PANTACOUR — Physical Attacks: New Targets and Countermeasures

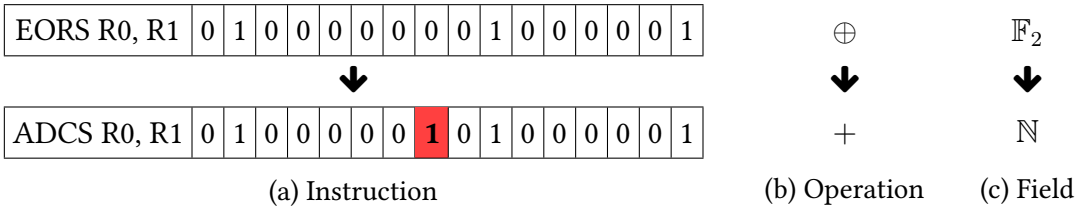
Brice Colombier
Univ Grenoble Alpes, CNRS, Grenoble INP, TIMA, 38000 Grenoble, France

Public-key cryptography is a cornerstone of secure communications. Its security is based on the hardness of number theoretic problems like the prime factorization problem or the discrete logarithm problem. In the classical computing paradigm, no efficient algorithm exists to solve these problems. However, in his work published in 1999, Peter Shor proposed quantum algorithms that can solve these problems in polynomial time. While the practical realisation of a large-scale quantum computer that can execute these algorithms seemed difficult at the time, the constant advances in engineering make it more and more plausible every day.

To tackle this issue, the National Institute of Standards and Technology (NIST) started a competition[1] in 2016 for the development of post-quantum cryptography, that is, algorithms that remain hard to break even if an attacker has a quantum computer at their disposal. In the framework of this competition, the security of the proposed algorithms is first theoretically evaluated against cryptanalysis techniques. However, another important aspect to consider is their practical security against physical attacks.

Indeed, these algorithms will be deployed in the field, in embedded systems for example. They will be then subject to physical attacks, which are not carried out against the mathematical structure of a cryptographic algorithm but against its implementation on a physical target, such as a microcontroller or a dedicated integrated circuit.

The first step of the project will consist in evaluating the security of these algorithms against physical attacks. A promising approach has already been identified, which consists in performing the arithmetic operation of addition in the field of natural numbers $\mathbb{N}$ rather than in the finite field $\mathbb{F}_2$ in which addition is an exclusive OR. To this end, we corrupt the microcontroller instruction with a laser shot, setting one of its bits to 1. This is illustrated below in Figure 1. The next step will consist in designing countermeasures against the previously identified attacks and evaluate their efficiency and their cost.



(a) Instruction (b) Operation (c) Field

Figure 1: A modification feasible by laser fault injection, seen at different abstraction levels

This project is the occasion to continue the collaboration with research teams in Laboratoire Hubert Curien in Saint-Étienne and École des Mines de Saint-Étienne in Gardanne.

[1] https://csrc.nist.gov/projects/post-quantum-cryptography