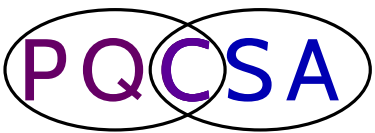
Urgency of reliable program for PQC support

Tanja Lange and Bart Preneel
Eindhoven University of Technology, KU Leuven

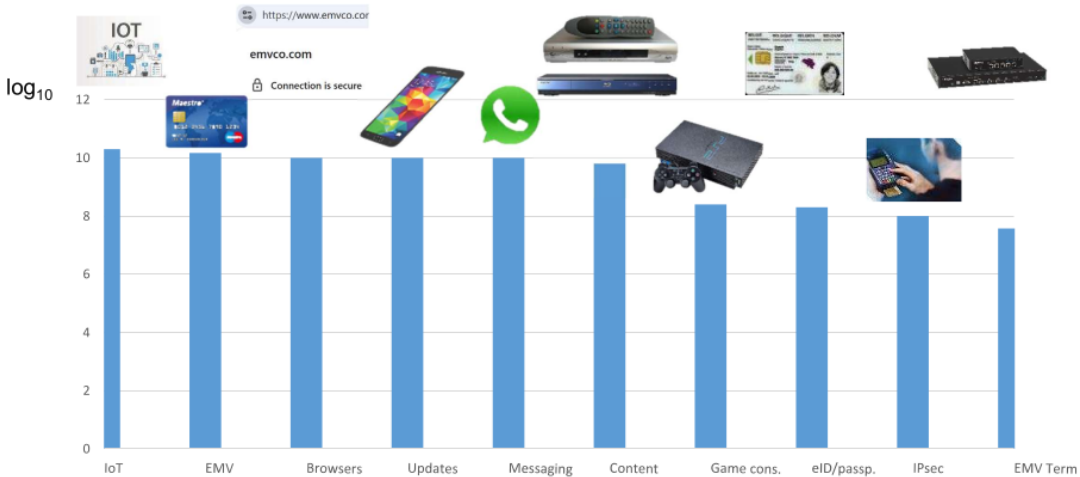
PQCSA – Post-Quantum Cryptography Support Action



PQCSA

- Funded under call DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC
- 3 key objectives:
  1. Organize and coordinate the European ecosystem for PQC standardization.
  2. Collect and synthesize approaches to PQC migration into a European PQC migration roadmap.
  3. Raise broad awareness for the need to migrate to PQC in industry, administration, and civil society and provide the necessary knowledge.

Public-key cryptography deployments – 70 B



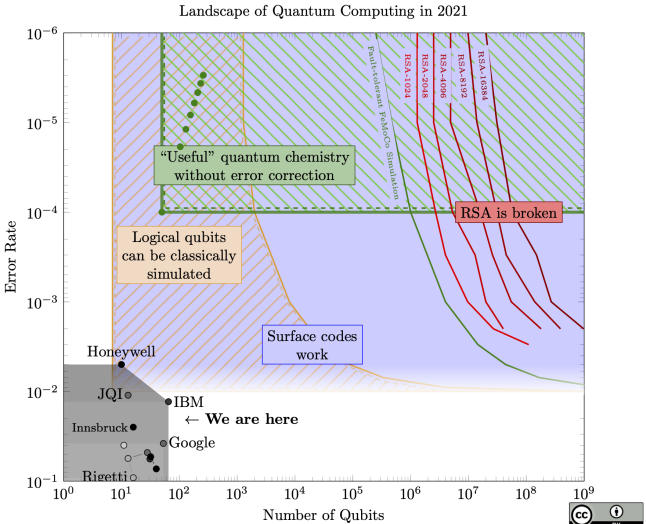
What's this all about?

Need for and urgency of PQC migration

- Most current usage of cryptography involves RSA and ECC which will be broken with a sufficiently large and stable quantum computer.
- Post-quantum cryptography produces systems that resist even quantum attacks.
- Store now decrypt later. Our enemies (and friends) are busy recording encrypted data for later breaks.
- PQC migration comes too late for today's data, we must protect tomorrow's asap.

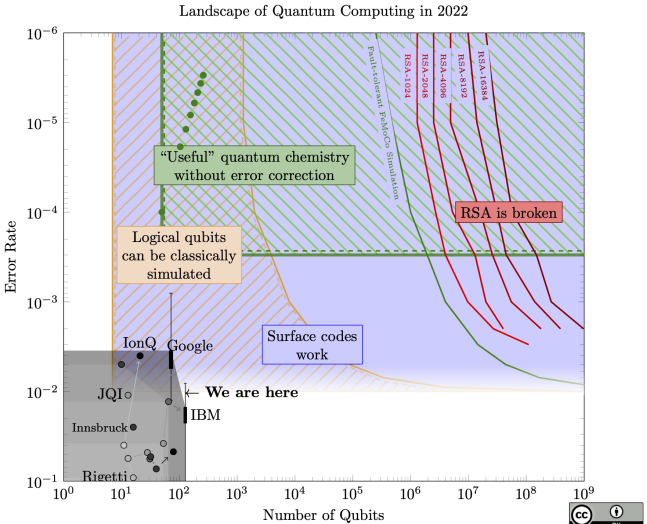
Urgency comes from multiple advances

https://sam-jaques.appspot.com/quantum_landscape_2026



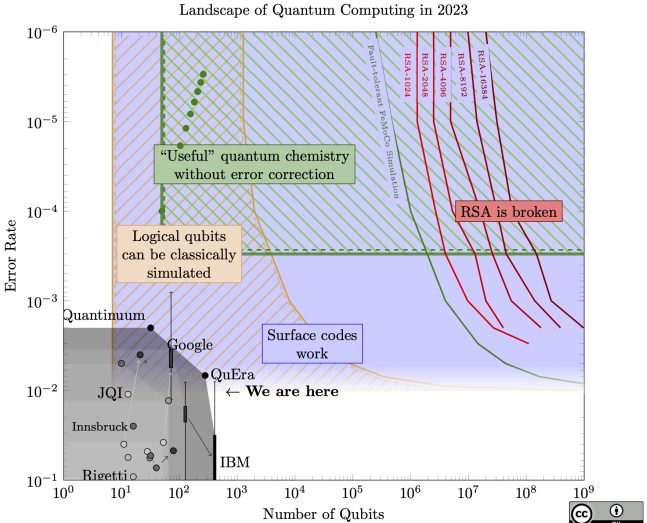
Urgency comes from multiple advances

https://sam-jaques.appspot.com/quantum_landscape_2026



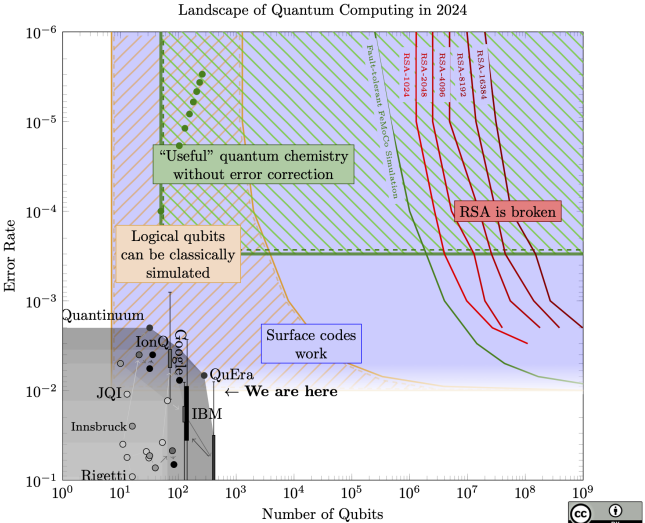
Urgency comes from multiple advances

https://sam-jaques.appspot.com/quantum_landscape_2026



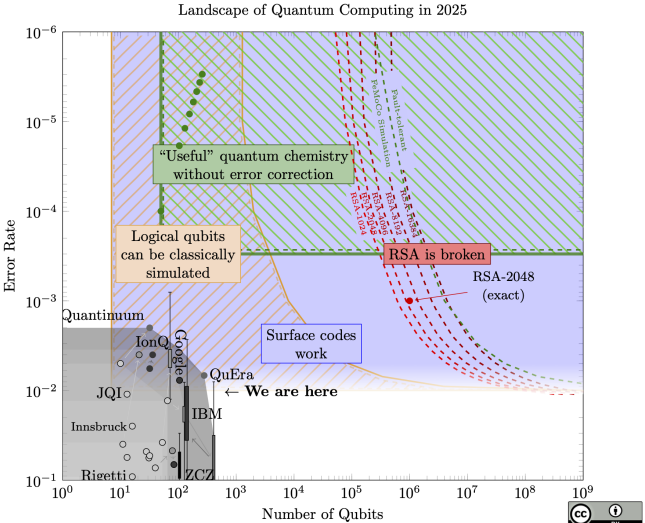
Urgency comes from multiple advances

https://sam-jaques.appspot.com/quantum_landscape_2026



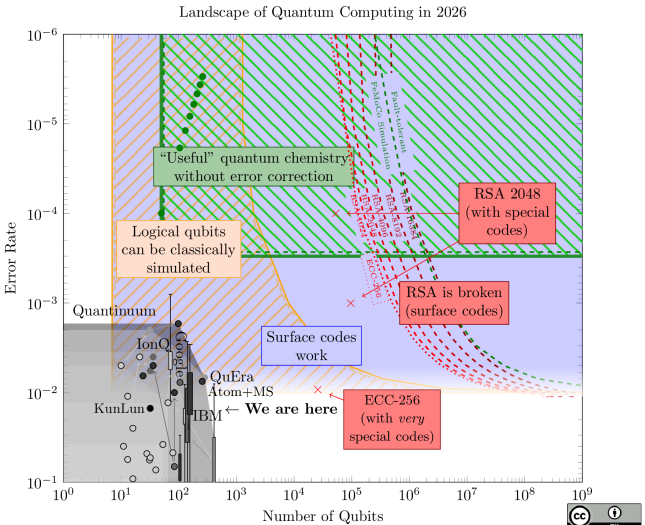
Urgency comes from multiple advances

https://sam-jaques.appspot.com/quantum_landscape_2026



Urgency comes from multiple advances

https://sam-jaques.appspot.com/quantum_landscape_2026



23 Jun 2025. 1st NIS2 PQC workstream roadmap (link)

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC).

Quantum computing has been identified as a threat to many cryptographic algorithms used to protect the confidentiality and authenticity of data. This threat can be countered by a timely, comprehensive and coordinated transition to Post-Quantum Cryptography (PCQ).

AdobeStock © ipopba

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

p.7 of EU PQC Workstream Roadmap

22 Jun 2026 US White House executive order (link)

EXECUTIVE ORDER 14409

Sec. 4. Accelerating the PQC Transition. (a) Within 30 days of the date of this order, each agency head shall identify its PQC migration lead and provide the name and contact details of the PQC migration lead to the Director of OMB and the National Cyber Director.

(b) Within 90 days of the date of this order, the Director of OMB shall, in consultation with the Secretary of Homeland Security through the Director of CISA and the National Cyber Director, and consistent with 6 U.S.C. 1526(c), issue guidance requiring each agency to:

(i)
Sy

(ii)
De

(iii)
December 31, 2031; and

(ii) transition all HVAs and high impact systems to use PQC for key establishment by December 31, 2030;

(iii) transition all HVAs and high impact systems to use PQC for digital signatures by December 31, 2031; and

(iv) develop and submit to the Director of OMB and the National Cyber Director a plan to accomplish this directive.

(c) Within 180 days of the date of this order, the Secretary of Commerce, through the Director of NIST, shall initiate a pilot project for PQC migration on an appropriate subset of information systems owned or operated by NIST, to be completed no later than December 31, 2027.

Sec 6 – Problem for EU Digital Sovereignty

(c) Within 180 days of the date of this order, the Federal Acquisition Regulatory Council (FAR Council), in consultation with the Secretary of Homeland Security through the Director of CISA and the Director of NIST, shall publish a proposed rule amending the Federal Acquisition Regulation (FAR) to require covered contractors to comply by December 31, 2030, with NIST's FIPS, including all applicable FIPS incorporating PQC compliant algorithms.

(d) Within 270 days of the date of this order, the FAR Council, in consultation with the Secretary of Homeland Security through the Director of CISA and the Director of NIST, shall publish a proposed rule amending the FAR requirements and contract clauses for contractor vulnerability disclosure programs to ensure that covered contractors implement vulnerability disclosure policies (VDPs), consistent with NIST guidelines, and that VDPs incorporate reports of cryptographic vulnerabilities, including testing for lack of encryption and the use of non-FIPS approved algorithms.

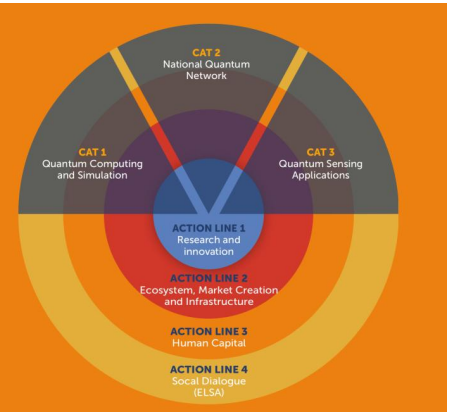
Quantum Act must address collateral damage on 70 B devices/applications/libraries

- Urgent investment needed for R&D and deployment of PQC.
- Users: some R&D results ready to use, but **every IT department** has to act.
- Security suppliers: revise all hardware & software products and services.
  - Design new chips.
  - Buy different chips and integrate.
  - Write new customized software, integrate new libraries.
  - Test, verify, get certification.
- Major EU initiatives, e.g, EUDI Wallet, AI systems, and Digital Euro, require advanced cryptography which is currently not (efficiently/securely) available.
- PQC needs to be recognized as integral part of quantum ecosystem.
- PQC offers guaranteed progress and deployment.

Quantum Act must address collateral damage on 70 B devices/applications/libraries

- Urgent investment needed for R&D and deployment of PQC.
- Users: some R&D results ready to use, but **every IT department** has to act.
- Security suppliers: revise all hardware & software products and services.
  - Design new chips.
  - Buy different chips and integrate.
  - Write new customized software, integrate new libraries.
  - Test, verify, get certification.
- Major EU initiatives, e.g, EUDI Wallet, AI systems, and Digital Euro, require advanced cryptography which is currently not (efficiently/securely) available.
- PQC needs to be recognized as integral part of quantum ecosystem.
- PQC offers guaranteed progress and deployment.
- QKD is at best a niche solution (< 100M)
  at worst a closed black-box system with high risk of supply-chain backdoors.
- QKD uses quantum technology but security benefits are limited.

Showcase: Quantum Delta NL



Full details (via archive.org)

Action line 1: Realization of research and innovation breakthroughs in six fields:

- Quantum computing
- Quantum sensing
- Quantum simulation
- Quantum algorithms
- Quantum communication
- Post-quantum cryptography

Action line 2: Ecosystem development, market creation and infrastructure

Action line 3: Human capital

Action line 4: Promotion of social dialogue regarding quantum technology

Impact of AI

- Diverts attention and resources.

Impact of AI

- Diverts attention and resources.
- May shorten time to Q-day:
  - Faster quantum circuits for cryptanalysis.
  - More compact quantum error correction.
  - More stable physical qubits.
- Help with inventory (finding use of pre-quantum crypto).
- May help with migration of software and faster development of verified implementations (but do not expect miracles).
- Makes side-channel attacks more efficient.

Need reliable program for PQC support

- Short-term need, e.g.,
  - Development of secure and efficient hardware for current PQC standards.
  - Migration of standards and relevant protocols
    (as CSA, PQCSA can coordinate and highlight needs, but not do the work).
  - Migrate PKI and explore new trust architectures.
- Continuous need, e.g.,
  - Security evaluation incl. quantum cryptanalysis.
  - Validation and testing of (open source) libraries, formal verification.
  - Side-channel attacks and countermeasures for implementations.
- Challenging research problems, e.g.,
  - Design advanced systems: OPRF, VRF, NIKE, blind signatures, anonymous credentials & ZK proofs, fully homomorphic encryption.
  - Develop solutions with full crypto-agility
  - Miniaturize HW footprint of PQC, incl. new systems.

For much more details see D1.3 Hot Topics and Open Problems in PQC.

Links to further information

- PQCSA deliverables (so far)
  - D1.1 Survey of PQC algorithms
  - D1.3 Hot Topics and Open Problems in Post-Quantum Cryptography
  - D2.1 Survey of PQC protocols
- NIST PQC competition.
- Quantum Threat Timeline 2019; updates from 2021, 2022, 2023, and 2024.
- Status of quantum computer development (by German BSI).
- ENISA studies: Post-quantum cryptography: Integration study, Post-quantum cryptography: current state and quantum mitigation
- YouTube channel Tanja Lange: Post-quantum cryptography.
- PQCRYPTO summer school with 21 lectures on video; slides; exercises.
- Less math, more perspective: Executive school I and Executive school II.
- pqcrypto.org overview page by D.J. Bernstein & T. Lange.
- PQCrypto 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026.
- PQCRYPTO project (ended in 2018, but still lots of useful resources).
- PQConnect ready-to-use tunnel, adding extra PQC layer.