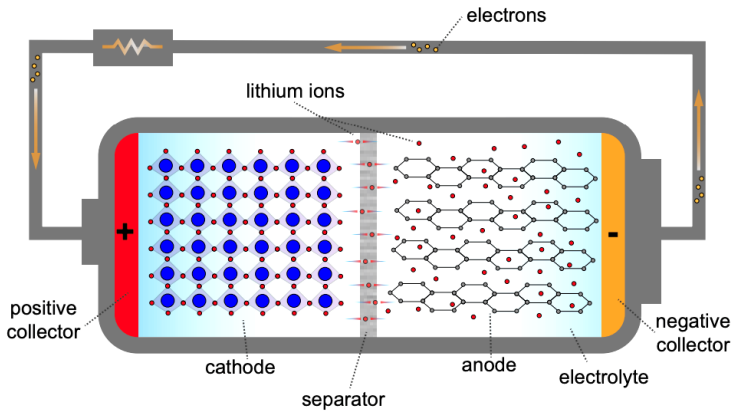
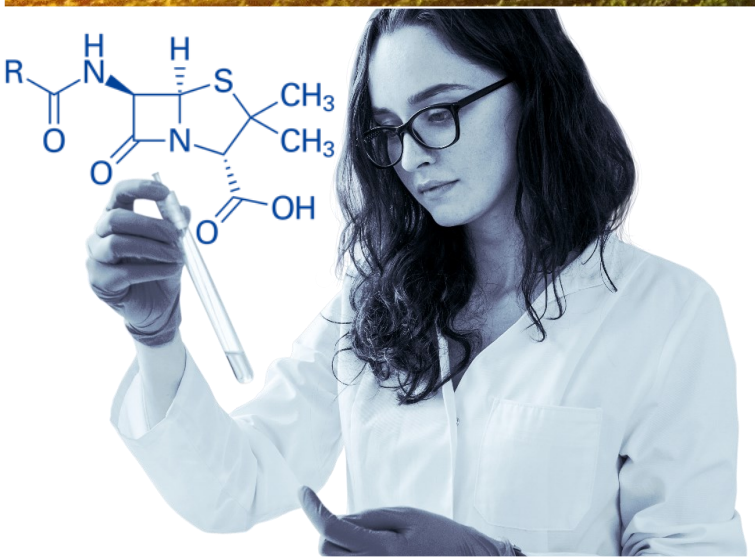
Miten kvanttilaskennan kehitys vaikuttaa kyberturvallisuuteen?

Jouni Flyktman
Vice President, Defence and Security

Arvopotentiaali yli 1 000 000 000 000 €



LÄÄKETEOLLISUUS
KEMIANTEOLLISUUS
AKKUTEOLLISUUS
RAHOITUS
LIIKENNE JA LOGISTIIKKA
KYBERTURVALLISUUS

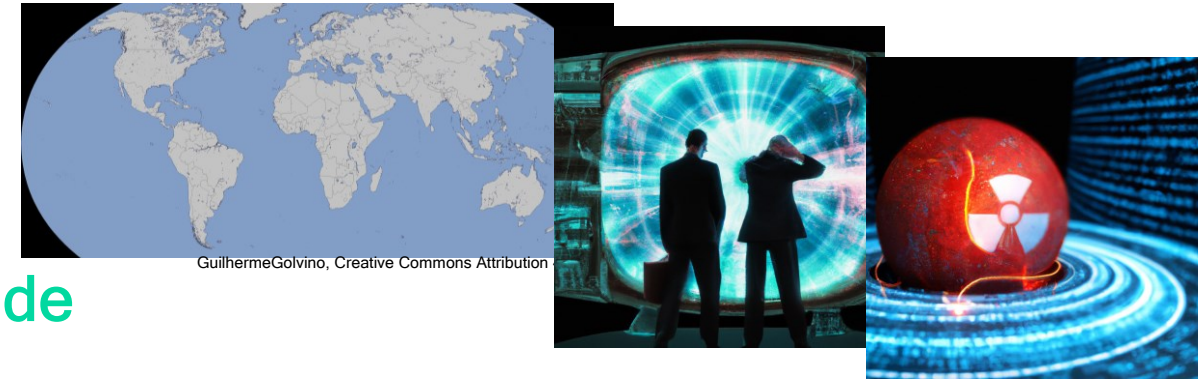


Kyberturvallisuuden arvioidaan olevan 16% kvanttilaskentamarkkinasta 2025 mennessä ($1.2 mrd).

- Hyperion Research 2023

Geopoliittinen kilpailu

Kvanttiteknologiat ovat seuraava geopoliittisen ja sotilaallisen ylivoiman lähde



GuilhermeGolvino, Creative Commons Attribution

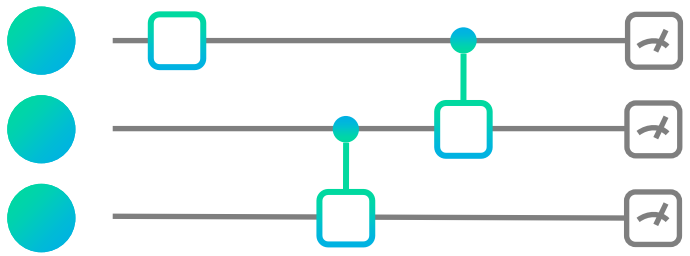
- Etulyöntiasema vaatii strategisia investointeja
- Kiina johtaa investoinneissa $15.3 mrd (2022)
- Yhdysvallat pyrkii vastaamaan $3.7 mrd (2022)
- EU etsii suuntaa $8.4 mrd (2022)
- Suomella mahdollisuus olla mukana pelissä
- Regulointi lisääntyy nopeasti, standardit kehittyvät

Julkinen rahoitus

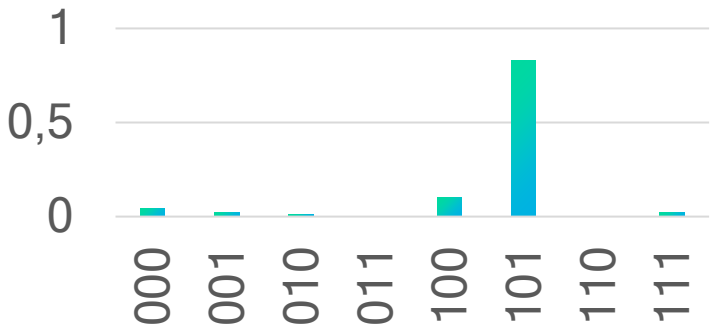
Kvanttilaskenta ja -algoritmit

- Kvanttialgoritmit hyödyntävät superpositiota ja kietoutumista
- Kvanttialgoritmit käyvät läpi kaikki mahdolliset ratkaisut samanaikaisesti.

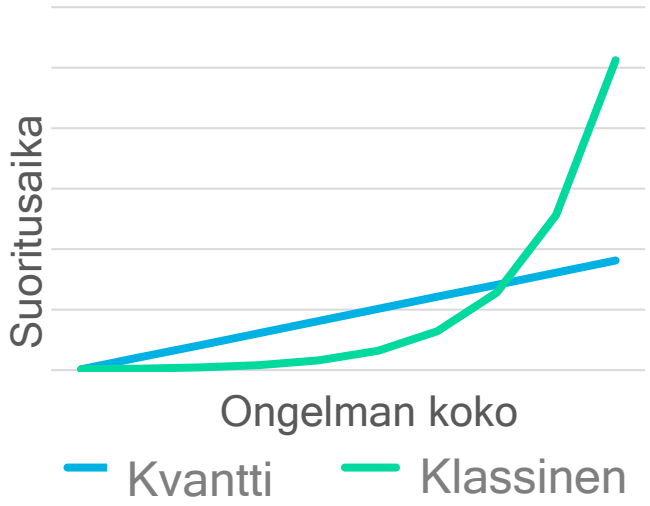
Kvanttipiirit



Laskennan tulos

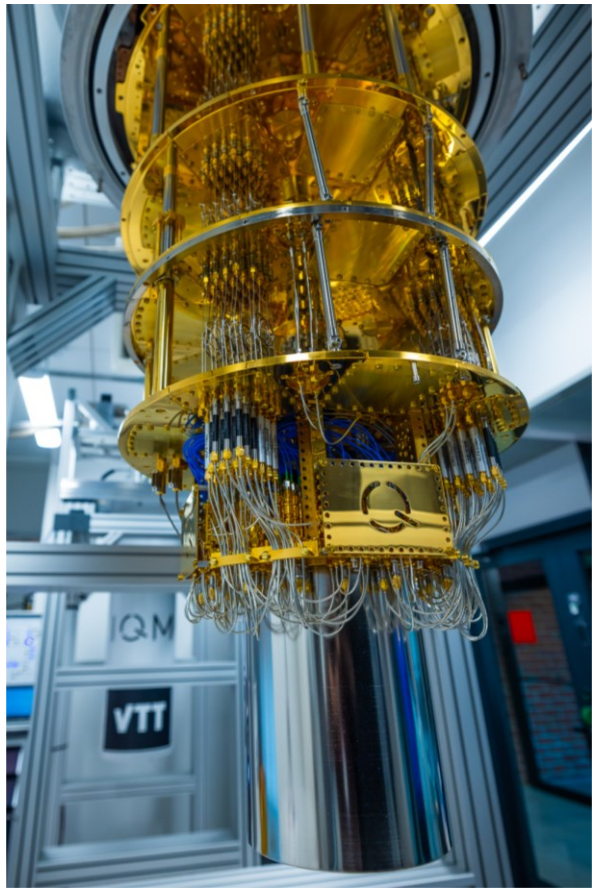


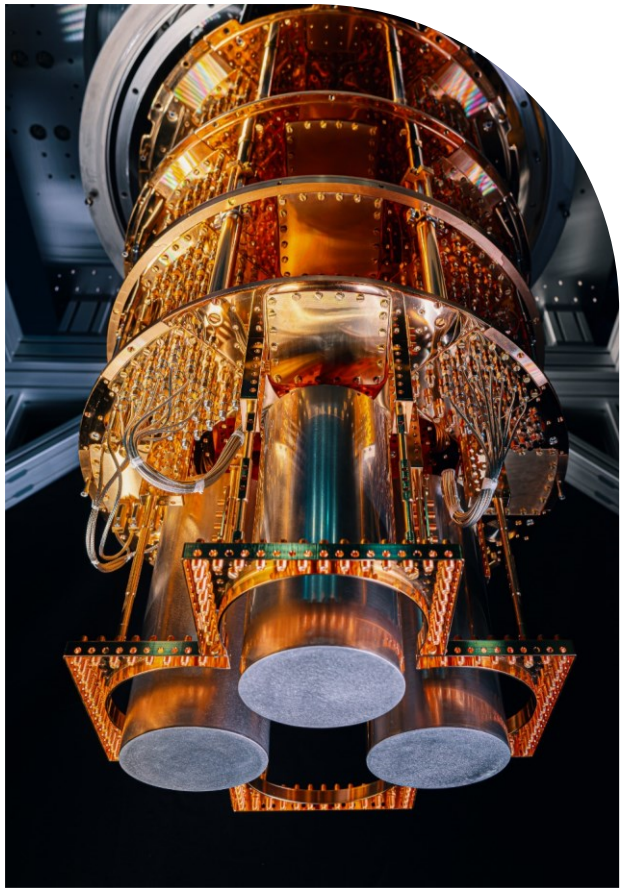
Eksponentiaalinen nopeutus



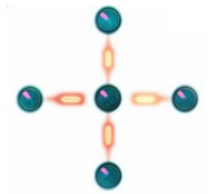
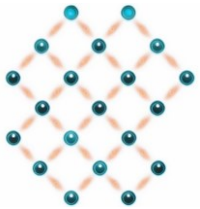
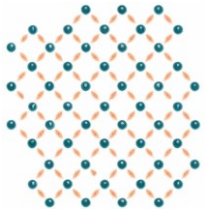
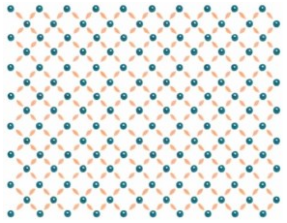
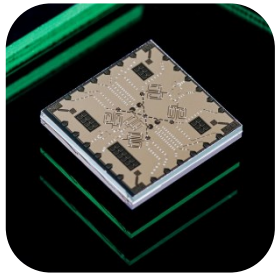
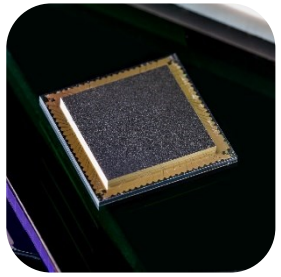
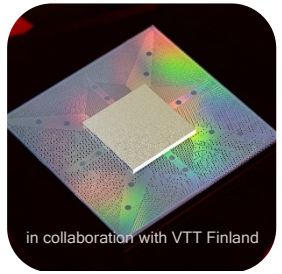
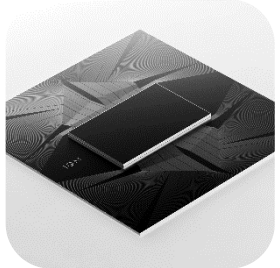
Uudet sovellukset mahdollisia

IQM:n kvanttitietokone





IQM:n kvanttiprosessorit (QPU)

KUBITTIEN LUKUMÄÄRÄ	5	20	54	150
SAATAVUUS	2022	2023	2024	2025
ARKKI-TEHTUURI				
				

IQM:n kvanttilaskentapino

Sovellukset

Lääke | Rahoitus | Akut | Liikenne | AI/ML | ⋮

Ohjelmisto

Kirjastot

Kvanttialgoritmit → HPC-integraatio → Klassiset algoritmit

Laitteisto

Laskennan suoritus

Firmware

Mittalaitteet

QPU

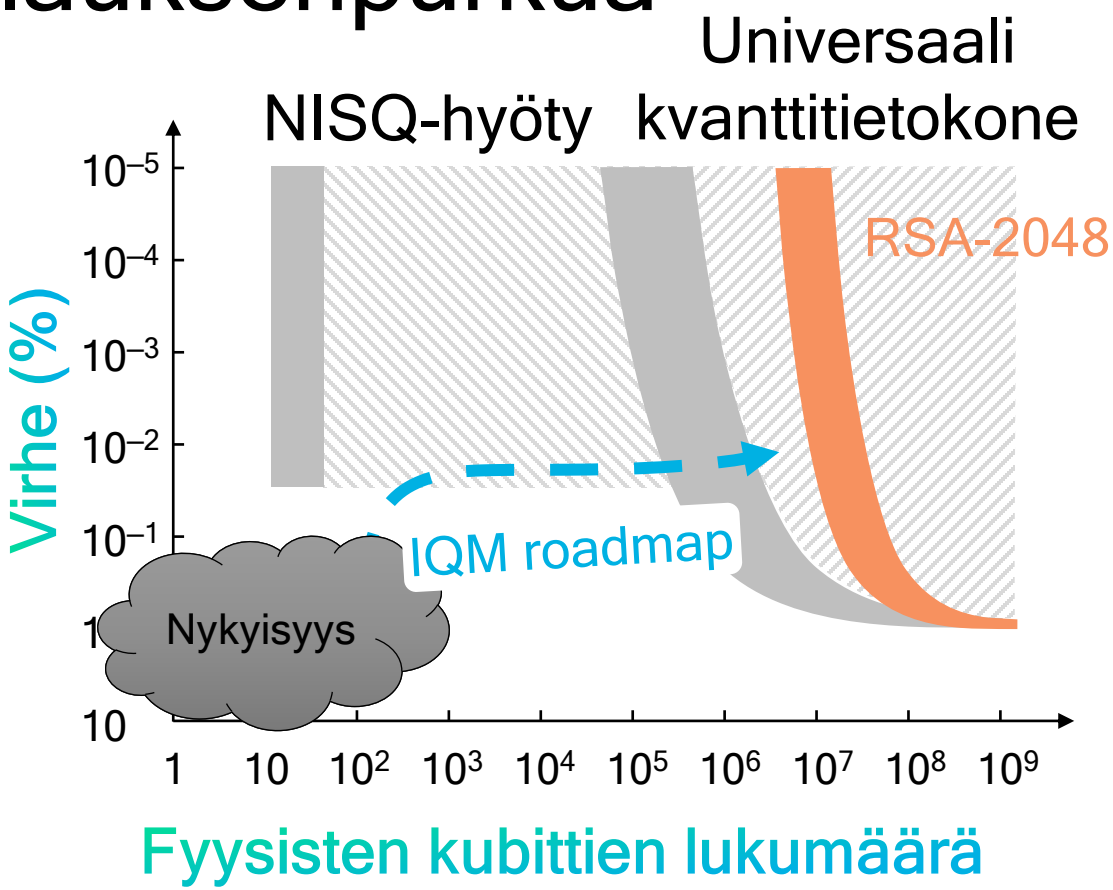
QPU

Klassinen laskenta-laitteisto

Polku kohti salauksenpurkua

CRQC:n vaatimukset

- Fyysisten kubittien **lukumäärä**
  20 miljoonaa
- Kubittien **laatu**
  99,999% fideliteetti
- Kvanttipiirien
  suoritusnopeus



Tarvitaan teknisiä läpimurtoja

- Valmistus-teknologi
- Skaalaus ja miniaturisointi
- Algoritmit
- Virheenkorjaus

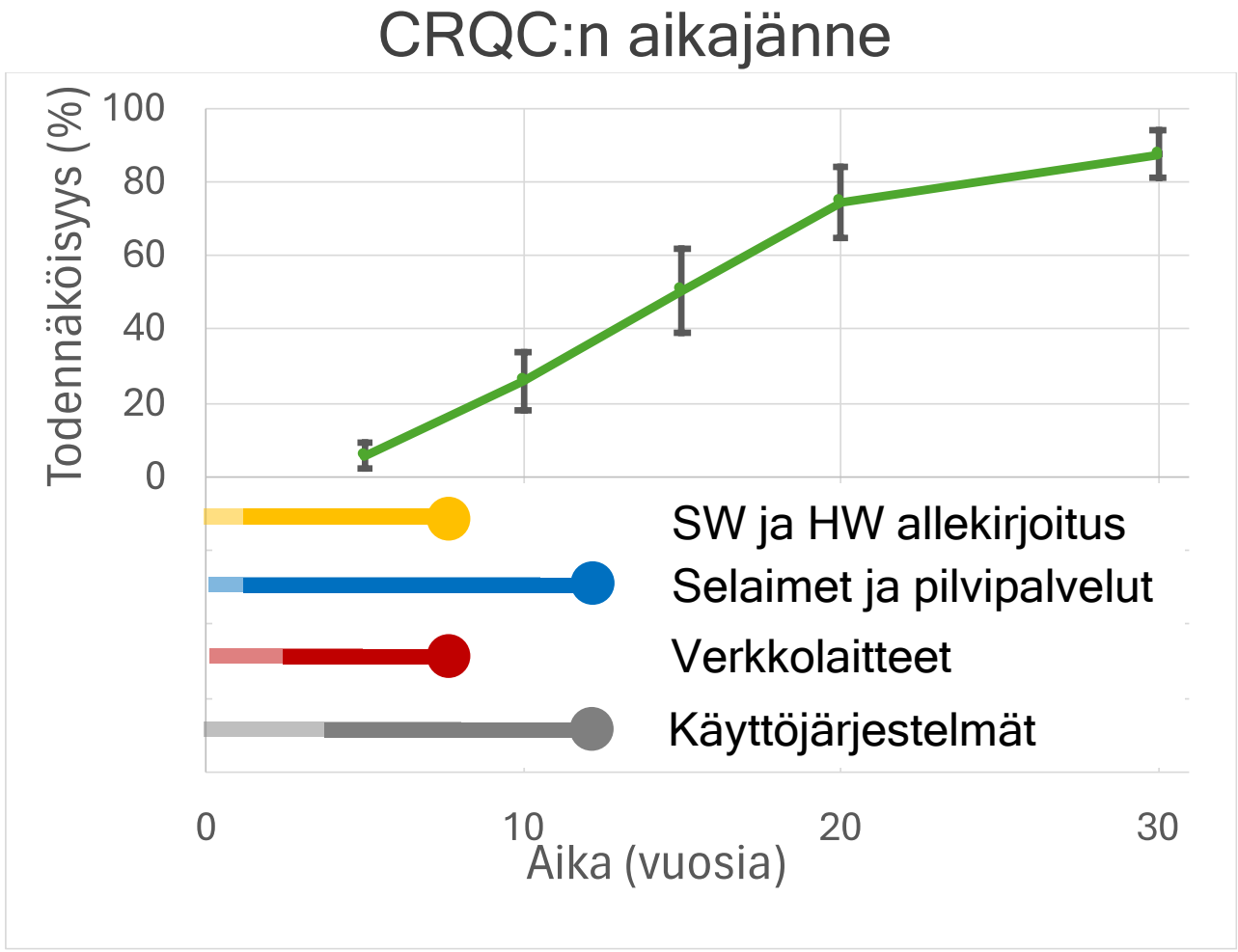
CRQC = Cryptografically Relevant Quantum Computer
NISQ = Noisy Intermediate Size Quantum

Vaikutukset ja aikajänne

Asymmetrinen salaus:
PQC-algoritmit

Symmetrinen salaus:
Pitkä salausavain

Vaikutukset erityisesti seuraavilla aloilla:
- Puolustus- ja turvallisuus
- Terveydenhuolto
- Teleyritykset
- Rahoitus
- Lääketeollisuus
- Valmistava teollisuus
- Juridiikka
- ...



Lähde: *Announcing the Commercial National Security Algorithm Suite 2.0*

Johtopäätökset

50% kvanttilaskentayrityksistä arvioi kyberturvallisuuden olevan lupaavin loppukäyttäjäsegmentti 2025 mennessä. - Hyperion Research 2023

Suosituksia

- Kvanttiteknologiat osaksi tietoturvan kokonaisuutta
- Opiskele, analysoi ja ymmärrä uhkat ja mahdollisuudet
- Toteuta oikealla aikajänteellä

Kvanttilaskenta mullistaa (myös) kyberturvallisuuden

“Kvanttimekaniikan maailma ei ole sama kuin intuitiosi maailma” - Peter Shor