Post Quantum Cryptography – A game changer for electronic ID documents?

Robert Bach

Mindshare 2023

Gelsenkirchen, 19.09.2023

Post Quantum Cryptography – A game changer for electronic ID documents?

Agenda

- Quantum computers and cryptanalysis
- What is Post Quantum Cryptography (PQC)?
- Status of PQC standardization
- Challenges for electronic ID documents
- Recommendations
- Summary

Rapid developments in the field of quantum computers

- **Rapid developments** of quantum computers
  - **2016:** 5 Qubits by IBM
  - **2019:** 53 Qubits by Google ("quantum supremacy")
  - **2025:** 4158 Qubits predicted by IBM
  - **~2030:** 1’000’000 Qubits predicted by several companies

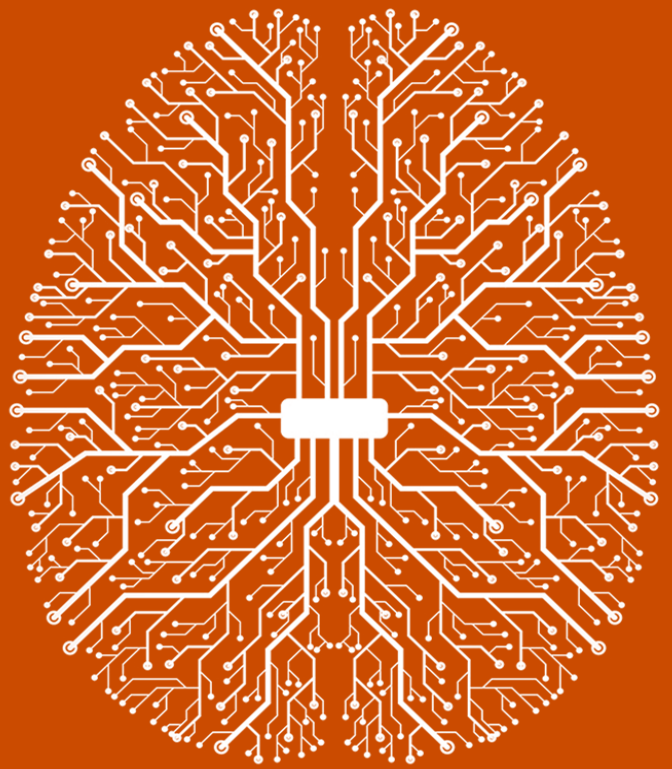
- May lead to breakthroughs in Artificial Intelligence, chemical simulation, cryptography and **cryptanalysis**

Are quantum computers fast?

- “**Multiplying of long integers**” – quantum computers are **slow** compared to a “classical” computer
- “**Prime factorization of long integers**” – quantum computers are **very fast** compared to a “classical” computer
- Basis for **cryptanalysis**

Quantum cryptanalysis on a universal quantum computer will heavily affect RSA, ECDSA, ECDH

A universal Quantum Computer will have a game changing effect on the cryptographic security of Identity Documents like eID cards, often with a regular lifetime of 10 years.
There´s still the “physical security” of the document, but i.e. a digital signature will not be safe anymore…



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

Grover’s algorithm weakens algorithms with short symmetric keys.
In a quantum world, AES-128 has only 64-bit security

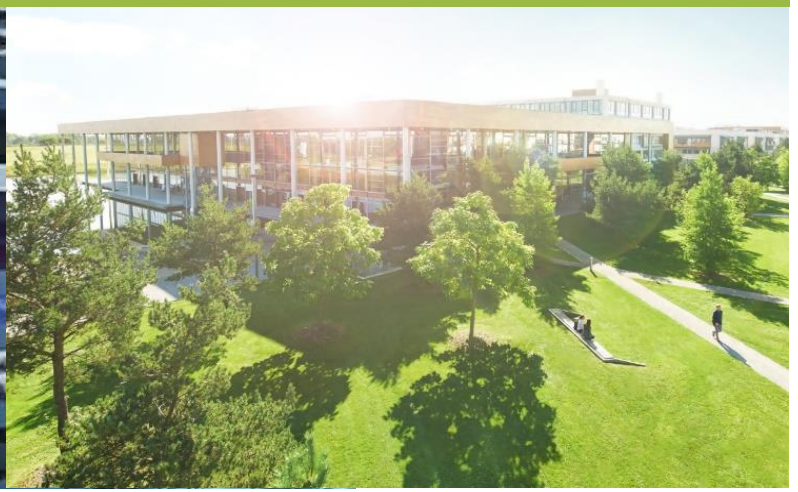
Affected: AES-128, 3DES

Shor’s algorithm could break common asymmetric cryptography like RSA, ECC, Diffie-Hellman.
In a quantum world, i.e. ECC-256 and RSA-3072 have almost no security

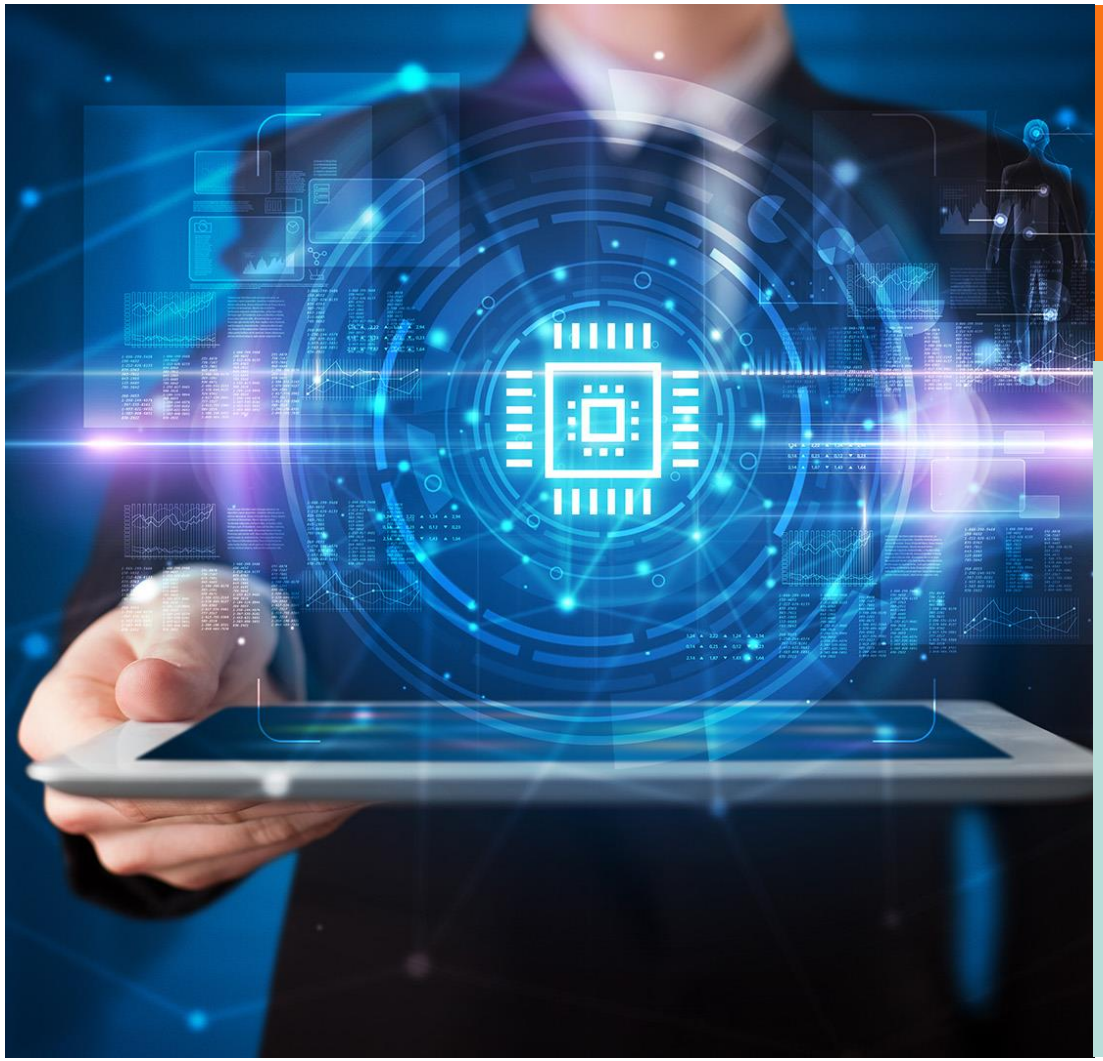
Heavily affected: RSA, ECDSA, ECDH

The equation with unknowns:
The universal quantum computer – when and how?

- A universal quantum computer provides an adequate **number of logical quantum bits**, excellent execution **quality** and high calculation **speed**
  - ~4100 “logical” Qubits might instantly affect an RSA-2048
  - How many “physical” Qubits will be needed to achieve these “logical” Qubits (catchword: “error correction”)?
- Which **size** will a quantum computer have? A small rack? Or is a big building needed?



Post Quantum Cryptography (PQC): After algorithm selection, standardization activities continue



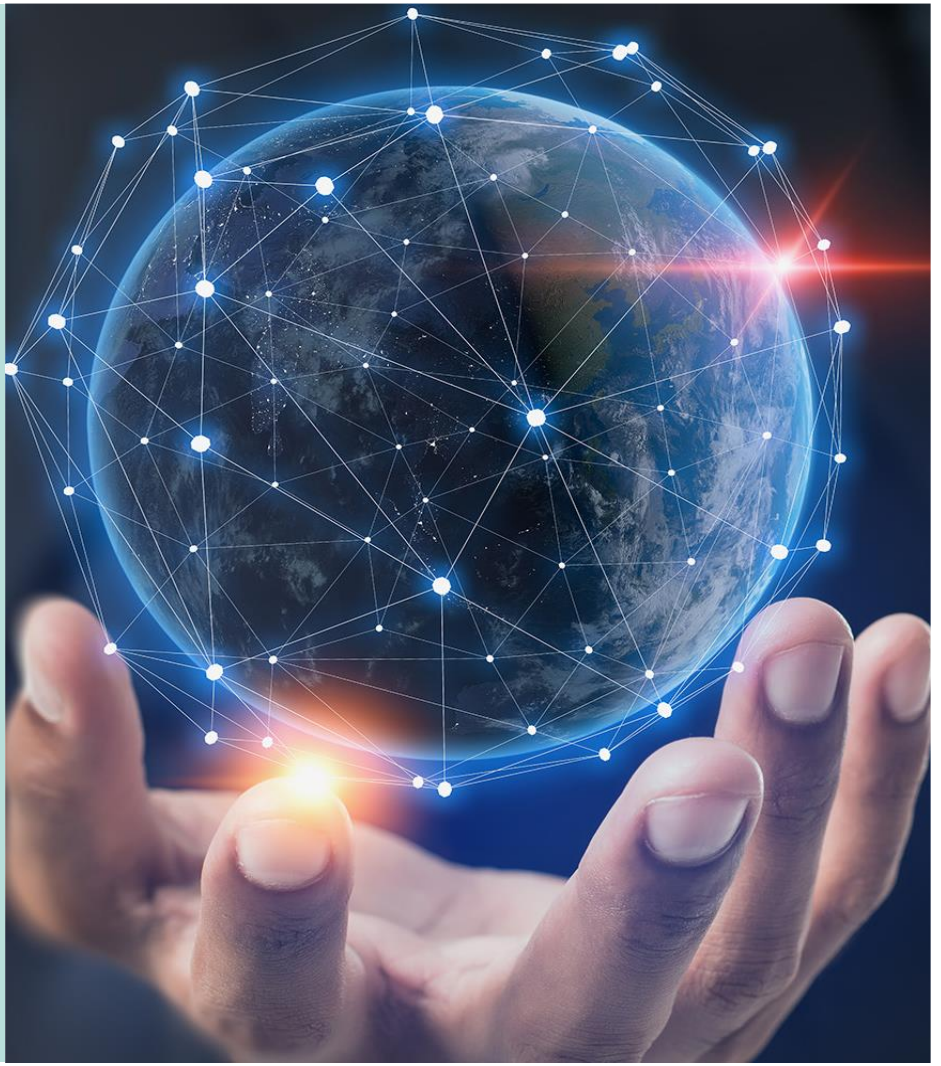
- **Post Quantum Cryptography** (PQC) **aims to repel cryptanalysis** performed by a quantum computer
- PQC is to be deployed in security controllers and is aimed to provide security against attacks with classical and quantum computers
- The National Institute for Standards and Technology (NIST) started in 2015 a **competition** towards a transition to PQC
- First algorithm candidates selected in 2017
- Final candidates have been selected in **2022**
- Development of **draft standards** is ongoing, now available for public comment (including KYBER, DILITHIUM, SPHINCS+)
- **Final standardization** expected 2024 and beyond

Integration in ID standards and adoption of infrastructure is required

- The **selection** of PQC-algorithms is the beginning of standardization
- **Communication protocols need to be adapted** and **standardized**
- **Documents**, **infrastructure** including **background systems** need to be upgraded
- **Long transition periods** expected, from a
  - continuing use of **conventional** cryptographic protocols to a
  - use of “**hybrid**” protocols combining conventional cryptography and PQC to a
  - migration to “**PQC-only**-powered” protocols

Challenges of a „PQC-migration“ include crypto agility, a secured PQC-implementation and require learning cycles

- What happens to **issued documents**?
  - **Crypto agility** is helpful
  - **Field-upgrade mechanisms** are helpful
- Challenge is the **implementation of PQC secured** against manipulating, observing and semi invasive attacks
  - Hardware resources help to maintain adequate **transaction performance**
  - Hardware resources support **secured implementations**
- PQC will require **learning cycles** during the evaluation and certification of first implementations
- **Hybrid approaches** (combination of conventional and Post-Quantum Cryptography) reduce risks



There are several approaches towards a quantum computer world - Best is to start preparation right now

- **Short-term ignore the topic?**
  - ... but at a moment in the future, issued documents might be compromised
  - ... probably not an option

- **Reduce the validity of electronic ID-documents?**
  - The shorter the document lifetime, the better the risk position
  - Payment cards are valid for three years, but **Identity documents** have a lifetime of five to **ten years**
  - Reducing document validity is difficult to implement
  - ... probably not an option

- Search for mitigation with a variety of actions
  Start the preparation right now!

Mitigation: Start preparation right now

- Start to get the **information** on PQC
- **Start making strategic plans**
- Start to work on **migration strategies**
  - „How to migrate infrastructure?“
  - „How to upgrade documents?“
  - „Which cryptographic infrastructure do I use?“
  - “When to start …?”
- Reflect on implications of PQC - I**mpacts on software & hardware**: increasing key sizes, memory footprints, …
- **Moving to PQC affects the whole lifecycle** of a document - industrialization, personalization, issuance, operational usage and field updates

Summary and key statements
Start the preparation right now!

- There are **rapid developments in the field of quantum computers**
- The **conventional cryptography** deployed in current electronic ID documents and smart cards **will be affected by the cryptanalysis** performed on a future universal quantum computer
- **Post-quantum cryptography** is intended to repel this cryptanalysis, but **standardization and market introduction will take many years**
- **Documents**, **infrastructure** including **background systems** need to be upgraded, but **long transition periods** expected
- **Start the preparation right now!**


infineon