Physical Security of Code-based Cryptosystems based on the Syndrome Decoding Problem

Brice Colombier[1], Vlad-Florin Drăgoi[2], Pierre-Louis Cayrel[3], Vincent Grosso[3]
[1] Univ Grenoble Alpes, CNRS, Grenoble INP, TIMA, 38000 Grenoble, France
brice.colombier@grenoble-inp.fr
[2] Faculty of Exact Sciences, Aurel Vlaicu University, Arad, Romania
vlad.dragoi@uav.ro
[3] Univ Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516
F-42023, Saint-Etienne, France
{pierre.louis.cayrel; vincent.grosso}@univ-st-etienne.fr

Submission to Cryptarchi 2022

Code-based cryptosystems, like the McEliece cryptosystem, published in 1978 [McE78] and the Niederreiter cryptosystem, published in 1986 [Nie86], are among the oldest public-key cryptosystems. Their security is founded on hard problems. One of them is the syndrome decoding problem, which was shown to be NP-hard [BMT78] and is defined as follows:

Inputs: $H \in \mathbb{F}_2^{m \times n}$, $s \in \mathbb{F}_2^m$, t an integer
Output: $e \in \mathbb{F}_2^n$ such that $H.e = s$ with HammingWeight$(e) = t$

Hardware implementations of code-based cryptosystems drew a lot of attention recently with *Classic McEliece* [Alb+20], based on the Niederreiter cryptosystem, being selected as one of the four finalists of the NIST post-quantum cryptography standardisation process in the Key Encapsulation Mechanism category [RKK20; CC21]. This brings up the question of the physical security of these implementations.

In this work, we study the matrix-vector multiplication over $\mathbb{F}_2$ which is used to compute the syndrome s as $H.e = s$. We present two physical attacks, one based on laser fault injection and one on side-channel analysis. These two techniques achieve the same goal of performing the syndrome computation over $\mathbb{N}$ instead of $\mathbb{F}_2$. In this setting, the hard problem on which the security of the cryptosystem is based does not stand anymore. An attacker can then solve the system using a standard linear programming solver. We also present an alternative method to solve the system, more tailored to the specific problem at hand, that performs significantly better from a computational and practical point of view.

This work contributes to the evaluation of post-quantum cryptography algorithms, by considering their physical security, which is a necessary addition to their theoretical evaluation with cryptanalysis.

References

[Alb+20] M. R. Albrecht et al. *Classic McEliece*. Tech. rep. National Institute of Standards and Technology, 2020.

[BMT78] E. R. Berlekamp et al. "On the inherent intractability of certain coding problems (Corresp.)" In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386.

[CC21] M.-S. Chen et al. "Classic McEliece on the ARM Cortex-M4". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.3 (2021), pp. 125–148.

[McE78] R. J. McEliece. *A public-key cryptosystem based on algebraic coding theory*. The Deep Space Network Progress Report 42-44. Jet Propulsion Laboratory, California Institute of Technology, 1978, pp. 114–116.

[Nie86] H. Niederreiter. "Knapsack-Type Cryptosystems and Algebraic Coding Theory". In: *Problems of Control and Information Theory* 15.2 (1986), pp. 159–166.

[RKK20] J. Roth et al. "Classic McEliece Implementation with Low Memory Footprint". In: *International Conference on Smart Card Research and Advanced Applications*. Vol. 12609. Springer, 2020, pp. 34–49.