ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

XXXV Cycle

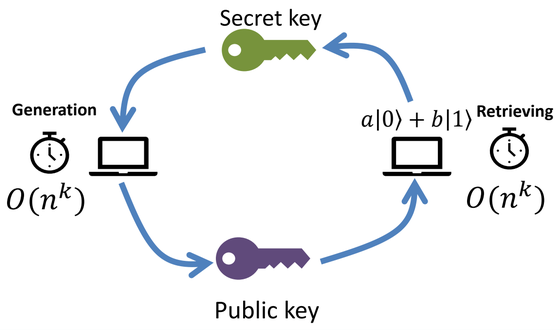
Architectures for Post Quantum Cryptography

Kristjane Koleci

Supervisors: Profs. Maurizio Martina, Guido Masera

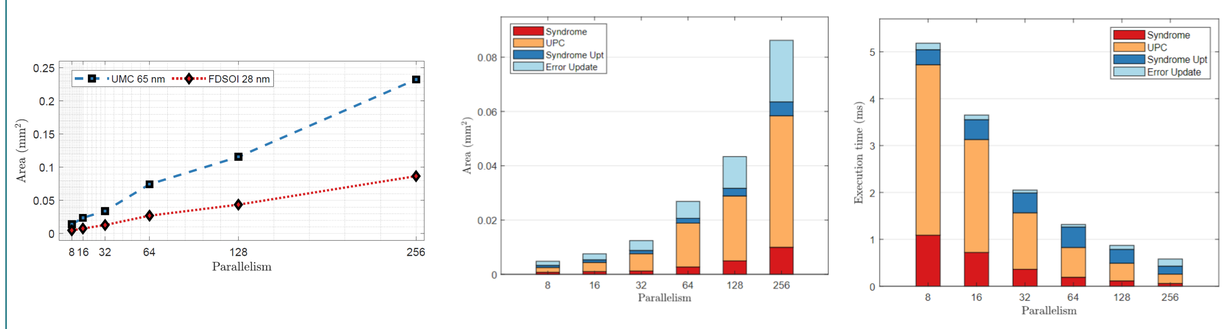
Research context and motivation

- The Quantum Era is approaching thanks to researchers from all over the world that are working hard to make this future the present. The improvement in the computational capabilities that such computers could bring is huge and could solve problems that nowadays seems impossible, but the drawbacks could be that effect on the security of algorithms that we adopt.
- Post Quantum Cryptography (PQC) aims to provide a solution to this threat by proposing a new class of algorithms for Asymmetric Cryptography and Key Encapsulation that are Quantum Secure.
- The most know NP-hard problems are Code-based Crytosystems, Lattice Based Cryptosystems and recently cryptosystems based on Isogenies.



Novel contributions

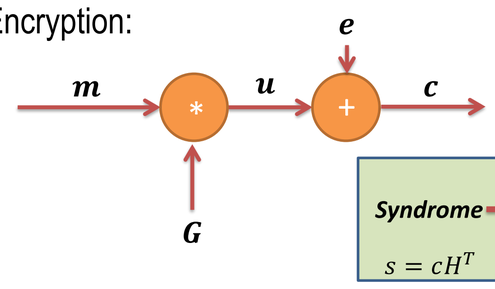
- The Encryption and Decryption have been implemented with a rotation-based multiplier, which is efficiently scalable to different parallelisms in the processing.

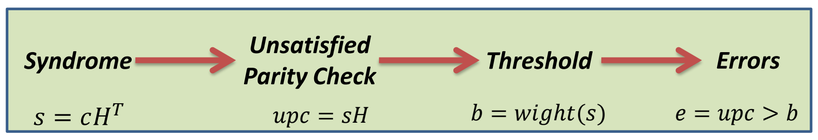


- The architecture has been tested towards a kind of Side-channel Attacks with the study of the simulated power traces of the netlist while the decryption has been run.
- The second main contribution, was the use of and NTT based multiplier in LEDAcrypt/BIKE. This was meant to prove that a convolution-based multiplier usually adopted Lattice-based Cryptosystems is easily adaptable to our case, making such an architecture the core of the PQC Processing for multiple proposals.

Addressed research questions/problems

- The research addressed mainly the FPGA/ASIC implementation of primitives from Code-based Post Quantum Algorithms.
- The Code-based proposals (LEDAcrypt/BIKE) adopts QC-LDPC/MDPC (Quasi-Cyclic Low/Moderate Density Parity Check) codes, thanks to their structure and dimension it is possible to efficiently compute the primitives. The drawback is the presence of polynomial with a huge dimension, (>10^4), which makes most of techniques adopted to process these variable, infeasible in most of the applications.
- The Encryption and Decryption adopts as Secret Key (SK) the Parity Check Matrix for the Decryption and the as Public Key (PK) the Generator Matrix is employed for the Encryption:





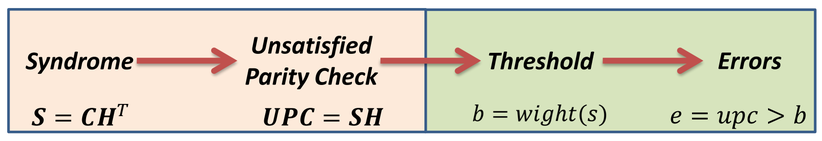
- The most common operation is the multiplication by a QC matrix with full density in case of Encryption and Moderately Sparse for the Decryption.
- Such product can be handled in different ways, but with the state of art of multipliers the execution time and area occupation of the Architecture makes in infeasible when compared to classic algorithms.
- The second open problem for these architectures, is their security. The algorithms provide the security towards known attacks that guess the SK from the PK, but a different method can be applied to break the asymmetry. Side-channel attacks can be applied to a chip running a primitive and thanks to their measures of execution time and power consumption can easily derive the SK.

Adopted methodologies/Results

- The product with a vector by a Quasi Cyclic Matrix has been studied and handled as an improved Schoolbook multiplier for sparse and dense vectors.
- The NTT-based multiplier implemented *as it is* with additional complexity reduction for sparse polynomials, turned out no to be the most efficient way to compute such products, but the Decoder processing has been slightly modified to make it competitive with the other proposals.

$$X(k) = \sum_{j=0}^{N/2-1} x(2j)\alpha^{(2j)k} \mod P + \sum_{j=0}^{N/2-1} x(2j+1)\alpha^{(2j+1)k} \mod P$$

- The quantities are computed in the number domain in order to reduce the time lost during the two consecutive transform/antitransform, the possibility to perform some computations in the number domain is possible thanks to the properties of the transform.



- The simulated Side-channel Attack applied to the Schoolbook multiplier of the Decoder, with the use of Synopsys Prime Time, Modelsim and a mathematical model written in Matlab allowed to derive the power consumption during the decryption and correlated it with the expected value, this process resulted successful in the derivation of the Secret Key.

List of attended classes

- 01QCOKG – Introduzione all'ottica e alle informazioni Quatistiche (20/2/2020, 20)
- 01TCTRV – Photonext: Hands on course on Photonics for Fiber Trans. (24/9/2021, 30)
- 01SFURV – Programmazione scientifica avanzata in matlab (25/5/2020, 28)
- 01QWFBG – Signal Processing: method and algorithms (24/4/2020, 60)
- 01QORRV – Writing Scientific Papers in English (20/2/2020, 15)
- 02LWHRV – Communication(3/10/2020, 5)
- 01UNVRV – Navigating the hiring process: CV, tests, interview(12/5/2021, 2)
- 01UNYRV – Personal Branding(11/5/2021, 1)
- 08IXTRV – Project Management(29/12/2020, 5)
- 01ISRV – Public Speaking(7/10/2020, 5)
- 01SYBRV – Research Integrity(13/5/2021, 5)
- 01UNXRV – Thinking out of the box(11/3/2021, 1)
- 01SWPRV– Time Management(12/10/2020, 2)

Future work

- The Schoolbook multiplier for Code-based PQC is going to be improved in order to reduce the effect of Side-channel attacks and study potential leakages of the new design.
- The same attack can be applied to the NTT-based multiplier, to show possible problems and overcome them.
- In the end, the NTT-based multiplier, up to now, has been studied for an ASIC and FPGA implementation, in the following this is going to be included in a RISC-V processor in order to have a starting point to develop a processor suitable for multiple PQC primitives.

Submitted and published works

- Koleci, K. , Baldi, M. , Martina, M and Masera, G., "*A Hardware Implementation for Code-based Post-quantum Asymmetric Cryptography*", ITASEC20, Ancona, 2020
- Koleci, K. , Santini, P. , Baldi, M. , Chiaraluce, F. , Martina, M and Masera, G., "*Efficient hardware implementation of the LEDAcrypt Decoder*", IEEE ACCESS, vol. V, no. 9, 2021
- Koleci, K. , Cecchetti, L. , Martina, M. , Masera, G., Ruo Roch, M., ,"*A Side Channel Attack methodology applied to Code-based Post Quantum Cryptography*", ApplePies2022, Genova, 2022

Politecnico di Torino

PhD program in
Electrical, Electronics and Communications Engineering