XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Tuesday, September 6, 2022
10:00 EET

Post-quantum cryptography:

Current status and future consequences

Embedded Conference Finland

Helsinki, Finland

Speaker

Kimmo Järvinen

CTO & Co-founder, Xiphera

Agenda

I. Brief introduction to cryptography

II. The quantum threat and PQC

III. The future PQC standards

IV. What are the effects of PQC in practice?

Cryptography

Cryptography vs. cryptanalysis

Foundation of computer & communication security

Security is based on the secrecy of keys

Cryptography

Cryptography vs. cryptanalysis

Foundation of computer & communication security

Security is based on the secrecy of keys

SHA3

SHA2

MD5

AES

HMAC

SHA1

DES

AES-GCM

ECDH

DSA

TLS

ECDSA

RSA

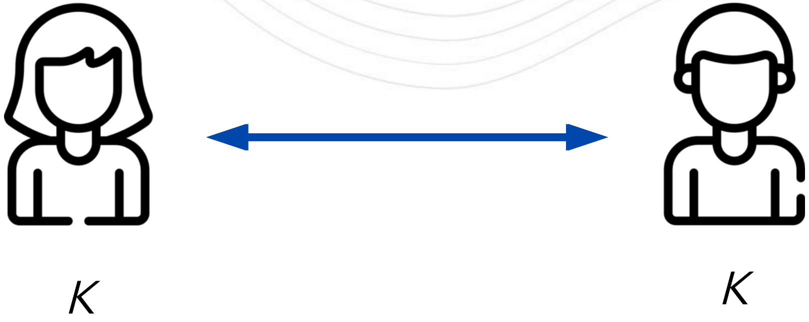
MACsec

IPsec

Secure-boot

Symmetric vs. asymmetric

Symmetric

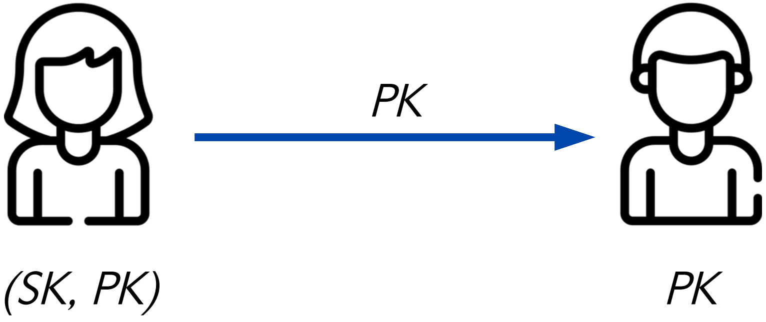


AES

Shared key K

- Must be secret

Asymmetric



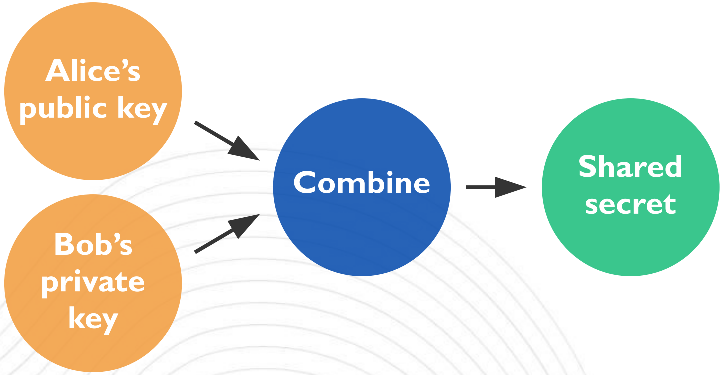
ECC RSA PQC

Key-pair

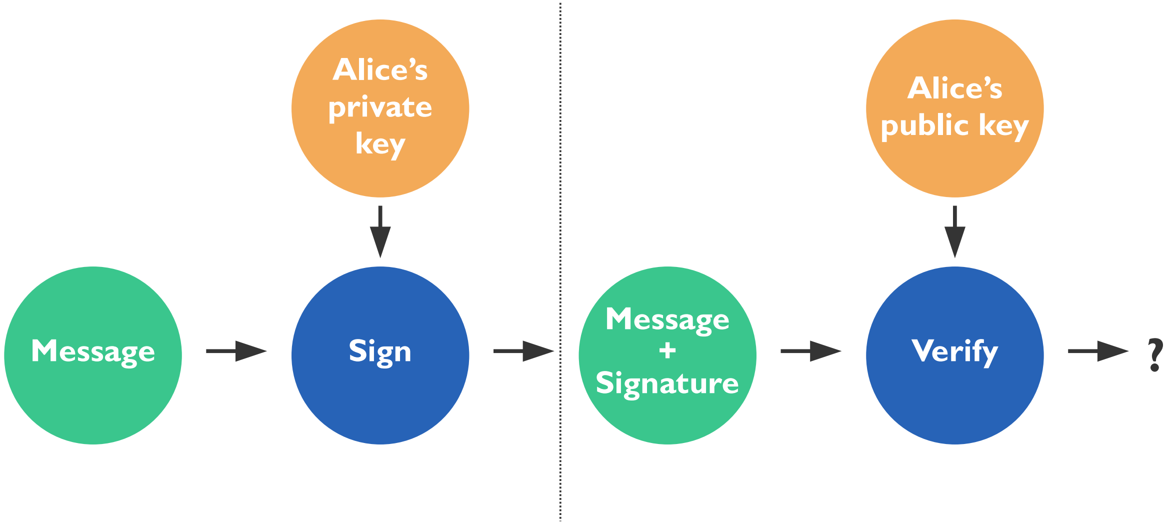
- Private key (SK) → Public key (PK)
- Public key (PK) ↛ Private key (SK)

Asymmetric cryptography

Key exchange

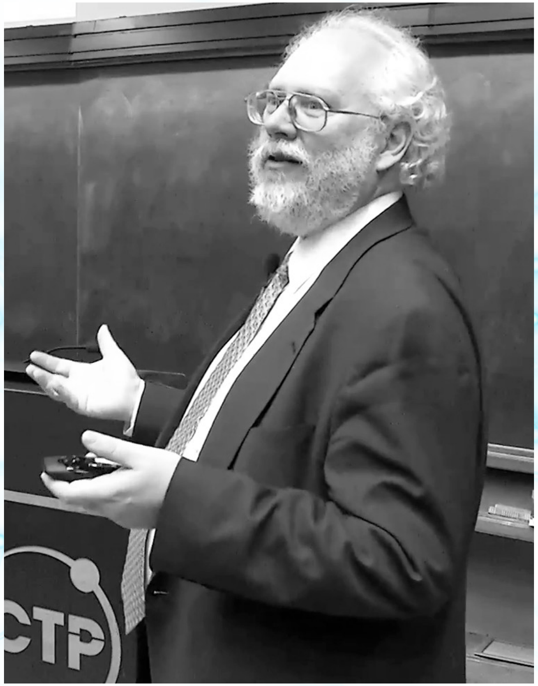


Digital signatures



The quantum threat

- **Shor's algorithm** on a large-scale quantum computer
  - Discrete logarithm will be "easy" to solve
    - ➡ ECC broken
  - Factoring will be "easy" to solve
    - ➡ RSA broken
- Shor's algorithm does not apply to symmetric cryptography
  - **Grover's algorithm** does, but doubling the key size is enough (256 bits instead of 128 bits)



Peter Shor speaking after receiving the 2017 Dirac Medal from the ICTP.
Author: International Centre for Theoretical Physics
Source: https://www.youtube.com/watch?v=J7HeDX_7Heg&t=7075

The imminent quantum threat

**“Record today,
break tomorrow.”**

Post-quantum cryptography

- Post-Quantum Cryptography (PQC) refers to asymmetric cryptography that ***cannot be broken with quantum computers***
  - Based on mathematical problems that are not affected by Shor
  - Algorithms running on **traditional computers** (≠ quantum cryptography)
- Active area of research in the cryptography community since 2000s

Lattice

Multi-variate

Hash-based

Code-based

Elliptic curve isogenies

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

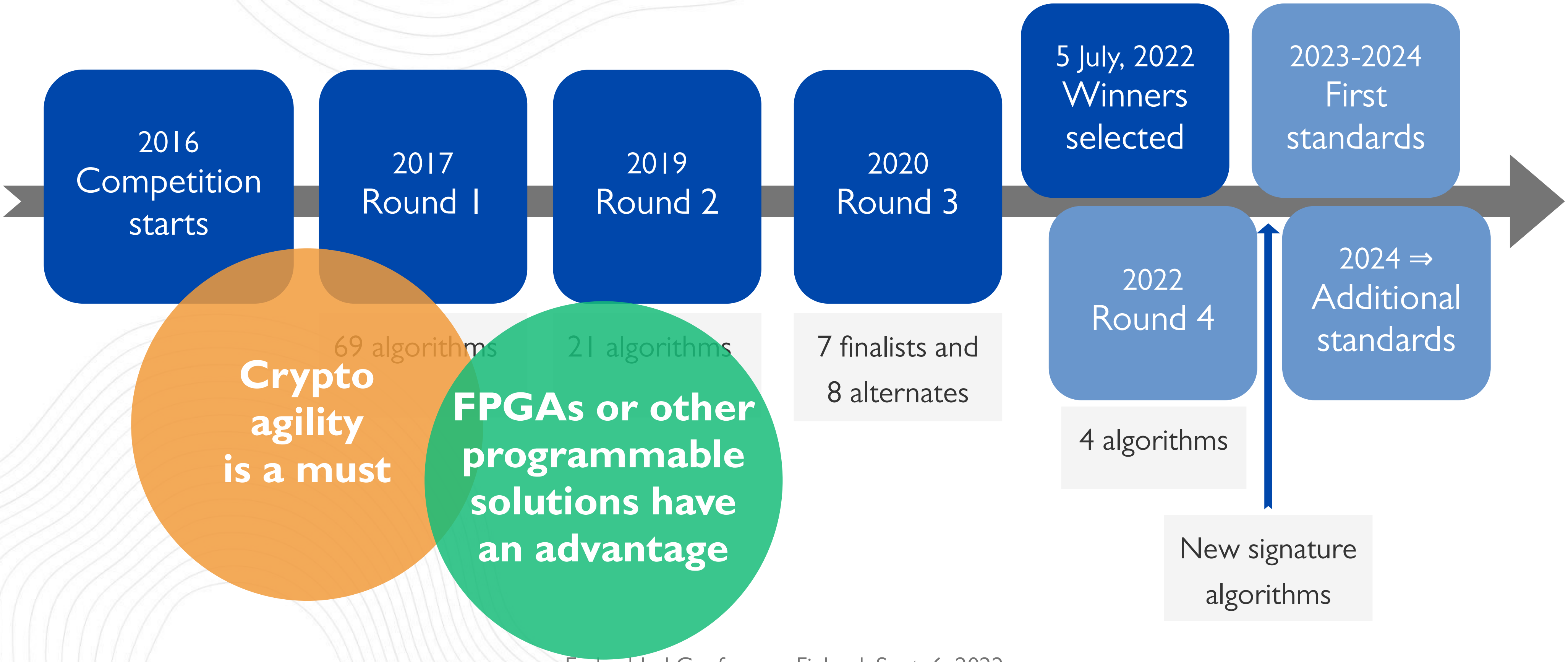
4 algorithms

2023-2024
First standards

2024 ⇒
Additional standards

New signature algorithms

NIST PQC competition



NIST selections

Round 3 Winners

KEM

CRYSTALS-Kyber (lattice)

Signature

CRYSTALS-Dilithium (lattice)

Falcon (lattice)

SPHINCS+ (hash)

Round 4 Candidates

KEM

BIKE (code)

Classic McEliece (code)

HQC (code)

~~SIKE (isogeny)~~

KEM stats

Algorithm	Status	Security	Private key (B)	Public key (B)	Ciphertext (B)
ECC (ECDH)	Pre-Quantum	~128	32	32	32
		~256	64	64	64
Kyber	Winner	~128	1632	800	768
		~256	3168	1568	1568
HQC	Round 4	~128	40	2249	4481
		~256	40	7245	14469
BIKE	Round 4	~128	2244	12323	12579
		~256	4640	40973	41229
SIKE	Round 4 (broken)	~128	374	330	346
		~256	644	564	596
Classic McEliece	Round 4	~128	6492	261120	128
		~256	13932	10449922	240

KEM stats

Algorithm	Status	Security	Private key (B)	Public key (B)	Ciphertext (B)
ECC (ECDH)	Pre-Quantum	~128	32	32	32
		~256	64	64	64
Kyber	Winner	~128	1632	800	768
		~256	3168	1568	1568
HQC	Round 4	~128	40	2249	4481
		~256	40	7245	14469
BIKE	Round 4	~128	2244	12323	12579
		~256	4640	40973	41229
SIKE	Round 4 (broken)	~128	374	330	346
		~256	644	564	596
Classic McEliece	Round 4	~128	6492	261120	128
		~256	13932	1044992	240

Significantly larger keys & ciphertexts

Larger communication and storage overhead

Latencies will stay similar or even become slightly faster

Signature stats

Algorithm	Status	Security	Private key (B)	Public key (B)	Signature (B)
ECC (ECDSA)	Pre-Quantum	~128	32	32	64
		~256	64	64	128
Dilithium	Winner	~128	2544	1312	2420
		~256	4880	2592	4595
Falcon	Winner	~128	1281	897	666
		~256	2305	1793	1280
SPHINCS$^+$ (s)	Winner	~128	64	32	7856
		~256	128	64	29792
SPHINCS$^+$ (f)	Winner	~128	64	32	17088
		~256	128	64	49856

Signature stats

Algorithm	Status	Security	Private key (B)	Public key (B)	Signature (B)
ECC (ECDSA)	Pre-Quantum	~128	32	32	64
		~256	64	64	128
Dilithium	Winner	~128	2544	1312	2420
		~256	4880	2592	4595
Falcon	Winner	~128	1281	897	666
		~256	2305	1793	1280
SPHINCS+ (s)	Winner	~128	64	32	7856
		~256	128	64	29792
SPHINCS+ (f)	Winner	~128	64	32	17088
		~256	128	64	49856

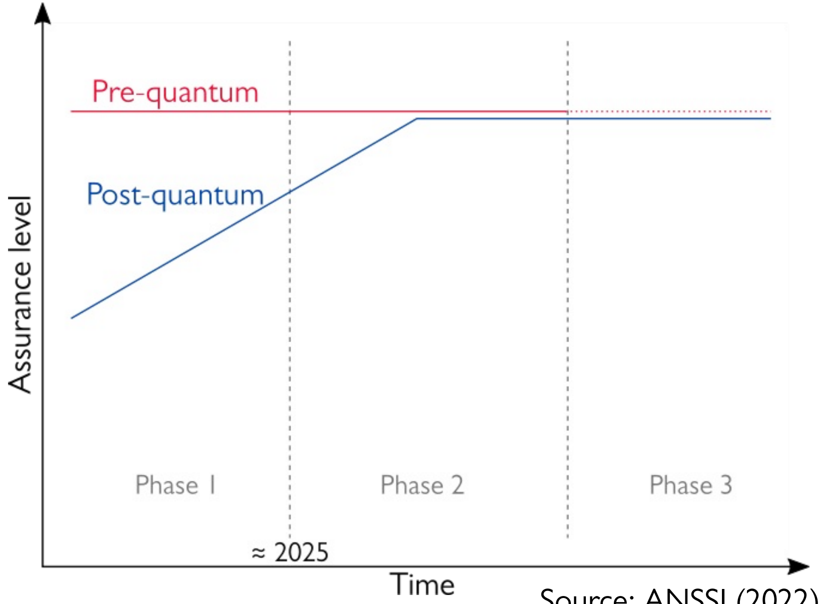
Significantly larger keys & signatures

PQC signature landscape will change when new algorithms enter Round 4

Larger communication and storage overhead

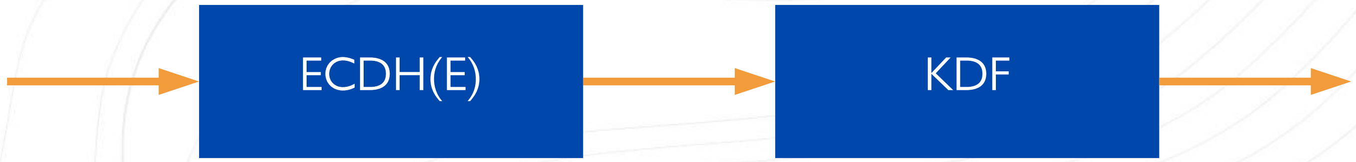
Why hybrid systems?

- We **cannot fully trust** that the new PQC schemes are secure
  - **Example:** NIST Round 3 finalist Rainbow and Round 4 candidate SIKE were broken!
- Many recommend using a **hybrid system**
  - **Combine PQC with ECC**
  - ANSSI (France) recommends it at least until 2030
- ECC will not go away for a long time!

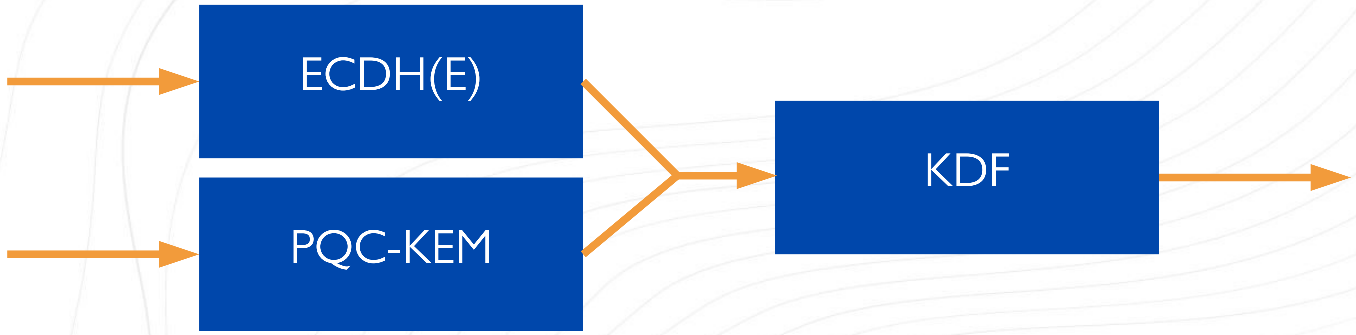


Source: ANSSI (2022)

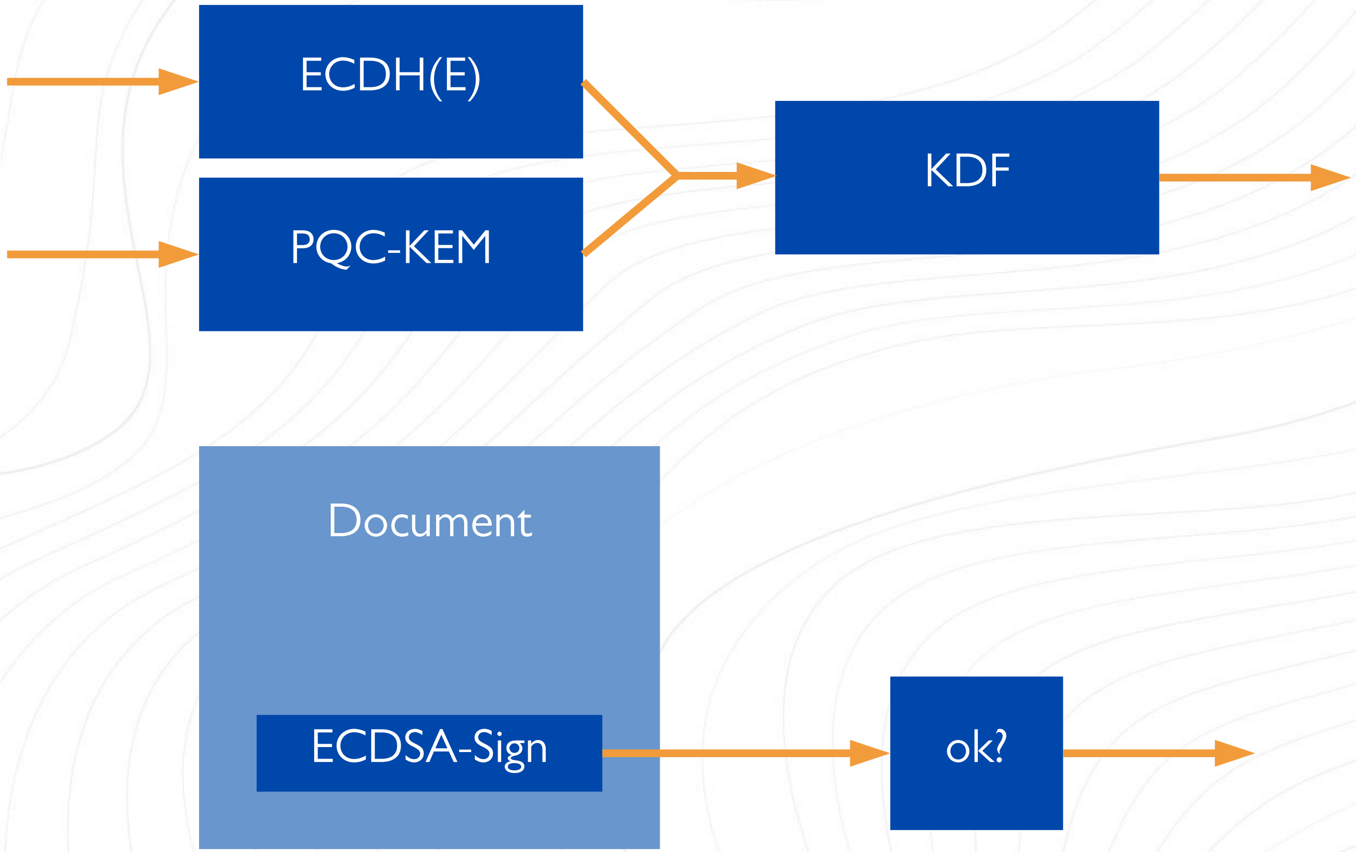
Hybrid systems: PQC + ECC



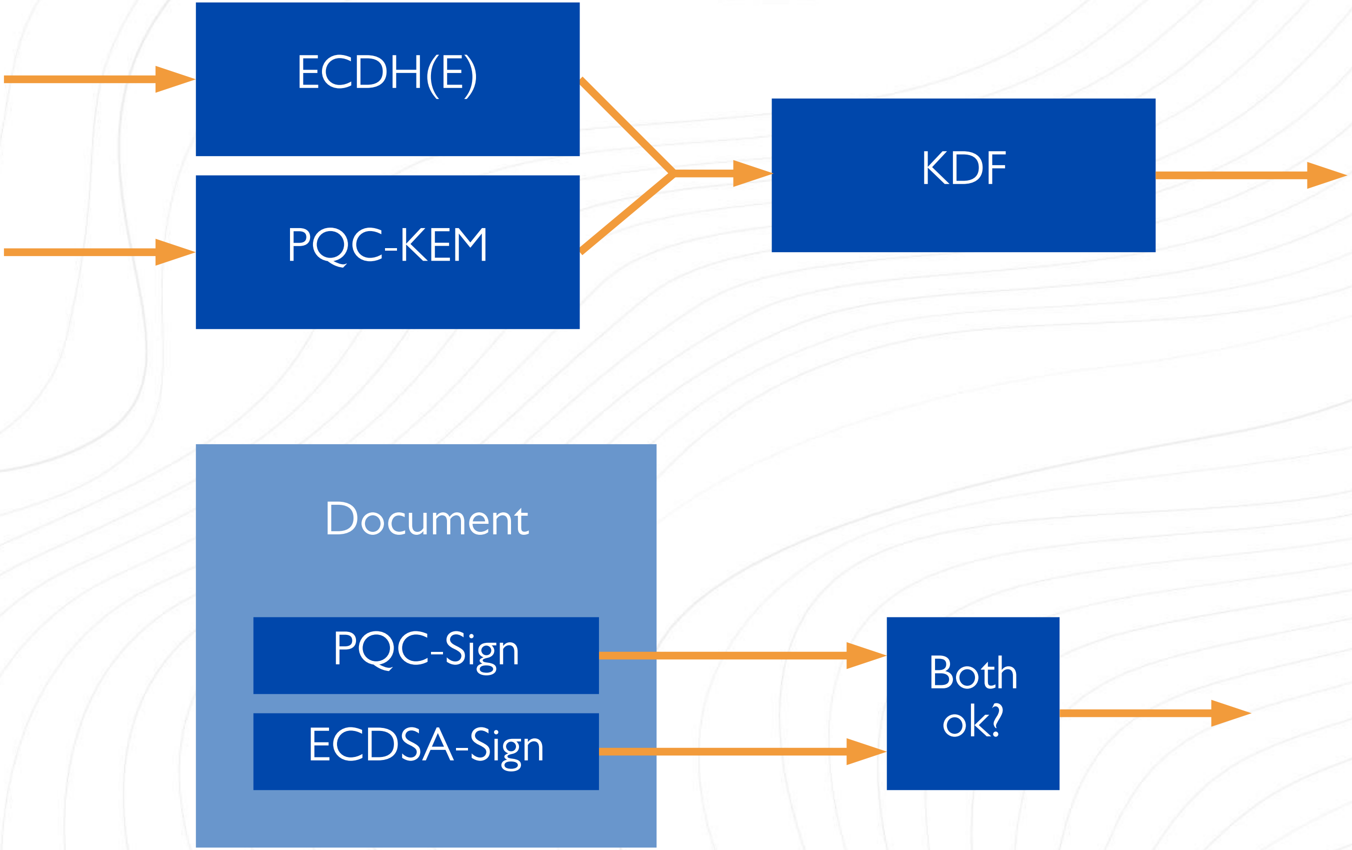
Hybrid systems: PQC + ECC



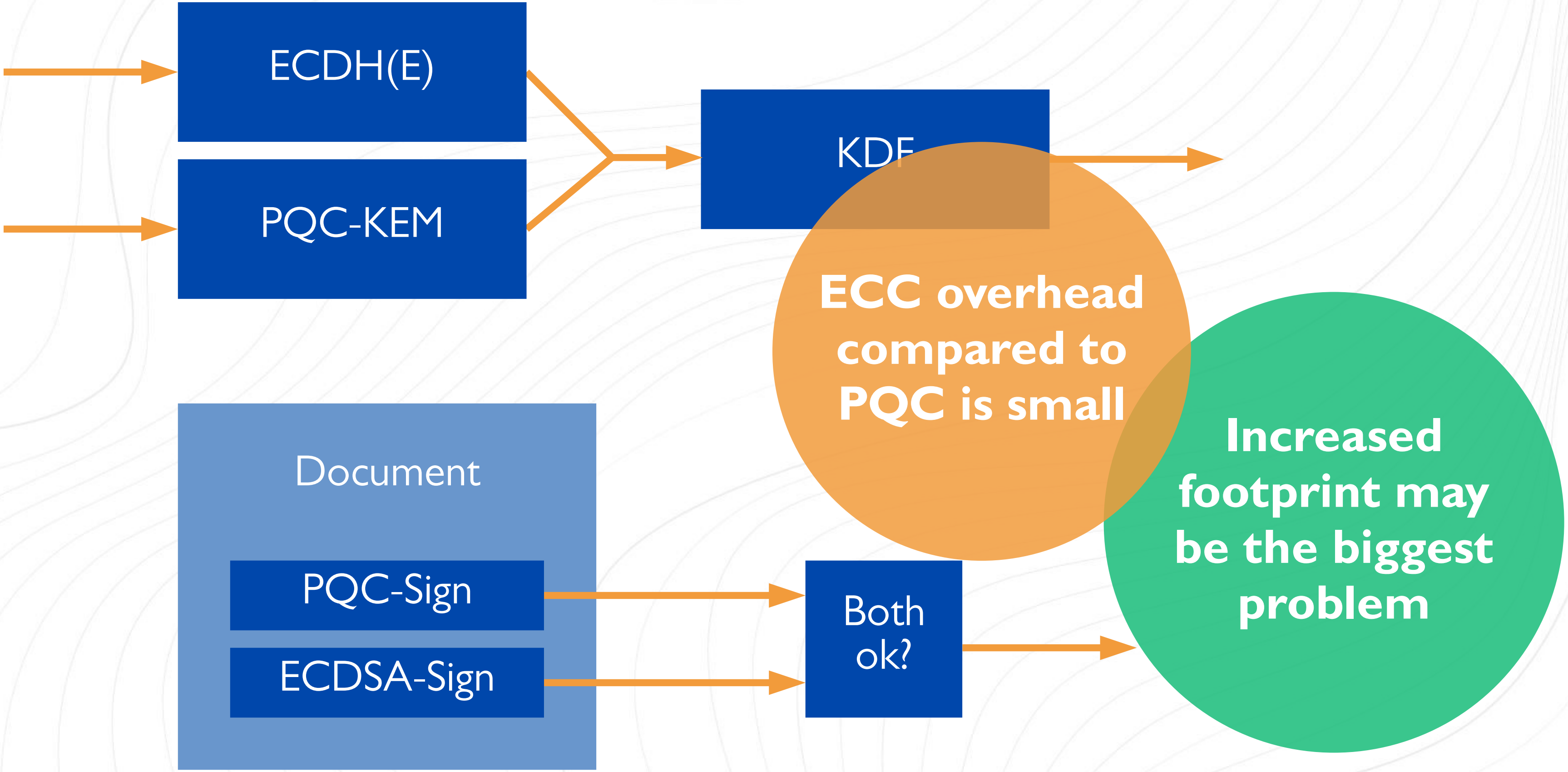
Hybrid systems: PQC + ECC



Hybrid systems: PQC + ECC



Hybrid systems: PQC + ECC



Key take-aways

Systems designed today should have the ability to support PQC in the future.

Co-existence of classical and PQC algorithms.

Reprogrammability of FPGA is an advantage.

Fixed solutions (ASIC, TPM) lack crypto agility.

2-3 years from algorithms to standards.

Quantum cryptography for niche applications.


XIPHERA
Thank you!
www.xiphera.com
info@xiphera.com
kimmo.jarvinen@xiphera.com