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

Tania Richmond*†, Benoît Gérard†‡, Annelie Heuser †§ and Axel Legay*†
* TAMIS team, Inria Rennes - Bretagne Atlantique, France
Email: *{tania.richmond,axel.legay}@inria.fr
† IRISA, Rennes, France
Email: †{benoit.gerard,annelie.heuser}@irisa.fr
‡ DGA.MI, France
§ CNRS, France

***Abstract*—In this paper we provide a side-channel analysis on the syndrome computation done in different ways in code-based cryptography.**

***Index Terms*—Code-based cryptography, side-channel analysis, syndrome computation, Hamming metric**

I. Introduction

Public-key cryptography (PKC) used in practical real-world applications 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 exists 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 (irreducible classical) 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. All, including GRS codes but 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 the Hamming metric, there is always a syndrome computation to do regardless the chosen code (e.g. Goppa code or MDPC code). There are different possible methods to compute the syndrome: vector-matrix product [MS77, Ch. 1, §4]; 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.

II. Background and notations

Definition 1 (Linear code): Let q be a power of a prime p. We call a $[n,k]_q$-linear code any vector subspace of $\mathbb{F}_q^n$ of dimension k over $\mathbb{F}_q$. We denote by $\mathscr{C}$ a linear code.

Definition 2 (Parity-check matrix): A parity-check matrix is a basis of the $\mathscr{C}$ orthonogal. We denote by $\mathcal{H}$ such a matrix.

Notation 1 (Syndrome): Let y be a vector in $\mathbb{F}_q^n$, $\mathscr{C}$ a $[n,k]_q$-linear code and $\mathcal{H}$ a parity-check matrix of $\mathscr{C}$. The column vector S of length $n-k$ given by:

$$S = \mathcal{H} \cdot y^T \tag{1}$$

is called the syndrome of y.

Property 1: For a binary code, if there are errors at locations $a, b, c, \ldots$, so that,

$$e = \overbrace{0\ldots\underset{a}{1}0\ldots\underset{b}{1}0\ldots\underset{c}{1}\ldots0}^{n}$$

then from Equation (1),

$$\begin{aligned} S &= \bigoplus e_i \cdot \mathcal{H}_i \qquad (\text{where } \mathcal{H}_i \text{ is the } i^{th} \text{ column of } \mathcal{H}) \\ &= \mathcal{H}_a \oplus \mathcal{H}_b \oplus \mathcal{H}_c \oplus \ldots \end{aligned}$$

Remark 1: S is called the "syndrome" because it gives the symptoms of the errors.

Remark 2: The syndrome contains all the information needed about the errors.

Problem 1 (Syndrome Decoding (SD) problem): Given $\mathcal{H}$ a $n \times (n-k)$-random matrix, S a random vector in $\mathbb{F}_q^{n-k}$ and $t > 0$ an integer, is there a vector $y \in \mathbb{F}_q^n$ such that $w_H(y) < t$ (where w_H denoted the Hamming weight) for which $\mathcal{H} \cdot y^T = S$?

Remark 3: Problem 1 was proved to be nondeterministic polynomial time (NP)-complete for binary case in [BMvT78] and for q-ary case in [Bar94].

Security assumption for CBC relies mostly on Problem 1.

III. Syndrome computation

The syndrome computation is very important in CBC. In this section, we provide an overview of the different methods that can be used to compute the syndrome.

A. Vector-matrix product

The use of a vector-matrix (or matrix-vector) product to compute the syndrome is the first way to do it [MS77, Ch. 1, §4]. Figure 1 illustrates the well known method and Property 1 in the meantime.

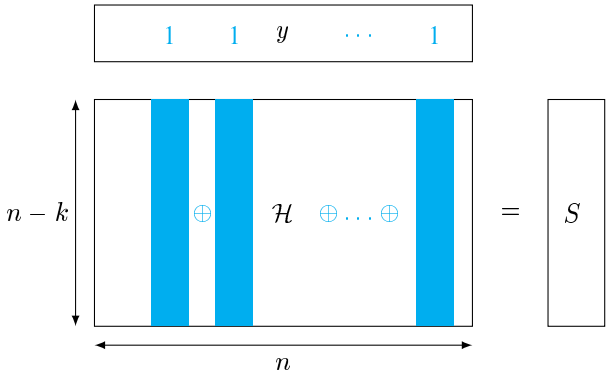

Fig. 1: Syndrome computation by vector-matrix product

B. Fast Fourier Transform (FFT)

To the best of our knowledge, the first use of FFT to compute the syndrome was proposed in [BCS13]. This method is claimed to be fast and in constant time.

C. XOR of rotations

The XOR of rotations to compute the syndrome is only available for parity-check matrices which are (quasi-)cyclic and written over the binary field. Otherwise in characteristic 2, this operation becomes a XOR of weighted rotations. QC-MDPC stands for Quasi-Cyclic Moderate Density Parity-Check. QC-MDPC codes have by definition quasi-cyclic parity-check matrices. Chou proposed in 2016 to compute the syndrome by a XOR of rotations in constant time in software [Cho16]. But this previously proposed in hardware in [vMG14a].

D. Multiplications in a polynomial ring

See the syndrome computation as multiplications in a polynomial ring is nothing more than the generalization of the XOR of rotations (seen just before).

E. Lookup table (and additions)

In HyMES [BS08], Biswas and Sendrier propose to use precomputed lookup tables for multiplications, then additions to write elements of finite fields in additive form.

IV. Side-channel analysis of the syndrome computation

The mathematical proof of the syndrome computation has already been studied [BMvT78], [Bar94], but what about its implementation?
The current state-of-the-art of side-channel analysis for the syndrome computation is given in Table I.

Our first goal was to reproduce the Differential Power Attack proposed in [RHHM17] against the XOR of rotations to compute the syndrome in QcBits [Cho16]. The idea then is to improve this attack (by generalization or with less requirements). Experiments are currently in progress.

The vector-matrix product was analyzed in [HMP10], [PRD+15], [PRD+16] for binary Goppa codes and in [CEvMS16b] for QC-MDPC codes. A masking technique was proposed in [CEvMS16b] over the parity-check matrix for QC-MDPC codes. However, this technique could not have been apply for Goppa codes, so another masking technique over the vector was proposed in [PRD+16].

Lookup tables are usually sensitive to cache-attacks. This has not yet been tested on HyMES [BS08].

In [vMG14a], a FPGA implementation was proposed for QC-MDPC codes. The positions of ones in the first row of the parity-check matrix are stored instead of the full first row. A simple power analysis attack was found few months later because of an overflow that could appear during the rotation of a row [vMG14b]. A differential power analysis was proposed against the XOR of one row of $\mathcal{H}$ (corresponding to a one in the vector) with the syndrome S [CEvMS15], as depicted in Figure 1, then improved in [CEvMS16a].

Finally, as mentioned before, the use of FFT is interesting in the sense that it is done in constant time. Moreover, there is no apparent leakage.

V. Conclusion and perspectives

We present in this paper a work in progess on the information leakage due to the syndrome computation. This operation is mandatory in code-based cryptography. Security of schemes relies on the associated SD problem. We focus here on Hamming metric. In future work, an analysis in rank metric must also be done.

References

[Bar94] S Barg. Some new NP-complete coding problems. *Problemy Peredachi Informatsii*, 30(3):23–28, 1994.

[BCS13] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. McBits: Fast constant-time code-based cryptography. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems (CHES 2013)*, volume 8086 of *Lecture Notes in Computer Science (LNCS)*, pages 250–272. Springer, Berlin, Heidelberg, 2013.

[BMvT78] Elwyn R. Berlekamp, Robert James McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, May 1978.

Methods	Attacks
vector-matrix product [MS77, Ch. 1, §4]	[HMP10], [PRD+15], [PRD+16]
Fast Fourier Transform (FFT) [BCS13], [Cho17]	
XOR of rotations [Cho16]	[RHHM17]
multiplications in a polynomial ring	
lookup table (and additions) [BS08]	

TABLE I: SCAs of the syndrome computation

[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.

[CEvMS15] Cong Chen, Thomas Eisenbarth, Ingo von Maurich, and Rainer Steinwandt. Differential power analysis of a McEliece cryptosystem. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *Applied Cryptography and Network Security (ACNS)*, volume 9092 of *Lecture Notes in Computer Science (LNCS)*, pages 538–556. Springer International Publishing, 2015.

[CEvMS16a] C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt. Horizontal and vertical side channel analysis of a McEliece cryptosystem. *IEEE Transactions on Information Forensics and Security*, 11(6):1093–1105, June 2016.

[CEvMS16b] Cong Chen, Thomas Eisenbarth, Ingo von Maurich, and Rainer Steinwandt. Masking large keys in hardware: A masked implementation of McEliece. *Selected Areas in Cryptography (SAC 2015)*, 9566:293–309, September 2016.

[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.

[MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. North-Holland, 1977.

[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.

[vMG14a] Ingo von Maurich and Tim Güneysu. Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices. In *Design, Automation and Test in Europe Conference and Exhibition (DATE 2014)*, pages 1–6, 3001 Leuven, Belgium, Belgium, March 2014. European Design and Automation Association. http://dl.acm.org/citation.cfm?id=2616606.2616654.

[vMG14b] Ingo von Maurich and Tim Güneysu. Towards side-channel resistant implementations of QC-MDPC McEliece encryption on constrained devices. In Michele Mosca, editor, *Post-Quantum Cryptography*, volume 8772 of *Lecture Notes in Computer Science (LNCS)*, pages 266–282. Springer International Publishing, October 2014.