Abstract

Post-Quantum Cryptography has become popular in recent years due to overcoming the threat posed by Quantum Computers; the field is a branch of Cryptography and aims to provide algorithms that can secure communication even if a quantum computer is employed.

In Post-Quantum Cryptography, the research focuses on algorithms for Asymmetric Cryptography, where the Public Key and a Secret Key pair are employed to secure our data. The main focus of this thesis is Code-based Post-Quantum Cryptographic schemes; the security of such schemes is based on the NP-hardness of decoding a general linear code. The algorithms considered are LEDAcrypt and BIKE; they adopt a variant of the Classic McEliece cryptosystems based on Quasi-Cyclic Moderate Density Parity Check Codes. The scheme has three primitives for Key Generation, Encryption, and Decryption.

The Encryption and Decryption algorithms have been implemented in this thesis; exploring the efficient design of such schemes is fundamental since they require more computational capabilities than preexisting algorithms. In LEDAcrypt and BIKE, the implementation exploits the Quasi-Cyclic structure and sparsity of the matrices to accelerate the decoding while simultaneously trying to keep the total area bounded. The fundamental component of Encryption and Decryption is the multiplier for cyclic matrices. Initially, the direction of the research has been dedicated to designing an efficient multiplier with sparse cyclic matrices. The decoder and encoder have been designed such that they can adapt to the updates on the parameters and the algorithm.

The architecture that has been developed targeted both Field Programmable Gate Arrays (FPGA) and Application Specific Integrated Circuits (ASIC); the design is scalable and thus can adapt to both low-end and high-end applications. The FPGA results for the Artix-7 200 device obtained a decoder latency of 0.6 *ms* and resource utilization of at most 30%. The ASIC design has been synthesized for the STM

FDSOI 28 nm technological node and achieved a latency of $0.15\ ms$ and a total area of $0.0\ 9\mu m^2$.

The decoder is the most critical unit for the security of the whole system since the Secret Key is fundamental in the inner computations. In the present work, a Side-channel attack that exploits the dynamic power consumption is applied to the multiplier in the decoder; the target is the Secret Key which is employed in the multiplication and results in the complete disclosing of the key. The method is applied to real and simulated measurements (from the netlist) to validate a methodology that aims to include a preliminary study of the security during the design phase.

In the last study, the multiplier is implemented as a Number Theoretic Transform-based multiplier due to the analogy between the cyclic matrix product and the cyclic convolution. The unit is fundamental for both the encryption and decryption stage of Code-based Post-Quantum schemes; in this work, has optimized it for both sparse and dense vectors to fully benefit from using the Number Theoretic Transform based multiplier. The result of such an approach has been provided for Field Programmable Gate Arrays (FPGA) and Application Specific Integrated Circuits (ASIC). In the end, it has been showing its flexibility when applied to both encryption and decryption since if we consider as a metric the product of latency and area; it is 3 to 10 times more efficient than other proposals. Moreover, such an approach's flexibility also extends to generic PQC primitives, where such a multiplier is employed.