PQC SEMINAARI - OHJELMA

8:30 Saapuminen ja aamukahvi

9:00 Tilaisuuden avaus, Business Finland (**Kirsi Kokko**)

9:05 Tilaisuuden avaus, PQC Finland hanke (**Jorma Mellin**)

9:15 PQC työpakettien katsaukset

10:00 Key note: Quantum Computing developments, **Joachim Schäfer**, IBM Quantum Ambassador

10:30 Posterisessio hankkeeseen liittyvistä lopputöistä / tauko

11:00 Kvanttipaneeli: Suomen tiekartta kohti kvanttiaikaa

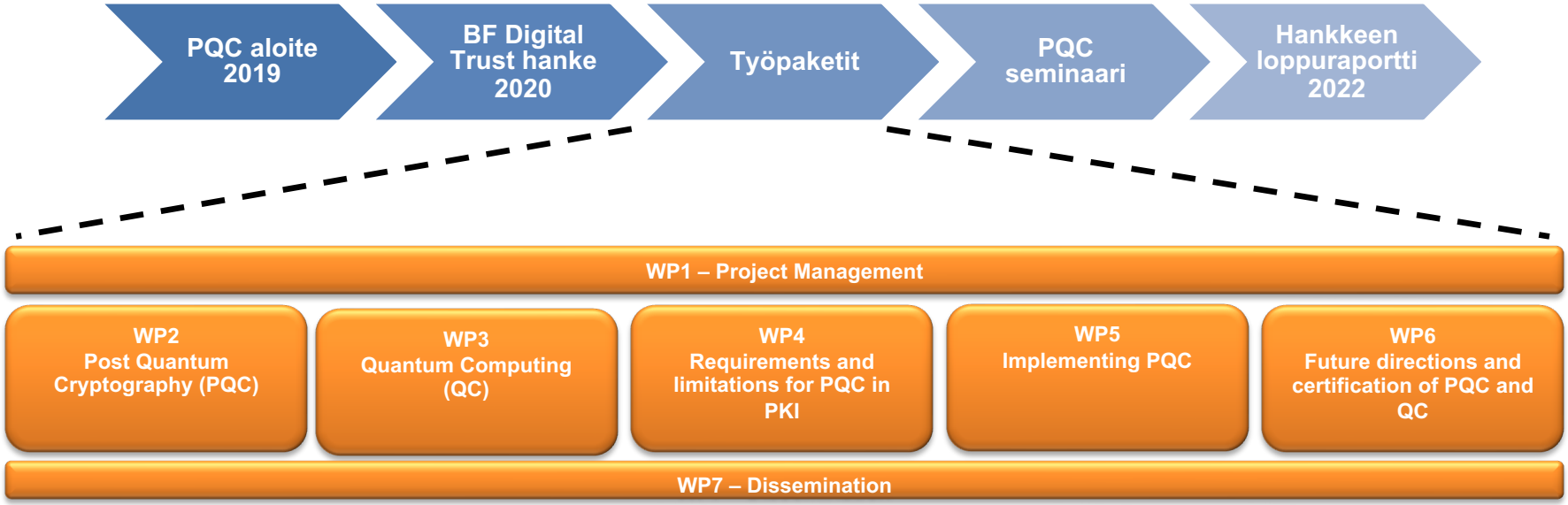
- Ville Heikkala, Traficom NCSA
- Kimmo Halunen, Oulun Yliopisto / MPK
- Visa Vallivaara, VTT
- Mikko Kiviharju, PV Tutkimuslaitos

Quantum Safe Cryptography
PQC Finland

BUSINESS
FINLAND

pqc.fi

POST-QUANTUM CRYPTOGRAPHY



KONSORTIO

Puolustusvoimat
The Finnish Defence Forces

BUSINESS
FINLAND

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

DIGI- JA
VÄESTÖTIETO-
VIRASTO

Aalto-yliopisto

FINNISH SECURITY AWARDS

PQC Finland -projektille parhaan tulevaisuuden kybertuvallisuusaloitteen 2020 palkinto

Encryption is Our Last Line of Defense

PQC FINLAND

BUSINESS FINLAND

- Post-Quantum Cryptography project: www.pqc.fi
- A Co-Innovation project funded by Busines Finland under the Digital Trust programme
- Duration: 1.1.2020-30.6.2022 with total budget ~ 6 M€
- Nine partners in the consortium
  - Three universities and research institutes
  - Six companies
- Final seminar on Friday 6.5. in Team Finland -talo

QUANTUM SAFE ALGORITMS FOR NATIONAL SECURITY – PQC PROJECT

Background

- Existing algoritms are quantum resilient and considered safe for use until 2023+ (international consensus)
- For asymmetric encryption none of existing algoritms are safe, when quantum computers reach relevant level
- Quantum Safe algoritms are currently being evaluated by U.S. NIST process, with release target during 2023-2025

Goals

- Develop Finnish cryptology knowhow with focus on algorithms
- Get understanding how Finland should prepare itself for Quantum Era 2025 →
- Strengthen national cybersecurity networks and public-private cooperation in areas of Quantum and Cryptography
- Create criteria and parameters for certification national products with Quantum Safe. features
- Explore export possibilities for products and services, at least within EU single market
- Enhance and expand international academic cooperation overall, also outside of science community

THE CONSORTIUM

- Research: VTT, Aalto- and Helsinki University
- Industry: SSH, Bittium, Insta, Sectra, Advenica and Tosibox, represent the very cutting edge of encryption technology and important security companies applying these in their solutions
- There is collaboration with NIST through research exchange
- In addition, there are important government stakeholders related to national security included

PQC-FI WORK PACKAGES

- **Työpaketit**

WP1 – Project Management
Steering Group chairman: Jorma Mellin / SSH Project Manager: Visa Vallivaara / VTT

WP2
Post Quantum Cryptography (PQC)

Lead org: Helsinki univ

Research of PQC security of PQC candidates including side-channel attacks.
Mitigations to these studied and proposed whenever possible.

WP3
Quantum Computing (QC)

Lead org: Aalto univ.

Overview of most likely scenarios of QC development and implications of those (research, education, critical computing, access to key materials, opportunities for Finnish companies).
Recommendations paper to be used as guideline for future development of QC.

WP4
Requirements and limitations for PQC in PKI

Lead org: Insta Oy

Study of PQC algorithm implementation and performance on Hardware Security Modules (HSM), smart cards and FPGA and IoT devices.
PKI related management protocols (e.g. CMP, EST, ACME) with PQC algorithms.

WP5
Implementing PQC

Lead org: SSH Oyj

PQC implementation to SSH NQX product family, test it thoroughly and analyze the gaps and effects for successful implementation into national use.

WP6
Future directions and certification of PQC and QC

Lead org: VTT Oy

Create vision and strategy for national digital security by utilizing cryptographic methods.

Set PQC criteria and certification parameters for nationally approved solutions ranging from ST IV to ST II.

WP7 – Dissemination (all)

PQC WP2: teoria

- Valtteri Niemi
- Helsingin yliopisto

KVANTTITURVALLINEN 5G

Mobiiliverkkojen turvallisuus perustuu **symmetriseen** kryptografiaan

- Käyttäjän autentikointi
- Radioyhteyden turvaaminen: salaus ja eheys
- Verkon sisäisen kommunikaation turvaaminen

KVANTTITURVALLINEN 5G

Mobiiliverkkojen turvallisuus perustuu **symmetriseen** kryptografiaan

- Käyttäjän autentikointi
- Radioyhteyden turvaaminen: salaus ja eheys
- Verkon sisäisen kommunikaation turvaaminen

→ 128-bittiset avaimet korvattava 256-bittisillä

KVANTTITURVALLINEN 5G

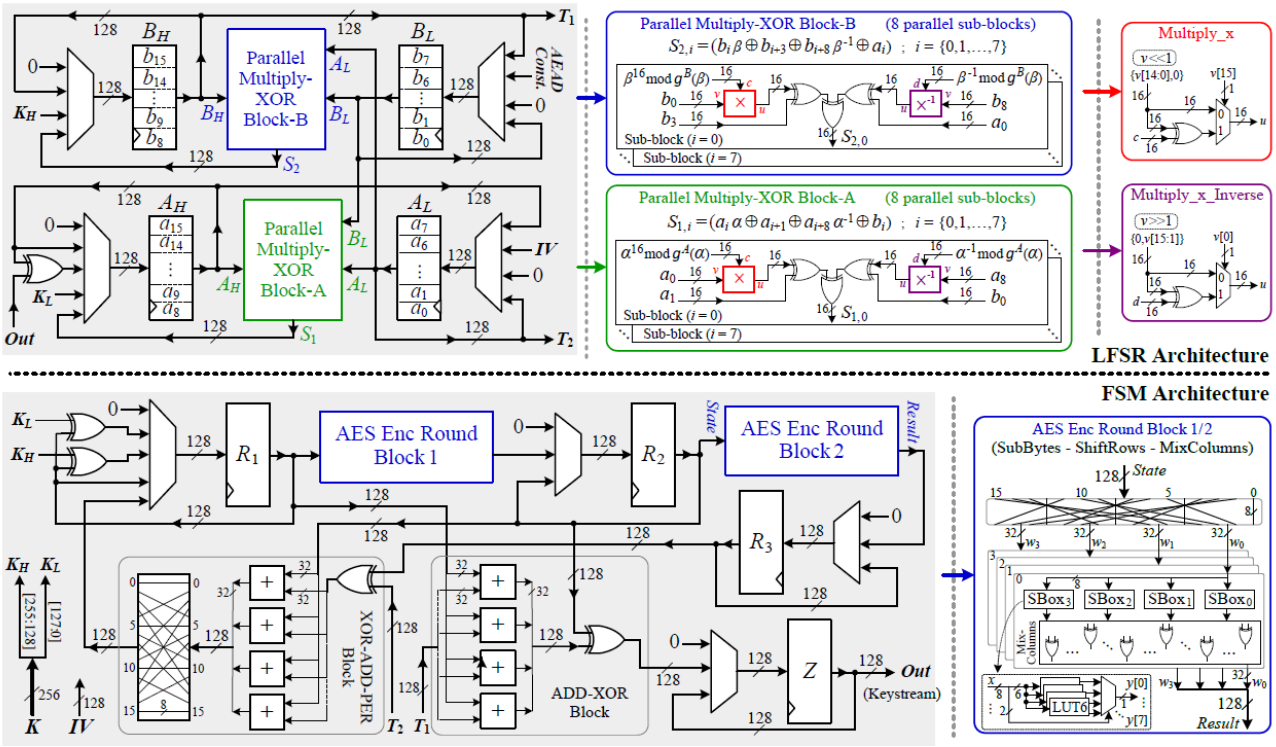
Mobiiliverkkojen turvallisuus perustuu **symmetriseen** kryptografiaan

- Käyttäjän autentikointi
- Radioyhteyden turvaaminen: salaus ja eheys
- Verkon sisäisen kommunikaation turvaaminen

→**128-bittiset avaimet korvattava 256-bittisillä**

→ **tarvitaan uudet algoritmit (jonosalaimet)**

SNOW V: RINNAKKAINEN FPGA TOTEUTUS



Milad Bahadori, Kimmo Järvinen and Valtteri Niemi : FPGA Implementations of 256-bit SNOW Stream Ciphers for Post-Quantum Mobile Security, *IEEE Trans. VLSI systems* , 2021

KVANTTITURVALLINEN 5G

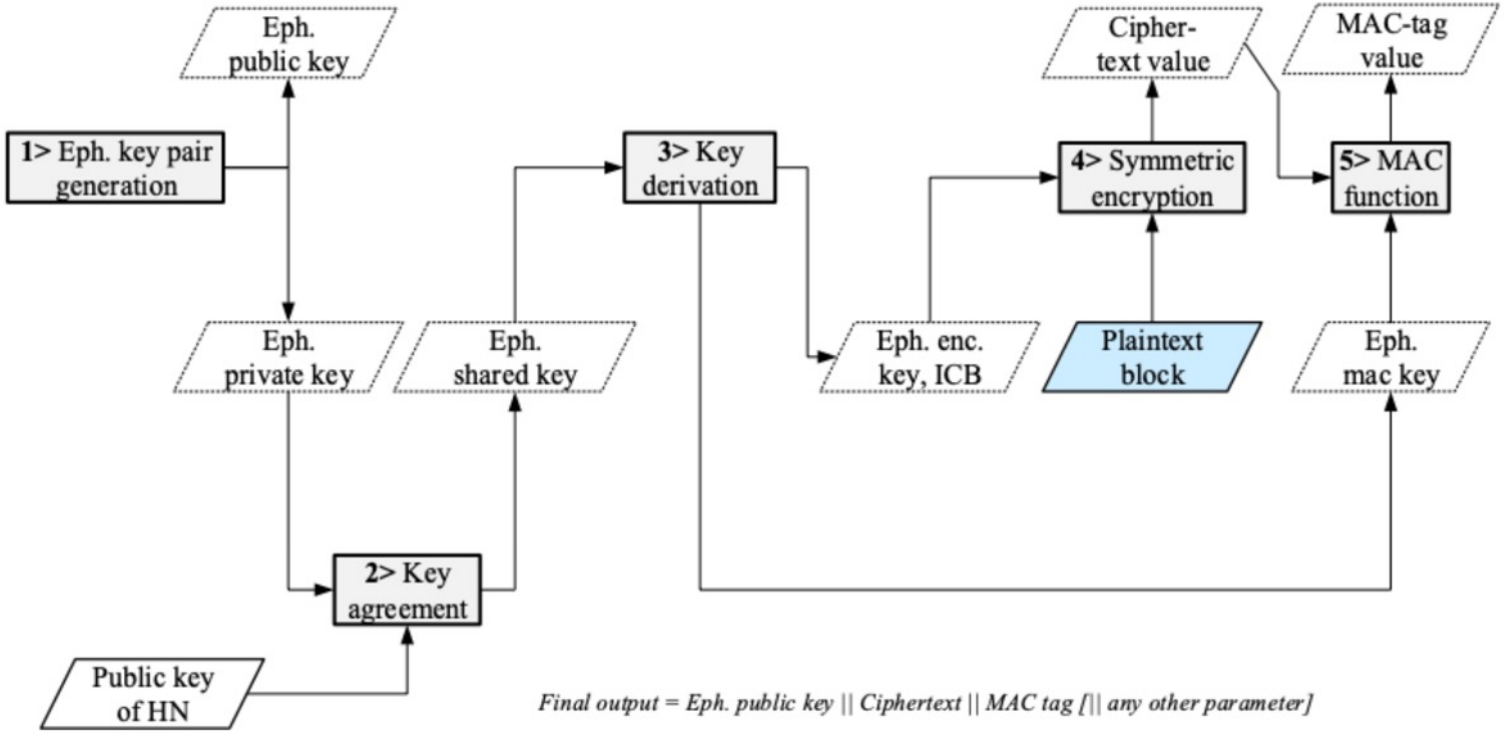
Mobiiliverkkojen turvallisuus perustuu **symmetriseen** kryptografiaan

- Käyttäjän autentikointi
- Radioyhteyden turvaaminen: salaus ja eheys
- Verkon sisäisen kommunikaation turvaaminen

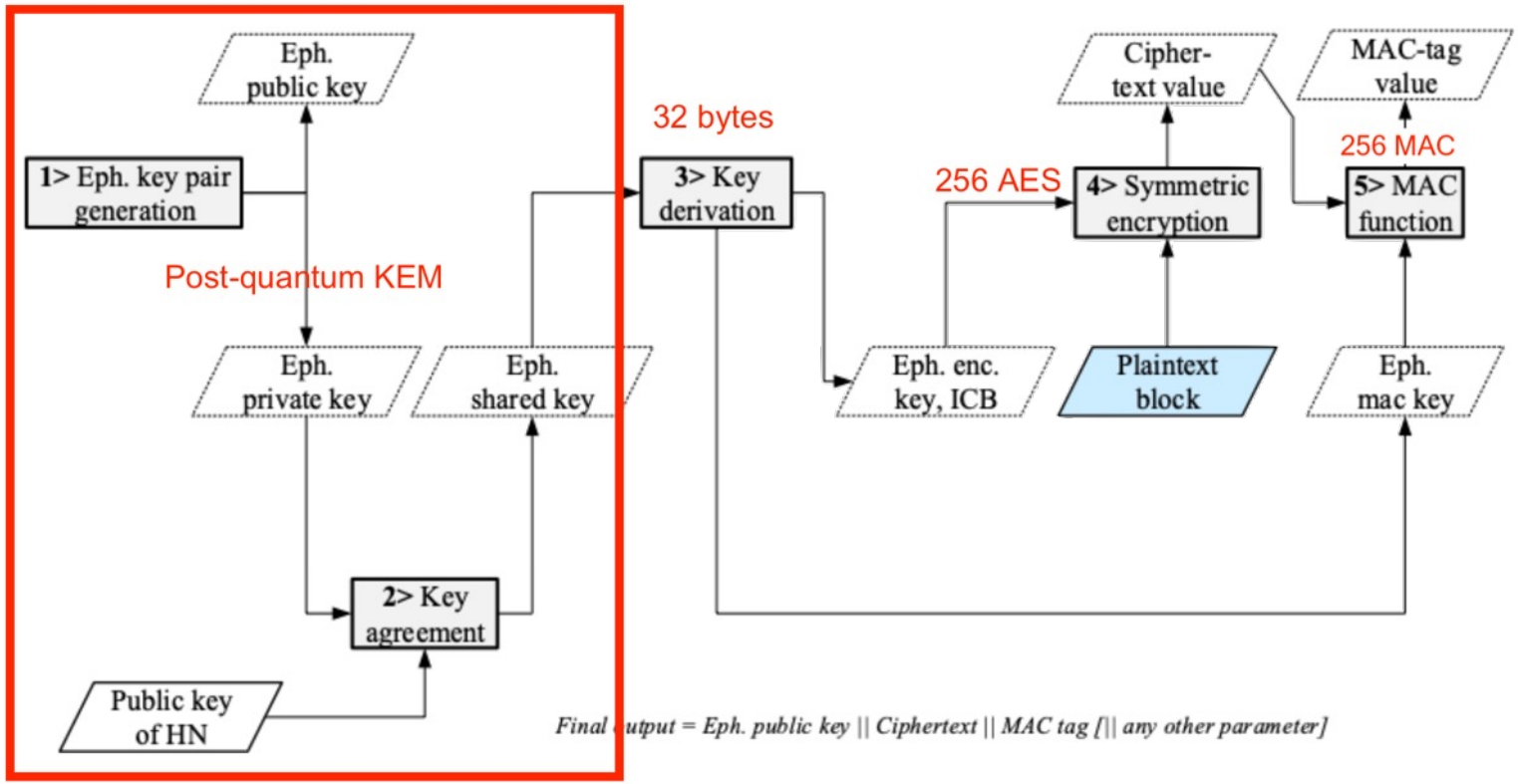
Mutta tarvitaan myös **epäsymmetristä** julkisen avaimen kryptografiaa

- Käyttäjän identifiointi
- Mobiiliverkkojen välinen kommunikointi
- Sovellustaso

KÄYTTÄJÄN IDENTITEETIN SUOJAAMINEN



KÄYTTÄJÄN IDENTITEETIN SUOJAAMINEN



Algorithm	At UE (μs)	At HN (μs)
ECIES Curve25519	49.221	48.110
ECIES Secp256r1	131.201	131.001
Classic-McEliece-348864	16.167	49.319
LightSaber-KEM	17.039	16.563
NTRU-HPS-2048-509	14.722	20.015
Kyber512	14.351	10.101

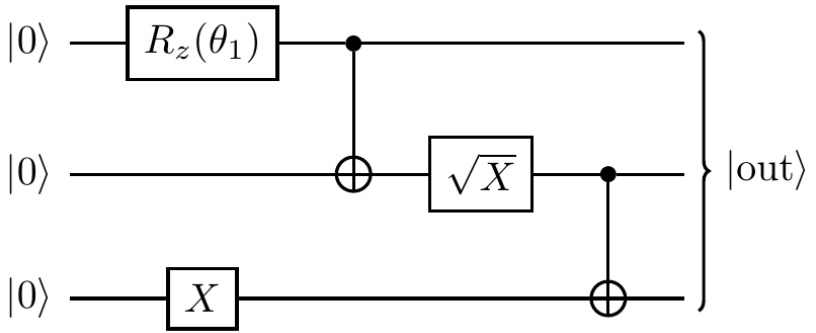
Mohamed Taoufiq Damir and Valtteri Niemi : On Post-Quantum Identification in 5G,
ACM WiSec '22, San Antonio, Texas, USA

PQC ALGORITMIEN INTEGROINTI AVOIMEN LÄHDEKOODIN KIRJASTOIHIN

Algoritmi	Toiminto	CPU-syklit (integrointi)	CPU-syklit (mallitoteutus)	Suoritusajan kasvu (%)
Kyber-512	Avainparin luominen	77452	70527	10
	Salaaminen	103454	90177	15
	Salauksen avaaminen	124722	106539	17
Kyber-768	Avainparin luominen	137032	119089	15
	Salaaminen	170474	141759	20
	Salauksen avaaminen	196737	162677	21
Kyber-1024	Avainparin luominen	213370	181525	18
	Salaaminen	251775	205682	22
	Salauksen avaaminen	283941	230457	23
LightSaber	Avainparin luominen	84330	43321	95
	Salaaminen	106420	56580	88
	Salauksen avaaminen	121883	62496	95
Saber	Avainparin luominen	158330	80317	97
	Salaaminen	193770	100271	93
	Salauksen avaaminen	218243	109088	100
FireSaber	Avainparin luominen	257348	132859	94

Julius Hekkala, Kimmo Halunen and Visa Vallivaara: Implementing Post-quantum Cryptography for Developers, *Proc. of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022),*

WP3 Quantum computing



WP3 Quantum computing

LEAD: Aalto University personnel

- Prof. Ilkka Tittonen
- PhD Arttu Pönni
- PhD Matti Raasakka
- BSc Oona Oinonen
- BSc Vivian Phan
- BSc Tom Rindell
- BSc Mikko Seesto
- BSc Qingxin Yang

OTHER PARTICIPANTS:

VTT
SSH
Traficom
Insta
University of Helsinki
Advenica
Sectra

Micro and Quantum Systems

WP3 Quantum computing

TASK 1: Estimation of expected limitations and development of QC

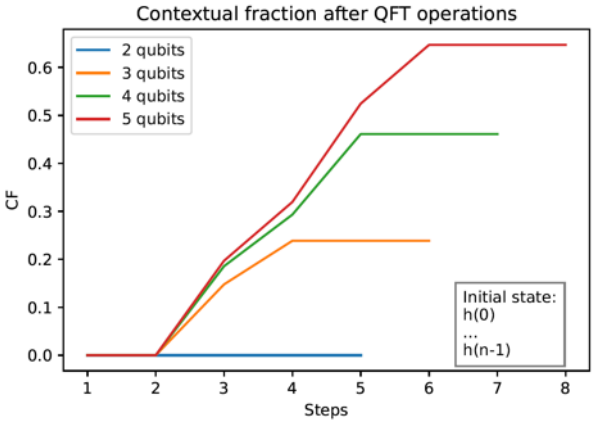
- Running Shor's algorithm for discrete log / integer factorization for any significantly sized input requires **fault-tolerant quantum computing**. => Overhead in physical qubit number.
- Survey of the current **quantum error-correction methods**, focusing on surface codes, the leading method for superconducting qubits. (WP presentation Feb 21)
- Most recent estimates [1] suggest that breaking 2048 bit RSA requires 10's of millions of physical qubits. E.g., according to IBM roadmap, doubling the number of physical qubits every year. => **Roughly 10 million qubits in about 15 years** (assuming no scaling issues!)
- Resource requirements can be reduced significantly by using a (yet non-existing) quantum memory [2] or possibly other hypothetical future technologies.
- Possible future developments in quantum hardware (e.g., quantum memory, other physical qubit implementations, scaling issues etc.) and error-correction methods cause **significant uncertainty** to these estimates.

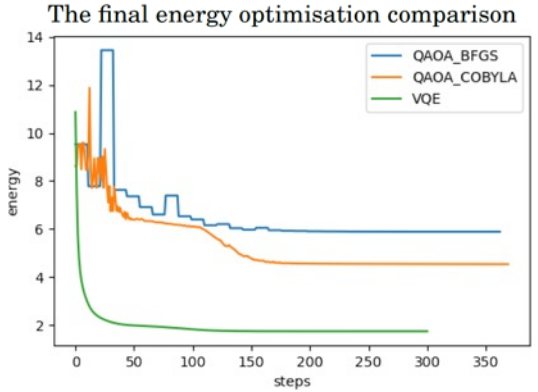
[1] Gidney, Ekerå, "How to factor 2048 bit RSA integers in 8 hours with 20 million noisy qubits", *Quantum* **5, 433** (2021).
[2] Gouzien, Sangouard, "Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory", *Phys. Rev. Lett.* **127, 140503**.

WP3 Quantum computing

TASK 2: Survey and analysis of existing quantum algorithms

- Implemented and tested Kuperberg's algorithm [3] for **dihedral hidden subgroup problem** (equivalent to unique SVP [4]).
  => BSc thesis, Oinonen (WP presentation Aug 21)
- Analyzed the **non-classicality of quantum Fourier transform**, key ingredient in Shor's algorithm, by measuring contextual fraction [5].
  => BSc thesis, Yang (WP presentation Feb 22)
- Focused also on heuristic approaches due to intense resource requirements of exact methods. E.g. **quantum machine learning** on a NISQ machine with quantum SVM. => BSc thesis, Seesto
- Overview of **error mitigation methods**. => BSc thesis, Kumar
- Numerical **data input** into quantum computer. => BSc, Lemola
- Variational quantum eigensolver (VQE) and quantum approximate optimization algorithm (QAOA) applied to **integer factorization**.
  => BSc thesis, Phan (WP presentation Apr 22)



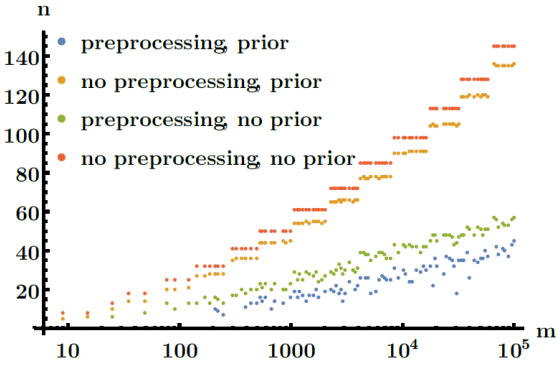


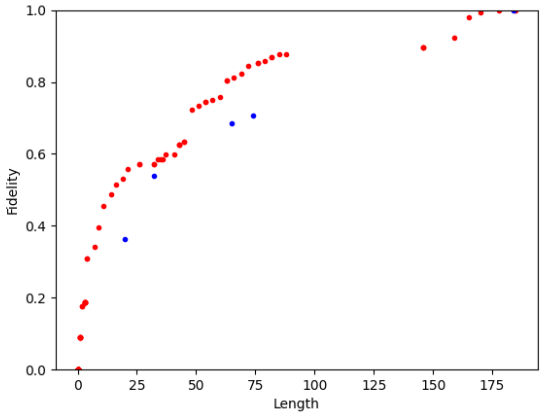
[3] Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem", *SIAM J. Comput.* **35** (2005).
[4] Regev, "Quantum computation and lattice problems" (2003), arXiv:cs/0304005.
[5] Abramsky, Barbosa, Mansfield, "The contextual fraction as a measure of contextuality", *Phys. Rev. Lett.* **119, 050504** (2017).

WP3 Quantum computing

TASK 3: Development and analysis of new quantum algorithms

- Refined the existing quantum machine learning approaches [6] applied to **integer factorization**.
- Found that switching to VQE optimization substantially increases variational quantum factoring (VQF) performance compared to QAOA optimization. **Results will be published in [7].**
- Studied the **role of entanglement** in the performance of VQF.
- Developed a **multi-objective genetic algorithm** for quantum circuit discovery. => BSc thesis, Kito (WP presentation Oct 21)
- First application to **approximate state preparation**. Improvements to the state-of-the-art algorithm [8]. **Results will be published in [9].**
- In the future can be used to study the **optimality of quantum circuits** designed, e.g., for solving crypto-relevant problems.





[6] Anschuetz, Olson, Aspuru-Guzik, Cao, "Variational quantum factoring", arXiv:1808.08927.

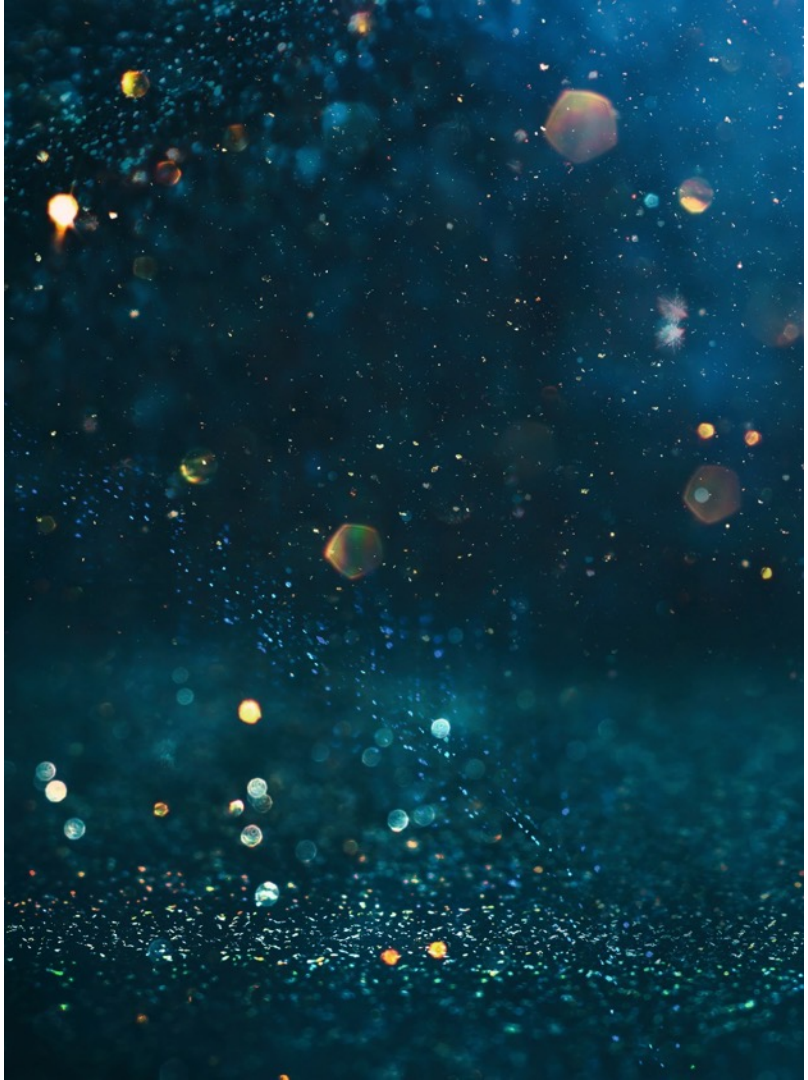
[7] Kornienko, Phan, Pönni, Raasakka, Tittonen, "On quantum factoring using noisy intermediate scale quantum computers", *to appear*.

[8] Araujo, Blank, da Silva, "Entanglement as a complexity measure for quantum state preparation" (2021), arXiv:2111.03132.

[9] Rindell, Yenilen, Pönni, Tittonen, Raasakka, "Generating quantum state preparation circuits with a genetic algorithm", *to appear*.

PQC WP 4 – PQC PKI

- Työpaketin tavoitteena arvioida PQC-allekirjoitusalgoritmien käytettävyyttä julkisen avaimen infrastruktuurissa ja niihin liittyviä rajoitteita.
- Työpaketissa mukana Insta, Bittium, SSH, VTT, UH, Aalto ja Advenica



PQC WP 4 – PQC PKI

Työpaketissa tehty:

- NIST PQC-standardoinnin seuranta
- Allekirjoitusalgoritmien testaus avoimen lähdekoodin toteutuksilla
  - Suorituskykyä, avainpituuksia, allekirjoituspituuksia
- Opinnäytetyöt yhdessä muiden työpakettien kanssa:
  - Juha Luukkanen: "Post Quantum Cryptography, Impact to the public key cryptography"
  - Sara Nikula: "Älykkään liikenteen varoitusviestien kvanttiturvallinen allekirjoittaminen"
- Julkaisu yhteistyössä työpaketin 6 kanssa
  - Sara Nikula: "Quantum-Safe Signing of Notification Messages in Intelligent Transport Systems"
- Insta-Bittium VPN tuote yhteistyössä työpaketin 5 kanssa
  - P521-Dilithium todennusvarmenteet IKE-protokollassa

INSTA

PQC WP 4 – PQC PKI

Johtopäätökset:

- Algoritmien turvallisuuden arviointi on aktiivisessa vaiheessa, joka hidastaa standardointia ja luottamuksen syntymistä uusiin algoritmeihin.
- Standardien keskeneräisyys sekä ymmärryksen ja luottamuksen puute algoritmien turvallisuudesta hidastaa algoritmien käyttöönottoa ohjelmistoissa ja laitteistoissa.
- Kaikki odottavat NIST:n PQC standardoinnin tuloksia.

INSTA

PQC Finland
WP5 – implementing PQC

BUSINESS
FINLAND

pqc.fi

PQC-FI WP5

SSH.COM

INSTA

Bittium

TOSIBOX®

SECTRA

advenica

- Toteuttaa PQC algoritmeilla varustettu tuote; Proof-of-Concept
- Kaupallinen malli ja asiakkuudet
- Kartoittaa vientimarkkinan kiinnostus ja haasteet
- Swetha Meeranath lopputyö

ACHIEVEMENTS

Bittium and Insta Are Developing Quantum Safe Technology

THU, MAR 31, 2022 11:00 CET

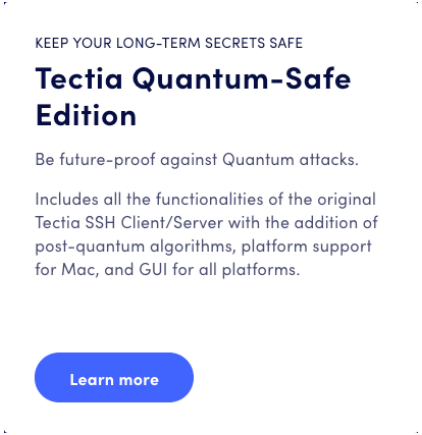
Report this content

Press Release

Free for publication on March 31st, 2022 at 12:00 pm (CEST +1)

Bittium and Insta Are Developing Quantum Safe Technology

Oulu, Finland, March 31st, 2022 – Bittium and Insta are part of a nationally significant Post Quantum Cryptography (PQC) project, funded by the Business Finland Digital Trust program. PQC project develops quantum secure encryption technology, integrating it as part of products and solutions. The goal of the project is to accelerate the increase of innovations based on digital trust and a growth of business. In this project, Bittium and Insta will combine their expertise in quantum secure key exchange and authentication, providing even stronger capability to protect customer information.



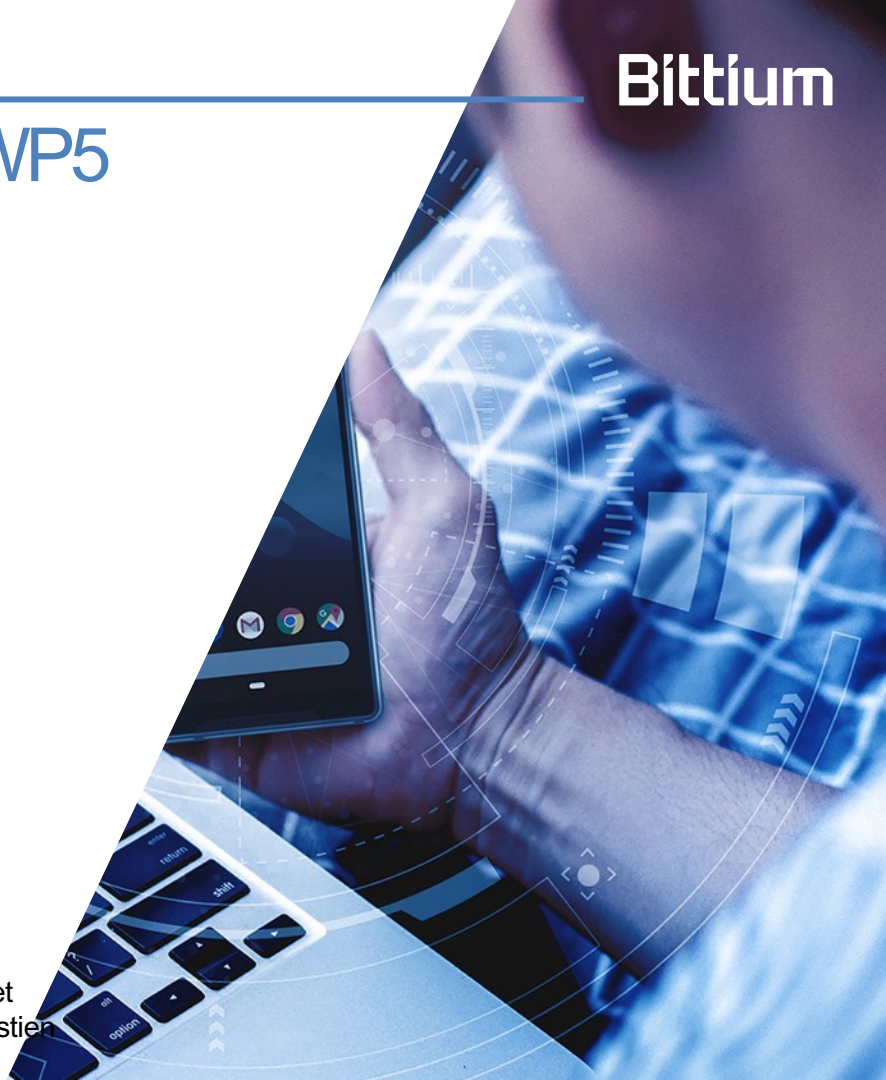
- Ensimmäinen kaupallinen tuotelanseeraus: syyskuu 2021
- Ensimmäiset kaupalliset tarjoukset: lokakuu 2021
- Ensimmäinen kaupallinen vientikauppa: tammikuu 2022 (Singapore)
- Kansainvälistyminen: Viro, Ranska, Ukraina, Japani, pohjois- ja etelä Amerikka

Insta – Business Finland PQC WP5

- PQC IPSec/IKEv2 toteutus Insta Safelink VPN-tuotteeseen
  - Toteutettu yhteistyössä Bittiumin kanssa
  - Testattu interop-yhteensopivuus Bittium SafeMove VPN tuotteen kanssa
- PQC toteutukseen valitut algoritmit
  - Salausalgoritmit (KEM) CRYSTALS Kyber512/768/1024(-90s)
  - Allekirjoitusalgoritmit CRYSTALS Dilithium2/3/5
  - Myös muut PQC-algoritmit mahdollista toteuttaa
- Toteutetut RFC + draft
  - RFC 7427 (Signature Authentication in the IKEv2)
  - RFC 7384 (IKEv2 Message Fragmentation)
  - RFC Draft Intermediate Exchange in the IKEv2 Protocol
  - RFC Draft Multiple Key Exchanges in IKEv2
  - IKEv2 -autentikaatio hybrid ECDSA- ja Dilithium X.509 -varmenteilla
- Kasvaneet PQC salausavain- ja varmennekoot lisäävät todennuksessa ja avainvaihdossa käytettävien viestien määrää ja vaikutusten arviointi järjestelmän suorituskykyyn vaatii vielä käyttökokemuksia operatiivisissa ympäristöissä

Bittium – Business Finland PQC WP5

- ✓ PQC IPSec/IKEv2 toteutus Bittium SafeMove VPN -tuotteeseen
  - Toteutettu yhteistyössä Instan kanssa
  - Testattu interop-yhteensopivuus Insta Safelink -tuotteen kanssa
- ✓ PQC-toteutukseen valitut algoritmit
  - Salausalgoritmit (KEM) CRYSTALS Kyber512/768/1024(-90s)
  - Allekirjoitusalgoritmit CRYSTALS Dilithium2/3/5
  - Myös muut PQC-algoritmit mahdollista toteuttaa
- ✓ Toteutetut RFC + draft
  - RFC 7427 (Signature Authentication in the IKEv2)
  - RFC 7384 (IKEv2 Message Fragmentation)
  - RFC Draft Intermediate Exchange in the IKEv2 Protocol
  - RFC Draft Multiple Key Exchanges in IKEv2
  - IKEv2-autentikaatio hybrid ECDSA ja Dilithium X.509 varmenteilla
- ✓ Peräkkäin suoritettavat avaintenvaihdot, sekä PQC-algoritmien kasvaneet avain- ja varmennekoot lisäävät neuvottelussa käytettävien protokollaviestien määrää. Näiden vaikutus järjestelmän suorituskykyyn vaatii vielä



PQC Finland
WP6 – Future and Certification

BUSINESS FINLAND

pqc.fi

WP6 – FUTURE DIRECTIONS AND CERTIFICATION OF PQC AND

- VTT
- Insta
- NCSC-FI (National Cyber Security Centre)
- DVV (Digital and Population Data Services Agency)
- University of Helsinki
- Advenica
- Bittium
- Sectra

WP6 - FUTURE DIRECTIONS AND CERTIFICATION OF PQC AND QC

- New methods used in PQC
  - Effects on certifications
- Research on measuring or assessing the new methods
- Future of QC and cryptography
  - Strategy planning
  - Policy brief at the end of the project

KVANTTIPANEELI

Moderaattorina Jorma Mellin

Teemat

- Kvanttitietokoneiden muutosvoimat toimialalla?
- Onko Suomi hereillä?
- Kansalliset vahvuudet ja heikkoudet?
- Mitä pitää saada aikaiseksi?
- EU:n rooli?
- Kyberturvallisuus ja kvantit, miten edistämme?