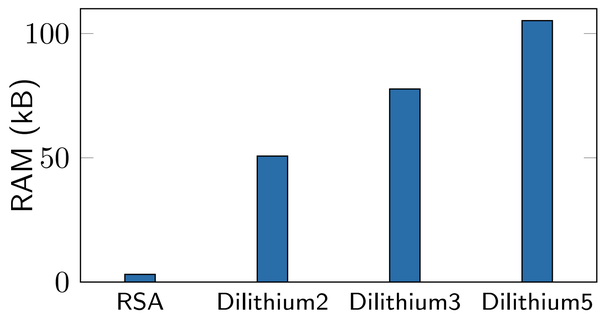
Implementations of Post-Quantum Cryptography Algorithms Secured Against Physical Attacks

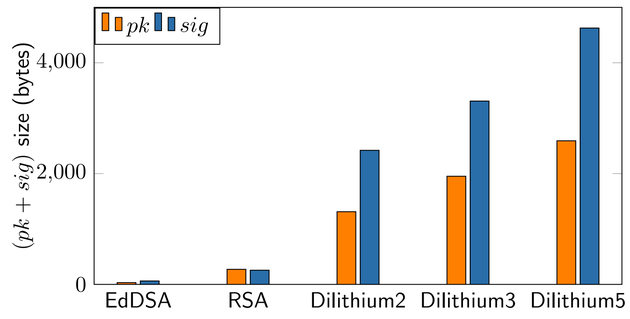
Andersson Calle Viera[1,2]
andersson.calle-viera@thalesgroup.com
[1]Sorbonne Université, Paris, France [2]Thales DIS, Meyreuil, France

Context of Post-Quantum Cryptography (PQC)

- **Quantum computers** threaten current cryptographic protocols $\Longrightarrow$ PQC aims at ensuring long-term security
- **NIST:** standardization of PQC algorithms
- **ML-DSA:** draft from Version 3.1 of Dilithium
- Implementations on embedded platforms:
  - Secured against Side Channel/Fault Attacks (SCA/FA)
  - Efficient regarding storage/speed

How to implement PQC securely?

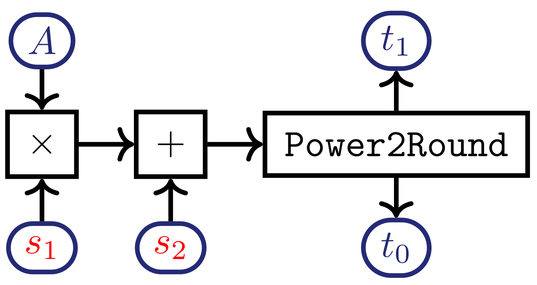




- **PhD. Objectives:** Study PQC | Develop Embedded Implem. | Identify New SCA/FA | Propose Countermeasures

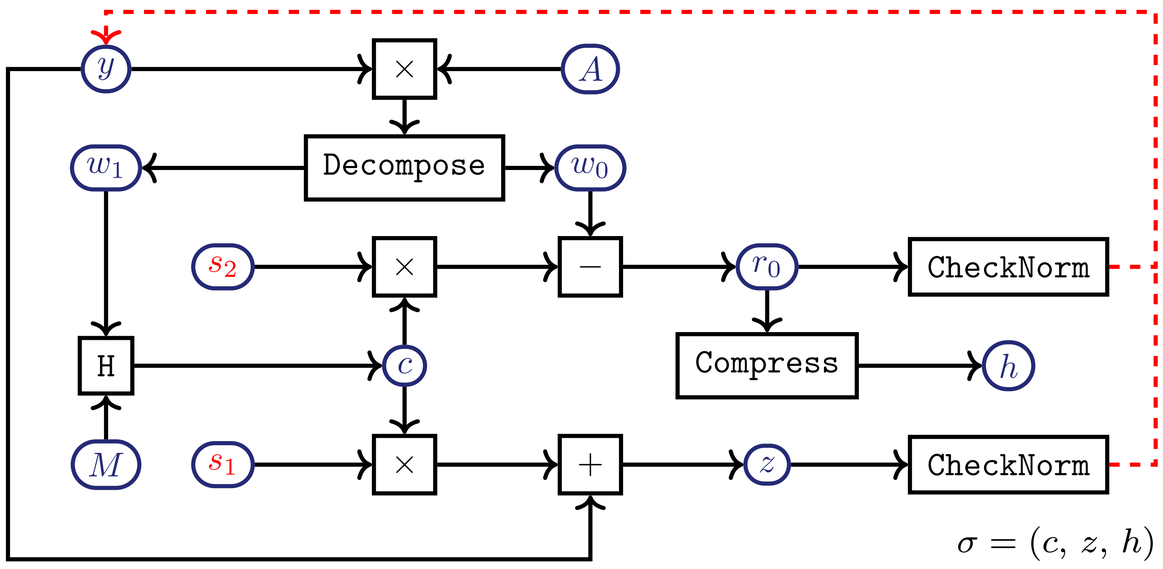
Dilithium Algorithm Description

KeyGen:



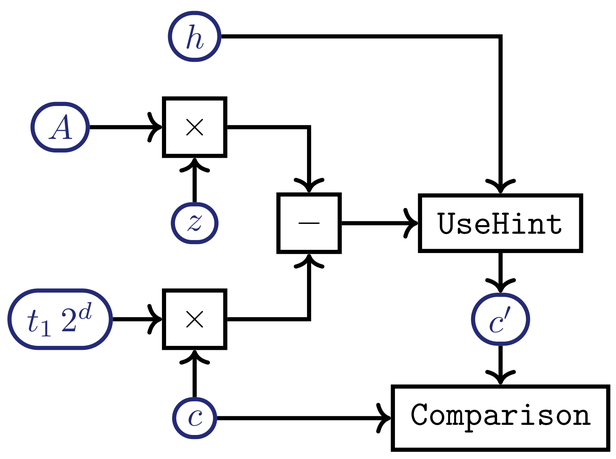
$pk = (A,\ t_1)$, $sk = (A,\ s_1,\ s_2,\ t_0,\ pk)$

Sign(M, sk):



$\sigma = (c,\ z,\ h)$

Verify(pk, M, σ):

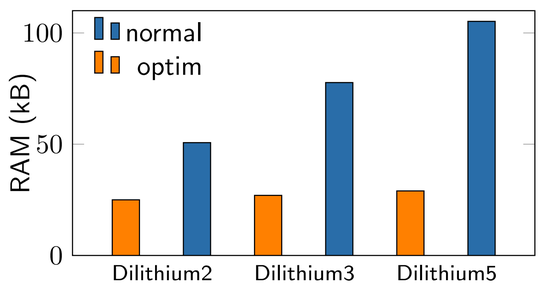


Optimizations

- Too much RAM for embedded systems

How to reduce RAM usage without impacting performances?
(fit all versions under 30 kB)

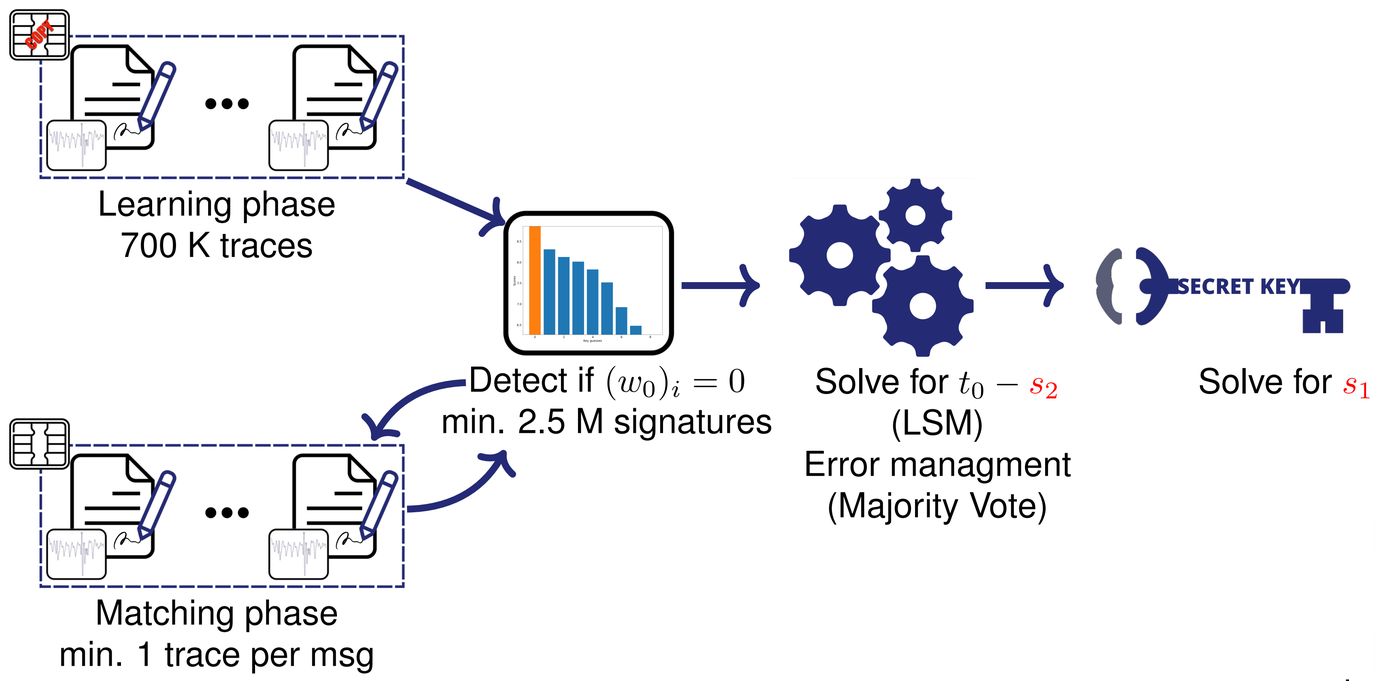
- Proprietary implementation
- Conform to standard Dilithium



- No change in modulus, no change in multiplication method, no code added
- Performances equivalent to standard
- Technique can be applied to Verify

Exploiting Intermediate Value Leakage

- First exploitation of a 0 value leakage on w_0
- Recover (partial) secret key and then forge signatures
- Confirms the need to protect w_0
- Practical demonstration through Template Attack



ia.cr/2023/050

- Simple known countermeasure to protect w_0 (shuffling, masking)

Fault Attacks Sensitivity of Dilithium Verify

- Sensitivity analysis of OpenSource Dilithium Verify implementation (PQClean)

Are public parameters vulnerable to FA?

- 4 Fault Models considered: Skipping, Test-inversion, Zeroizing, Randomization

Scenario 1: Sampling of c
Scenario 2: Shift by d

$$Az \ominus ct_1 2^d$$

Scenario 3: Subtraction
2 other scenarios in the paper

- Main Observation: $ct_1 2^d$ shouldn't be allowed to be small in practice
- Set of Countermeasures introduced with potentially small overhead

sbd-research.nl/cardis-2023

Future Work

Countermeasures
- Evaluate possible countermeasures for Dilithium/Kyber

Attacks
- Potential SCA/FA on Lattice-Based Crypto and NIST round 4 candidates

Optimizations
- Novel approaches in arithmetic to implement Dilithium and Kyber