Bridging 1st PQC-functions and principles with the smart card world

Thomas Pöppelmann – NIS Summer School 2018 - 24.09.2018

Agenda

1. Introduction to PQC
2. Challenges and standardization
3. PQC on smart cards
4. Conclusion

Agenda

1 Introduction to PQC

2 Challenges and standardization

3 PQC on smart cards

4 Conclusion

Cryptography in everyday life

Cryptography is used everyday for various purposes

- Writing an Instant Message
- Ordering at an online retailer
- Placing online stock orders at a bank
- Communication between a lawyer and his/her client
- Transfer of critical business information

The quantum computer world

The world with quantum computers

- Quantum computers use quantum mechanical effects for computation
- Different from classical computers: quantum bits (qubits), quantum gates, new programming model
- Universal quantum computers expected in 15-20 years
  - 2016: 5-qubit computer by IBM
  - 2017: IBM announces a 50-qubit computer
  - 2018: Preview of 72-qubit computer Bristlecone by Google

Possible applications of quantum computers

- Optimization problems
- Quantum chemistry
- Cryptanalysis

The threat of quantum computers to cryptography

Quantum cryptanalysis on a universal quantum computer

Currently used **asymmetric** cryptosystems (RSA/ECC) breakable by using **Shor's algorithm**

- Classical world (currently): ECC-256 has 128-bit of security
- Quantum world (in 15-20 years): ECC-256 has almost 0-bit of security

Bit-security level for **symmetric** cryptography is halved by **Grover's algorithm**

- Classical world (currently): AES-128 has 128-bit of security
- Quantum world (in 15-20 years): AES-128 has only 64 to 80 bits of security

Quantum world (in 15-20 years)

Heavily affected:
RSA, ECDSA, ECDH

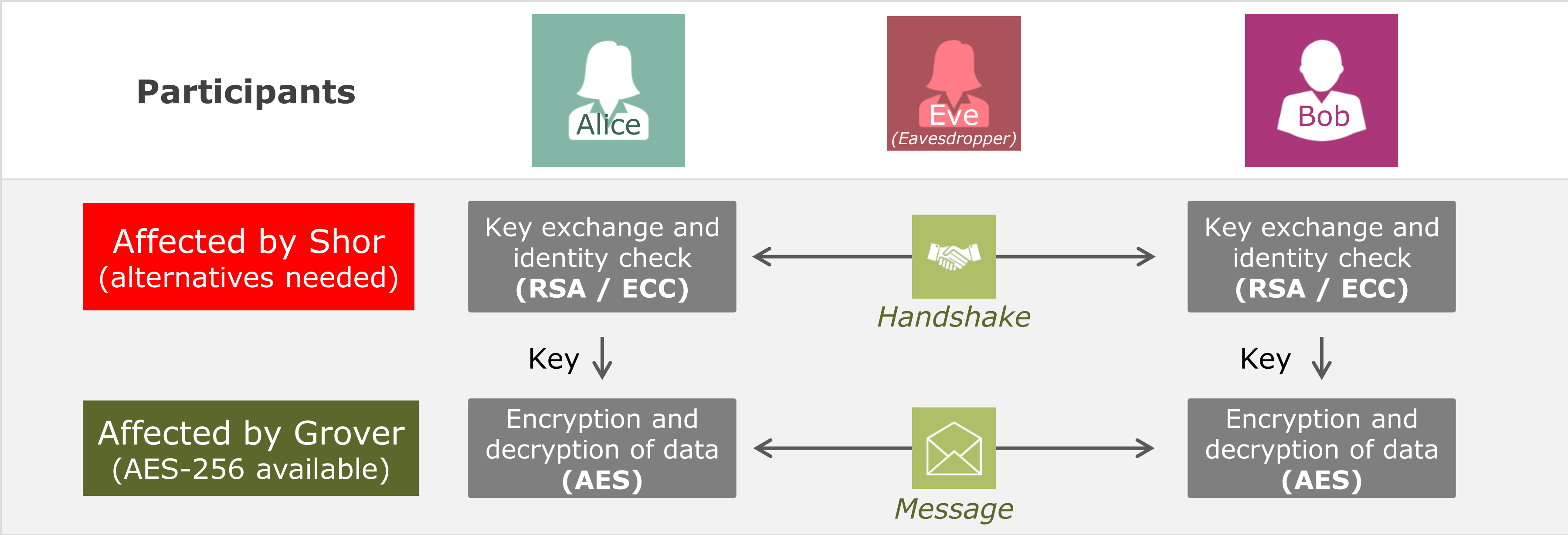
Affected:
AES-128, 3DES

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

The threat of quantum computers to cryptography (II / II)

Consequences of Shor's and Grover's algorithm

- RSA and ECC are the basis for <u>secured key exchange and secured digital identities</u> and <u>no immediate standardized alternatives are available</u>
- For symmetric cryptography, alternatives are available today (e.g. AES-256)



Post-quantum cryptography and quantum cryptography

Post-Quantum Cryptography and Quantum Cryptography are not the same

Post-Quantum Cryptography

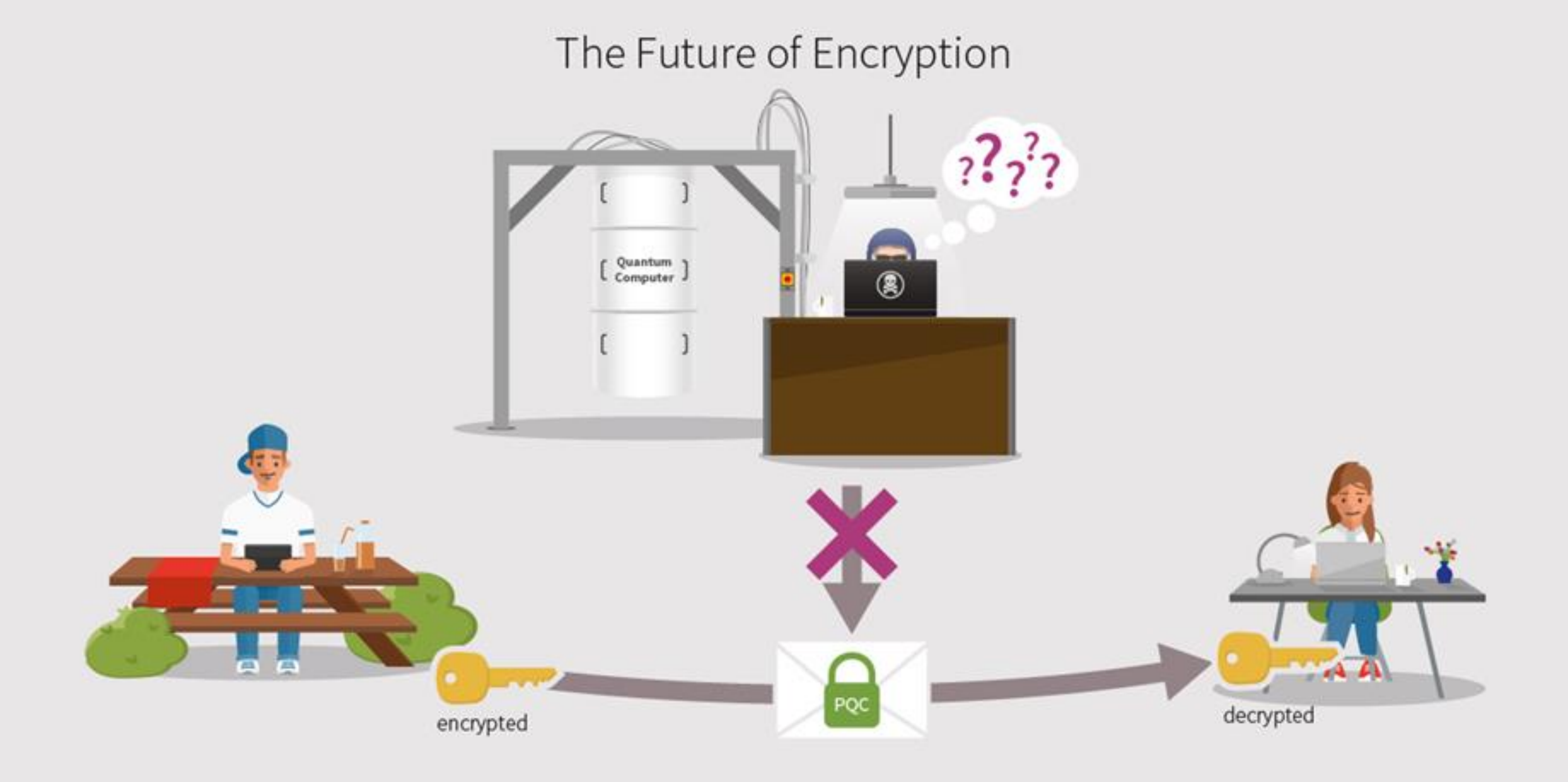
- New conventional cryptography deployable without quantum computers
- Believed to provide security against classical and quantum computer attacks
- Main research field are asymmetric algorithms to replace RSA/ECC

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

As the leading provider of security solutions, Infineon is actively pursuing intensive research on **post-quantum cryptography**

Summary of PQC



Post-quantum crypto: The families

Five popular families known to build post-quantum asymmetric cryptography

Family (assumption)	Signatures	Encryption or Key Exchange	Description
Hash-based	x	-	› Based on security of symmetric hash function; number of signatures limited per public/private key for stateful schemes
Multivariate Quadratic-based	x	- (*)	› Based on multivariate polynomial equations; large public keys (27.9 kBytes to 75 kBytes); some schemes broken
Code-based	- (*)	x	› Old (1978) and trusted but large public-keys; less trust in more efficient variants (e.g., QC-MDPC)
Lattice-based	x	x	› Old proposals (NTRU in 1996) and newer ones (LWE/RLWE); good performance and reasonable sizes for key/signature/ciphertext (~1-4 kBytes)
Isogeny-based	- (*)	x	› Related to ECC (reuse); slow but small ciphertexts/keys; relatively new field of research

(Family/assumption: RSA = factorization assumption; ECC = discrete logarithm assumption)

(*) *Proposals may exist but they are currently not considered competitive*

The NSA's view and the quantum landscape

NSA Announcement

The NSA Information Assurance Directorate (IAD) announced on 19 August 2015 that a transition to post-quantum cryptography is upcoming for US governmental computer systems:

"IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."

Research Landscape

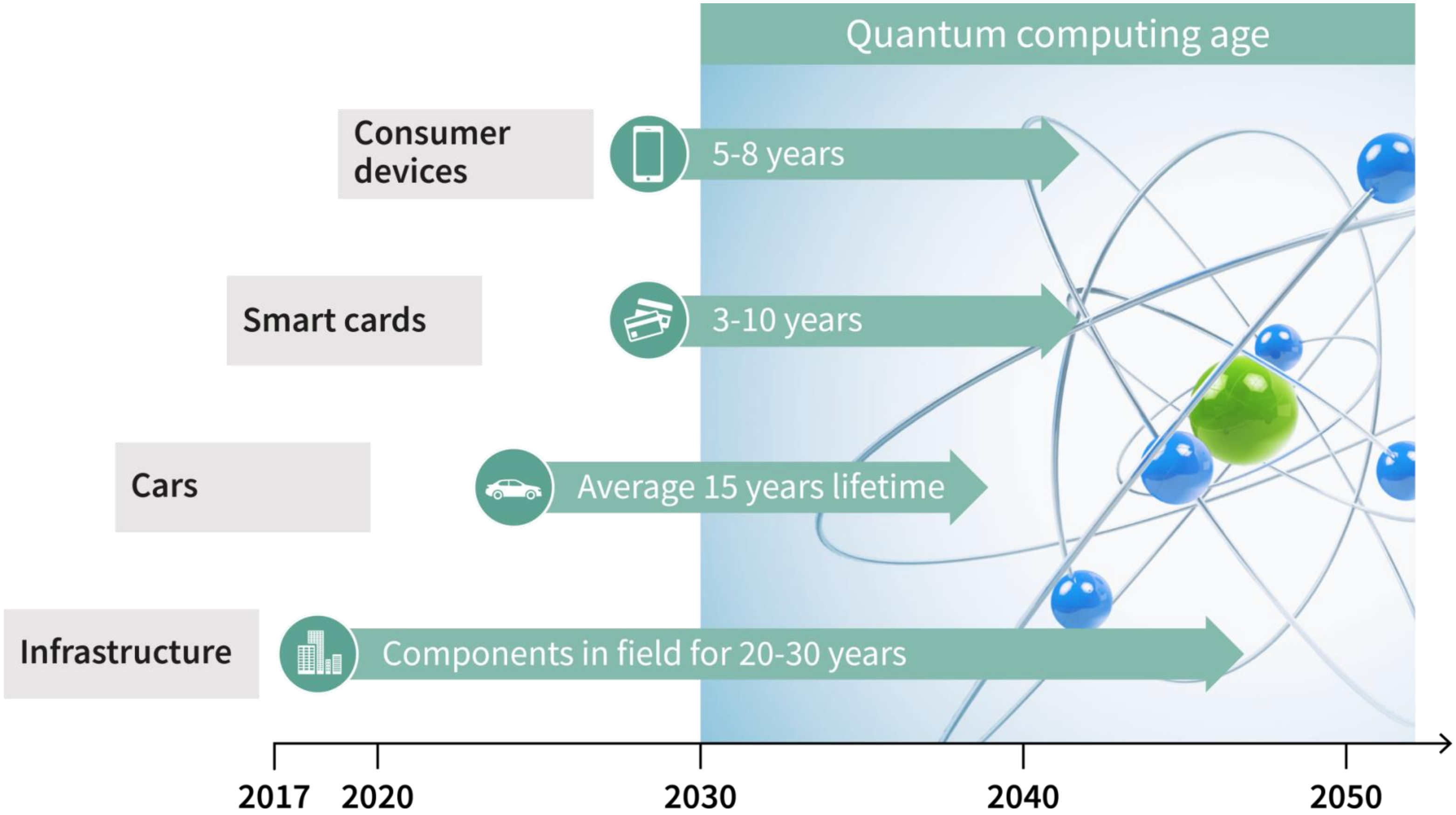
- EU has announced a one billion euro flagship project [1]
- 7000 researchers and 1.5 billion euro funding for quantum technology research in 2015 according to [2]
- NIST got 69 submissions for quantum resistant crypto standardization process
- ETSI is running a quantum safe crypto (QSC) group
- H2020 projects on quantum safe crypto (SAFEcrypto, PQCRYPTO, and now also FutureTPM)

IAD: https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm
[1] https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship
[2] http://qcit.committees.comsoc.org/files/2017/05/Industry-perspectives-of-Quantum-Technologies.pdf

Agenda

1. Introduction to PQC
2. Challenges and standardization
3. PQC on smart cards
4. Conclusion

Applications of post-quantum cryptography

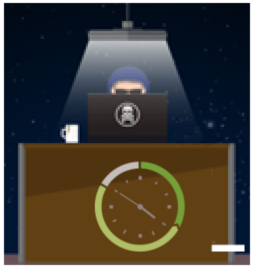


y + *x* + > *z*

y years for retooling and *x* years of required security vs. *z* years until quantum computer

Challenges for real world deployment of PQC

- Cryptanalysis of existing PQ schemes
  - Crypto needs the “test of time”
  - Parameter selection and optimization
  - Search for quantum algorithms to break PQC or accelerate PQC cryptanalysis




- Implementation research
  - Performance optimization (e.g., usage of special instructions)
  - Secured implementation of PQC on various platforms with limited resources
  - Feedback to cryptographers and standardization bodies

- Integration into applications
  - How can PQC replace RSA or ECC in a cost efficient manner in large scale infrastructure
  - Do we have to change the applications?
  - Introduction of crypto agility

Google's experiment:
New Hope (lattice-based PQC) in Chrome

"Post-quantum key exchange – a new hope"	
	Paper by Erdem Alkim (RU Nijmegen), Léo Ducas (CWI Amsterdam), Thomas Pöppelmann (IFX), Peter Schwabe (RU Nijmegen) at USENIX Security'16
	Key-exchange scheme based on ideal lattices with approx. 256-bit security
	Diffie-Hellman-like protocol to protect confidentiality of session keys

Google

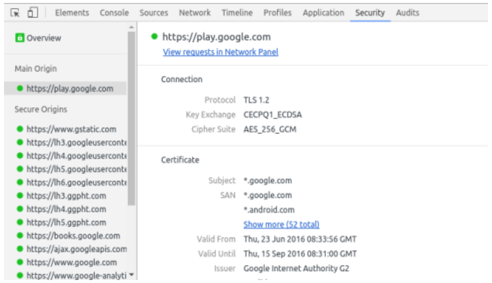
Announcement of the experiment (June 2016)

"Today (June 2016) we're announcing an experiment in Chrome where a small fraction of connections between desktop Chrome and Google's servers will use a post-quantum key-exchange algorithm in addition to the elliptic-curve key-exchange algorithm that would typically be used."

Results of the experiment (December 2016)

"<u>We did not find any unexpected impediment to deploying something like NewHope</u>. There were no reported problems caused by enabling it… It's likely that TLS will want a post-quantum key-agreement in the future but a more multilateral approach is preferable for something intended to be more than an experiment."

New Hope + ECDH



Examples of implementations

Post-quantum key exchange – a new hope (Alkim, Ducas, Pöppelmann and Schwabe)

New Hope key exchange on Intel CPUs

- Reference C implementation and optimized assembly implementation
- Transmits roughly 2000 bytes in each direction

Operation	Reference	Optimized
Key generation (server)	0.128 ms	0.044 ms
Key gen + shared key (client)	0.192 ms	0.056 ms
Shared key (server)	0.043 ms	0.0095 ms

Assuming a CPU @ 2 GHz (0.056 ms => 17800 executions/s)
Exemplary EC Diffie-Hellman (ECDH) implementation is 0.075 ms

A new hope on ARM Cortex-M (Alkim, Jakubeit and Schwabe)

New Hope on a constrained device

- Cortex-M is popular in IoT applications
- Fast without hardware accelerator

Operation	Cortex-M4
Key generation (server)	9.6 ms
Key gen + shared key (client)	14.8 ms
Shared key (server)	1.79 ms

Microcontroller @ 100 MHz (14.8 ms => 67 executions/s)
Exemplary EC Diffie-Hellman (ECDH) implementation is 16 ms

The NIST process

NIST

The National Institute of Standards and Technology (NIST) has started a standardization effort:

- Competition-like process
- Researchers can submit key exchange, PKE, signature schemes
- Selection metrics: “security”, “cost”, “algorithm and implementation characteristics”

The timeline:

- Nov 2017 – Deadline for submissions
- April 12-13, 2018 “First PQC Standardization Conference” with 69 submissions entering first round
- 3-5 years – Analysis phase
- 2 years later – Draft standards ready (2023-2025)

The hard questions:

- How should NIST choose between similar proposals?
- Will other standardization groups besides NIST emerge?
- Is the NIST process too fast or too slow?
- When is the right moment for products with PQC?

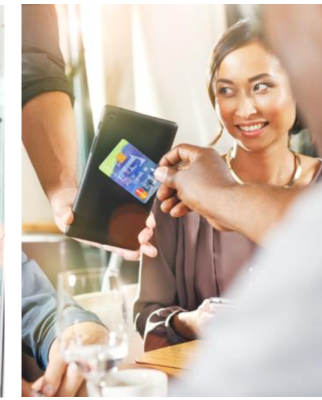
NIST: http://csrc.nist.gov/groups/ST/post-quantum-crypto/

Agenda

1 Introduction to PQC
2 Challenges and standardization
3 PQC on smart cards
4 Conclusion

Smart Cards and Embedded Security

Smart Cards and Embedded Security



Smart card or embedded secure element

- Low-power device sometimes supporting contactless operation used for payment, identification, or embedded security (e.g. TPM)
- Security features (Dual CPU, Error Detection, Alarm Systems) and hardware accelerator for cryptographic operations (e.g., RSA or AES)
- Protects secret key or other information against physical attacks (e.g. power analysis, micro-probing, laser fault injection)

Implementations of PQC needed that aim for secured operation on power and resource constrained device

Demonstrator of post-quantum cryptography

Demonstrator of post-quantum cryptography on a smart card chip

Setup a secured channel

Infineon's contactless smart card

Infineon succeeded to implement New Hope on an Infineon contactless smart card microcontroller

- This chip family is used in many high-security applications like passports
- The New Hope key exchange protects the communication between the smart card and the reader

Post-quantum cryptography is possible on smart cards

Latest research: Protection against differential power analysis (DPA) side-channel attacks

Protecting lattice-based PQC against power analysis attacks [OSPG18]

Implementation results

- Masked lattice-based public-key encryption scheme on a Cortex M4 (similar to NewHope)
- Chosen Ciphertext Attack (CCA) conversion to protect against ciphertext malleability
- Security proof in the probing model to counter basic side-channel attacks

Operation	Cycles on Cortex-M4	Time @100 MHz
Key generation	2.669.559	26 ms
Encryption	4.176.684	42 ms
Decryption (masked)	25.334.493	253 ms

NIST P-256 elliptic curve 81.60.000 cycles (81 ms); for countermeasures add factor 1.5; From "Practical Results of ECC Side Channel Countermeasures on an ARM Cortex M3 Processor", Samotyja and Lemke-Rust

Side-channel protection for real-world usage adds a significant performance overhead

- "textbook" CPA-secured decryption: 163.887 cycles (baseline)
- CCA-secured decryption: 4.416.918 cycles (factor ~**27**)
- CCA-secured and masked decryption: 25.334.493 cycles (factor ~**155**)

[OSPG18] Oder, Schneider, Pöppelmann, Güneysu: Practical CCA2-Secure and Masked Ring-LWE Implementation. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(1): 142-174 (2018)

Latest research: Usage of RSA co-processors for PQC

Enabling the transition towards PQC with existing co-processors [AHHPVW18]

- Implementation of Kyber post-quantum key encapsulation mechanism (KEM) on Infineon SLE78 smart card with 16 Kbyte RAM
- Use RSA co-processor to speed-up lattice-based cryptography
  - Convert polynomials used in lattice-based cryptography to big integers
  - Process big integers on RSA co-processor (big integer multiplier)
  - Convert back to polynomial representation
- CCA-secured Kyber768
  - Key generation in 79.6 ms
  - Encapsulation in 102.4 ms
  - Decapsulation in 132.7 ms

Kronecker substitution

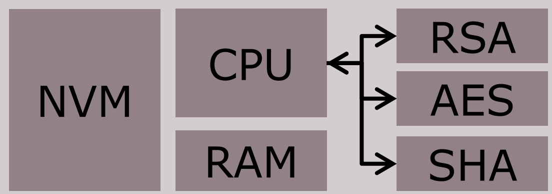
Polynomial multiplication

$$(3x+5)\cdot(2x+8) = 6x^2 + 34x + 40$$

Integer multiplication:

$$305 * 208 = 6\ 34\ 40$$

Chip card hardware



[AHHPVW18] Martin R. Albrecht, Christian Hanser, Andrea Höller, Thomas Pöppelmann, Fernando Virdia, Andreas Wallner: Learning with Errors on RSA Co-Processors. IACR Cryptology ePrint Archive 2018: 425 (2018)

Agenda

1 Introduction to PQC

2 Challenges and standardization

3 PQC on smart cards

4 Conclusion

Conclusion and call to action

Post-quantum cryptography is needed to secure a quantum computer world

A quantum computer world will probably have:

- More cryptographic standards
- Different schemes for encryption, signatures, and key exchange
- Larger keys, signatures and ciphertexts

We have to prepare our systems for the upcoming transition to quantum-safe cryptography and for cryptographic agility in general

Thank you for your attention!

Any questions?

http://www.infineon.com/pqc

pqc@infineon.com

https://futuretpm.eu/

Part of your life. Part of tomorrow.

Infineon