Hardware implementation of PQC Algorithms

Frederic Sauvayre

19.11.2024

European Cyber Week 2024, Rennes, France

Infineon at a glance

Growth areas

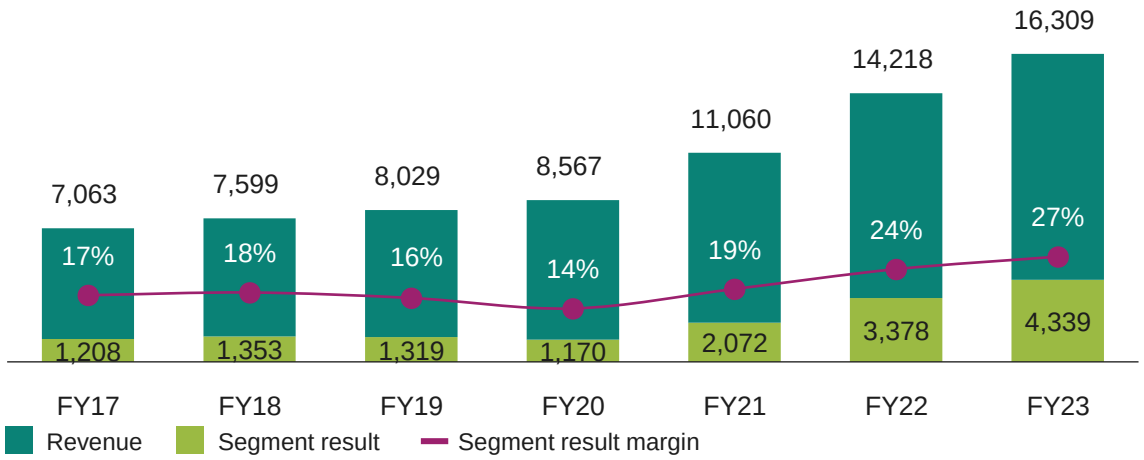
Energy
green and efficient

Mobility
clean and safe

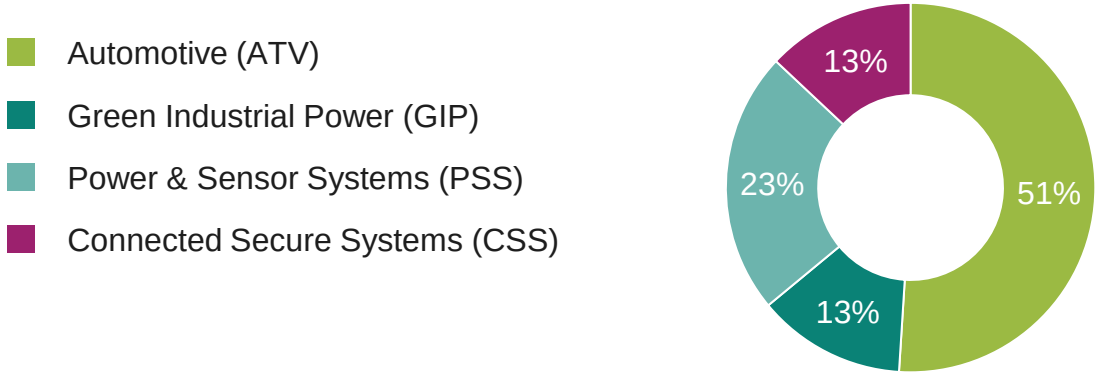
IoT
smart and secure

Financials

[EUR m]



FY23 revenue by segment[1]

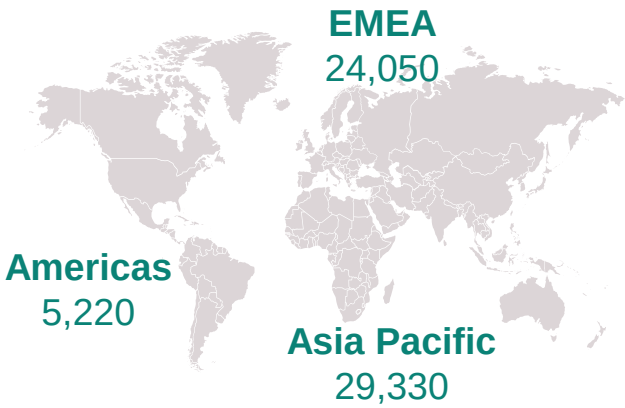


Employees[2]

58,600
employees worldwide

69
R&D and

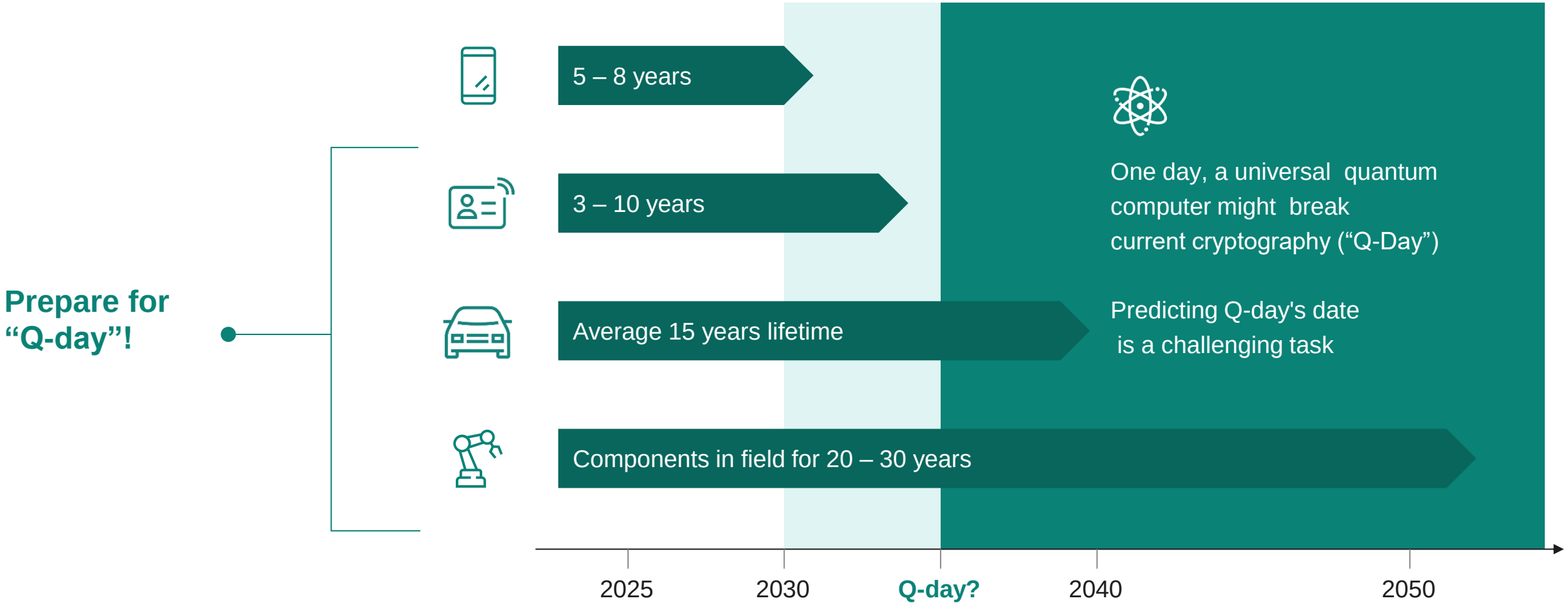
17
manufacturing locations[2]



For further information: Infineon Annual Report.

[1] 2023 Fiscal year (as of 30 September 2023) | [2] As of 30 September 2023

Assets with a long service life are particularly at risk



>> Devices with over 10 years lifecycle must be prepared for the quantum computing age

Post-quantum cryptography and quantum cryptography

Post-quantum cryptography and quantum cryptography are not the same

Post-Quantum Cryptography (PQC)

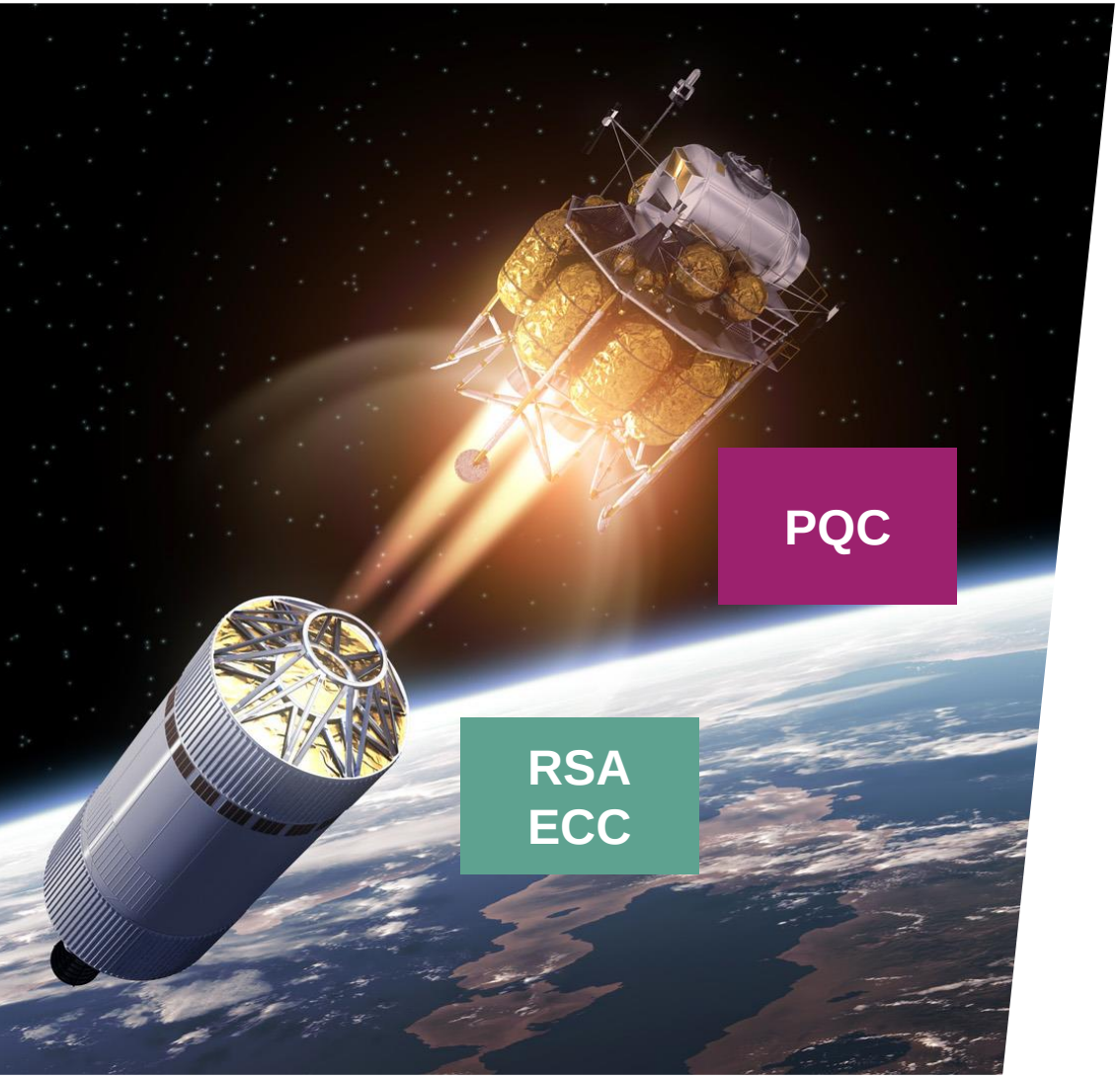
- New **conventional** cryptography deployable **without** quantum computers
- Believed to provide security against classical and quantum computer attacks
- **NSA announced** a transition to post-quantum cryptography in 2015

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

- Infineon is actively pursuing intensive research on **post-quantum cryptography**

Crypto agility



Challenge: migration and agility

- RSA and ECC are used almost everywhere (big investment)
- Integration of new crypto into old protocols
- Need for flexible replacement of crypto
- Ship today and update cryptography later
- The hardware needs to support PQC
- Hybrid requirements lead to cost increase
- **The firmware update mechanism is essential to enable long-term security**

Challenge: Physical security of PQC

Classic public-key cryptography

– More than 2 decades of research in implementation security (attacks and countermeasures)

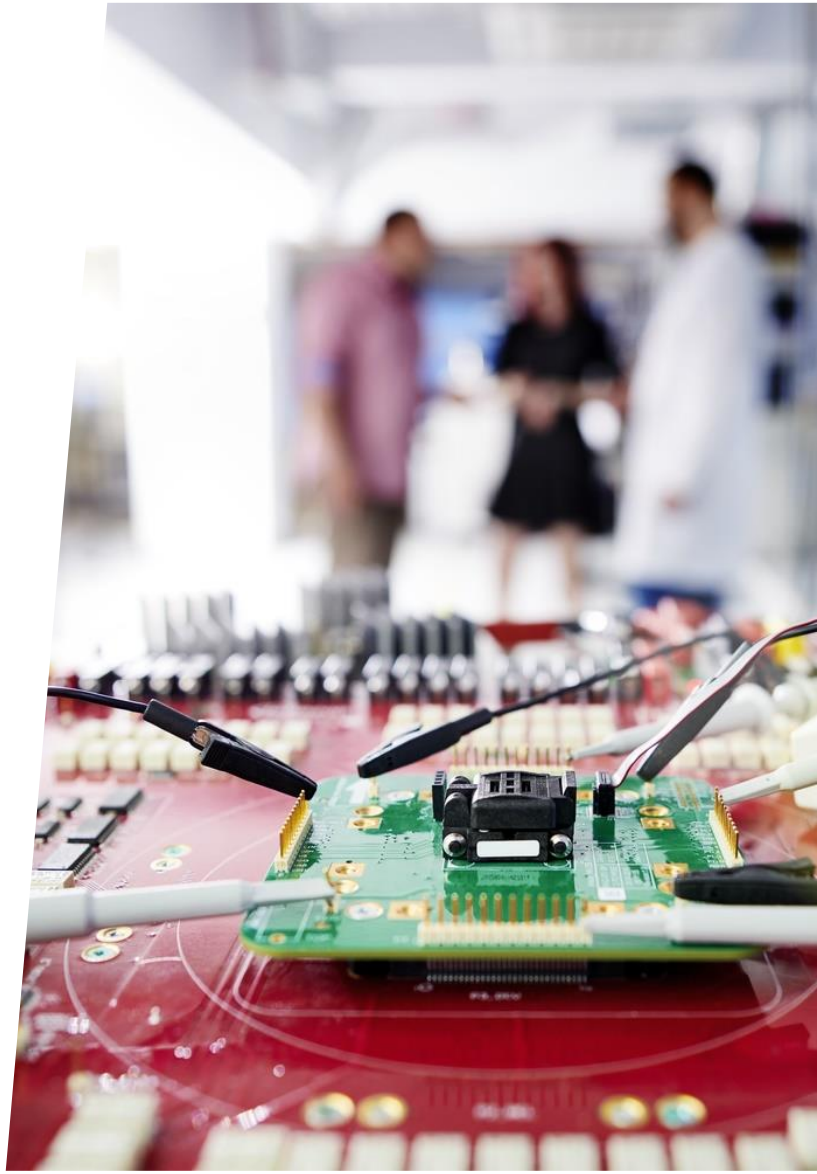
Post-quantum cryptography

– Fundamentally different algorithms lead to new attacks

– Attacks are a highly active research area, lots of development, but still many open questions

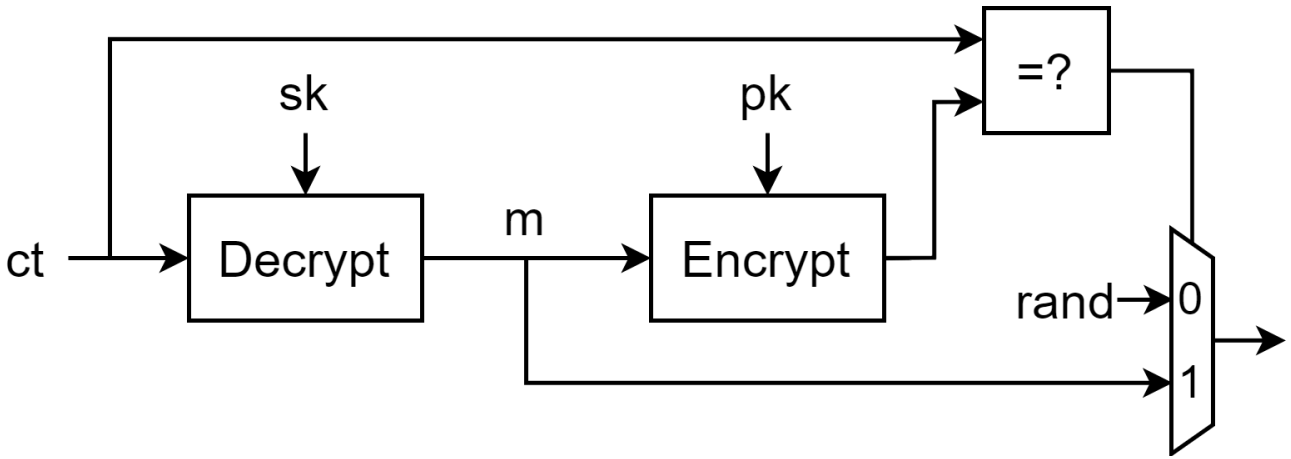
– Highly diverse set of involved operations (arithmetic, logic, ...) complicate protection mechanisms

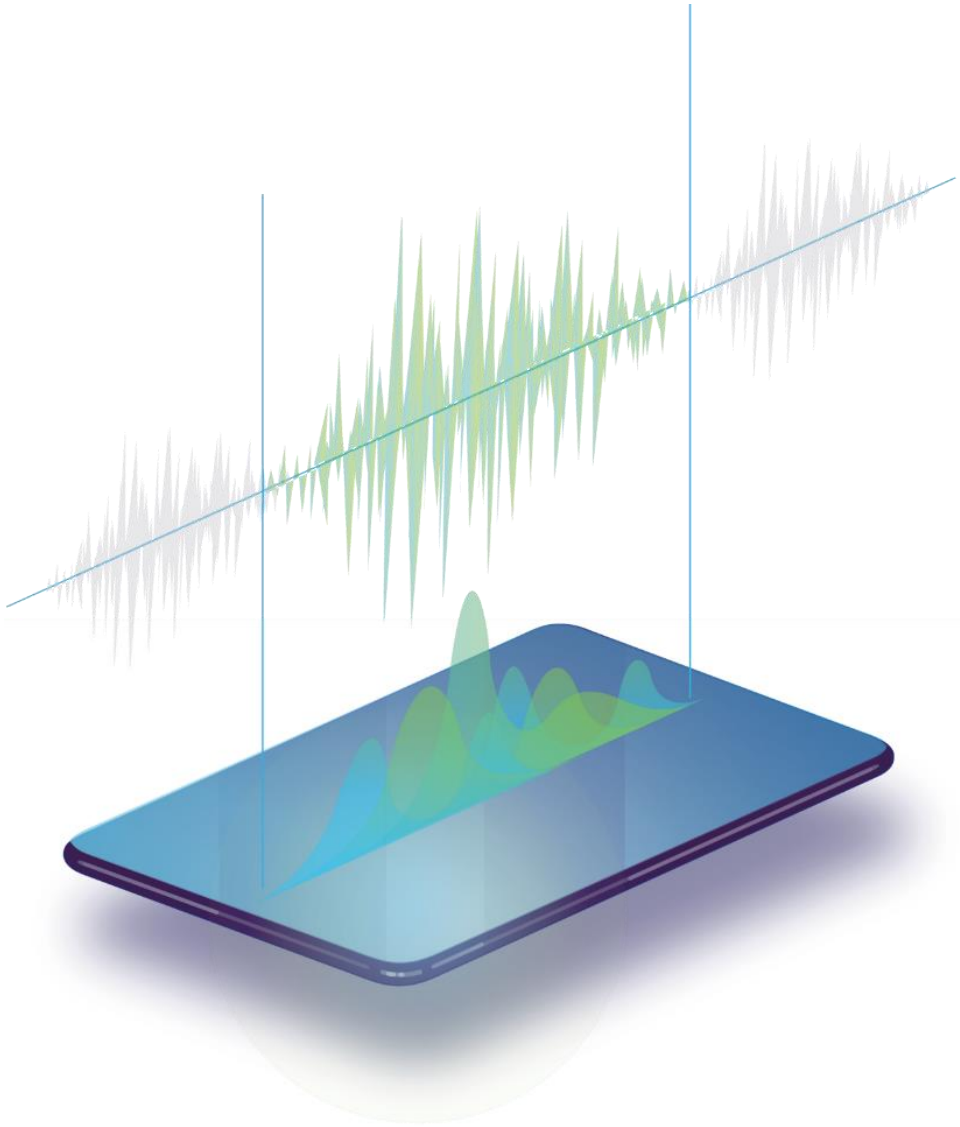
Generic and flexible HW/SW solutions needed to provide long-term security



A new attack vector: re-encryption

- Basic encryption scheme only offers “chosen plaintext” security
  - there exist “chosen ciphertext attacks” allowing key recovery (attacker crafts a ct, sends it, gets response...and can recover key)
- Method to establish chosen-ciphertext security: **re-encryption**
  - re-encrypt message and check if identical ct received
- Consequences for side-channel security?





Fundamental differences w.r.t. countermeasures

Classic cryptography (RSA/ECC)

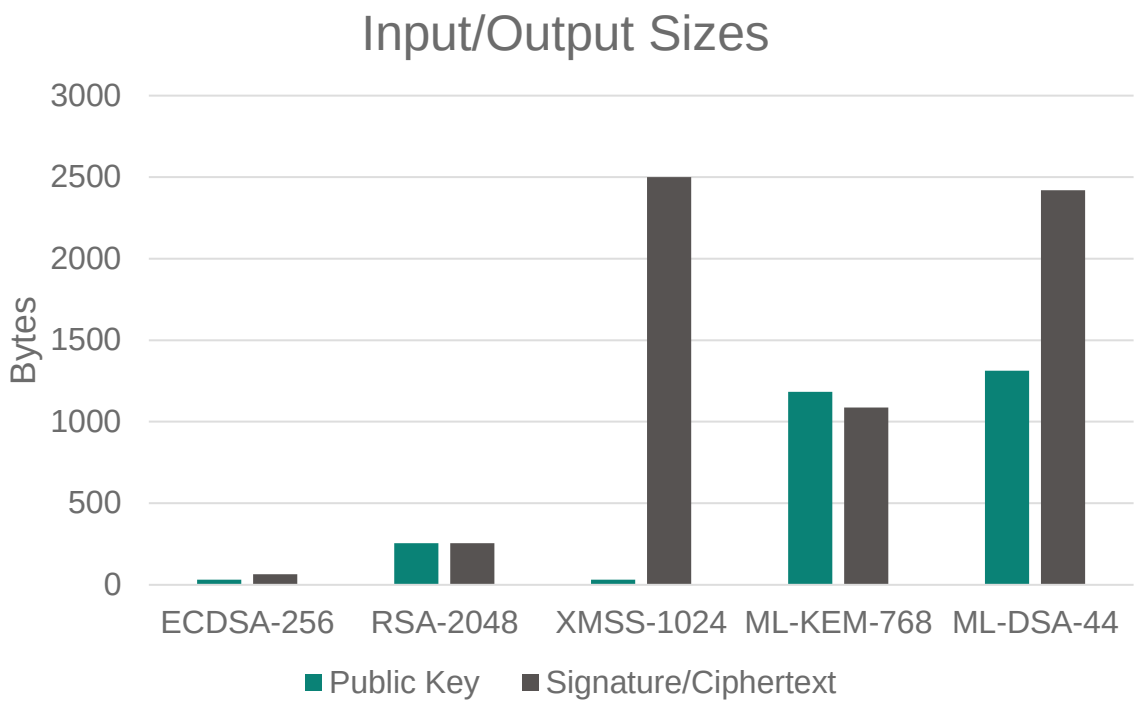
- Main factor: big-integer arithmetic
  - modular multiplications etc.
- Common: bit-scanning of secret
  - different operations depending on bit value
  - square & multiply / double & add
  - constant-time as a first important step
- Strong algebraic countermeasures (SCA & faults)
  - e.g., diverse set of randomizations
    - basepoint, addition of modulus, ...
  - implementable in SW (using a “generic” accelerator)

Lattice-based cryptography (Kyber, Dilithium, ...)

- Multiple components:
  - modular arithmetic, hashing, other processing...
  - must consider ALL components (also interfaces!)
- Constant (key-independent) time comes naturally
  - no bit-scanning etc.
- Need to consider protection of all components
  - approaches can differ drastically
    - protecting a hash vs. protecting modular arithmetic
  - important: think of interfaces

PQC for the Embedded World

- **Runtime: more complex HW acceleration**
  - ML-KEM / ML-DSA: many different subcomponents
  - XMSS / LMS: hashing (SHA2 / SHA3)
- **Significantly increased data sizes**
  - Public keys
  - Signatures/ciphertexts
- **Challenge: transmission and storage**
  - Transmission and buffering of: public keys, ciphertexts, signatures
  - Significantly larger certificate chains (multiple public key/signature pairs)
  - Secured storage of private key

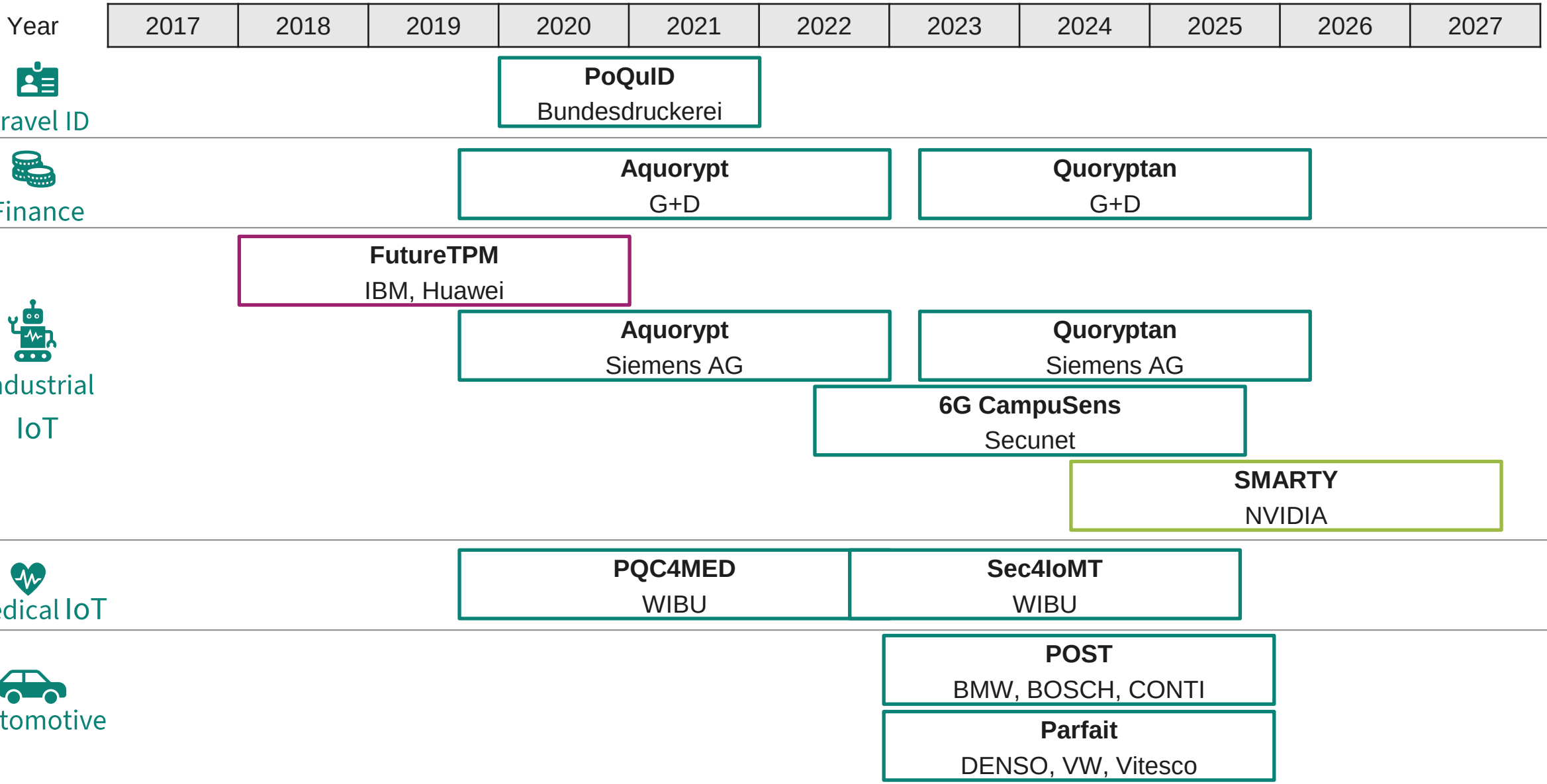


PQC in the Embedded World

- ...devices with limited resources (CPU, memory)
- …operating in potentially adverse environments
- …fulfilling high security requirements

Post-Quantum-Cryptography and Cryptoagility

Public funding projects and key partner



national KDT Horizon Europe

Conclusion

- Post-quantum cryptography is needed to secure a quantum computer world
- First standards are ready
- Novel challenges for secured implementations
- Enabling a smooth transition:
  - Crypto agility
  - Combination of conventional and PQC encryption algorithms


Infineon