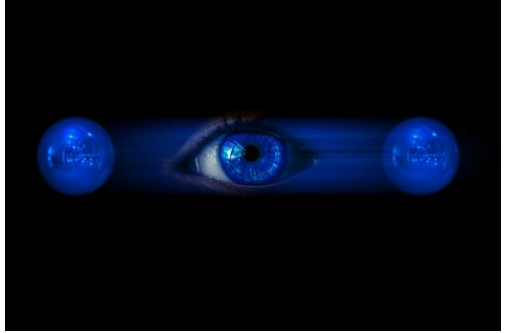
Kestävä yhteiskunta

Kvanttiturvallinen salausteknologia mahdollistaa kyberturvalliset yhteisöt

25.1.2021

Visa Vallivaara
Resaerch Scientist
Applied Cryptography

Kvanttitietokoneiden uhka



- Monet toimialat nojaavat yhä enemmän digitalisaatioon
- Digitaaliset toiminnot ja palvelut tarvitsevat luottamusta ja salausmenetelmät ovat tässä avainosassa
- Kvanttikoneet ovat uhka sekä salaukseen että todennukseen
- Kvanttiturvallisten salausalgoritmien standardointi on jo aloitettu
- Näillä uusilla standardeilla on suuri vaikutus myös monien suomalaisten yritysten liiketoiminaan

2

Nykyiset salausmenetelmät tulevat murtumaan

- Julkisten avainten salausalgoritmit perustuvat kolmeen erilaiseen matemaattiseen ongelmaan:
  - Tekijöiden jakoon, diskreetteihin logaritmeihin ja elliptisiin käyriin
- Shorin algoritmi murtaa nämä kaikki sopivalla kvanttikoneella
  - RSA, ECDSA, (EC)DH, DSA
- Myös symmetrinen salaus heikkenee, mutta ei yhtä vakavasti
  - Groverin algoritmi antaa neliöjuurellinen nopeutuksen symmetristen salausmenetelmien murtamiseen

Kvanttiturvalliset salausmenetelmät

- Perustuvat toisenlaisiin matemaattisiin ongelmiin
  - Hilat (lattice), monimuuttujat, isogeenit, koodiluokat
- Salaukseen ja allekirjoitukseen eri ratkaisuja
- Suuremmat avaimet, allekirjoitukset sekä salaustekstit
- Yleensä ei voi suoraan liittää nykyisiin järjestelmiin
- Tarvitaan järjestelmien uudelleen arviointia ja suunnittelua
  - Eri algoritmit sopivat erilaisiin käyttötarkoitusiin

PQC Standardisointi

Haasteellinen standardisointi

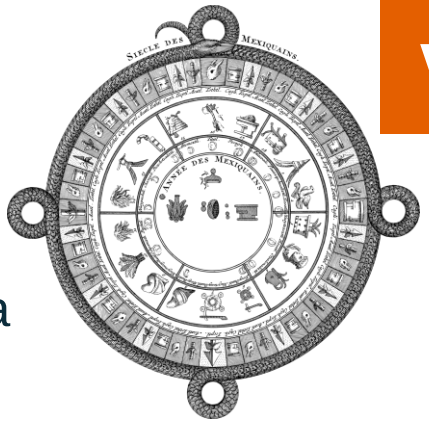
- NIST on aloittanut PQC standardisointi prosessin 2017
- Kvanttisalaus on monimutkaisempaa kuin AES/SHA-3
  - Ei ole yhtä helppoa ratkaisua – kaikilla on heikkoutensa
  - Monia uusia salausalgoritmeja ei ole vielä tutkittu riittävästi
- Standardiin joudutaan valitsemaan useita algoritmeja
- Uhkana sekä klassiset- ja kvanttihyökkäykset
  - Ei selkeää konsensusta kvanttihyökkäysten mittaukseen
- Yhteensopivuus haaste nykyisiin protokoliin ja tietoverkkoihin

Finaaliin päässeet algoritmit

National Institute of Standards and Technology
U.S. Department of Commerce

- Salaus finalistit: Kyber, NTRU, SABER, Classic McEliece
  - Varavaihtoehdot: Bike, FrodoKEM, HQC, NTRUprime, SIKE
- Allekirjoitus finalistit: Dilithium, Falcon, Rainbow
  - Varavaihtoehdot : GeMSS, Picnic, Sphincs+
- NIST todennäköisesti standardoi:
  - Kyber tai NTRU tai Saber ja Classic McEliece (salaus)
  - Dilithium tai Falcon (allekirjoitus)

PQC Standardin tilanne



- Finalistit ja varavaihtoehdot julkaistiin heinäkuussa
  - Viivästyksiä tuli useista syistä
- Varavaihtoja on, jos finalisteista löytyy uusia haavoittuvuuksia tai heikkouksia, ja niitä voidaan lisätä standardiin myöhemmin
- Algoritmien analyysi ja vertailu on hyvin konservatiivista
  - Vain ne joita on tarkasteltu pitkään ja syvällisesti ovat harkinnassa
- Lopullisen standardin on tarkoitus valmistua vuoteen 2024 mennessä.

Kvanttiturvallisuus Suomessa

Post-Quantum Cryptography Finland

- https://www.pqc.fi/index.php/home/
- Business Finland hanke, jonka tavoitteena on kehittää, analysoida ja tutkia kvanttiturvallisia algoritmeja ja niiden sopivuutta kansalliseen turvallisuuteen, tuotteisiin ja käytäntöihin
  - Post Quantum Cryptography (Helsinki university)
  - Quantum Computing (Aalto university)
  - Requirements and limitations for PQC in PKI (Insta Oy)
  - Implementing PQC (SSH Oyj)
  - Future directions and certification of PQC and QC (VTT Oy)

Milloin valmistautuminen pitäisi aloittaa?

Vastauksen saa tällä kaavalla:

2021 + Q – x –y,

jossa Q on # vuosien määrä ekaan suureen kvanttikoneeseen

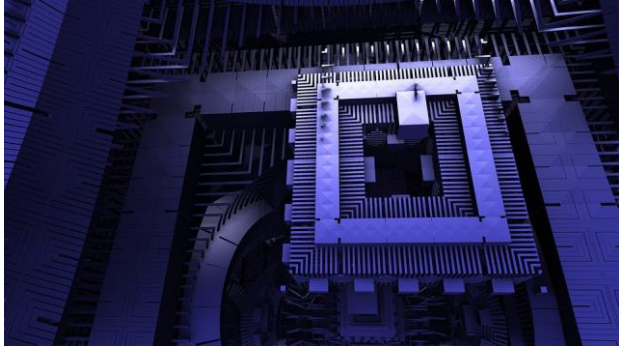
x on # vuosien määrä kauanko algoritmien vaihto kestää liiketoiminta alallanne (3-12 vuotta)

y on # vuosien määrä kauanko datan on säilyttävä salassa

Esimerkiksi, jos Q = 30, x = 10 ja y = 20 niin pitäisi valmistautuminen aloittaa jo tänään!

Kiitokset professerille Bart Preneel tästä kaavasta! (https://twitter.com/AnomalRoil/status/1192463323104763904?s=20)

Miten aloittaa valmistautuminen?



- Sisäinen kvanttiriskienarvointi
  - Tunnistetaan kriittiset tietovarannot ja niiden nykyinen salaus/suojaus
  - Määritetään oman alan ‘x’ ja ‘y’ – kvanttiriskin laskeminen
  - Kvanttiuhan tiedostaminen ja siirtyminen kvanttiturvallisiin ratkaisuihin
- Arvioidaan tavarantoimittajien tuotteiden kvanttiturvallisuutta
- Kehitetään tietopohjaa IT-henkilöstön keskuudessa
- Seurataan kvanttilaskennan ja tietoturvan kehitystä
- Toimitaan etunojassa – se tulee lopulta halvemmaksi, vakaammaksi ja turvallisemmaksi, kun ei tarvitse hätiköidä

beyond

the obvious

Visa Vallivaara
Visa.vallivaara@vtt.fi

25/01/2021