SCIENCES SORBONNE UNIVERSITÉ

THALES
Building a future we can all trust

Implementations of Post-Quantum Cryptography Algorithms Secured Against Physical Attacks

CALLE VIERA Andersson
Director : VERGNAUD Damien
Supervisor: BERZATI Alexandre
PhD. Session CARDIS 2023, 16 Nov. 2023

[1] Thales DIS, France
[2] Sorbonne Université, France

Context

Shor's **quantum algorithm** can **break** standard public key cryptosystems (based on **integer factorization** and **discrete logarithm**), in polynomial time

Context

Shor's **quantum algorithm** can **break** standard public key cryptosystems (based on **integer factorization** and **discrete logarithm**), in polynomial time

NIST: National Institute of Standards and Technology

- 2017: International competition to standardized PQC public-key algorithms
- 2024: First KEM and DSA Standards finalized

Context

Shor's **quantum algorithm** can **break** standard public key cryptosystems (based on **integer factorization** and **discrete logarithm**), in polynomial time

NIST: National Institute of Standards and Technology

- 2017: International competition to standardized PQC public-key algorithms
- 2024: First KEM and DSA Standards finalized

Importance: These algorithms will be implemented **securely** in a variety of use cases

Banking

Personal Data

Communication

PhD. Roadmap

- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)

Study PQC

PhD. Roadmap

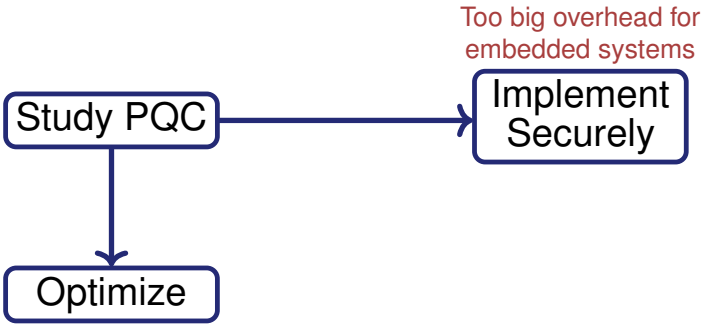
- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)

PhD. Roadmap

- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)

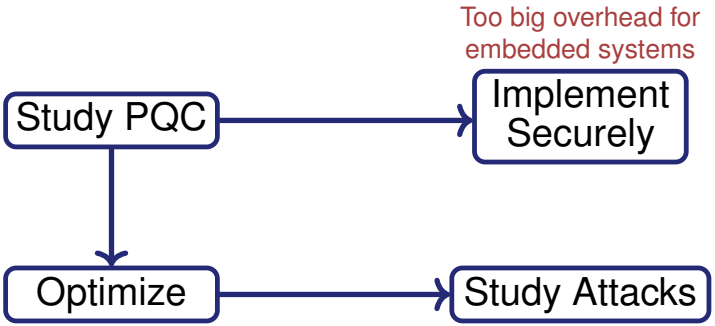
PhD. Roadmap

- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)



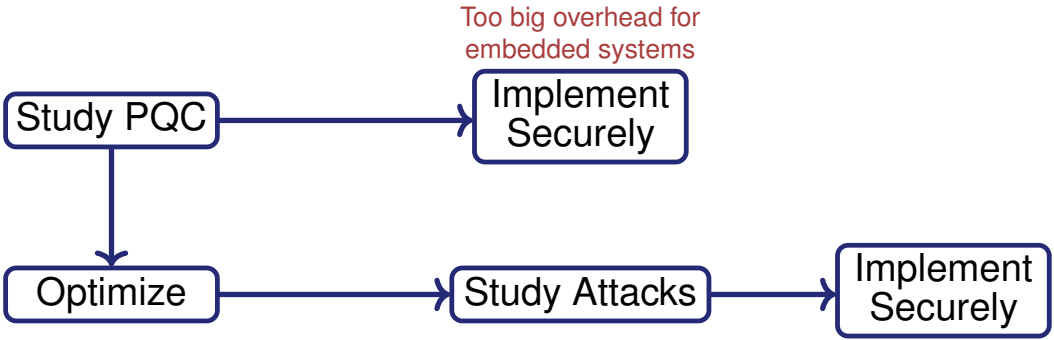
PhD. Roadmap

- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)



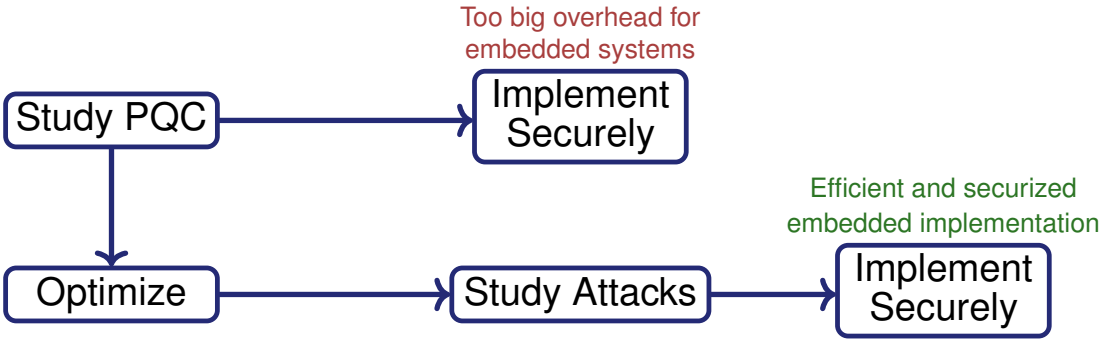
PhD. Roadmap

- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)



PhD. Roadmap

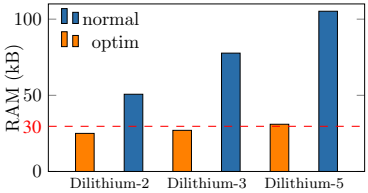
- CALLE VIERA Andersson
- PhD in cryptography from may 2022 to may 2025 (currently 2nd year)
- ALMASTY (Lip6, Sorbonne University) & THALES DIS (Meyreuil)



Optimizing Dilithium Signature Scheme

- Key size storage larger than secure element RAM size
- Reduce RAM consumption for the 3 security levels of Dilithium
- Up to 30% reduction for Dilithium-5
- Conform to standard Dilithium without fancy tricks

- Proprietary Implementation



A Practical Template Attack on Dilithium

Authors: BERZATI Alexandre, CALLE VIERA Andersson, CHARTOUNI Maya, MADEC Steven, VERGNAUD Damien, VIGILANT David

- Exploits zero value leakage during signature execution
- Allows to Recover (partial) secret key and forge signatures
- Confirms the need to protect this intermediate value
- Practical demonstration through Template Attack

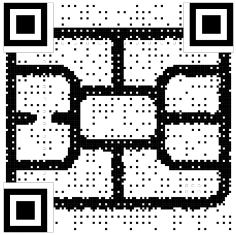
- Published at CHES 2023

ia.cr/2023/050

Fault Attacks sensitivity of Dilithium Verify

Authors: BERZATI Alexandre, CALLE VIERA Andersson, HEYDEMANN Karine

- Sensitivity Analysis of an implmentation of Verify
- Based on the idea to make $ct_1 2^d$ smaller than it is
- 4 faults models considered $\implies$ 3 main scenarios detailed
- Allow to accept false signatures



- Published at CARDIS 2023

sbd-research.nl/cardis-2023

Future Work

- Identify vulnerable operations within PQC schemes
  - SCA/FA on Dilithium/Kyber and NIST round 4 candidates
- Keep studying countermeasures for Dilithium and Kyber
  - Analyze the security of a potential efficient masking of the `Decompose` function
- Study novel approaches for implementing Dilithium and Kyber
  - Balance security and efficiency (changes in arithmetic used for example)

Future Work

- Identify vulnerable operations within PQC schemes
  - SCA/FA on Dilithium/Kyber and NIST round 4 candidates
- Keep studying countermeasures for Dilithium and Kyber
  - Analyze the security of a potential efficient masking of the `Decompose` function
- Study novel approaches for implementing Dilithium and Kyber
  - Balance security and efficiency (changes in arithmetic used for example)

Thank you

Questions?