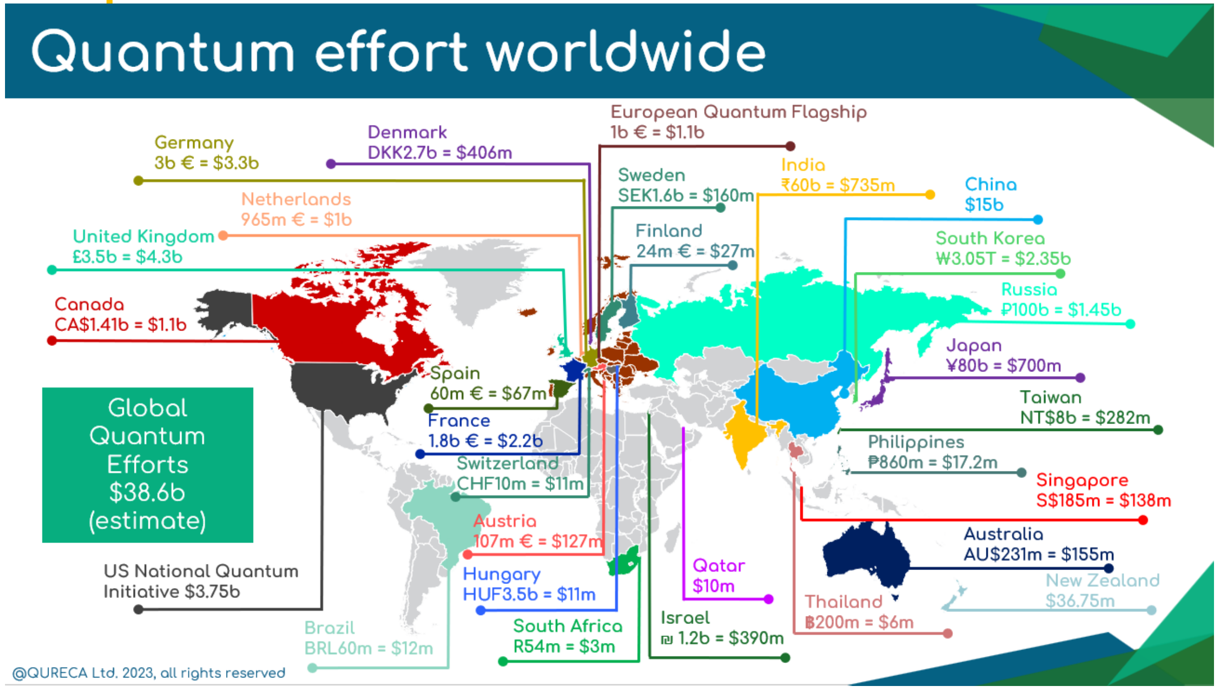
Post-Quantum Cryptography @ DG CONNECT

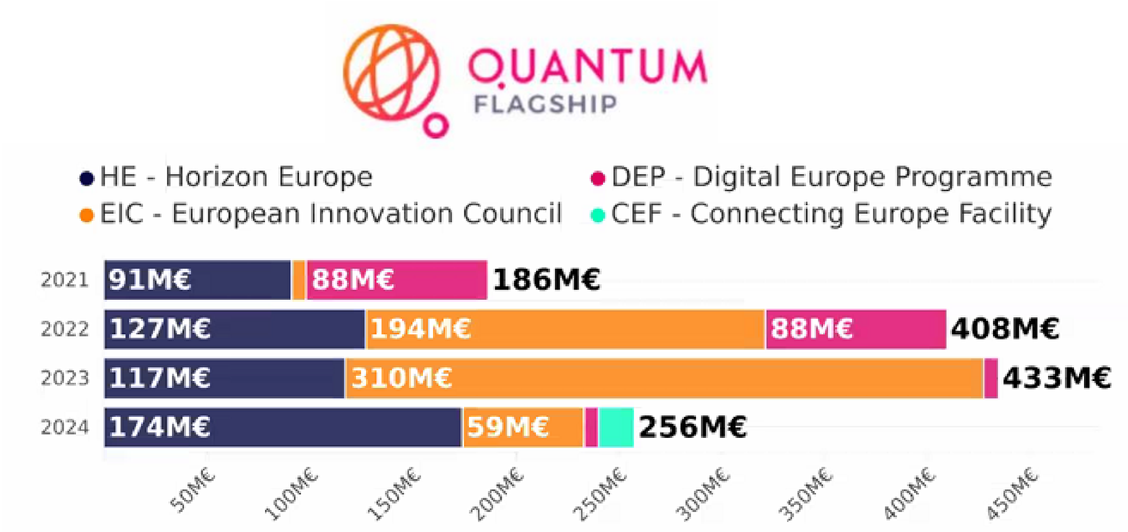
Fabiana Da Pieve

Unit Emerging and Disruptive Technologies
Directorate General for Communications Networks, Content, and Technology (DG CONNECT)
European Commission

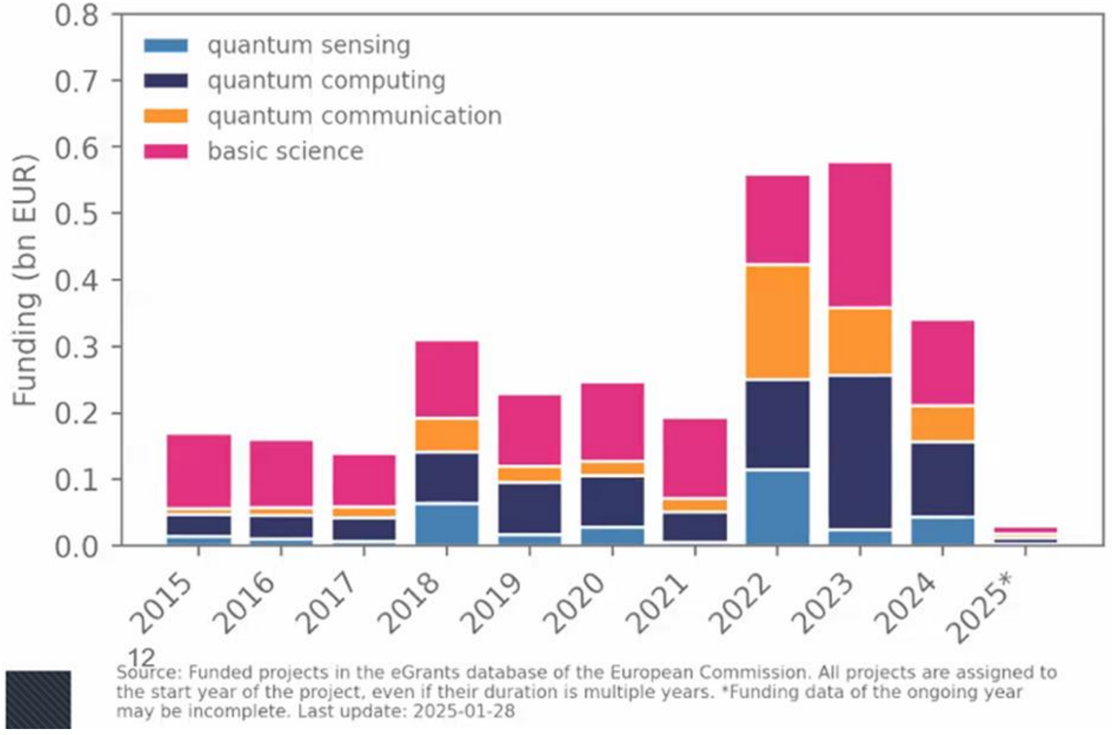
Worldwide efforts in quantum computing and the EC Quantum flasghip



[Overview of Quantum Initiatives Worldwide 2023 - Qureca]



The EU approach to quantum technologies



Source: Funded projects in the eGrants database of the European Commission. All projects are assigned to the start year of the project, even if their duration is multiple years. *Funding data of the ongoing year may be incomplete. Last update: 2025-01-28

Developments of quantum computing platforms are moving fast

Google Quantum AI – Dec 2024

“Willow can reduce errors exponentially as we scale up using more qubits. This cracks a key challenge in quantum error correction that the field has pursued for almost 30 years.”

currently the only chip which is both "break even" (= error correction removes errors instead of adding them) and "below threshold" (= adding more qubits results in lower error rates)

IBM - Q1 2025: The impact of quantum low-density parity-check (Q-LDPC) codes on error correction and thermal management challenges

Amazon Web Services (AWS) – Q1 2025: Transmon qubit lifetimes and the challenges of scaling hybrid architectures

Microsoft – Q1 2025: The road to topological qubits - fidelity and error correction

Post-Quantum Cryptography (PQC) as answer to quantum threats

- based on problems hard to solve even for quantum computers
- can be deployed on existing infrastructure in several cases but **implies a fundamental shift in algorithms, protocols → key sizes, signature size, … often lack of compatibility with current protocols. Management of identities particularly challenging.**
- **High on the agenda of many countries:**
  - ○ **US Cybersecurity and Infrastructure Security Agency (CISA) PQC Initiative** [1]
  - ○ **Guidelines by US National Security Agency & National Institute Standards and Technology (NIST)** [2] , Transition to Post-Quantum Cryptography Standards [3]
  - ○ **EU Recommendation on a Coordinated Roadmap**[4], reports by **ANSSI, BSI, ENISA** [5]

[1] Post-Quantum Cryptography Initiative | CISA

[2] Migrating to Post-Quantum Cryptography (whitehouse.gov)

[3] NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards

[4] Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography | Shaping Europe's digital future (europa.eu)

[5] anssi-avis-migration-vers-la-cryptographie-post-quantique.pdf; Migration zu Post-Quanten-Kryptografie - Handlungsempfehlungen des BSI (bund.de); Post-Quantum Cryptography - Integration study — ENISA (europa.eu)

There are, in fact, (at least) two transitions

Confidentiality (& could authenticate):
KEY ENCAPSULATION MECHANISMs (KEMs)
Urgent !

- ML-KEM (FIPS 203) – despite some occasional difficulty with its larger key sizes, in several cases it allows for a drop-in upgrade – at least for Post-Quantum Internet
- Sectors with constrained devices: problems

> **Cloudflare:** Urgent and the easier of the two transitions to deploy. We're on track for ~30% client-side deployment in 2024. That took **5 years**.

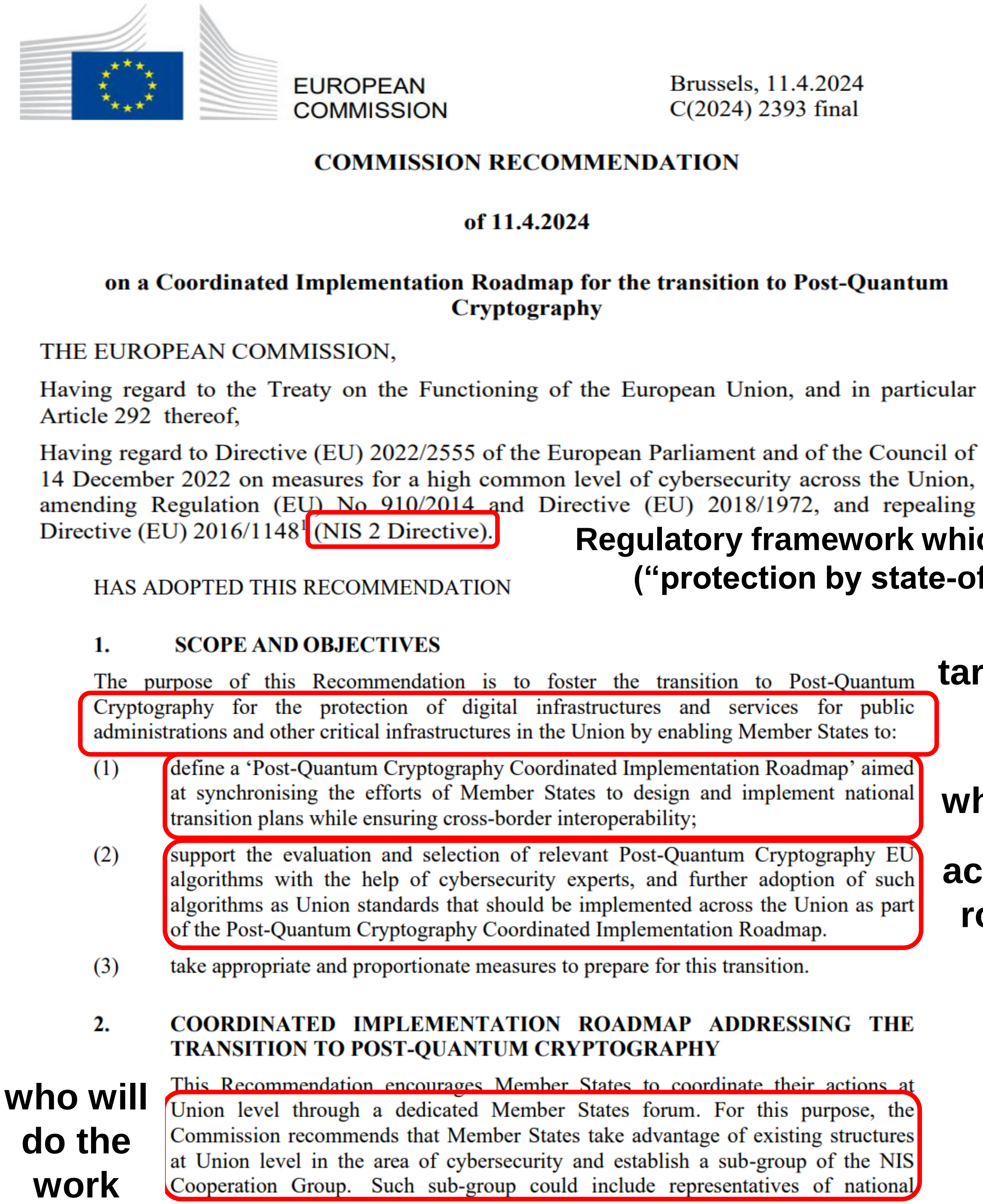
Authentication, integrity and non-repudiation:
SIGNATURES & CERTIFICATES
less urgent but more complex !

- to attack authentication, you need to perform the attack in real time; doing attack later not effective
- it may seem less urgent … but the use of digital signatures is more complex than key agreement
- none of the current PQC signatures scheme is ideal

> For certain applications, better to balance signing and verification time, while for others it is worth to have better verification time at the cost of slower signing

- Also, in general, remember about **devices with long service lifetimes**, not urgent but difficult to upgrade once deployed: *satellites in orbit, sensors in cars, airplanes, cell phone towers, smart water and electricity meters in people's homes, chips in a 10-year ePassport, …*

- Also, other transitions: more advanced cryptographic schemes (anonymous credentials, attribute-based encryption, …)



EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148[1] (NIS 2 Directive).

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

(1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;

(2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national

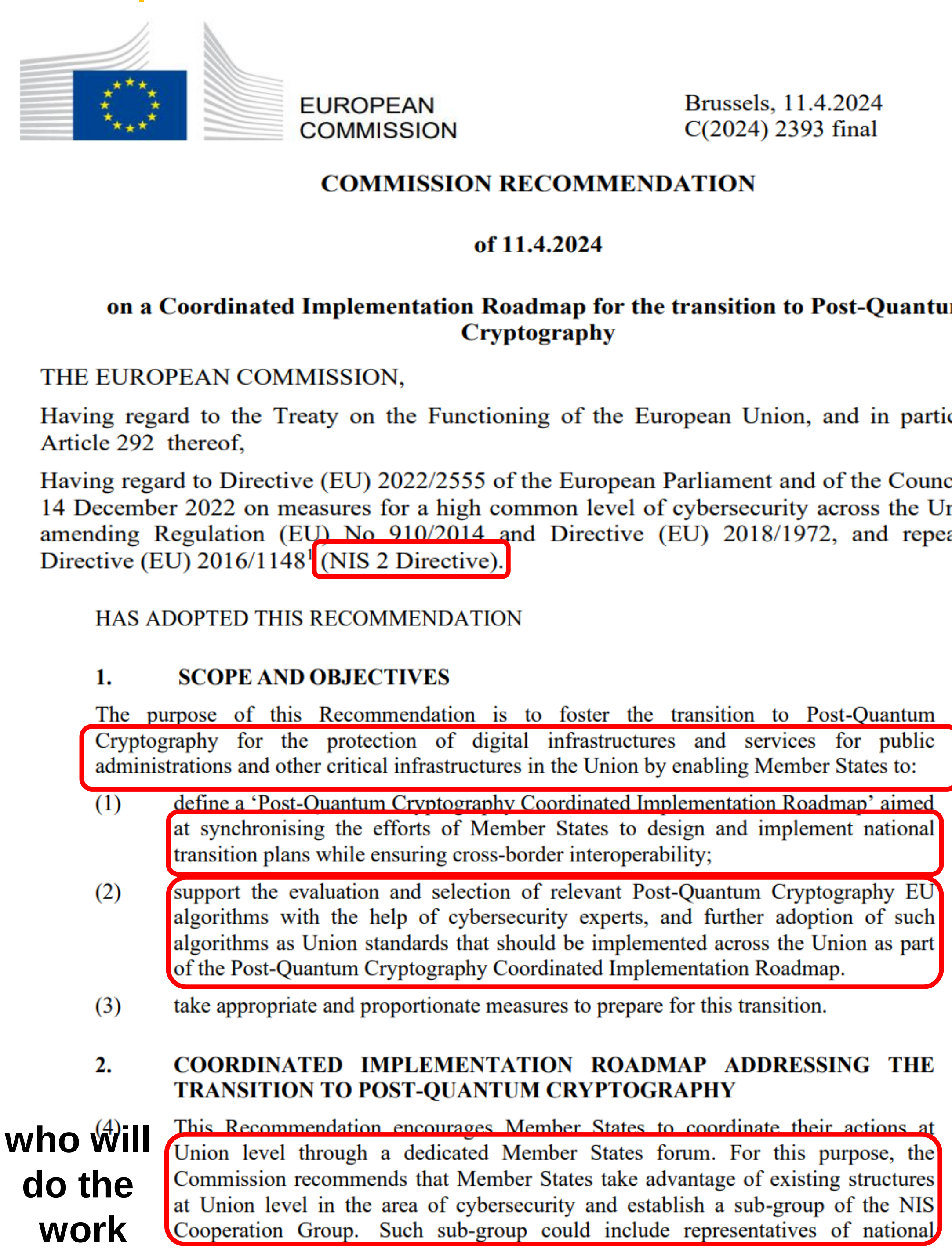
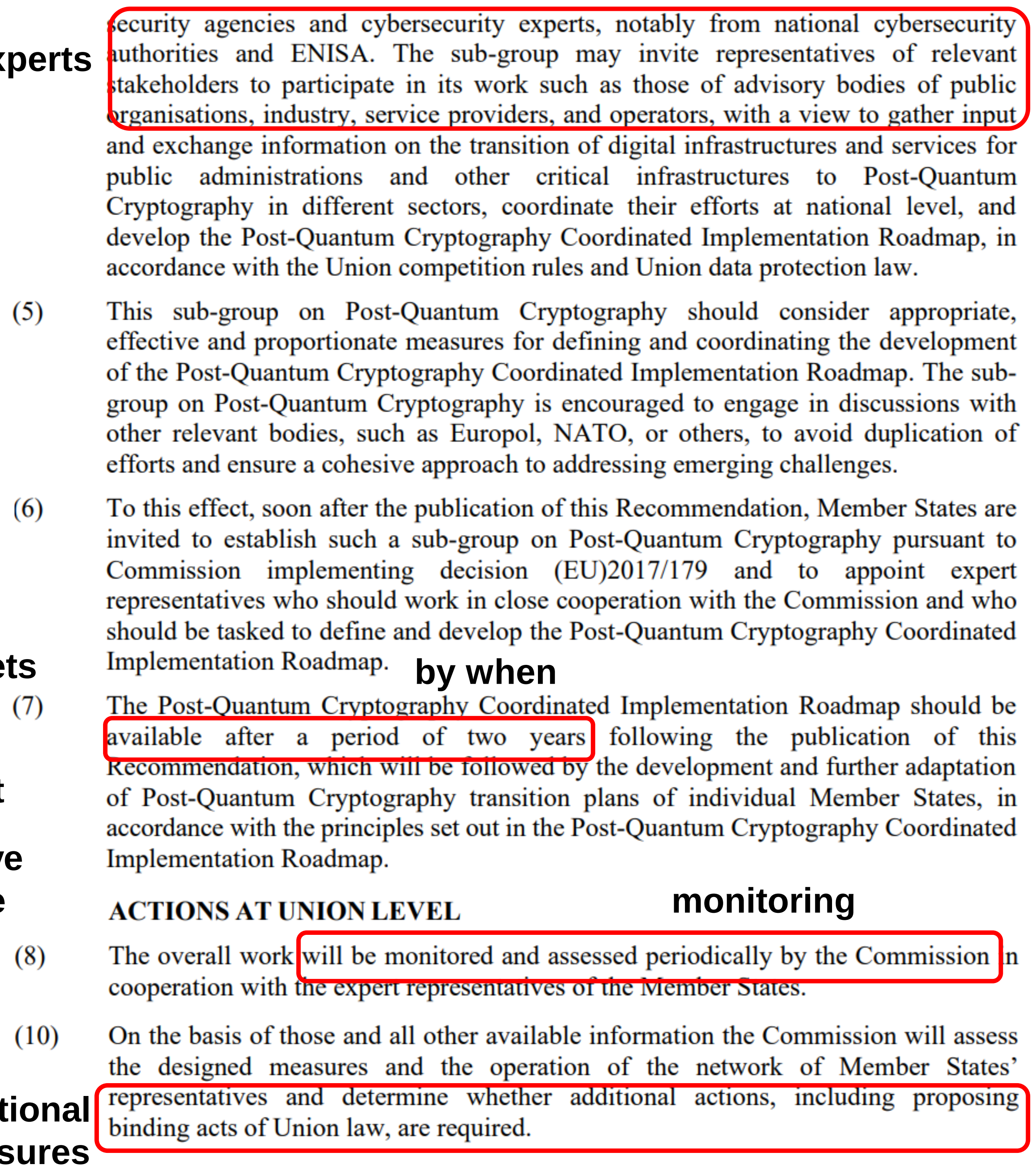
Regulatory framework which touches cybersecurity
("protection by state-of-the-art technology")

targets

what

active role

who will do the work

EUROPEAN COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Having regard to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148[1] (NIS 2 Directive).

HAS ADOPTED THIS RECOMMENDATION

1. SCOPE AND OBJECTIVES

The purpose of this Recommendation is to foster the transition to Post-Quantum Cryptography for the protection of digital infrastructures and services for public administrations and other critical infrastructures in the Union by enabling Member States to:

(1) define a 'Post-Quantum Cryptography Coordinated Implementation Roadmap' aimed at synchronising the efforts of Member States to design and implement national transition plans while ensuring cross-border interoperability;

(2) support the evaluation and selection of relevant Post-Quantum Cryptography EU algorithms with the help of cybersecurity experts, and further adoption of such algorithms as Union standards that should be implemented across the Union as part of the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(3) take appropriate and proportionate measures to prepare for this transition.

2. COORDINATED IMPLEMENTATION ROADMAP ADDRESSING THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY

(4) This Recommendation encourages Member States to coordinate their actions at Union level through a dedicated Member States forum. For this purpose, the Commission recommends that Member States take advantage of existing structures at Union level in the area of cybersecurity and establish a sub-group of the NIS Cooperation Group. Such sub-group could include representatives of national security agencies and cybersecurity experts, notably from national cybersecurity authorities and ENISA. The sub-group may invite representatives of relevant stakeholders to participate in its work such as those of advisory bodies of public organisations, industry, service providers, and operators, with a view to gather input and exchange information on the transition of digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography in different sectors, coordinate their efforts at national level, and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap, in accordance with the Union competition rules and Union data protection law.

(5) This sub-group on Post-Quantum Cryptography should consider appropriate, effective and proportionate measures for defining and coordinating the development of the Post-Quantum Cryptography Coordinated Implementation Roadmap. The sub-group on Post-Quantum Cryptography is encouraged to engage in discussions with other relevant bodies, such as Europol, NATO, or others, to avoid duplication of efforts and ensure a cohesive approach to addressing emerging challenges.

(6) To this effect, soon after the publication of this Recommendation, Member States are invited to establish such a sub-group on Post-Quantum Cryptography pursuant to Commission implementing decision (EU)2017/179 and to appoint expert representatives who should work in close cooperation with the Commission and who should be tasked to define and develop the Post-Quantum Cryptography Coordinated Implementation Roadmap.

(7) The Post-Quantum Cryptography Coordinated Implementation Roadmap should be available after a period of two years following the publication of this Recommendation, which will be followed by the development and further adaptation of Post-Quantum Cryptography transition plans of individual Member States, in accordance with the principles set out in the Post-Quantum Cryptography Coordinated Implementation Roadmap.

ACTIONS AT UNION LEVEL

(8) The overall work will be monitored and assessed periodically by the Commission in cooperation with the expert representatives of the Member States.

(10) On the basis of those and all other available information the Commission will assess the designed measures and the operation of the network of Member States' representatives and determine whether additional actions, including proposing binding acts of Union law, are required.

experts

targets

what

active role

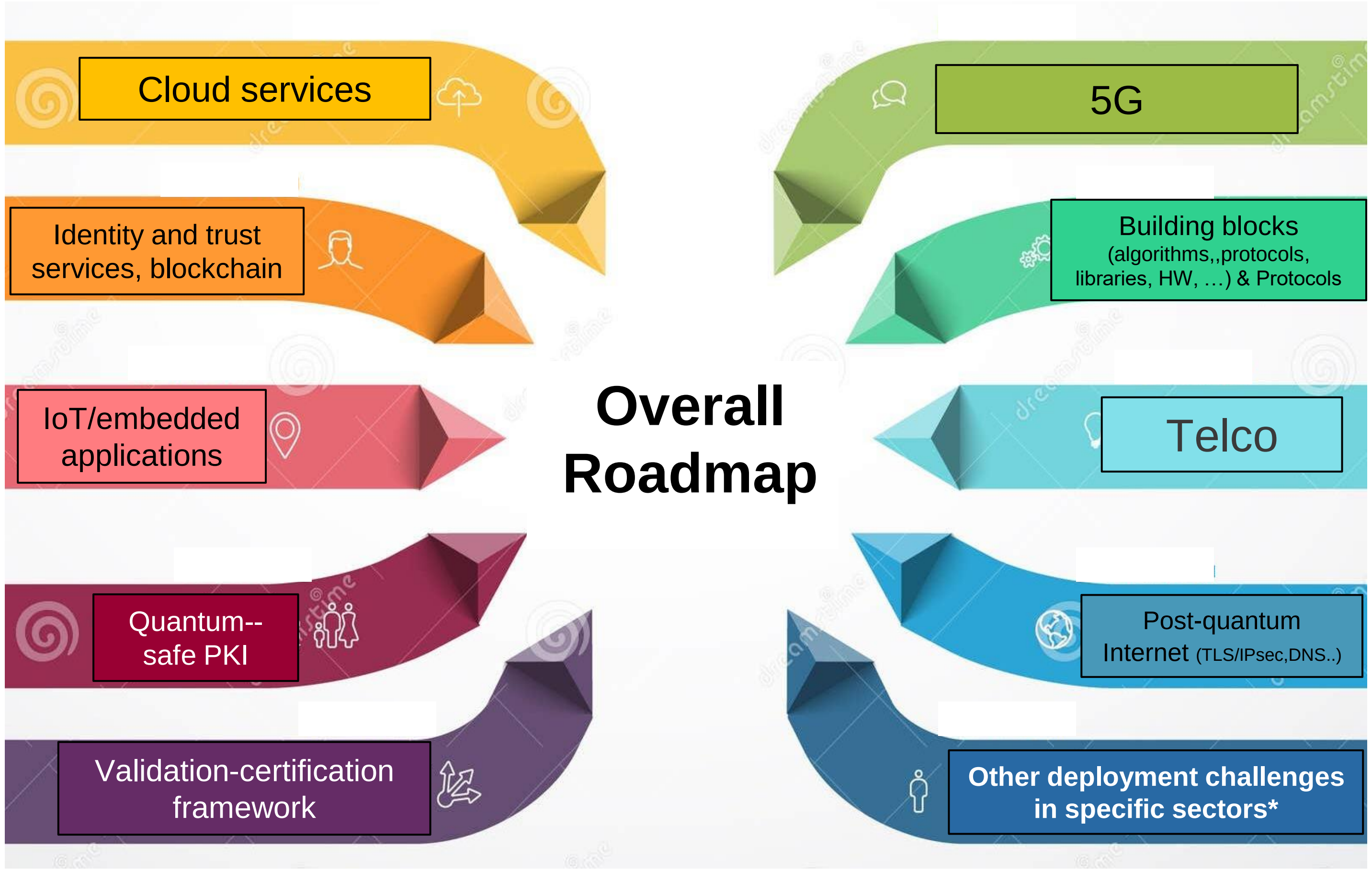
who will do the work

by when

monitoring

additional measures

Ongoing, past, just started EU-projects



Overall Roadmap

PQCRYPTO

Cloud services

QUBIP, PQC4eMRTD, PQ-REACT, PROMETHEUS, PRIViLEDGE

Identity and trust services, blockchain

QUBIP, PQCRYPTO

IoT/embedded applications

PQC4eMRTD, PiQASO, HAPKIDO (NL, national)

Quantum--safe PKI

WORK IN ECCG CHAIRED BY ENISA

Validation-certification framework

5G

Projects for both 6G we have CONFIDENTIAL6G

Building blocks (algorithms,,protocols, libraries, HW, …) & Protocols

QUBIP, ERC EPOQUE (integ. in procotols), ERC ARTICULATE (libraries), SAFECrypto, PiQASO (HW), ERC ISOCRYPT (non-lattice based)

Telco

QUBIP, PQ-REACT

Post-quantum Internet (TLS/IPsec,DNS..)

QUBIP, PQCRYPTO

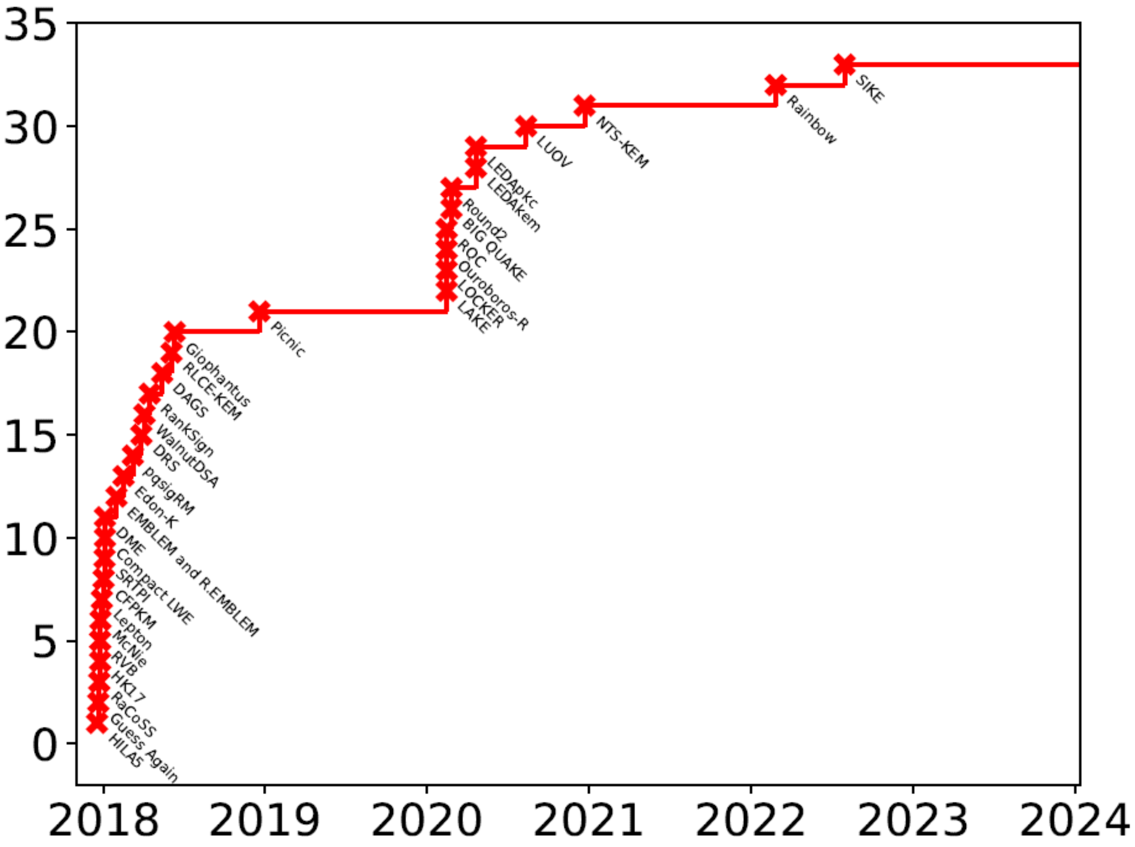
Other deployment challenges in specific sectors*

Work by our EU-funded researchers In space, energy grids …

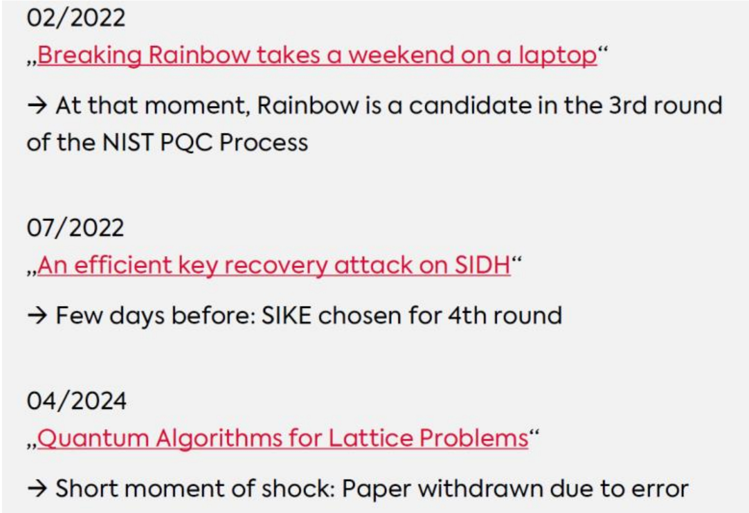
(*) Specificities related to sectors: Energy, Financial sector (NGI-TALER, EPOQUE), Healthcare and Medicine, Space, Automotive (PQCSA), ... PiQASO will deal with several industrial sectors. Several other projects will provide partial roadmaps (PQCSA, Q-PREP, …), Hybridization (PQ-REACT).

European Commission

1. Security of PQC algorithms
- when the PQC breaks were published



Daniel J. Bernstein, Post-quantum cryptography for developers



02/2022

„Breaking Rainbow takes a weekend on a laptop“

→ At that moment, Rainbow is a candidate in the 3rd round of the NIST PQC Process

07/2022

„An efficient key recovery attack on SIDH“

→ Few days before: SIKE chosen for 4th round

04/2024

„Quantum Algorithms for Lattice Problems“

→ Short moment of shock: Paper withdrawn due to error

❑ Hybrid solutions - combination of PQC and conventional crypto

❑ Pre shared Keys

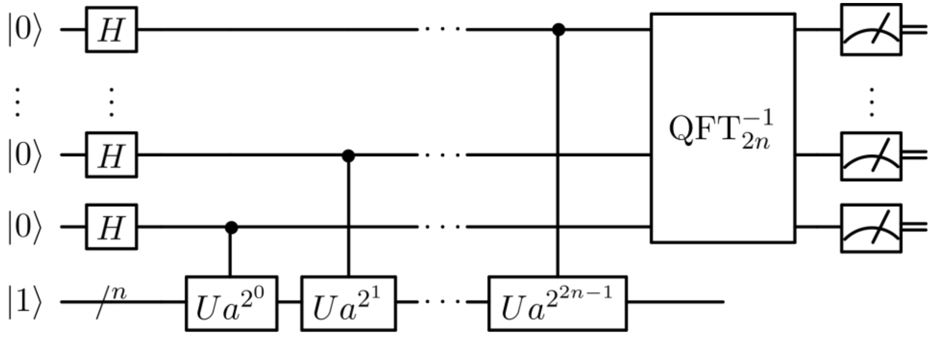
❑ Cryptoagility

+ monitoring of ongoing work by Meta AI, SALSA PICANTE: a machine learning attack on LWE with binary secrets
[2306.11641] SALSA VERDE: a machine learning attack on Learning With Errors with sparse small secrets

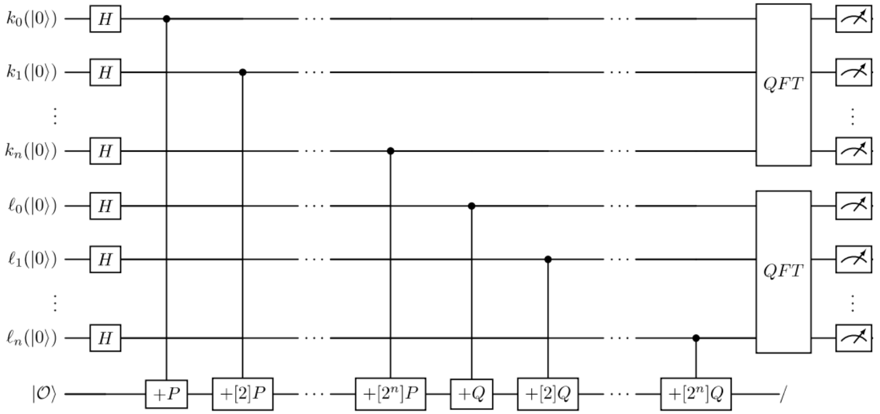
1. Security of PQC algorithms

- A quantum computer acts on quantum states by applying quantum gates to its qubits
- Standing on the shoulder of giants - including but not limited to

C. Gidney and M. Ekera, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,”(2019); https://arxiv.org/abs/1905.09749
G. Banegas, D. Bernstein, I. van Hoof, T. Lange "Concrete quantum cryptanalysis of binary elliptic curves" (2020); https://doi.org/10.46586/tches.v2021.i1.451 472
T. Haner, S. Jaques, M. Naehrig, M. Roetteler, M. Soeken, "Improved quantum circuits for elliptic curve discrete logarithms“https://link.springer.com/chapter/10.1007/978-3-030-44223-1_23
D.S.C. Putranto, R. W. Wardhani, H.T. Larasati, H. Kim. “Another concrete quantum cryptanalysis of binary elliptic curves” (2022) https://eprint.iacr.org/2022/501
R.Taguchi and A. Takayasu. “Concrete quantum cryptanalysis of binary elliptic curves via addition chain. In Cryptographers” (2023) https://eprint.iacr.org/2023/553



Circuit of Shor’s algorithm for solving RSA



Circuit of Shor’s algorithm for solving ECDLP

1. Security of PQC algorithms

- A quantum computer acts on quantum states by applying quantum gates to its qubits

Final goal: design of post-quantum cryptosystems with improved security against quantum attacks

- Development of quantum computing attacks to PQC
- efficient representation of lattice, coding (and other families) problems in qubit registers
- Optimizing number of gates for different circuits, number of physical and logical qubits, execution time, parallelization of quantum circuits, quantum algorithm failure
- New quantum algorithms with significant quantum speed-up for lattice-based, code-based, and potentially other mathematical problem-classes
- Open-source quantum computing software development (Eclipse Qrisp or Qiskit to solve mathematical problems forming the core of cryptosystems
- Parameter suggestions to create a robust set of cryptographic building blocks

2. PQC transition in Hardware

- **Processors.** The transition to PQC s not just the software stack – Impact on chips, computers.

- **Internet-of-Things (IoT) devices / Microcontroller SoCs**. Often have memory-mapped bare metal accelerators for asymmetric cryptography.
  - IoT: Inexpensive consumer electronics with wireless/wired connectivity:
  - Low-power CPU is often supported by a (memory-mapped) crypto *accelerators*
  - HW & Firmware update for PQC

- **Secure Elements and Root of Trust (RoT) subsystems.** *Physically hardened* microchips.
  - Smart Cards, SIMs, discrete TPM chips.
  - Root of Trust (RoT) integrated into SoCs.
  - Smart Cards provide authentication, key management. TPM chips and SoC RoT subsystems manage the secure boot process and configuration of the system.

- **Dedicated cryptographic devices.** HSMs, Rack-mounted Cryptographic Devices (secure routers, encryptors)
  - ASIC & FPGA
  - Performance: HW Acceleration

- **Other protocols.** Multiparty computation, threshold cryptography, etc. **The computational overhead of homomorphic encryption is very large**: Large-scale HW acceleration of FHE is an active research field.

2. PQC transition in Hardware – Secure boot

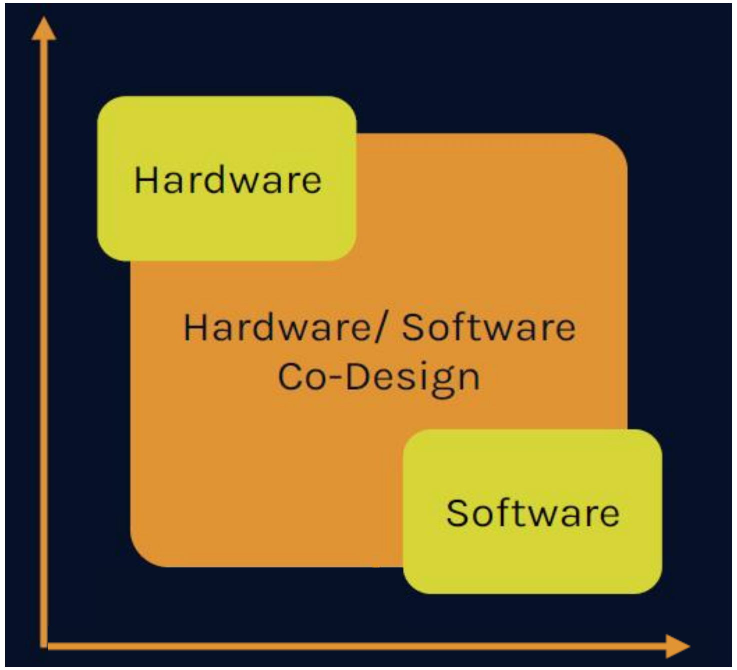
- Optimized, flexible HW/SW solutions required
- For the foreseeable future a zoo of algorithms – both current PKC and PQC need to be supported

Quantum-safe HSM

supplier of post-quantum cryptographic services:
key generation, management and operational usage of cryptographic services via cryptographic APIs to external applications

consumer of cryptographic services:
how does it do firmware updates ? how is the external key storage (extended storage, backup, archival, etc…) done ? HSM-to-HSM Communications ? Attestation, Anti-tamper, Secure-boot …

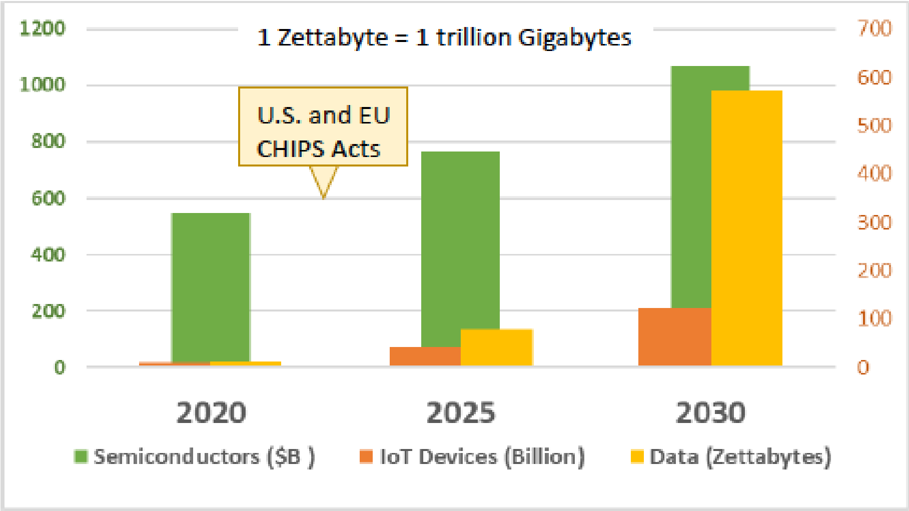
Performance & security



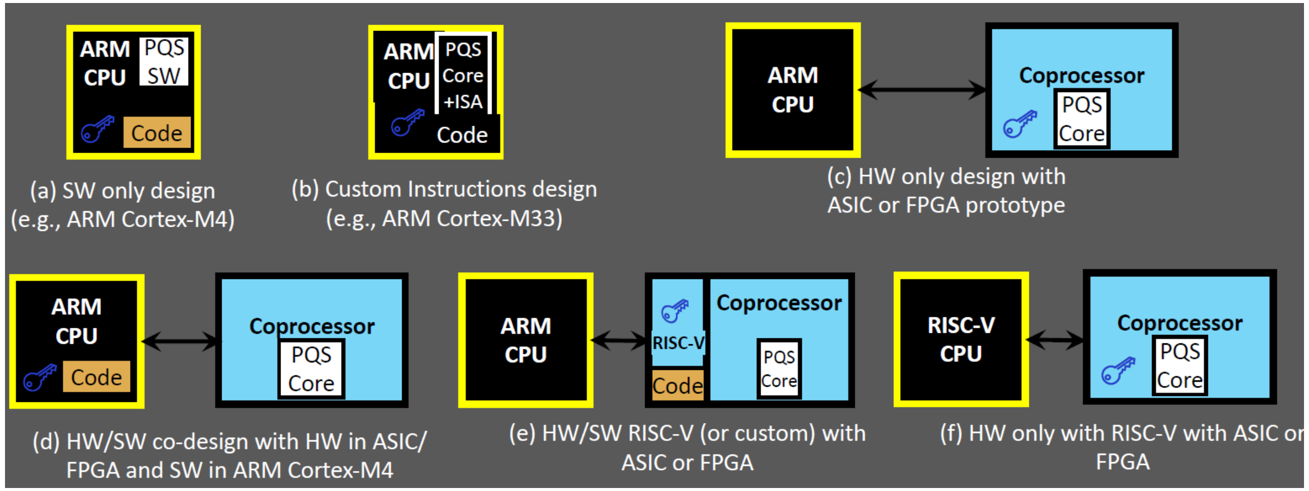
Agility

2. PQC transition in Hardware – new Chips

Semiconductor Enabled IoT Devices & Data by 2030



Sources: Congress DIGIT Act, Sven Balnojan The Future of Good Data



(a) SW only design (e.g., ARM Cortex-M4)

(b) Custom Instructions design (e.g., ARM Cortex-M33)

(c) HW only design with ASIC or FPGA prototype

(d) HW/SW co-design with HW in ASIC/ FPGA and SW in ARM Cortex-M4

(e) HW/SW RISC-V (or custom) with ASIC or FPGA

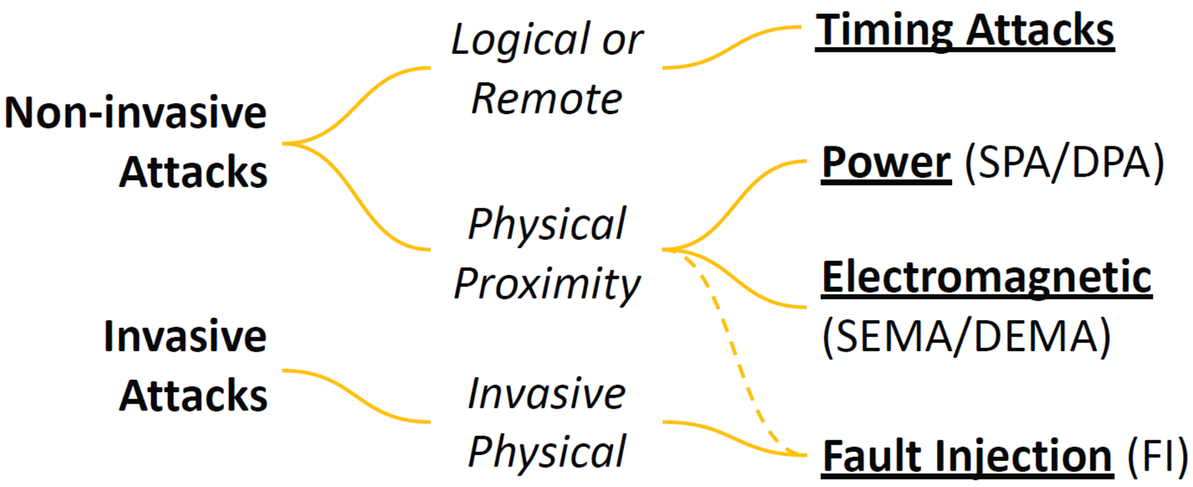
(f) HW only with RISC-V with ASIC or FPGA

- IoT devices projected to grow to 125 Billion and data(the new gold) to 570 Zettabytes
- The semiconductor industry that enables IoT is projected to exceed $1 trillion in revenues

Many practical challenges
- Memory
- Available hardware (accelerator, co-processors)
- Efficient side-channel countermeasures

Courtesy of R. Azarderakhsh, PQSecure Technologies – do NOT re-use this slide

3. Implementation attacks & countermeasures



Countermeasures to side-channel and fault attacks countermeasures are hard to implement and cause ovehead

What does it mean to secure PQC implementations in “practice”?

Active research area resulting in increasingly powerful attacks.

Early stage of academic research. Limited industrial results.

4. Hybrids

Combine one (or more) post-quantum schemes with ECC or RSA

Public-key signatures: All individual signatures must be valid for the hybrid signature to be valid

Public-key encryption: Use multiple systems to jointly generate key for use in symmetric cryptography

Different options to hybridize

Choice of systems depends on risk profile:

- most efficient systems (hybrid with ECC or RSA), to ease usage and gain familiarity
- most conservative systems (hybrid with ECC or RSA), to ensure that data really remains secure

Some PQ libraries exist, quality is getting better

4. Hybrids are a complex matter

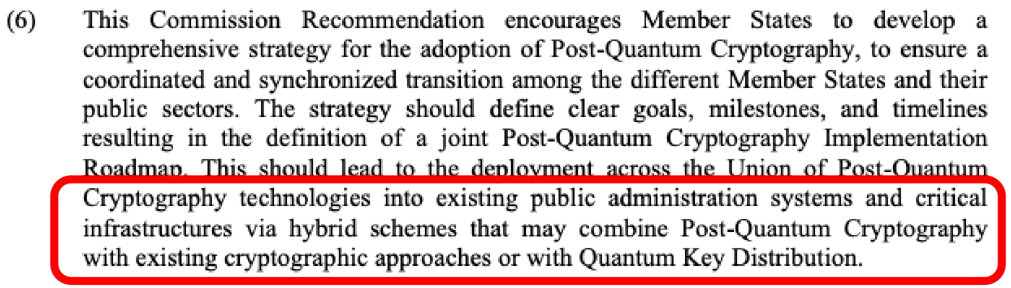
- hybrid modes (meant here as using PQC alongside with pre-quantum algorithms) can offer a promising approach for enhancing both security (as PQC algorithms and their implementations are not yet as mature as their pre-quantum counterparts) and migration flexibility during the transition to a post-quantum world

- However, at the same time, hybrid solutions **may introduce complexity** (so, they may not make things easier !), may increase attack surfaces, and may delay full adoption of streamlined quantum-safe algorithms

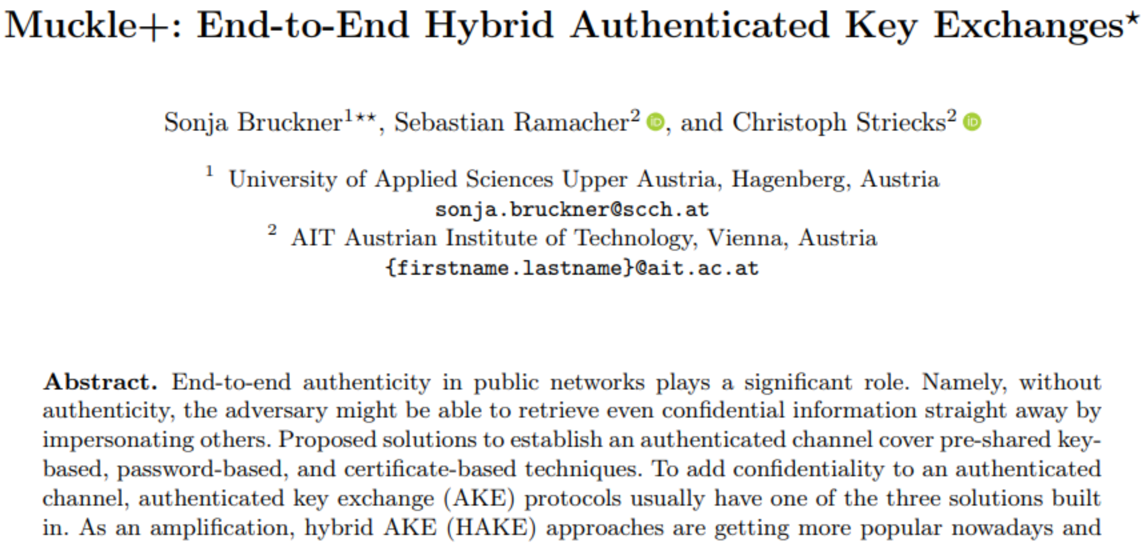
- While the Commission recognizes the complexity that hybrids could bring, and that certain applications may even not be based on hybrids at all, its position is that the potential benefits of hybrids overpass the challenges of combining multiple quantum-resistant algorithms, and this is simply because there is a **whole, very diversified ecosystem that has to move to PQC.** The transition will not take place in one step for everybody.

Another type of hybridization:

In-depth Defense by PQC +QKD



(6) This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition among the different Member States and their public sectors. The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap. This should lead to the deployment across the Union of Post-Quantum Cryptography technologies into existing public administration systems and critical infrastructures via hybrid schemes that may combine Post-Quantum Cryptography with existing cryptographic approaches or with Quantum Key Distribution.



Muckle+: End-to-End Hybrid Authenticated Key Exchanges*

Sonja Bruckner[1]**, Sebastian Ramacher[2], and Christoph Striecks[2]

[1] University of Applied Sciences Upper Austria, Hagenberg, Austria
sonja.bruckner@scch.at
[2] AIT Austrian Institute of Technology, Vienna, Austria
{firstname.lastname}@ait.ac.at

Abstract. End-to-end authenticity in public networks plays a significant role. Namely, without authenticity, the adversary might be able to retrieve even confidential information straight away by impersonating others. Proposed solutions to establish an authenticated channel cover pre-shared key-based, password-based, and certificate-based techniques. To add confidentiality to an authenticated channel, authenticated key exchange (AKE) protocols usually have one of the three solutions built in. As an amplification, hybrid AKE (HAKE) approaches are getting more popular nowadays and

Combining:

- Keys from QKD layer
- PQC key encapsulation mechanism
- Optional: keys from classical cryptography (helps for migration to quantum-safe systems)
- PSK for authentication

Benefits:

- End-to-end authentication and confidentiality (relying on PSKs)
- Resilience (e.g., if PQC fails, guarantees for QKD still hold)
- "Backwards-compatibility" (i.e., add a PQC/QKD layer to existing classical one)

5. Advanced primitives

- Privacy-Enhancing Cryptography

- **Zero knowledge proofs (ZKPs) and SNARK variants**. Ex: to prove that a computation has been performed correctly, with a proof more efficient to check than it is to redo the computation

- **Fully Homomorphic Encryption (FHE),** extends encryption. Ex:
  - to preserve confidentiality of data in computations, protect databases from hacking (biometrics, searches in text, searches in DNA, searches in movies)
  - to protect machine learning queries and model training. AI requires a lot of data to be effective, but this impacts privacy. Also, some training cannot be performed as some data is classified. Handing this with FHE allows to remove tension between functionality and privacy.

- bring those constructions from where they are now to concrete instantiations with concrete parameters, implementations, etc. This may also nicely align (or maybe be slightly late) for the NIST call for threshold schemes

6. Acceleration

- Several critical applications need high-throughput PQC (cloud service providers, financial institutions, telecommunications companies, IoT companies, blockchain companies, healthcare systems,, Big Data Analytics, ..)

- GPU-based algorithms are accelerating cryptographic research by examining technical challenges in parallelizing cryptographic workloads across GPUs, managing memory bandwidth, optimizing performance, and overcoming hardware limitations

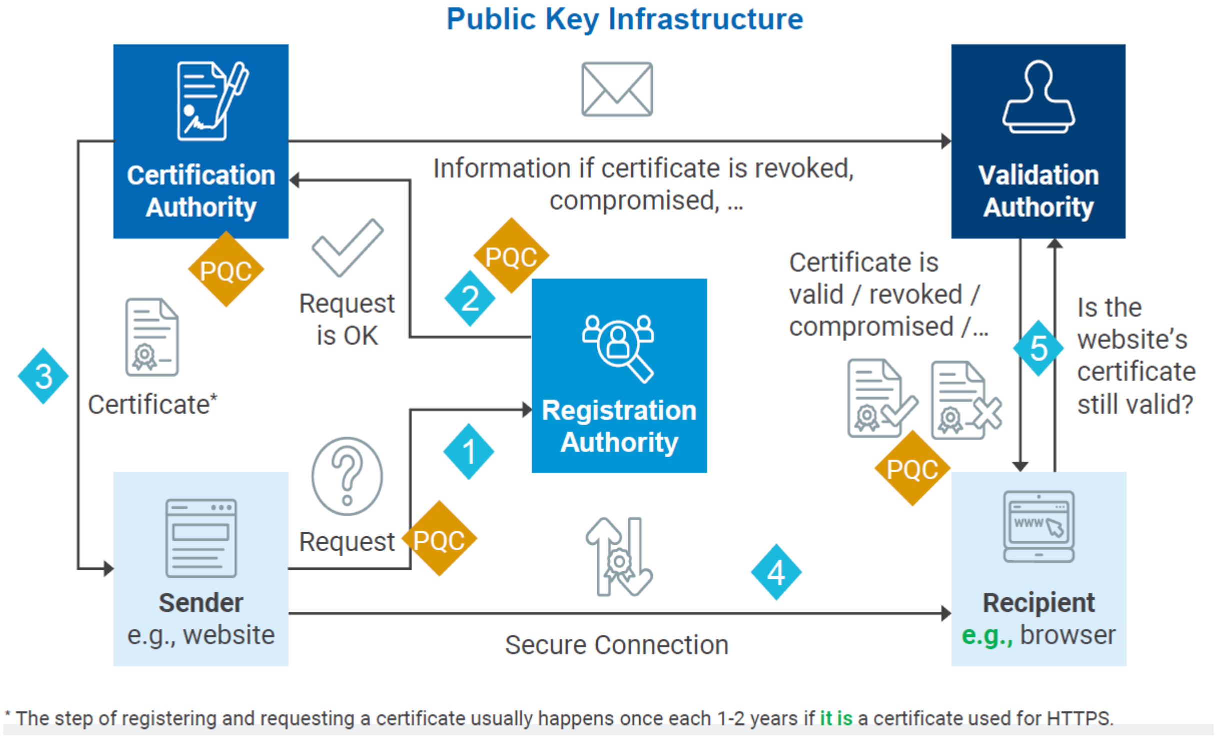
- GPU-Hardware Optimizations

  - Algorithms need to be reorganized with hardware considerations
  - Certain mathematical subroutines are suitable for parallelization
  - Optimization techniques to allow register-heavy components to be spread across multiple threads

7. PKI – need for flexible PQ migration strategies

- Server & Client Certificates
- Authentication certificates
- Identity certificates
- Signing certificates
- User certificates
- …

- Heterogenous vs homogeneous PKI. Use different algorithms in the PKI stack ? hash-bases signature at the CA root level ensure high level of security



* The step of registering and requesting a certificate usually happens once each 1-2 years if it is a certificate used for HTTPS.

picture from Nils Gerhardt - Ultimaco – PKI conference 2025
please do not re-use this slide

- Certificates ? combiners for issuance of new certificates for the different applications, taking into consideration compatibility with legacy systems, different cryptographic protocols across certificate chains, the applications requirements (security level, time-constraints in signing and verification steps, hardware optimization requirements)

European Commission

THE EU RESEARCH & INNOVATION PROGRAMME

2021 – 2027

Research and Innovation

Evaluation (award) criteria

Three evaluation criteria

‘**Excellence**’, ‘**Impact**’ and ‘**Quality and efficiency of the implementation**’.

(Only one evaluation criterion for ERC grants - Excellence)

- Evaluation criteria are **adapted** to each **type of action**, as specified in the WP
- Each criterion includes the ‘**aspects to be taken into account**’. The same aspect is not included in different criteria, so it is not assessed twice.
- **Open Science** practices are assessed as part of the scientific methodology in the excellence criterion.

Evaluation criteria (RIAs and IAs)

Research and innovation action (RIA)

Activities to establish new knowledge or to explore the feasibility of a new or improved technology, product, process, service or solution.

This may include basic and applied research, technology development and integration, testing, demonstration and validation of a small-scale prototype in a laboratory or simulated environment.

Innovation action (IA)

Activities to produce plans and arrangements or designs for new, altered or improved products, processes or services.

These activities may include prototyping, testing, demonstrating, piloting, large-scale product validation and market replication.

EXCELLENCE

- ✓ Clarity and pertinence of the **project's objectives**, and the extent to which the proposed work is ambitious, and goes beyond the state-of-the-art.
- ✓ Soundness of the proposed **methodology**, including the underlying concepts, models, assumptions, inter-disciplinary approaches, appropriate consideration of the **gender dimension** in research and innovation content, and the quality of **open science practices** including sharing and management of research outputs and engagement of citizens, civil society and end users where appropriate.

IMPACT

- ✓ Credibility of the **pathways** to achieve the expected **outcomes and impacts** specified in the work programme, and the likely scale and significance of the contributions due to the project.
- ✓ Suitability and quality of the **measures to maximize expected outcomes and impacts**, as set out in the dissemination and exploitation plan, including communication activities.

QUALITY AND EFFICIENCY OF THE IMPLEMENTATION

- ✓ Quality and effectiveness of the **work plan**, assessment of risks, and appropriateness of the effort assigned to work packages, and the resources overall.
- ✓ Capacity and role of each **participant**, and extent to which the **consortium** as a whole brings together the necessary expertise.

Proposals aspects are assessed to the extent that the proposed work is within the scope of the work programme topic

Thank you !

European
Commission