On the Current Status of Post-Quantum Cryptography

JCF Webinar
Peter Pessl

The quantum computer world

Quantum computers

- Use quantum mechanical effects for computation
- Universal quantum computers expected in 15-20 years
  - **2016:** 5-qubit by IBM (online accessible)
  - **2017:** 50-qubit by IBM
  - **2019:** 53-qubit by Google ("quantum supremacy")
  - **2020:** 28-qubit by IBM (better "quantum volume")
  - **2021**: 127-qubit by IBM
- Goal: increase number of **stable** quantum bits
- May lead to breakthroughs in AI, chemical simulation, optimization, cryptography and **cryptanalysis**

Funding and commercial landscape

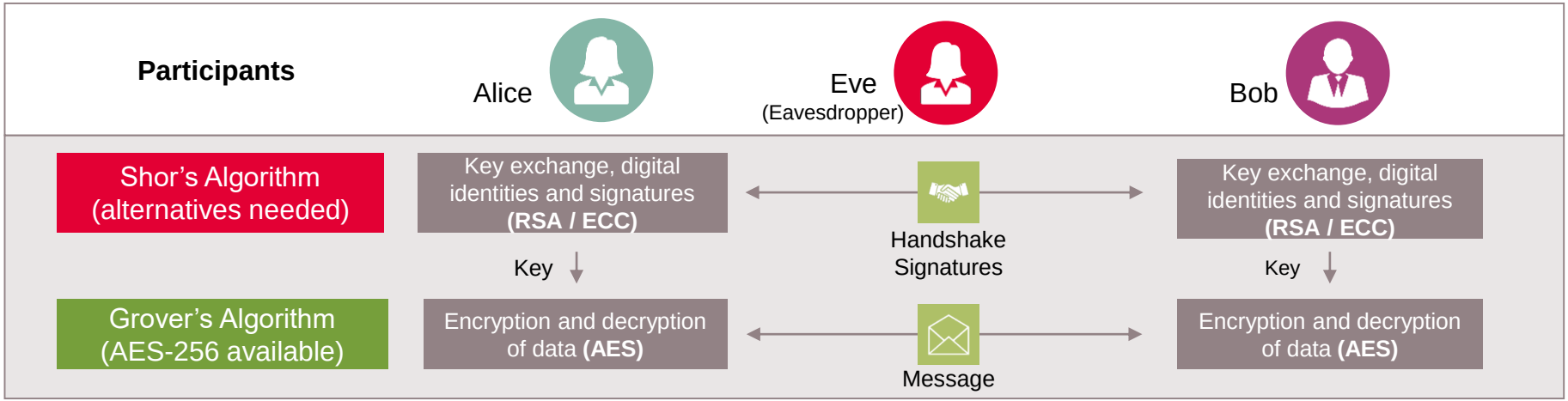
- EU: €1 billion quantum technologies flagship
- Germany: €650 million quantum initiative
- Market for QC hardware: $6.2 billion by 2025 (*)

(*) According to ResearchAndMarkets.com

The threat of quantum computers to cryptography

Cryptographic Landscape

- Public-Key Cryptography (RSA, ECC) is the basis for **key exchange, digital identities and signatures**
- Symmetric cryptography (AES) is used for bulk data encryption



The threat of quantum computers to cryptography

Quantum **cryptanalysis** on a universal quantum computer

Currently used **asymmetric** cryptosystems (RSA/ECC) are **completely broken** using **Shor's algorithm**

- Classical world (currently): ECC-256 and RSA-3072 have **128-bit** security
- Quantum world (in 15-20 years): ECC-256 and RSA-3072 have almost **no** security

Security level for **symmetric** cryptography is **halved** by **Grover's algorithm**

- Classical world (currently): AES-128 has **128-bit** security
- Quantum world (in 15-20 years): AES-128 has only **64-bit** security

Quantum world (in 15-20 years)

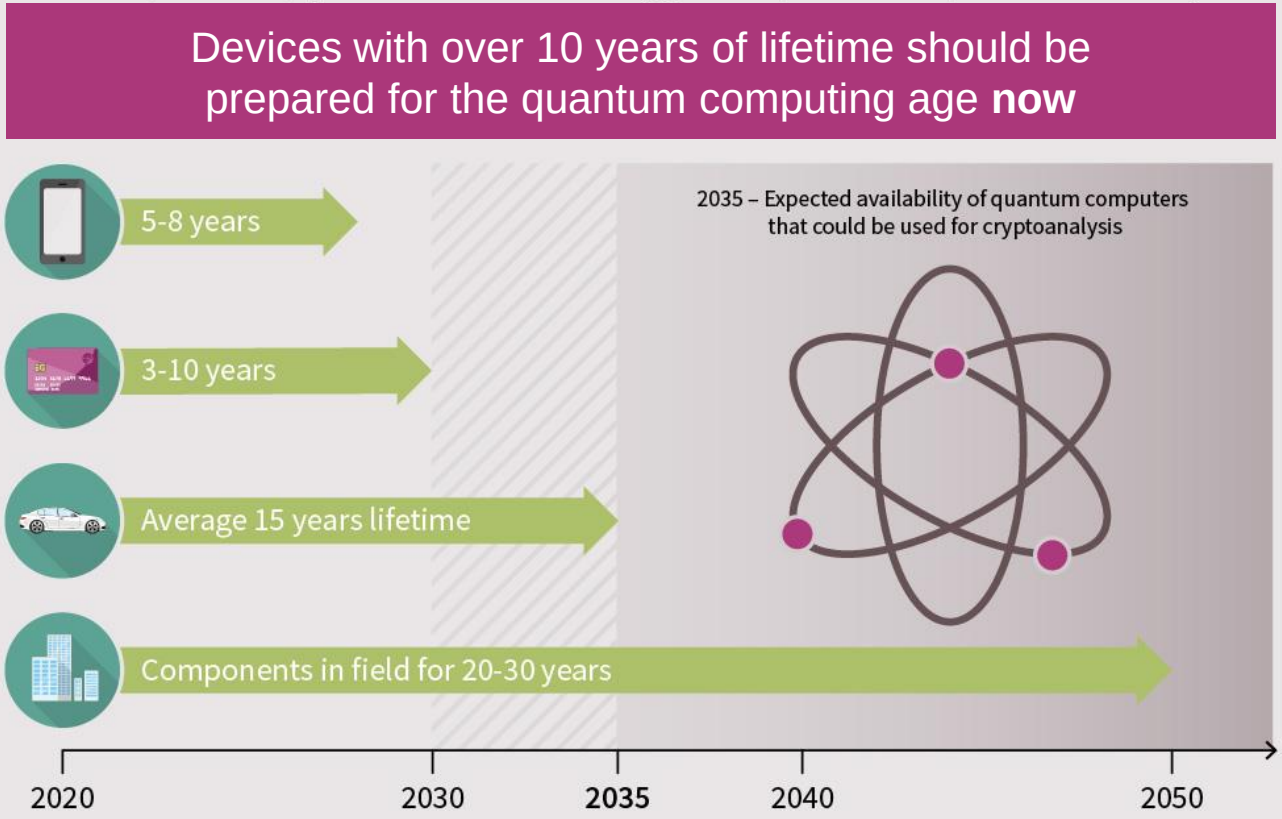
Heavily affected:
RSA, ECDSA, ECDH

Affected:
AES-128, 3DES

Currently considered safe:
AES-256, SHA256*, SHA512, SHAKE256, SHA3-512, …

* Preimage resistance

Timeline



Post-quantum cryptography and quantum cryptography

Post-quantum cryptography and quantum cryptography are not the same

Post-Quantum Cryptography

- New **conventional** cryptography deployable **without** quantum computers
- Believed to provide security against classical and quantum computer attacks
- **NSA announced** a transition to post-quantum cryptography in 2015

Quantum Cryptography

- Mainly **Quantum Key Distribution** (QKD) to secure communication using quantum mechanics
- Security relies on quantum mechanics not computational assumption
- Physical requirements like fiber-optical cable
- NSA discourages use of QKD

- As the leading provider of security solutions, Infineon is actively pursuing intensive research on **post-quantum cryptography**

Post-quantum cryptography: the options

Large landscape of alternatives

- **Families of schemes**, grouped based on common underlying hard-to-solve mathematical problem (hard even for quantum computers)
- Previous (non quantum secure) problems: Integer Factorization (RSA), Discrete Logarithm (ECC)
- Each family offers different advantages/disadvantages.

Family	Description
Hash-based	- Problem: “Inverting” a Hash-function - Well established and already standardized - Stateful schemes, number of signatures limited
Lattice-based	- Problem: Solving approximate linear equations - good performance and reasonable sizes - ongoing debates about security
..and others	Isogeny-based, Code-based, Multivariate-Quadratic-based, Symmetric-ZKP-based, …

Features of hash-based signatures (HBS)

HBS high-level overview

Key Generation

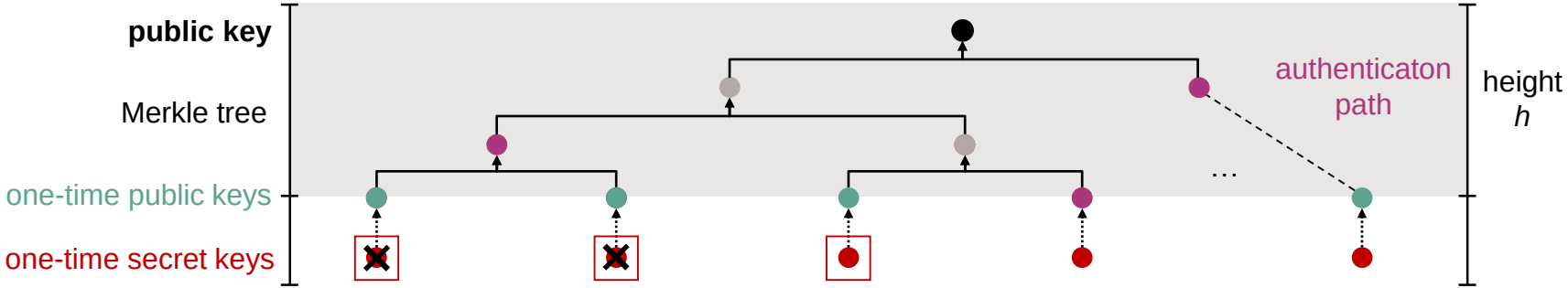
- Generate a set number of hash-based **one-time key pairs**: each one must only be used once!
- Combine them in a binary tree (hash two children to receive parent) to receive **public key**

Signing

- Sign the message using first unused one-time key pair
- Compute the authentication path: allows to recompute the tree up to the public key
- Signature is composed of the message signature and the authentication path

Verification

- Verify message signature, recompute public key using authentication path



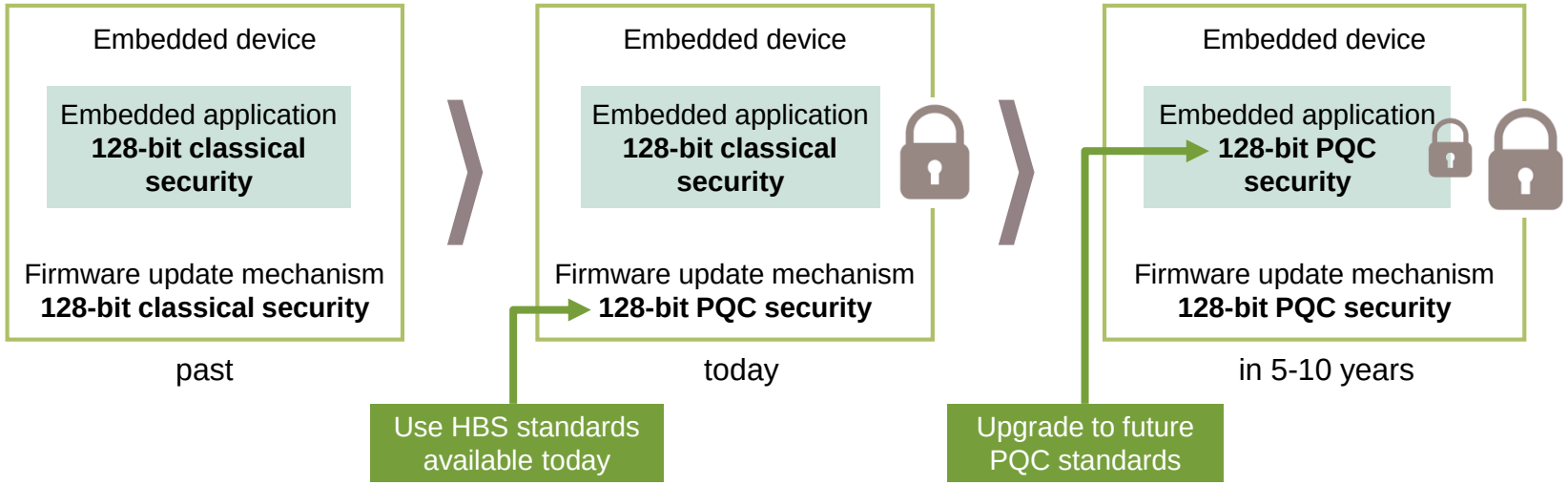
HBS applications

Caveats

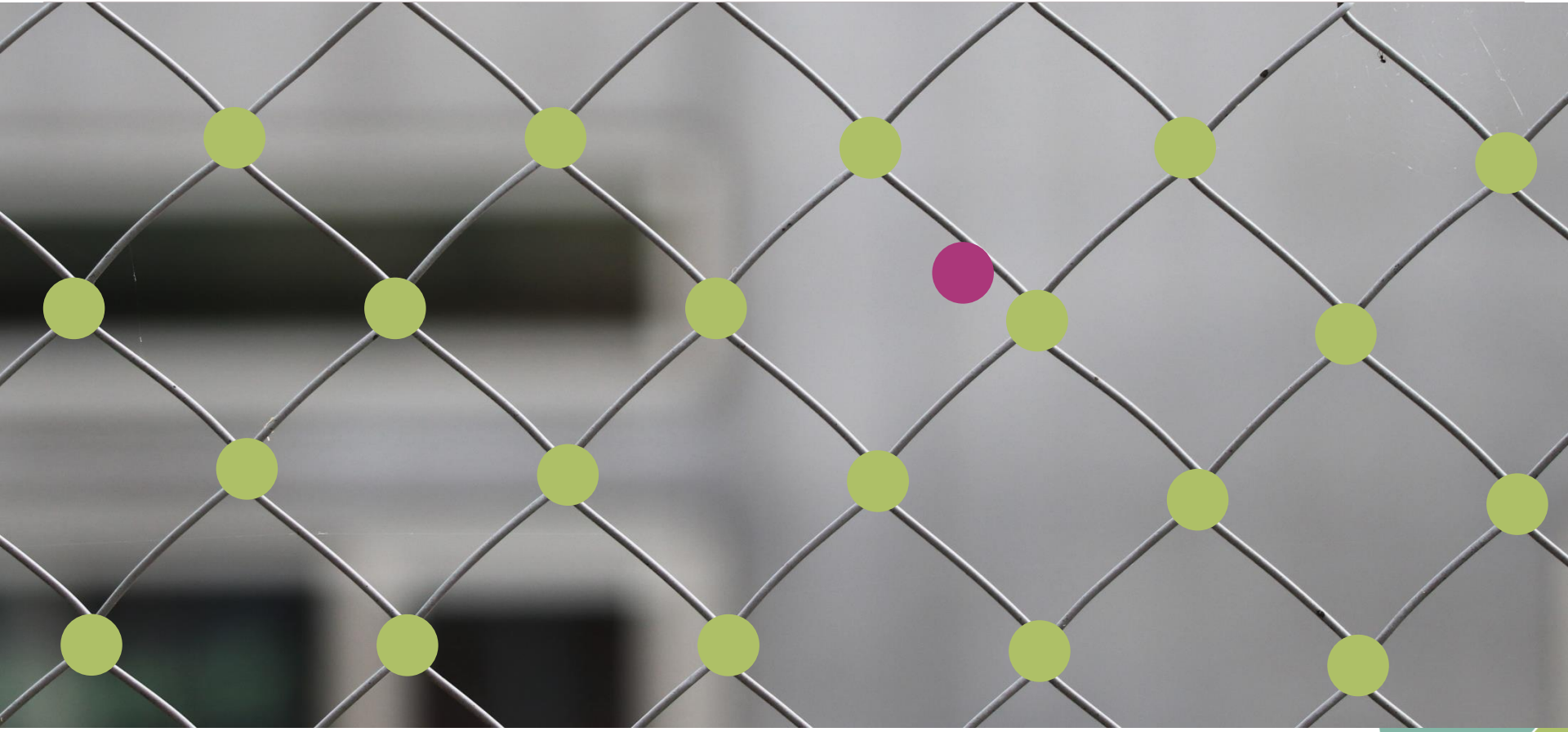
› The number of possible signatures is fixed and needs to be chosen for key generation.
› State (counter) needs to be maintained (beware of backups, multiple signing parties, fault attacks, …)

Suitable applications:

› Single signer, predictable number of signatures, security needed now: Firmware Updates



Lattice-based cryptography



A related problem: Learning with Errors (LWE)

Solving a system of linear equations ($\mathbb{Z}_{13}$ = integers mod 13)

public				secret		public
$\mathbb{Z}_{13}^{7\times4}$				$\mathbb{Z}_{13}^{4\times1}$		$\mathbb{Z}_{13}^{7\times1}$
4	1	11	10	**6**	=	4
5	5	9	1			8
3	9	0	10			1
1	3	3	2	**11**		10
12	7	3	4			4
6	5	11	4			12
3	3	5	0			9

Use Gaussian elimination

Green is given; Find (learn) **red**

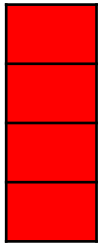
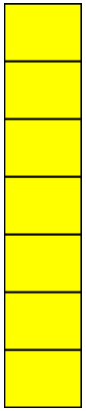
A related problem: Learning with Errors (LWE)

Solving of a system of linear equations *with (small) noise*

public **secret** **secret** **public**

$\mathbb{Z}_{13}^{7\times4}$ $\mathbb{Z}_{13}^{4\times1}$ $\mathbb{Z}_{13}^{7\times1}$

4	1	11	10
5	5	9	1
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

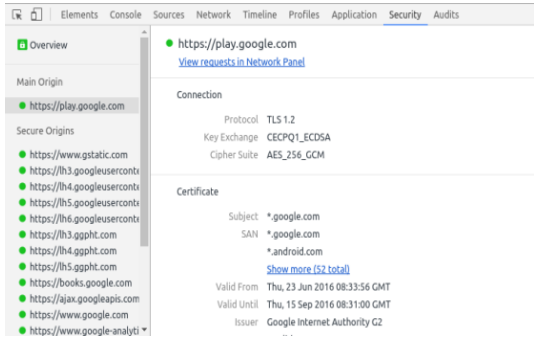
$\times$  $+$  $=$

5
8
0
11
4
11
7

Green is given; Find (learn) **red**

Lattice-based cryptography

- LBC has proven to be highly flexible:
  key exchange, signatures, fully homomorphic encryption
- Efficient, with a reasonable footprint:
  Most suitable class for embedded devices
- First large-scale experiments in TLS:
  CECPQ1/ CECPQ2(b) by Google and Cloudflare



The NIST process

Round 1
(69 schemes)
Start: Dec 2017

Round 2
(26 schemes)
Start: Jan 2019

Round 3
(15 schemes)
Start: Jul 2020

Draft standards:
2022-24

The National Institute of Standards and Technology (NIST) has started a standardization effort:

- Competition-like process
- Researchers can submit key exchange, PKE, signature schemes
- Selection metrics: “security”, “cost”, “algorithm and implementation characteristics”
- Ongoing evaluation and discussion by experts (academia, industry, standardization bodies)
- Public mailing list/forum: https://groups.google.com/a/list.nist.gov/g/pqc-forum

Nov 2017	Deadline for submissions and start of Round 1
Jan 2019	Round 2 candidates announced
Jul 2020	Start of Round 3 with finalists (and alternate schemes)
End of 2021	Announcement of first algorithms to be standardized (planned)
2022-2024	Draft standards available

The NIST process is a global effort
https://csrc.nist.gov/projects/post-quantum-cryptography

Current status of PQC standardization

	Lattice-Based	Code-Based	MQ-Based	Symmetric/ Hash	Isogenies
NIST PQC process Public-Key Encryption/ KEMs	**KYBER** **SABER** **NTRU** *FrodoKEM* *NTRU Prime* } plan to pick only one	**Classic McEliece** *BIKE* *HQC*			*SIKE*
NIST PQC process Signature Schemes	**DILITHIUM** **FALCON** } plan to pick only one		**Rainbow** *GeMSS*	*Picnic* *SPHINCS+*	
NIST hash-based signature “fast track” Stateful Signature Schemes			NIST Special Publication 800-208	XMSS LMS	(Stateful Hash)

› **bold**: : Finalists. Most promising to fit the majority of use cases and most likely to be ready for standardization soon.
› *italic*: Alternates. Potential candidates for future standardization, but more analysis needed.

› First picks this year, but process will keep on going (4th round for alternates, new call for proposals for signature schemes)

NIST PQC process: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions
NIST hash-based signature “fast track”: https://csrc.nist.gov/Projects/stateful-hash-based-signatures
The Homestretch: the beginning of the end of the NIST PQC 3rd Round: https://pqcrypto2021.kr/download/program/2.2_PQCrypto2021.pdf

Challenge: Implementing PQC on constrained platforms

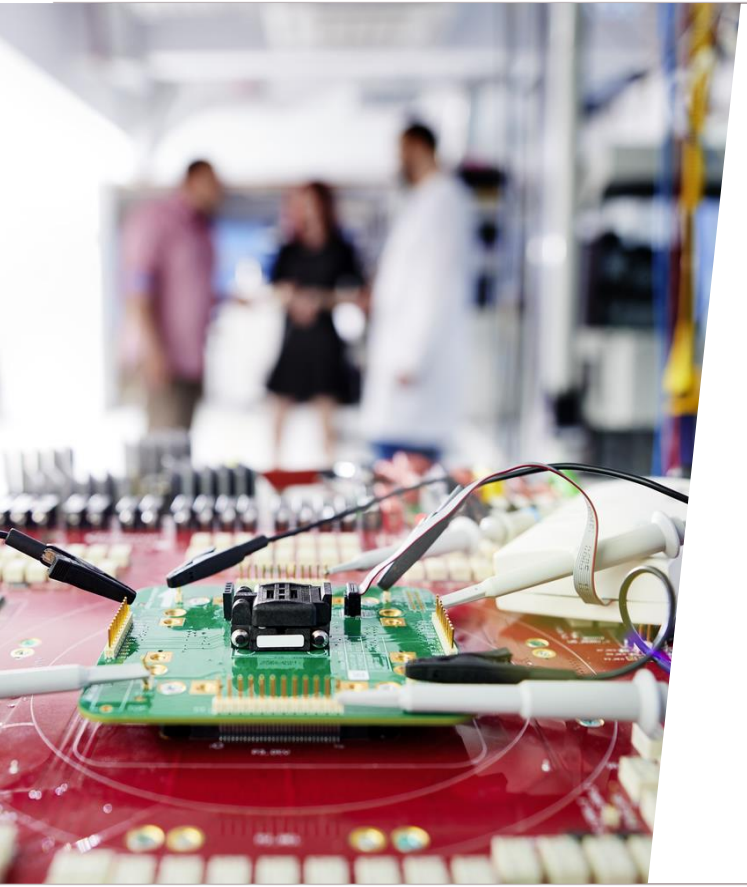
- Positive: runtime for lattice-based schemes is very good, some ms (pure software, no side-channel protection)
- Negative: high memory requirements (public keys, ciphertexts, NVM, RAM)

Scheme	|pk|	|ctxt|	Gen	Enc	Dec
Kyber768	1184	1088	744,136	898,630	838,939
Saber	992	1088	645,222	820,799	774,055
ntruhrss701	1138	1138	149,737,679	375,948	867,921
SIKEp503	378	402	67,365,114	110,843,233	117,990,911
Curve25519 (ECC)	64	64	894,391		

pqm4: https://github.com/mupq/pqm4

Fuji, Aranha: Curve25519 for the Cortex-M4 and Beyond

Challenge: Implementation security



- Cards operate in a potentially adverse environment, need to secure against implementation attacks (fault attacks, side-channel attacks)
- PQC schemes come with novel challenges
  - new attack paths
  - new countermeasures needed
- Highly active research area (academia and industry)
- Goal: efficient and holistic protection approach, with anticipation of future attacks

Challenge: Integration into applications

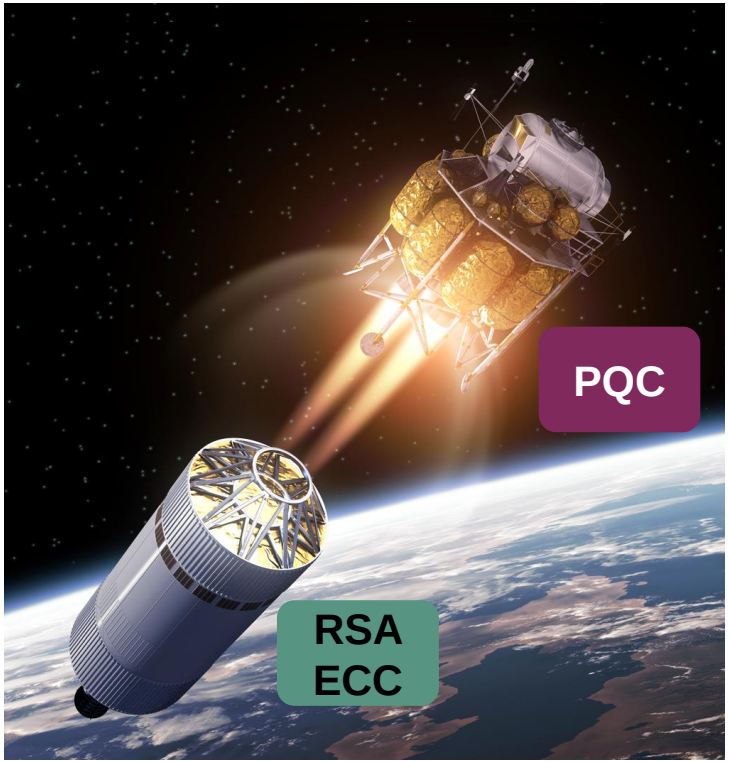
We need to build applications on top of cryptographic schemes!

- PQC schemes are not always drop-in replacements:
  - Some protocols require schemes with a Diffie-Hellman property
  - Currently no direct DH analogue in the NIST process
  - Adaptation is likely needed
- Shifting costs: PQ signatures are more expensive than KEMs (runtime, size)
  - Replacement of signatures with KEMs?
  - Possible for, e.g., online authentication, but needs protocol adaptation
  - Demonstrated in Cloudflare's KEMTLS experiment
- Standardization of new or adapted protocols/applications needed

KEMTLS experiment: https://blog.cloudflare.com/kemtls-post-quantum-tls-without-signatures/

Challenge: Migration

- RSA and ECC are used almost everywhere (big investment)
- Replacements are not fully usable in production yet (standardization etc.)
- Important: keep PQC in mind!
- **Crypto Agility:**
  anticipate updates of cryptography and provide update mechanism, consider effects of PQC (key sizes…)



Conclusion and call to action

- Post-quantum cryptography is needed to secure a quantum computer world
- First standards are ready (HBS) or will appear soon
- Prepare to transition to a quantum-safe cryptography
- Provide applications with crypto agility and upgrade to standardized PQC algorithms in the near future

Part of your life. Part of tomorrow.