Side-channel Information Leakage of the Syndrome Computation in Code-Based Cryptography (Work in progress)

Tania Richmond[1,4], Benoît Gérard[2,4], Annelie Heuser[3,4] and Axel Legay[1,4]

[1] Inria Rennes - Bretagne Atlantique, France
[2] DGA.MI, France
[3] CNRS, France
[4] IRISA, Rennes, France

Abstract. Public-key cryptography (PKC) used in practical real-world application is about to change. The nowadays used PKC schemes based on number theory (like integer factorization or discret logarithm problems) will not be secure in the quantum area [Sho97]. However, recently proposed schemes are based on problems for which no classical or quantum algorithm exist to solve them in polynomial time. So-called post-quantum cryptography (PQC) is mainly classified into code-based cryptography (CBC), lattice-, hash-, multivariate- and isogeny-based cryptography.

In this work we focus on CBC. The first PKC based on error-correcting codes was proposed by McEliece in 1978 using binary Goppa codes [McE78]. A dual version was then proposed by Niederreiter in 1986 using generalized Reed-Solomon (GRS) codes [Nie86]. Since then, many variants using different families of codes were proposed until 2013. But, all including GRS codes except two were cryptanalyzed because they are too structured. The first exception is for QC-MDPC codes, proposed by Misoczki et al. in [MTSB13]. The second one is for LRPC codes, proposed by Gaborit et al. in [GMRZ13]. LRPC codes are equivalent in Rank metric to QC-MDPC codes in Hamming metric.

Considering Hamming metric, there is always a syndrome computation to do regardless the chosen code. There are different possible methods to compute the syndrome:

- vector-matrix product;
- Fast Fourier Transform (FFT) [Cho17];
- XOR of rotations [Cho16];
- multiplications in a polynomial ring;
- lookup table (and additions) [BS08].

Depending on the chosen method, particular information leakage appears. In this work, we analyze the side-channel resilience of each method. The current state-of-the-art in side-channel analysis of the syndrome computation is given in Table 1.

Keywords: Code-based cryptography, side-channel analysis, syndrome computation

Methods	**Attacks**
vector-matrix product	[HMP10, PRD+15, PRD+16]
Fast Fourier Transform (FFT)	
XOR of rotations	[RHHM17]
multiplications in a polynomial ring	
lookup table (and additions)	

Table 1: SCAs of the syndrome computation

References

BS08. Bhaskar Biswas and Nicolas Sendrier. McEliece cryptosystem implementation: Theory and practice. In Johannes Buchmann and Jintai Ding, editors, *Proceedings of the Second International Workshop on Post-Quantum Cryptography (PQCrypto 2008)*, volume 5299 of *Lecture Notes in Computer Science (LNCS)*, pages 47–62. Springer, Berlin, Heidelberg, 2008.

Cho16. Tung Chou. *QcBits: Constant-Time Small-Key Code-Based Cryptography*, pages 280–300. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

Cho17. Tung Chou. *McBits Revisited*, pages 213–231. Springer International Publishing, Cham, August 2017.

GMRZ13. Philippe Gaborit, Gaétan Murat, Olivier Ruatta, and Gilles Zémor. Low rank parity check codes and their application to cryptography. pages 168–180, 2013.

HMP10. Stefan Heyse, Amir Moradi, and Christof Paar. Practical power analysis attacks on software implementations of McEliece. In Nicolas Sendrier, editor, *Proceedings of the Third international conference on Post-Quantum Cryptography (PQCrypto 2010)*, volume 6061 of *Lecture Notes in Computer Science (LNCS)*, pages 108–125. Springer, Berlin Heidelberg, 2010.

McE78. Robert James McEliece. A public-key cryptosystem based on algebraic coding theory. Technical Report 44, California Inst. Technol., Pasadena, CA, January 1978.

MTSB13. Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *IEEE International Symposium on Information Theory Proceedings (ISIT 2013)*, pages 2069–2073, July 2013.

Nie86. Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of control and information theory*, 15(2):159–166, 1986. PROBLEMY UPRAVLENIYA I TEORII INFORMATSII.

PRD+15. Martin Petrvalský, Tania Richmond, Miloš Drutarovský, Pierre-Louis Cayrel, and Viktor Fischer. Countermeasure against the SPA attack on an embedded McEliece cryptosystem. In *Radioelektronika (RADIOELEKTRONIKA), 2015 25th International Conference*, pages 462–466. IEEE, April 2015.

PRD+16. Martin Petrvalský, Tania Richmond, Miloš Drutarovský, Pierre-Louis Cayrel, and Viktor Fischer. Differential power analysis attack on the secure bit permutation in the McEliece cryptosystem. *RadioElektronika 2016*, pages 132–137, April 2016.

RHHM17. Mélissa Rossi, Mike Hamburg, Michael Hutter, and Mark E. Marson. A side-channel assisted cryptanalytic attack against QcBits. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, pages 3–23, Cham, 2017. Springer International Publishing.

Sho97. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.