XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Webinar series:

Cryptography under the hood

Tuesday, September 6, 2022
15:00 CET

Post Quantum Cryptography Round-up

Where Are We Now and What's Next?

Speaker

Perttu Saarela

Developer,
Xiphera

Agenda

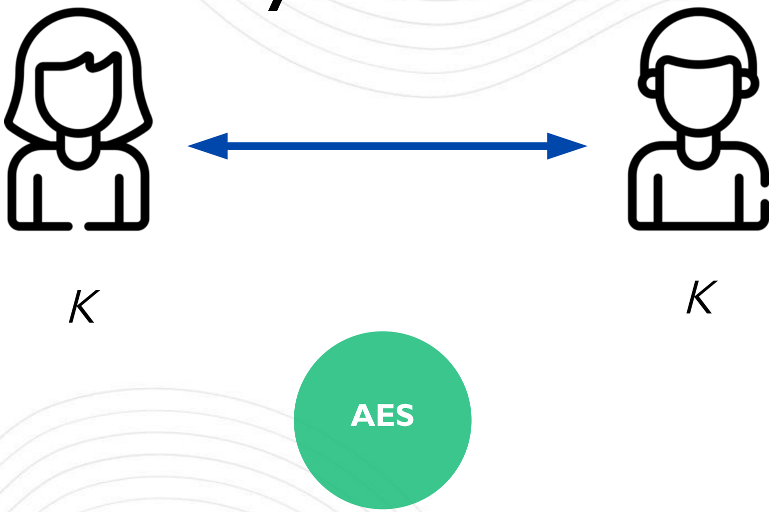
I. What is PQC?

II. Foundations of new standards

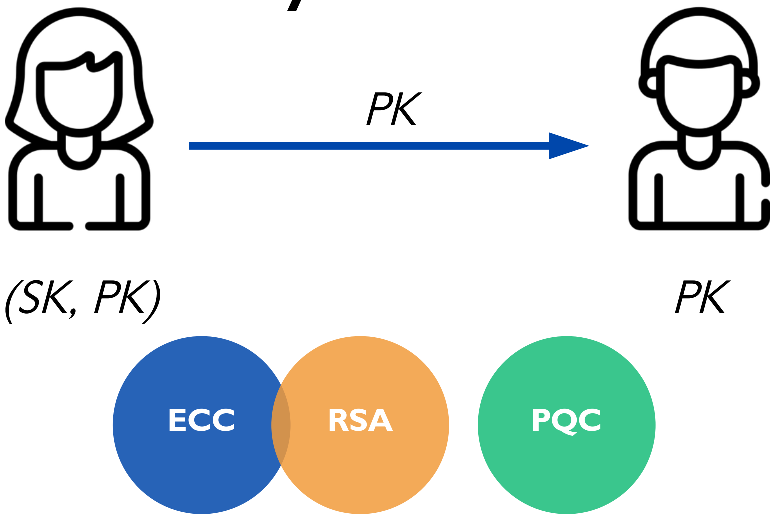
III. Secure implementation and the hybrid model

Symmetric vs. Asymmetric

Symmetric



Asymmetric



Shared key *K*

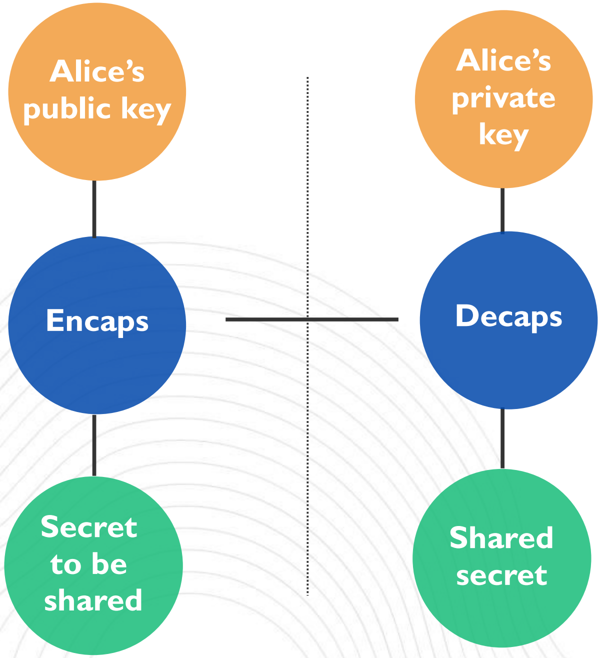
- Must be secret

Key-pair

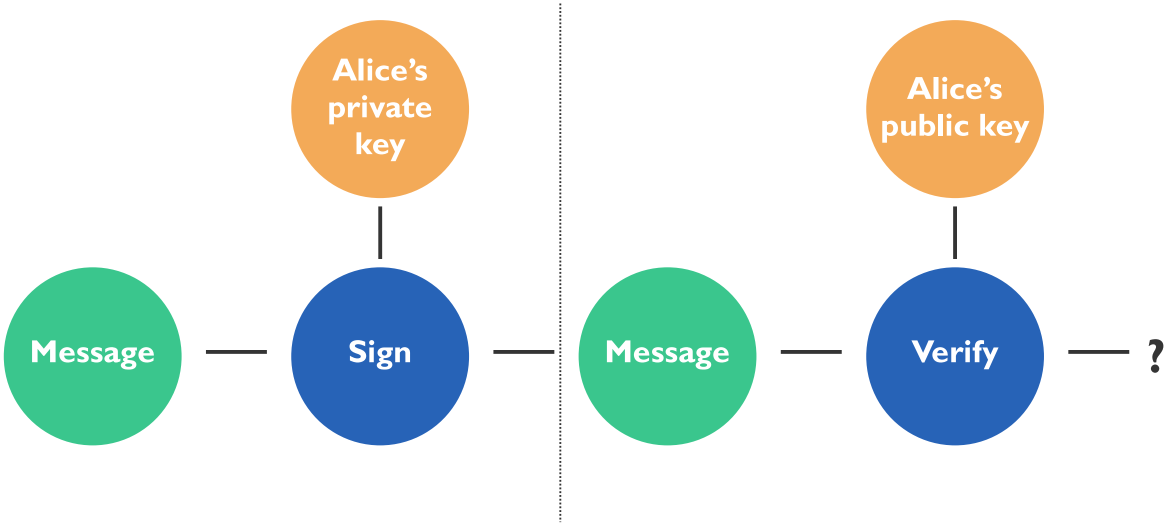
- Private key (SK) $\rightarrow$ Public key (PK)
- Public key (PK) $\nrightarrow$ Private key (SK)

Asymmetric Cryptography

Key encapsulation



Digital signatures



Post-Quantum Cryptography

- Quantum computers pose a threat to modern public key encryption
- Need for new types of PKE algorithms based on different hard problems
- Quantum computers capable of running these attacks don't exist yet
- Symmetric encryption is not in danger

Post-Quantum Cryptography (PQC)

Cryptography resilient to quantum computers.

$\neq$

Quantum Cryptography

Cryptography using quantum mechanical phenomenon.

NIST PQC Competition

- 2016 Competition starts
- 2017 Round 1 — 69 algorithms
- 2019 Round 2 — 21 algorithms
- 2020 Round 3 — 7 finalists and 8 alternates
- 5 July, 2022 Winners selected
- 2022 Round 4 — 4 algorithms
- 2023-2024 First standards
- 2024 ⇒ Additional standards

New signature algorithms

NIST Results

Round 3 Winners

KEM

- Crystals-Kyber (lattice)

Signature

- Crystals-Dilithium (lattice)
- Falcon (lattice)
- Sphincs$^+$ (hash)

Round 4 Candidates

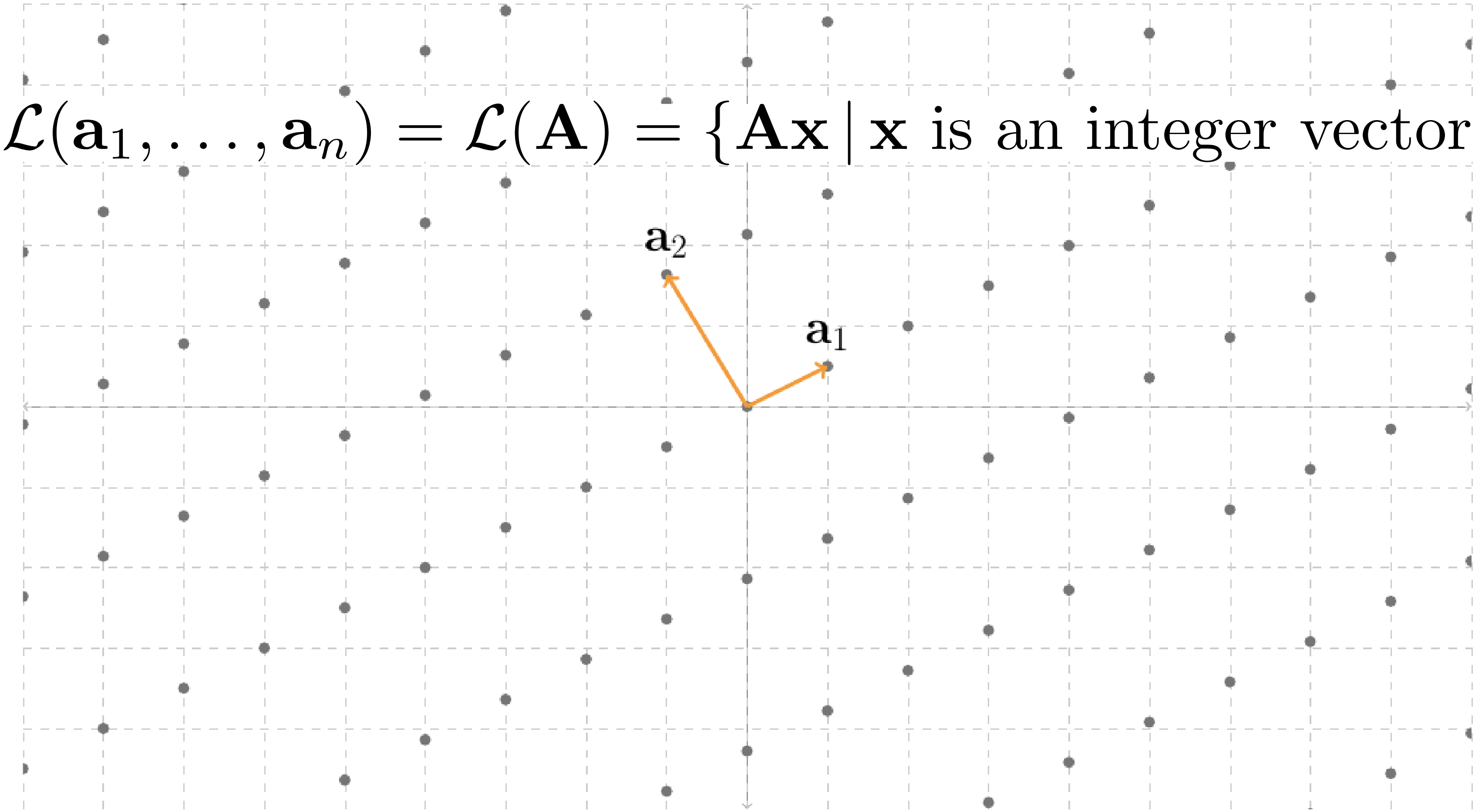
PKE

- BIKE (code)
- Classic McEliece (code)
- HQC (code)
- SIKE (isogeny)

Foundations of PQC

Lattices

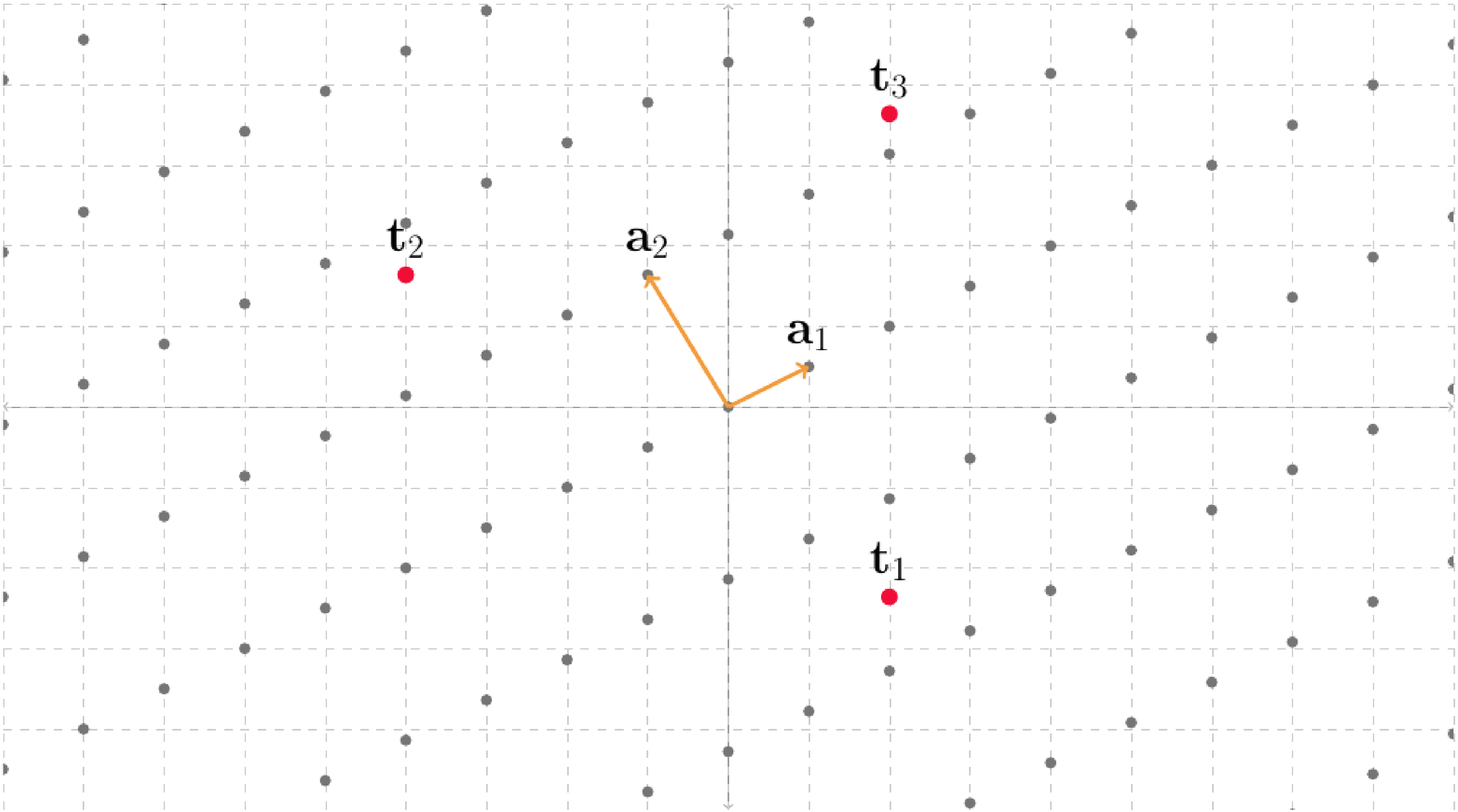
$$\mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_n) = \mathcal{L}(\mathbf{A}) = \{\mathbf{A}\mathbf{x} \,|\, \mathbf{x} \text{ is an integer vector} \}$$

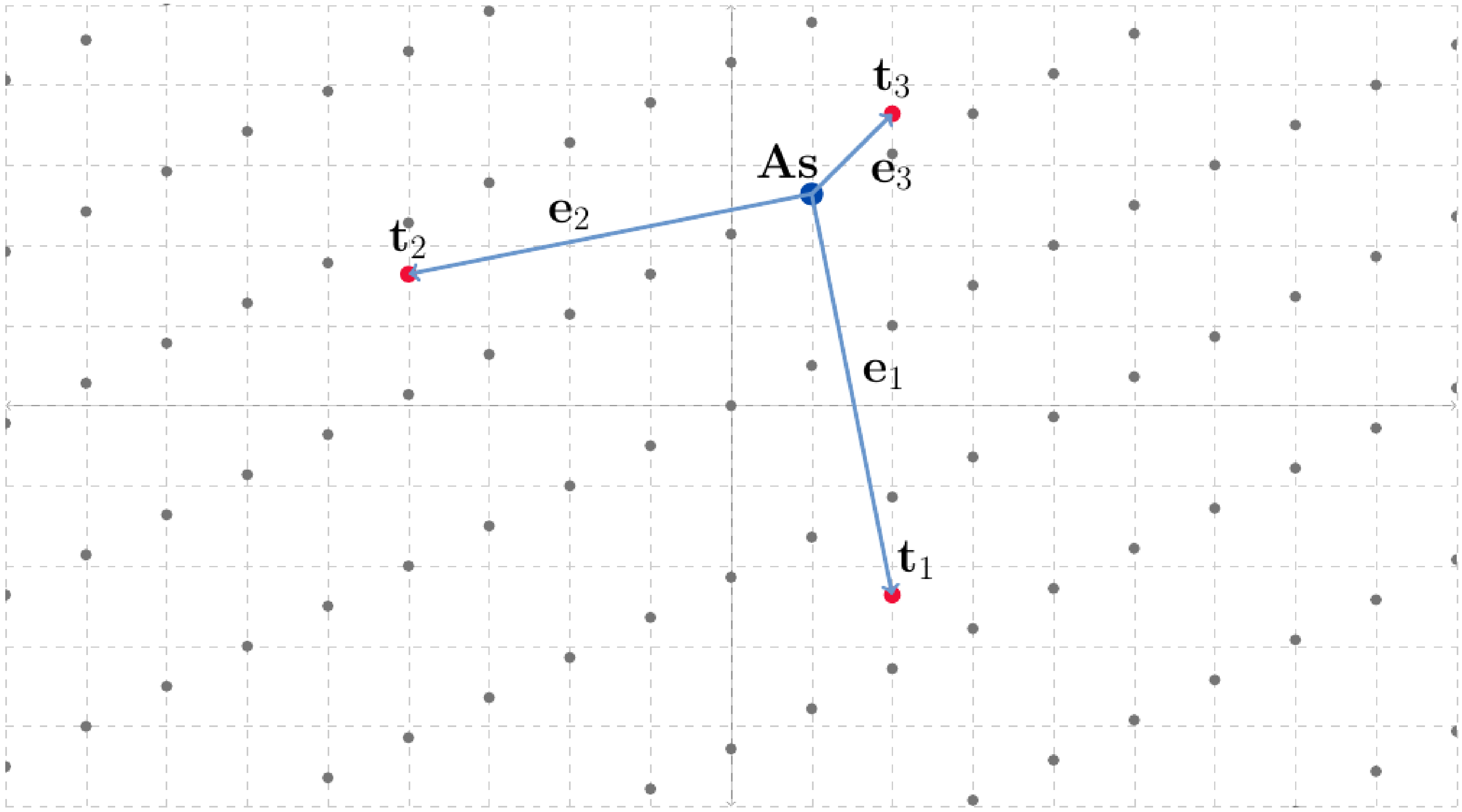


Lattice Problems

- Learning-with-errors (LWE) instance:
  - Generator (matrix) for a lattice $\mathbf{A}$
  - Secret $\mathbf{s}$
  - Challenge $\mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e}$
- LWE problem
  - Given $(\mathbf{A}, \mathbf{t})$
  - Solve for $\mathbf{s}$

→ *The LWE problem is hard.*


$\mathbf{t}_3$
$\mathbf{t}_2$
$\mathbf{a}_2$
$\mathbf{a}_1$
$\mathbf{t}_1$


$\mathbf{t}_3$
$\mathbf{As}$
$\mathbf{e}_3$
$\mathbf{e}_2$
$\mathbf{t}_2$
$\mathbf{e}_1$
$\mathbf{t}_1$

Lattice-Based Cryptography

- Lattice-based cryptosystems:
  - Public key: the LWE instance $(\mathbf{A}, \mathbf{t} = \mathbf{A}\mathbf{s} + \mathbf{e})$
  - Private key: the secret $\mathbf{s}$
  - Encryption: for message m, $\text{ct} = (\mathbf{A}\mathbf{m}, \mathbf{m}^T\mathbf{t} + \text{noise})$
  - Decryption:
    $m = \text{decode}(\mathbf{t}^T\mathbf{m} - \mathbf{s}^T\mathbf{A}\mathbf{m} + \text{noise}) = \text{decode}(\mathbf{e}^T\mathbf{m} + \text{noise})$
- Variants:
  - Ring LWE, Module LWE

Linear Codes

$$\begin{bmatrix}\mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_k\end{bmatrix}\begin{bmatrix} & & \\ & \mathbf{G} & \\ & & \end{bmatrix} = \begin{bmatrix}\mathbf{c}_1 & \mathbf{c}_2 & \cdots & \mathbf{c}_{n-1} & \mathbf{c}_n\end{bmatrix}$$

- What are linear codes?
- Widely used outside of cryptography
- Examples:
  - Reed-Solomon, Reed-Muller, Hamming codes
- Generator matrix G gives the code its properties
- Linear codes = Error-correcting codes

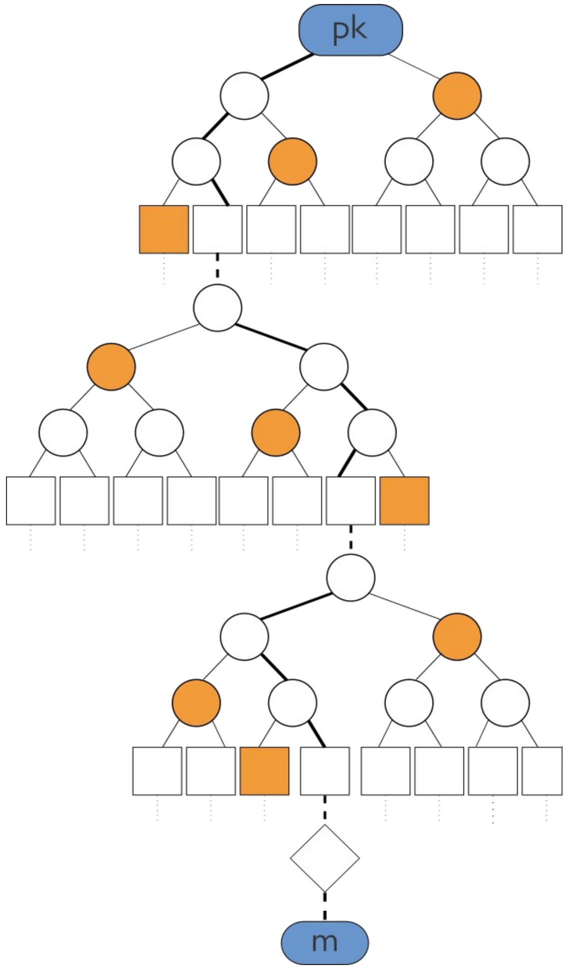
Code-Based Cryptography

- Based on the Syndrome Decoding Problem
- Code-based cryptosystems:
  - Public key: a Generator matrix G
  - Secret key: A decoder tolerating t errors $\Psi(\cdot)$
  - Encryption of message m: $ct = mG + e$
  - Decryption: $\Psi(ct) = \Psi(mG + e) = m$

→ *Syndrome decoding is hard!*

Hash-Based Signatures

- In a nutshell: a huge amount of hashing combined with an elaborate data structure
- One-time signatures (OTS) from hashing
- Extend to Many-time signatures with Merkel tree
- Combine Merkel trees to form a Hypertree (a tree of trees)
  - Bottom layer signs messages
  - Other layers sign public keys of the layers below
- Stateful versus Stateless



Isogeny

- SIKE = supersingular isogeny key encapsulation
- Builds on Elliptic curve cryptography
- Isogeny = maps between elliptic curves
- SIKE broken, doubts casted on Isogeny-based crypto

Practical consideration

KEM Stats

Algorithm	Status	Security	Private key	Public key	Ciphertext
ECC	Pre-Quantum	1	32	32	32
		5	64	64	64
Kyber	**Winner**	1	1632	800	768
		5	3168	1568	1568
HQC	Round 4	1	40	2249	4481
		5	40	7245	14469
BIKE	Round 4	1	2244	12323	12579
		5	4640	40973	41229
SIKE	Round 4 (broken)	1	374	330	346
		5	644	564	596
Classic McEliece	Round 4	1	6492	261120	128
		5	13932	1044992	240

Signature Stats

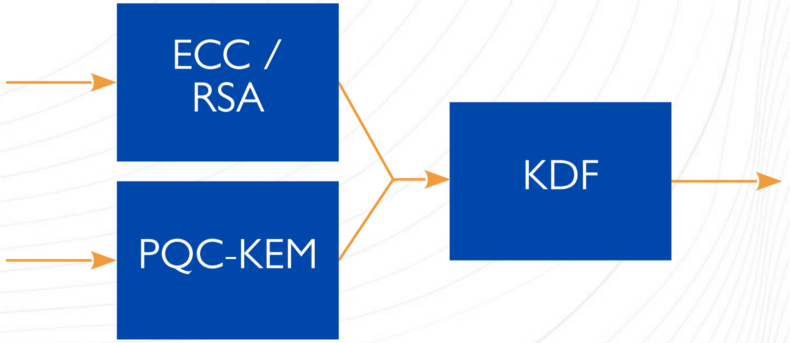
Algorithm	Status	Security	Private key	Public key	Signature
ECC	Pre-Quantum	1	32	32	64
		5	64	64	128
Dilithium	**Winner**	2*	2544	1312	2420
		5	4880	2592	4595
Falcon	**Winner**	1	1281	897	666
		5	2305	1793	1280
Sphincs$^+$ (s)	**Winner**	1	64	32	7856
		5	128	64	29792
Sphincs$^+$ (f)	**Winner**	1	64	32	17088
		5	128	64	49856

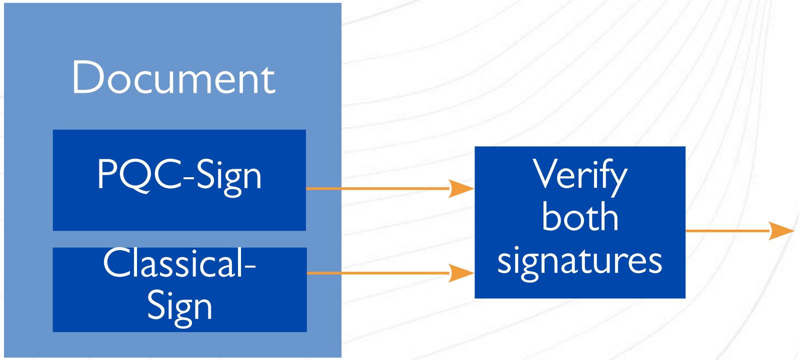
Secure Implementation

- The standards are coming and now is a good time to get involved
  - Systems designed today should have the ability to support PQC in the future
- Very complicated and optimized algorithms → implement with care
- New does not immediately imply secure
  - Two algorithms from Round 3 have been broken (Rainbow, SIKE)
- *FPGAs for the win*

Hybrid Model

- Combines the usage of classical and PQC algorithms
- Intermediate step before implementing PQC by itself
- Recommended by, for example, ANSSI
- Concretely:
  - For KEMs, the outputs of both classical and PQC PKEs are fed into a KDF
  - For signatures, the document is signed twice. Both signatures must verify to true.
- *FPGAs for the win again*





What's Next?

Standards coming out in ~2024 - 2025

Round 4 finishes

Non-lattice-based solutions

Ongoing research

Side-channel attacks

New potential attacks?

XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Cryptography under the hood

will continue in January 2023!

More info coming soon.

www.xiphera.com
info@xiphera.com
perttu.saarela@xiphera.com