Tampereen yliopisto

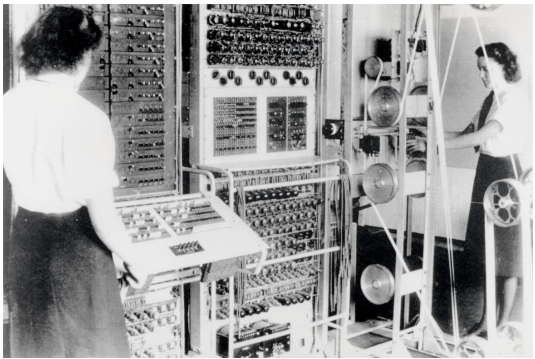
SALAUSASIAA KVANTTITIETOKONEISTA

Kvanttilaskennan rajat

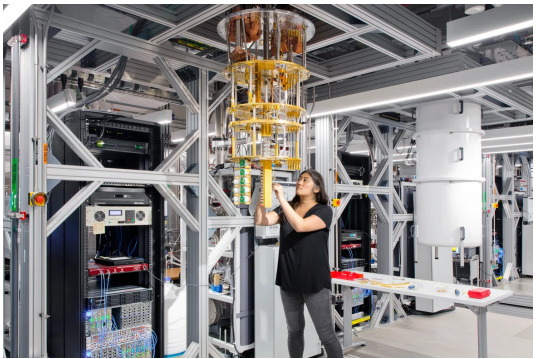
Dosenttien päivä 13.03.2025

Markku-Juhani O. Saarinen
<markku-juhani.saarinen@tuni.fi>
Tampere University, Tampere, Finland

Kryptologia ja laskennan vallankumoukset



Ensimmäinen ohjelmoitava digitaalinen tietokone oli *Colossus* (1943) jota “Bletchley Park” käytti Lorenz-salaimen murtamiseen. Saksalaisissa turva-arvioissa oli varauduttu enintään mekaaniseen laskentavoimaan.



1990-luvulta lähtien on tiedetty että tarpeeksi tehokas kvanttitietokone pystyy murtamaan kryptografian joka perustuu tekijöihinjakoon tai diskreettiin logaritmiin – *(toistaiseksi) yleisimmät salausmenetelmät.*

Aikajanaa: Julkisen avaimen kryptologia ja kvanttilaskenta

1975-: Julkisen avaimen salaus. (GCHQ, Diffie-Hellman, RSA.) Mahdollistaa yksityisen viestinnän yleisissä tietoverkoissa ilman etukäteen jaettua salaista avainta.

1980-: Kvanttilaskentaa pohditaan. Kvantti-ilmöiden simulointi on havaittu vaikeaksi tietokoneilla. Richard Feynman ehdottaa tähän erityistä *"kvanttitietokonetta"*. [Fey82]

1990-: Internet ja mobiililaitteet. Maailmanlaajuisen julkisen tietoverkon suojaus mahdollista vain julkisen avaimen salausmenetelmillä.

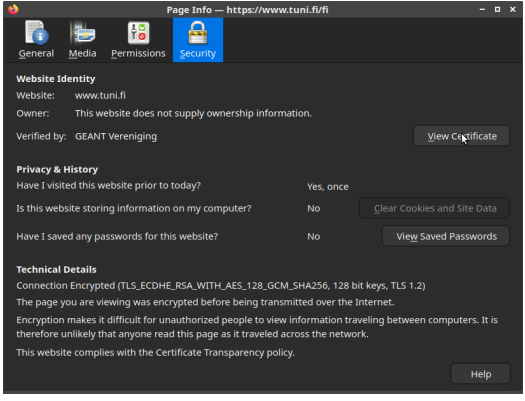
1994: Peter Shor kehittää tehokkaat (polynomiseen ajan) algoritmit *tekijöihinjakoon* ja *diskreettiin logaritmiin* kvanttitietokoneilla.

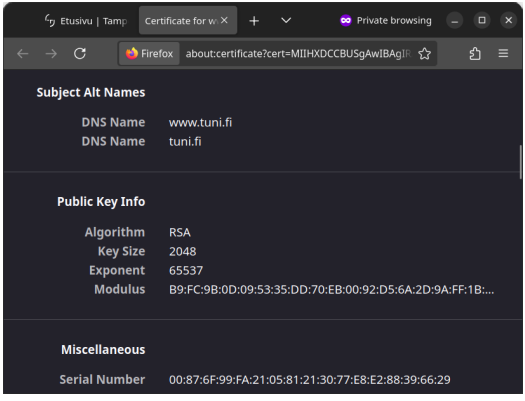
2000-: Monet taloudelliset ja yhteiskunnaliset toiminnot ovat tulleet riippuvaisiksi verkosta – *ja RSA (tekijöihinjako) ja elliptisten käyrien (diskr. log.) salausmentelmistä.*

2009-: Kvanttiturvallisten julkisen avaimen menetelmien kehitystä omana alanaan.

2016-: Kansainvälinen standardointiprosessi: NIST Post-Quantum Cryptography.

Tilanne 2025: Laajalti yhä RSA & Diskreetti Logaritmi

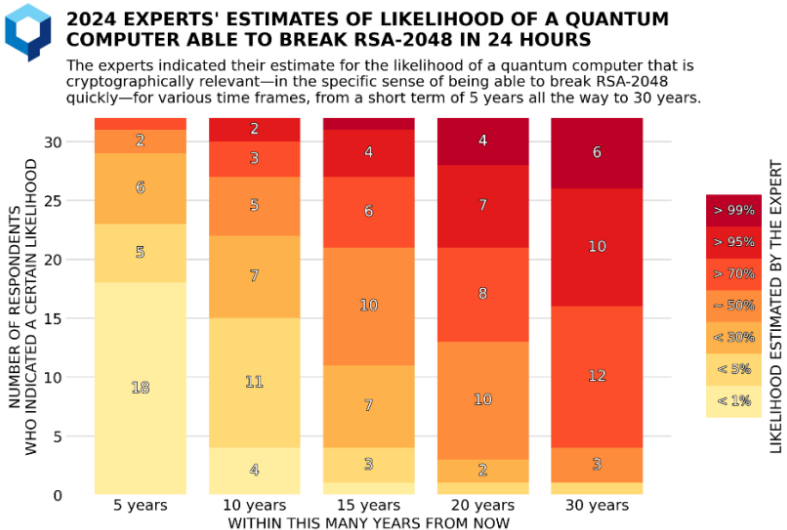




Suurin osa verkkopalveluista käyttää yhä ECDH (elliptisten käyrien diskreetti logaritmi) menetelmää salaus- ja eheysavainten (AES-GCM) muodostamiseen.

Tunnistautumiseen käytetään yhä RSA-allekirjoitukseen perustuvia varmenteita.

Asiantuntijakysely [MP24]: RSA-2048 murrettavissa ehkä 2040



Hieman kvanttilaskennasta

Yksittäinen **kubitti:** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ jossa $\alpha, \beta \in \mathbb{C}$ *todennäköisyysamplituudeja*.
Kubitin $|\psi\rangle$ tilat $|0\rangle$ ja $|1\rangle$ voivat ovat **superpositiossa** kunnes kubitti **mitataan**.
Kannalla $\{|0\rangle, |1\rangle\}$ tulos on 0 todennäköisyydellä $|\alpha|^2$ tai 1 todennäköisyydellä $|\beta|^2$.

Kvanttilomittuminen (*entanglement*): n kubitin järjestelmällä voi olla 2^n eri todennäköisyysamplituudia $c_x \in \mathbb{C}$ jossa $x \in \{0,1\}^n$. Esim. $n = 3$ kubittia:

$$|\psi\rangle = c_{000}|000\rangle + c_{001}|001\rangle + c_{010}|010\rangle + c_{011}|011\rangle + c_{100}|100\rangle + c_{101}|101\rangle + c_{110}|110\rangle + c_{111}|111\rangle.$$

Jos kaikki n kubittia mitataan, tämä *eksponentiaalinen* määrä tiloja kuitenkin **romahtaa** peruuttamattomasti joksikin bittijoksi $x \in \{0,1\}^n$. (Tod. näk. $|c_x|^2$).

Kvanttitietokone manipuloi kubittien tilaa **kvanttiporteilla** (esim. Toffoli) jotka ovat yksinkertaisia lineaarisia tilamuunnoksia. Yleisesti kubittien lukumäärä on “kvanttitietokoneen koko” kun taas porttien määrä on suhteessa “laskenta-aikaan”.

Yksi toteutustapa: Suprajohteisiin perustuva kvanttitietokone (IQM)

Inside look: Superconducting quantum computer

Cryogenic cooling process

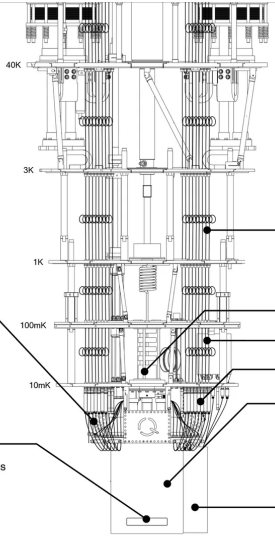
Superconducting quantum computers must be kept at extremely low temperatures, typically close to absolute zero, to maintain the superconducting state. This cooling is achieved using advanced cryogenic systems, using liquid helium.

Microwave coaxial cables

These cables (some are superconducting) direct microwave pulses to and from the QPU. These signals enable the control and readout of the states of individual qubits, and also turning on/off interactions between qubits for logical operations.

Quantum Processing Unit (QPU)

This is the "heart" of the quantum computer. Here the chip contains interconnected quantum bits that perform calculations based on the laws of quantum mechanics. Fundamentally, the qubits utilize superposition and entanglement as computing resources for information processing.



To manipulate the quantum states of qubits, superconducting quantum computers use microwave sources and transmission lines.

Quantum gates are impremented by sending specific microwave pluses to the qubits. These pluses have precise frequencies and durations, and they can be used to apply different operations on the qubits.

After quantum computations, the state of the qubits is measured using microwave pulses.

Microwave signal lines

Mixing chamber

Shielded microwave isolators

Filters

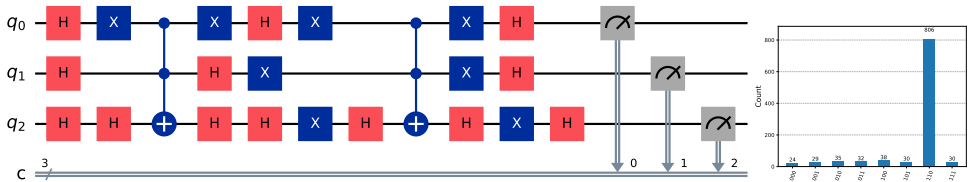
Magnetic shields

Magnetic fluctuations interfere with the qubits. Shielding is necessary to maintain the quality of the quantum processor.

Magnetic shields for the quantum limited amplifier

Mitä sillä voi tehdä?

Laskentamalli: Aseta syötetila, manipuloi kubitteja “kvanttipiirin” porteilla, mittaa.



- Kaikki n kubitin piirit voidaan kuvata jollain $2^n \times 2^n$ *unitaarimatriisilla* U.
- Kaikki piirit ovat peruutettavia (U^{-1}). Ei hypppyjä tai ehdollista suoritusta.

Klassinen tietokone siis “ajaa” kvanttitietokonetta (hybridi); asettaa syötteet, antaa porttikomennot, analysoi mittaustulokset, ja toimii niiden perusteella.

Vaikkakin superpositio ja lomitus ovat erittäin vahvoja työkaluja, kvanttilaskennalla on rajoituksia. Viimeisen 30 vuoden aikana on löytynyt vain harvoja uusia ja relevantteja ongelmia joille kvanttitietokone tarjoaa “eksponentiaalisen” nopeutuksen.

Voidaanko symmetriset salaimet (esim. AES) murtaa?

Symmetrisissä salaimissa (yleisin: AES) on jaettu salainen avain. Tarkoituksellisesta matemaattisen struktuurin puutteesta johtuen pitää etsiä koko avainavaruus.

Yleiseen etsintään kvanttilaskenta tarjoaa **Groverin algoritmin** [Gro96] joka löytää n-bittisen avaimen $O(\sqrt{2^n}) = O(2^{n/2}) = O((\sqrt{2})^n)$ ajassa klassisen $O(2^n)$ sijaan.

Groverin (eksponentiaalinen) kompleksisuus on osoitettu optimaaliseksi [Zal99].

- Groverin algoritmi ei ole rinnakkaistettavissa kuten klassiset hakualgoritmit.
- Erittäin pitkä sarjallinen laskenta aiheuttaa virheitä / dekoherenssiongelmia.

Näistä käytännön rajoituksista johtuen:

Monien tutkijoiden mielestä nykyiset symmetriset salaimet ovat turvallisia 128-bittisellä avaimella myös pitkälle kvanttiaikakauteen [Jaq24, DC24].

Vaihto 256-bittisiin avaimiin ei ole kovin hankalaa, joten sen voi kuitenkin tehdä.

Entäs se julkisen avaimen salaus?

Kuten todettua, RSA ja Elliptiset Käyrät murtuvat tehokkaasti Shorin algoritmeilla: n-bittinen RSA tai elliptinen käyrä vaatii $O(n)$ kubittia ja $O(n^3)$ porttia/aikaa.

Shorin algoritmit perustuvat jakson etsintään (period finding) kvantti-Fourier muunnoksen avulla. Ne edellyttävät aivan tietynlaista matemaattista struktuuria.

Toisaalta: Yleinen hypoteesi on että *kaikki* NP-vaikeat ongelmat pysyvät vaikeina (olennaisesti eksponentiaalisina) myös kvanttitietokoneiden kanssa.

Kvanttiturvallinen salaus toimii klassisilla tietokoneilla mutta perustuu uusiin matemaattisiin ongelmiin joita kvanttitietokoneet eivät helposti ratkaise.

Avaintenmuodostus- ja allekirjoitusmenetelmiä on kehitetty näistä:

- Hilaperusteinen salaus (lattice-based cryptography): *Learning With Errors*.
- Koodiperusteinen salaus (code-based cryptography): *Syndrome Decoding*.
- Tiivistefunktioihin perustuvat (hash-based) allekirjoitusmenetelmät.

Siirtymä kvanttiturvalliseen salaukseen on meneillään

2016: NIST PQC Standardointiprosessi alkoi.
Kilpailuun lähetettiin 82 kandidaattialgoritmia.

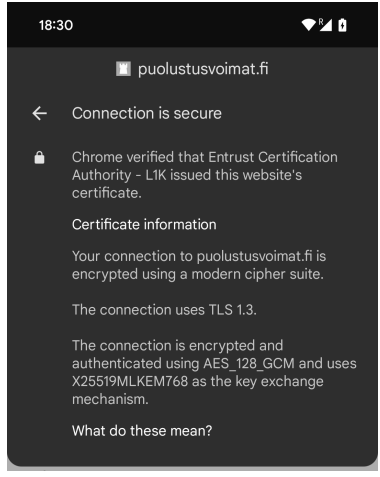
2022: Kolmen karsintakierroksen jälkeen valittiin:

- ML-KEM (“Kyber”) avaintenmuodostus (hila).
- ML-DSA (“Dilithium”) allekirjoitus (hila).
- SLH-DSA (“Sphincs+”) allekirjoitus (hash).
- FN-DSA (“Falcon”) allekirjoitus (hila).

2024: FIPS standardit 203–205 valmistuvat.
Esim. Google (Chrome-selain, Android) ottaa ML-KEM algoritmin laajalti käyttöön.

2025: Neljäs karsintakierros, yksi lisäalgoritmi:

- HQC avaintenmuodostus (koodiperusteinen).



ML-KEM Android-kännykässä.

Viittauksia I

[DC24] Sarah D and Peter C.
On the practical cost of Grover for AES key recovery.
Fifth PQC Standardization Conference, April 10–12, 2024, 2024.
URL: https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/on-practical-cost-of-grover.pdf.

[DH76] Whitfield Diffie and Martin Hellman.
New directions in cryptography.
IEEE Transactions on Information Theory, 22(6):644–654, 1976.
doi:10.1109/TIT.1976.1055638.

[Fey82] Richard P. Feynman.
Simulating physics with computers.
International Journal of Theoretical Physics, 21:467–488, 1982.
doi:10.1007/BF02650179.

[Gro96] Lov K. Grover.
A fast quantum mechanical algorithm for database search.
In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.
URL: https://arxiv.org/abs/quant-ph/9605043, doi:10.1145/237814.237866.

[Jaq24] Samuel Jaques.
Quantum attacks on AES.
Invited talk at IACR CHES 2024, 2024.
URL: https://ches.iacr.org/2024/Jaques_CHES_2024.pdf.

[MP24] Michele Mosca and Marco Piani.
Quantum threat timeline report 2024, 2024.
URL: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

Viittauksia II

[NIS24a] NIST.
Module-Lattice-Based Digital Signature Standard.
Federal Information Processing Standards Publication FIPS 204, August 2024.
doi:10.6028/NIST.FIPS.204.

[NIS24b] NIST.
Module-Lattice-based Key-Encapsulation Mechanism Standard.
Federal Information Processing Standards Publication FIPS 203, August 2024.
doi:10.6028/NIST.FIPS.203.

[NIS24c] NIST.
Stateless Hash-Based Digital Signature Standard.
Federal Information Processing Standards Publication FIPS 205, August 2024.
doi:10.6028/NIST.FIPS.205.

[Sho94] Peter W. Shor.
Algorithms for quantum computation: Discrete logarithms and factoring.
In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134. IEEE Computer Society, 1994.
URL: https://arxiv.org/abs/quant-ph/9508027, doi:10.1109/SFCS.1994.365700.

[Zal99] Christof Zalka.
Grover's quantum searching algorithm is optimal.
Physical Review A, 60(4):2746–2751, October 1999.
URL: https://arxiv.org/abs/quant-ph/9711070, doi:10.1103/physreva.60.2746.