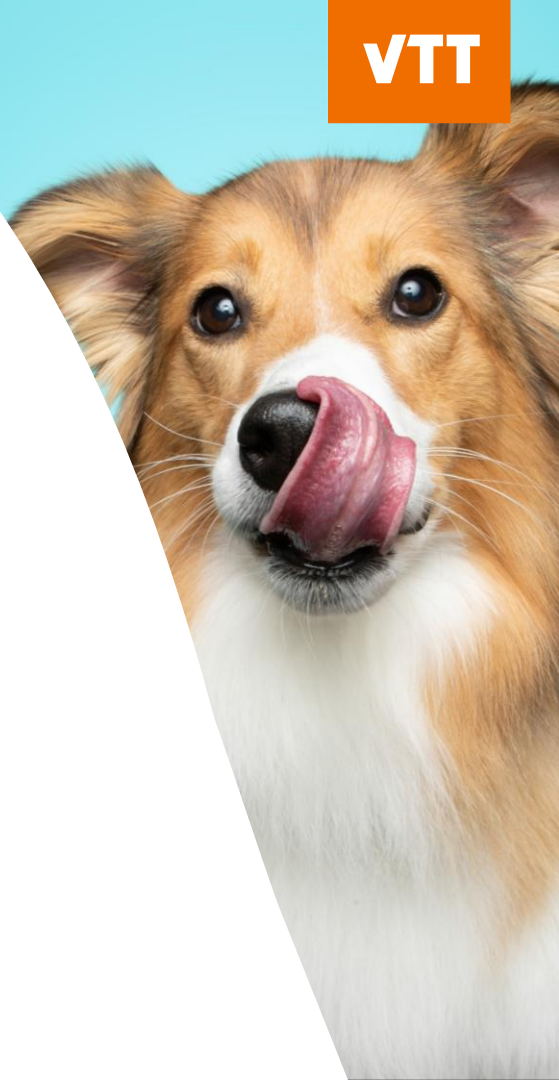
- ”Tammikuusta 2025 alkaen Business Finlandin T&K-rahoitus voi tukea yliopistosairaaloiden hankkeita hyvinvointialueilla yhteistyössä yritysten ja tutkimusorganisaatioiden kanssa”
- Olemme kiinnostuneita valmistelemaan **sairaaloiden kvanttiturvallisuuteen** liittyvää hanketta
- Mukaan suunnitteluun ja toteutukseen haluttaisiin nyt erityisesti hyvinvointialueita ja yliopistosairaaloita

Hankkeen sisältö

- Tutkittavia teemoja: sairaalan viestintäverkkojen luotettavuus ja kvanttiturvallisuus
- Sairaaloissa hyödynnetään heterogeenistä viestintäympäristöä, joka koostuu useista osajärjestelmistä
- Luodaan työkaluja, joilla voidaan kartoittaa järjestelmien muutostarpeita kvanttiturvallisuuden aikaan saamiseksi
- Selvitetään, mitkä osajärjestelmät ovat helposti päivitettävissä, mitkä vaativat erityistä huomiota, mitkä olisivat parhaat tavat päivittää niitä
- Selvitetään, mitkä ovat kriittisiä järjestelmiä, joiden päivittäminen on kiireellisintä
- Mahdollisuuksien mukaan hankkeessa aloitetaan päivityksen suunnittelu
- Osa hanketta on myös luoda kriteerejä uusille tehtäville hankinnoille, jotta varmistuttaisiin niiden kvanttiturvallisuudesta
- Ei kehitetä uusia salausalgoritmeja vaan tutkitaan olemassa olevien vaihtoehtojen sopivuutta käytössä oleviin järjestelmiin

Aikataulu ja osallistujat

- Tavoiteltu toteutusaikataulu: 2027–2028
- BF:n co-innovation –hanke:
  - Rahoitusosuus tutkimusorganisaatiolle ja yliopistosairaaloille on 80%
  - Yritysten rahoitus yrityksen koosta ja tutkimuksen sisällöstä riippuen 40-60% BF:n tutkimus- ja kehitysrahoitussääntöjen mukaisesti
- Pyrkimys myös kansainväliseen toimintaan
- Tavoittelemme vähintään kahta tutkimuslaitosta ja vähintään noin kuutta yritystä mukaan hankkeeseen (terveysalan sovelluksia tuottavia yrityksiä sekä tietoturva-alan kvanttiturvaan perehtyneitä yrityksiä)
- Mukana olevat osallistujat:
  - VTT
  - Istekki
  - Terveysala – Mediconsult kiinnostunut
  - Tietoturva – SSH kiinnostunut
  - Yliopistosairaaloita?
  - **Hyvinvointialueita? ← tarvitaan!**



Johdon tiivistelmä

1 Mistä on kyse?

Nykyinen kyberturva perustuu salaukseen, jonka riittävän tehokas kvanttitietokone voi murtaa.

2 Miksi tämä koskee jo tätä päivää?

Hyökkääjä voi kerätä salattua dataa jo nyt ja purkaa sen myöhemmin, kun kvanttitietokoneet ovat riittävän tehokkaita.

3 Mikä muuttuu?

Suurin muutos koskee julkisen avaimen salausta: symmetrinen salaus säilyy pääosin käyttökelpoisena, mutta avainpituuksia on tarpeen kasvattaa kriittisissä kohteissa.

4 Mitä tehtäväksi?

Nimetään omistaja ja tiimi. Kartoitetaan, missä varmenteita, allekirjoituksia, VPN-yhteyksiä ja avaintenhallintaa käytetään.

5 Miten edetään ja mitä toimittajilta vaaditaan?

Aloitetaan piloteilla ja vaiheistetulla käyttöönotolla. Tavoitteena kriittiset järjestelmät vuoteen 2030 mennessä ja laaja siirtymä vuoteen 2035 mennessä. Edellytetään kvanttiresilienttiä tukea uusissa ja uudistettavissa toimittajasopimuksissa.

Ydinviesti

- Kyberuhka kohdistuu ennen kaikkea julkisen avaimen salausmenetelmiin.
- Valmistautuminen alkaa nyt kartoituksesta, priorisoinnista ja suunnittelusta.
- Johto vastaa: omistaja, budjetti ja seuranta on nimettävä ja varmistettava.