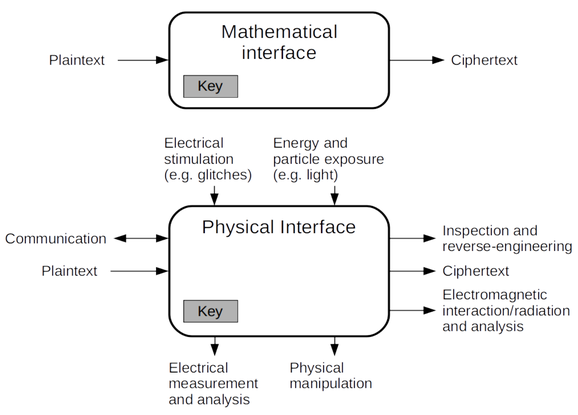
Performance and Physical Attack Security of Lattice-Based Cryptography

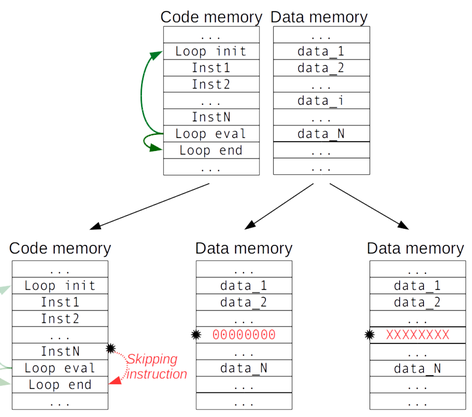
Felipe Valencia
Faculty of Informatics
Università della Svizzera Italiana
valena@usi.ch

- Quantum computer threatens public key cryptography
- Lattice-Based cryptography resists classical and quantum attacks
- Physical attacks are a main concern for embedded systems and internet of things

Efficient and secure implementation of lattice-based cryptography is needed.



Fault attacks on RLWE encryption



Algorithm 2 RLWE Encryption

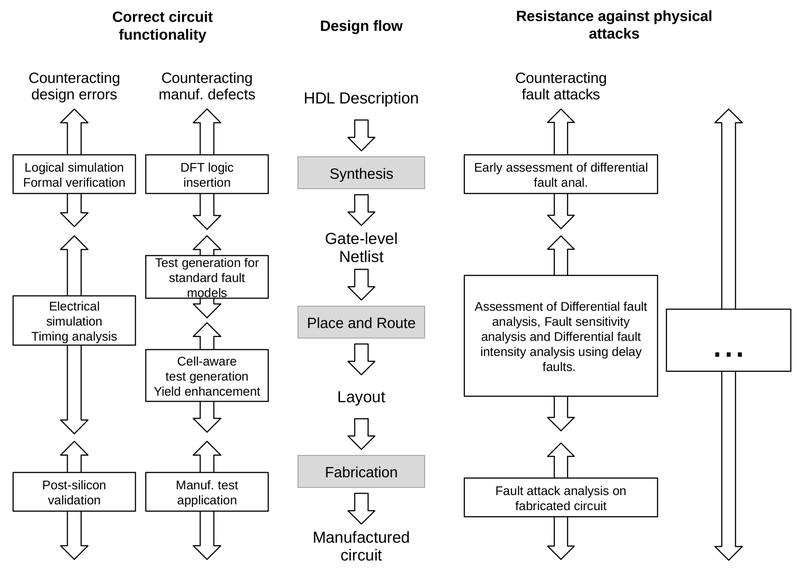
Require: Access to a global constant **a** that was uniformly chosen from R_q and to a message $\mu \in \{0,1\}^n$

1: **function** $RLWE_{enc}(pk, \mu)$
2: $e_1, e_2, e_3 \leftarrow D_{\mathbb{Z}^n,\sigma}$
3: $\bar{m} \leftarrow Encode(\mu)$
4: $c_1 \leftarrow ae_1 + e_2$
5: $c_2 \leftarrow pke_1 + e_3 + \bar{m}$
6: **return** (c_1, c_2)
7: **end function**

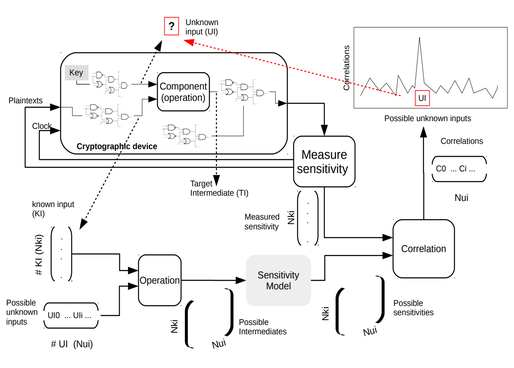
Algorithm 3 RLWE Decryption

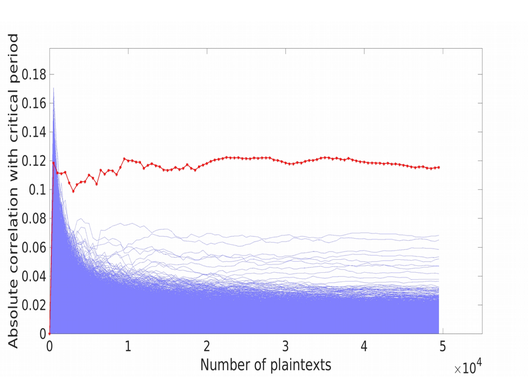
1: **function** $RLWE_{dec}(c_1, c_2, sk)$
2: $\mu' \leftarrow Decode(c_1 sk + c_2)$
3: **return** μ'
4: **end function**

Methodology for early analysis of fault attacks vulnerabilities



Fault Sensitive Analysis on arithmetic operators of LBC

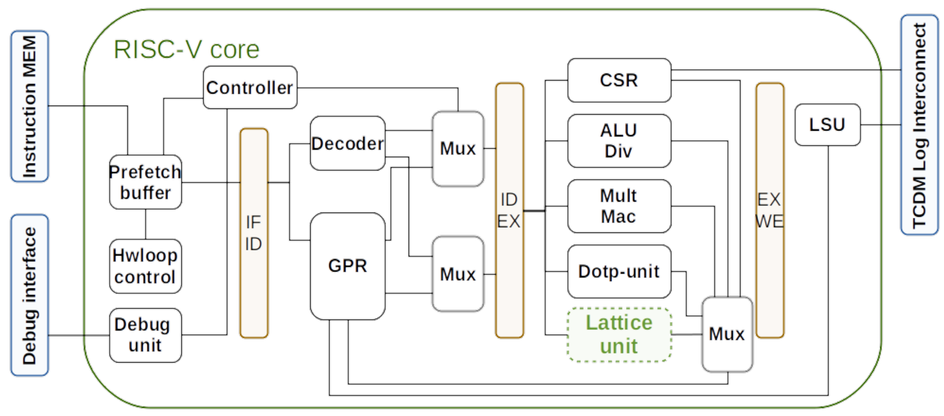




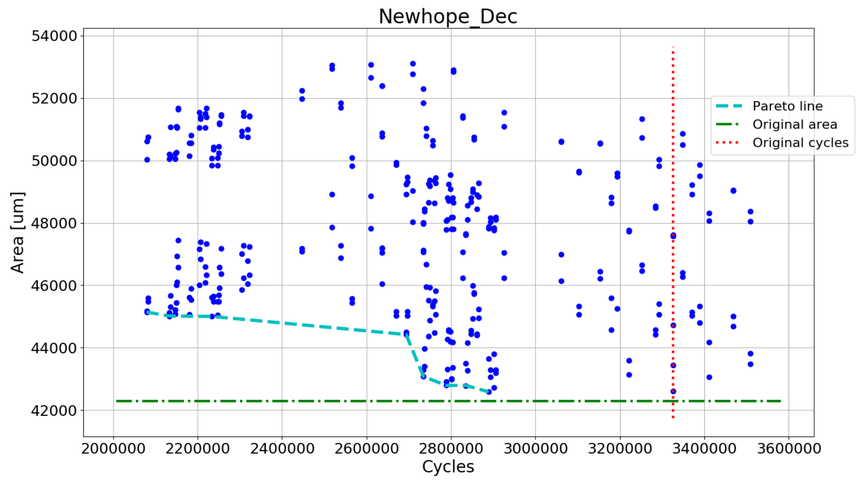
Module	HW	Min	Mean	Max
Mult15	++	−−	−−	−−
MultMod12289	−−	++	++	+
MultMod32768	−	−	+	+
MultMod8192	−−	−−	+	+
Add15	−−	−	−−	−−
AddMod12289	−−	−−	+	+
AddMod32768	−−	−	+	+
AddMod8192	−−	−−	−	−
LotusDec	++	−−	−−	−−

- ++ : Correlation of correct key is the highest, much higher that second key.
- + : Correlation of correct key is the highest, close to second key.
- − : Correlation of correct key is NOT the highest, but it is in first positions.
- −− : Correlation of correct key is NOT the highest and it is NOT in first positions.

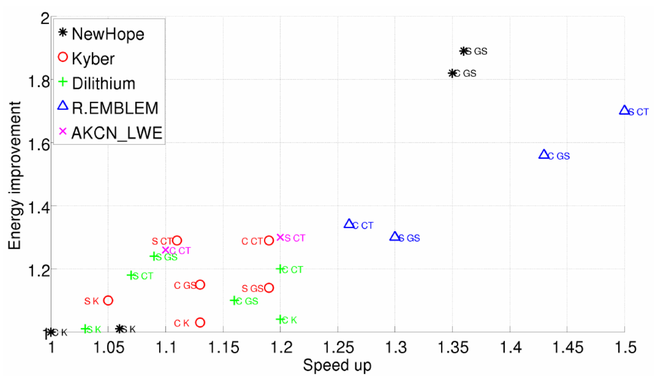
Instruction set extension for LBC



Pipeline: Prefetch Decode Execute Memory



Flexible accelerators for RLWE post-quantum cryptography



This thesis explores the vulnerabilities of RLWE encryption to different fault attacks. We have also evaluated vulnerability of hardware modules used in LBC and Lotus encryption circuit against Fault Sensitivity Analysis. A methodology and framework for early assessment of the vulnerabilities against fault attacks has been developed.

We show the design of cache-based hardware accelerators for LBC and an instruction set extension. We focus on keccak and NTT functions. The results present the trade-off between execution time improvements and cost (area/energy).