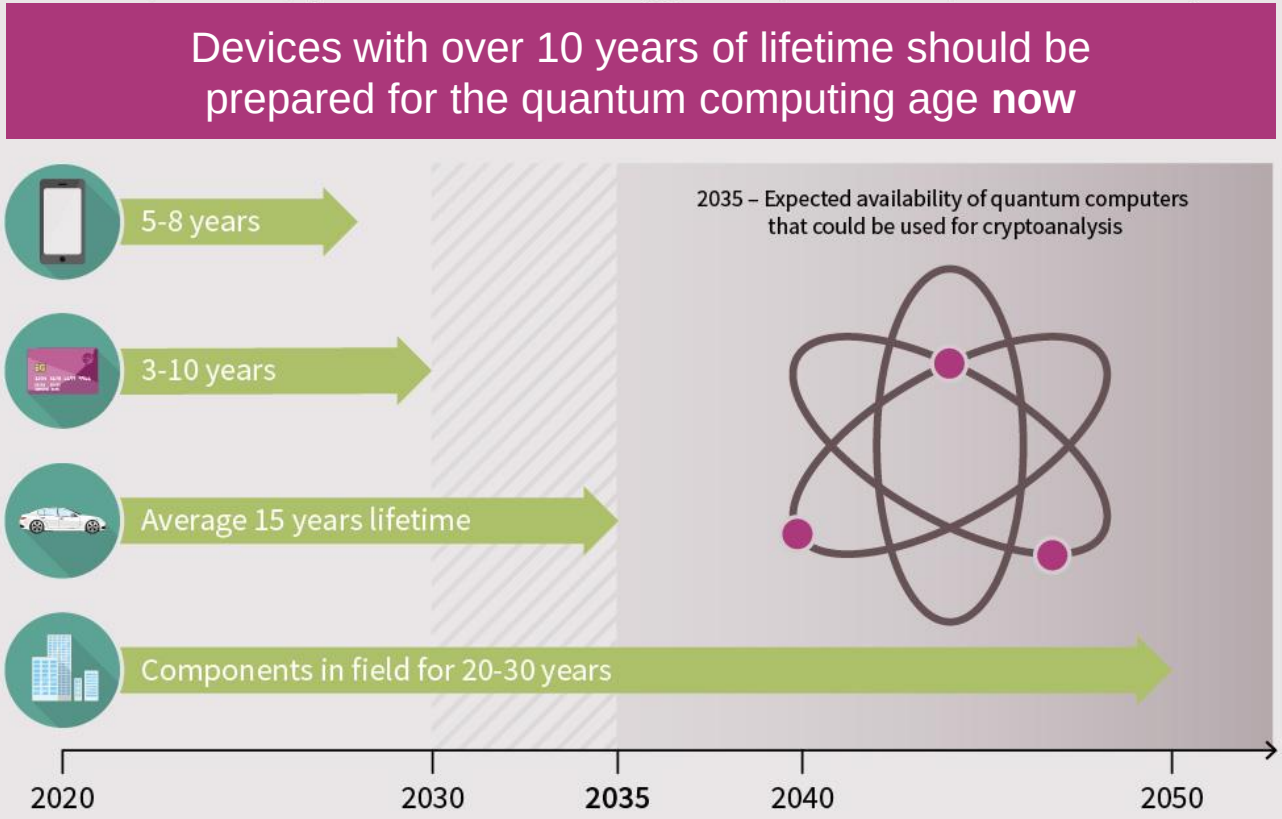
Progress and Challenges in the Industrial Adoption of PQC

Peter Pessl

PQCrypto 2021, Industrial Track

Timeline



Time to act…

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

Outline

Standardization	› Efforts by German agencies
Implementation	› Efficient and secured implementations
Adaptation	› Further challenges

Government views

Many different views on future standardization of post-quantum cryptography

- Complementary to the NIST standardization project
- …as seen in previous talks

BSI Recommendations

- Generic recommendations
  - crypto agility, larger symmetric keys, hybrid protocols
- stateful hash-based signatures XMSS+ and LMS (and tree variants)
  - limited number of signatures, non-trivial state management
  - …but ready now
  - mentioned application by BSI: firmware updates
- recommended key-encapsulation mechanisms
  - FrodoKEM (unstructured lattices)
  - Classic McEliece (codes)
- future extension with NIST-selected algorithms expected

Source: Migration zu Post-Quanten-Kryptografie: Handlungsempfehlungen des BSI, August 2020

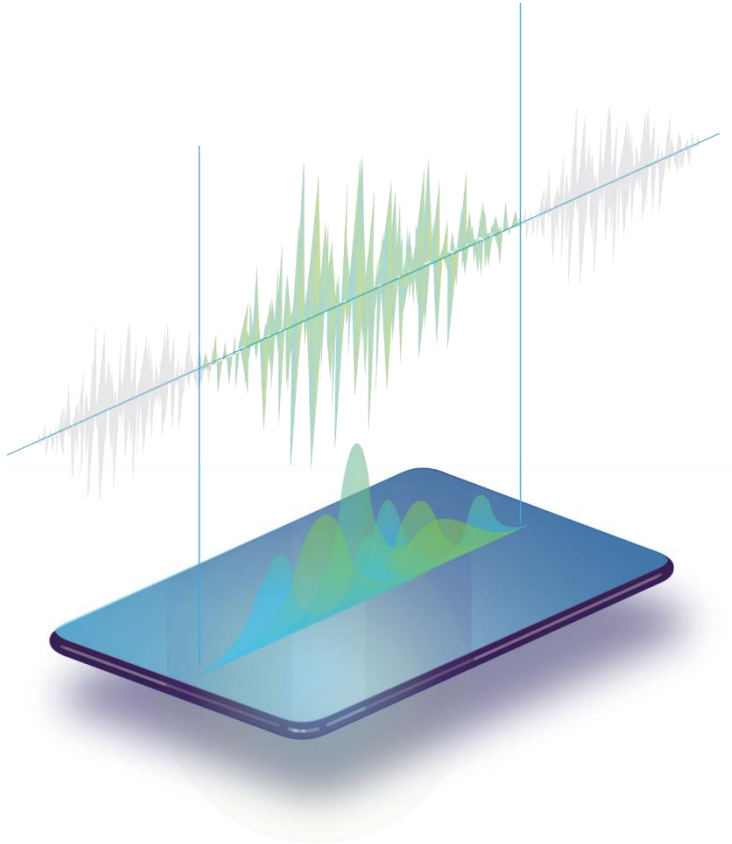
Outline

Standardization	› Efforts by German agencies
Implementation	› Efficient and secured implementations
Adaptation	› Further challenges

Implementations

- Huge progress in implementation efficiency
  - on various platforms
  - runtime becomes less of a concern (memory still somewhat more)

- Implementation security
  - critical in the embedded world
  - progress in attacks and countermeasures (see, e.g., TCHES program)
  - but compared to the decades of work for RSA/ECC?



Implementation security – recent results

Fault Attacks on CCA-secure Lattice KEMs

Peter Pessl[1†] and Lukas Prokop[2]

[1] Infineon Technologies, Germany
peter@pessl.cc
[2] Graz University of Technology, Austria
lukas.prokop@iaik.tugraz.at

Abstract. NIST's post-quantum standardization effort very recently entered its final round. This makes studying the implementation-security aspect of the remaining candidates an increasingly important task, as such analyses can aid in the final selection process and enable appropriately secure wider deployment after standardization. However, lattice-based key-encapsulation mechanisms (KEMs), which are prominently

https://ia.cr/2021/064

A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM

Kalle Ngo[1], Elena Dubrova[1], Qian Guo[2] and Thomas Johansson[2]

[1] Royal Institute of Technology (KTH), Stockholm, Sweden
{kngo,dubrova}@kth.se
[2] Lund University, Lund, Sweden
{qian.guo,thomas.johansson}@eit.lth.se

Abstract. In this paper, we present the first side-channel attack on a first-order masked implementation of IND-CCA secure Saber KEM. We show how to recover both the session key and the long-term secret key from 16 traces by deep learning-based power analysis without explicitly extracting the random mask at each execution. Since the

https://ia.cr/2021/079

Personal Opinion

- Likely many more possible attack venues
  - faults, algebraic SCA, side-channel assisted CCA
- Anticipate future potential attacks while developing countermeasures

Outline

Standardization	› Efforts by German agencies
Implementation	› Efficient and secured implementations
Adaptation	› Further challenges

PQC on a protocol/application level

- Drop-in replacement of existing primitives
  - Possible?
  - Ideal?

- Example: Signature vs. KEMs (finalists)
  - signatures generally lower performance (see PQM4)
  - Falcon: unknown SCA resistance
  - Dilithium: non-deterministic runtime (real-time)

- Can we replace signatures with KEMs?
  - sometimes: KEMTLS [SSW'20]

Source: [SSW'20] Schwabe, Stebila, and Wiggers, Post-quantum TLS without handshake signatures, https://ia.cr/2020/534

Our case study

- Implementation of a PQ key exchange protocol on the Infineon Aurix microcontroller
- Approach in our case study:
  - General AKE by de Saint Guilhem, Smart, and Warinschi [GSW'17]
  - 3-pass authenticated key exchange (AKE), no signatures, offers forward secrecy
  - XMSS for certificate signature
- Internal: generation of an ephemeral key
  - ephemeral key: CPA-secure primitive suffices

Quantum Safe Authenticated Key Exchange Protocol for Automotive Application

Julius Hermelink[1], Thomas Pöppelmann[2], Marc Stöttinger[3], Yi Wang[4], and Yong Wan[4]

[1] Research Institute CODE
Universität der Bundeswehr München
[2] Infineon Technologies, Germany
[3] Continental AG, Germany
[4] Continental Automotive, Singapore

Abstract. In this work, we propose an instantiation of a quantum-safe security protocol for authenticated key establishment (AKE) with forward secrecy. As core primitives, we use Newhope and XMSS and avoid signatures in the key exchange to achieve better performance. Exemplary, the implemented protocol could be used to establish a secured and authentic communication channel between the electrical control unit (ECU) and a testing device for on-board diagnosis (OBD). To verify the feasibility, we implement an XMSS-based public key infrastructure (PKI) and the AKE protocol on the AURIX automotive embedded microcontroller platform. We provide a breakdown of cycle cost and communication overhead and demonstrate that a modern post-quantum AKE can be executed efficiently on our target platform.

Paper presented at Escar 2020

Source: [GSW'17] de Saint Guilhem, Smart, and Warinschi, Generic Forward-Secure Key Agreement Without Signatures, https://ia.cr/2017/853

Conclusion

- Preparation for transition in full swing
- Some challenges remain, e.g.,
  - novel side-channel attacks
  - adaptation of protocols (plus their standardization)
- Effort from many sides

Part of your life. Part of tomorrow.