Fault Attack Resistance of Post Quantum Algorithms

Felipe Valencia and Francesco Regazzoni

ALaRI – USI, Switzerland, email: valena@usi.ch, regazzoni@alari.ch

The aggressive pursuit of scalable quantum computer pushes for the design and the implementation of novel cryptosystems capable of withstand attacks carried out using quantum computational power. Post-quantum cryptography is a vibrant area of research aiming at developing a novel and quantum resistant public key infrastructure. Several possible candidates are currently begin proposed, studied and analyzed by the scientific communities. Candidates include code base algorithm, hash based algorithm, lattice based algorithms, and few other families.

Area and performance of different designs have been explored in a wide number of platforms, including embedded micro-controllers and reconfigurable hardware. However, only few previous works discusses the resistance of post-quantum constructions against physical attacks while few others propose related countermeasures. As a result, the topic, despite fundamental to guarantee security, remains to date largely unexplored.

In this talk we concentrate on fault attacks, a physical attack where the adversary maliciously induces the device into an erroneous state and, subsequently, exploits the wrong behavior to gain information about the secret key [1]. Resistance of some constructions, in particular on lattice based one, have been discussed in previous literature [2,3]. In this presentation, we extend these analysis and we systematically explore the resistance of lattice based implementations against attacks carried out tampering with the clock signal. We carefully analyze several components of R-LWE, and we identify the ones which could be targeted by an adversary aiming at recover the secret key. Each suitable module is then implemented in HDL, and the fault injection attack is practically validated using state of the art logic simulators. We conclude the presentation highlighting possible countermeasures to harden the constructions.

References

1. H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, 2006.
2. N. Bindel, J. Buchmann, and J. Krämer, "Lattice-based signature schemes and their sensitivity to fault attacks," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016 Workshop on*. IEEE, 2016, pp. 63–77.
3. F. Valencia, T. Oder, T. Güneysu, and F. Regazzoni, "Exploring the Vulnerability of R-LWE Encryption to Fault Attacks," *5th Workshop on Cryptography and Security in Computing Systems - Workshop - HiPEAC*, 2018.