Hardware attacks against cryptographic protocols based on error-correcting codes

Short Term Scientific Mission (STSM) Report

Tania RICHMOND

January 20, 2015

1 Project

ICT COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices

1.1 Involved Institutions

1.1.1 Home institution

Hubert Curien Laboratory, UMR 5516 CNRS
Jean Monnet University,
18 rue Pr. Lauras
42000 Saint-Etienne,
France

Web page: `http://laboratoirehubertcurien.fr/`

Supervisor: Prof. Viktor Fischer
fischer@univ-st-etienne.fr
`http://webperso.univ-st-etienne.fr/~fischer/`

1.1.2 Host institution

Department of Electronics
and Multimedia Communications
Technical University of Košice,
Park Komenského 13
041 20 Košice
Slovakia

Web page: http://kemt.fei.tuke.sk/en

Supervisor: Doc. Ing. Miloš Drutarovský, CSc
milos.drutarovsky@tuke.sk
`http://www.kemt.fei.tuke.sk/personal/drutarovsky.htm`

2 Visit Details

Visiting researcher: Tania Richmond
Visiting period: From the 15th on September to the 19th on December, in 2014

Mission Statement

I am a PhD student at the Hubert Curien Laboratory Saint-Etienne. I started to work on the PhD thesis in October 2012 and should defend it by the end of 2015. The title of my thesis is "Secure implementation of cryptographic protocols based on error-correcting codes". Besides timing attacks, no hardware attacks have been practically implemented on code-based cryptographic algorithms (some theoretical studies of attacks are known). So the aim of this mission was to investigate all possible hardware attacks and especially fault injection attacks (whether they are feasible).

In this context, my mission in Technical University of Košice had two objectives:

1. study hardware attacks (and in the context of the COST action, especially fault injection attacks) on cryptographic protocols based on error-correcting codes,
2. modify existing algorithms in order to make them more resistant to selected attacks.

3 Scientific Mission Details

3.1 Backgrounds

3.1.1 Code-based cryptography

Cryptography is the art to scramble a message for any undesirable reader. This principle appears in Antiquity. Nowadays, cryptography used in real life is based on number theory, with factorization and discret logarithm problems. But since 1994 [12], the cryptographer community knows that those problems can be solved in reasonable time with a sufficient quantum computer. That is why another hard problem has to be used. One solution can be found in coding theory with the so-called syndrome decoding problem [2]. The first code-based cryptosystem was proposed by McEliece in 1978 [7]. To prove that the McEliece cryptosystem is an interesting alternative to the RSA cryptosystem, it is essential to implement this cryptosystem on embedded devices in order to measure its performances.

3.1.2 Codes

Error-correcting codes were first considered as their name suggest to correct errors in a message sending via a noisy channel. Since 1978, codes are also used in cryptography. Linear codes are the most common because we can generate all codewords thanks to a base (smaller set) so it is easier to describe.
In this work, we are interested by one specific class of linear codes, namely binary Goppa codes [3]. Indeed, McEliece proposed his cryptosystem using this class of codes and until now Goppa codes are resilient against structural attacks. To decode them, we can use the so-called Patterson algorithm [9]. The reader interested by coding theory can find more details in [6].

3.1.3 Problematic

The main problem in my Ph.D. thesis is to find a secure implementation of the McEliece cryptosystem in embedded devices, using the Patterson algorithm (or another Goppa decoding algorithm). Even if the Patterson algorithm was proposed forty years ago, analysis of its resistance against side-channel attacks just started seven years ago and mainly by timing attacks. That is why during this mission, we investigated decryption in the McEliece public-key cryptosystem using Patterson algorithm. We revealed one weakness in an existing countermeasure [17] on the first step in decryption, before decoding, namely the syndrome computation. This computation is very important because in every case (independently from the decoding algorithm), we have to compute the syndrome.

3.2 Side-channel attacks

3.2.1 Definition

In so-called Side-Channel Attack (SCA), an attacker can exploit laws of physical phenomena in order to obtain information contained in channels associated to an implementation (software or hardware). The side-channel does not aim at transmitting voluntarily some information. It leaks information that an observer can interpret. The first one was proposed in 1996 [5]. The most famous attacks are timing attack and power consumption attack but they are not limited to that. Indeed, we can try for example to exploit electromagnetic or acoustic leaks. An attacker can use one of these methods to reduce the work factor to discover the message or in the worst case the private key.

3.2.2 State-of-the-art

In the context of the McEliece cryptosystem, only side-channel attacks against the Patterson algorithm were investigated. Several attacks are timing and message-aimed [17, 13, 1, 15]. Papers targeting the private key by timing attacks are [14, 16]. The second one is against the Goppa polynomial (polynomial used to define Goppa codes), however this target is very difficult to attack during the time of this mission. Only two papers use the Simple Power Analysis (SPA) [4, 8], one against the private key and one against the message. For those reasons, we decided to attack the secret permutation via a power consumption analysis.

As mentionned in [4], one may first think that the best side-channel attack on implementation of McEliece decryption scheme would be a Differential Power Analysis (DPA) to reveal the private key. However, the input (ciphertext) is processed in a bitwise fashion, and contrary to symmetric block ciphers, the private key does not contribute as a parameter of a computation. Moreover, power traces for different ciphertexts would not be aligned to each other based on the computations, and execution time of decryption also varies for different ciphertexts.

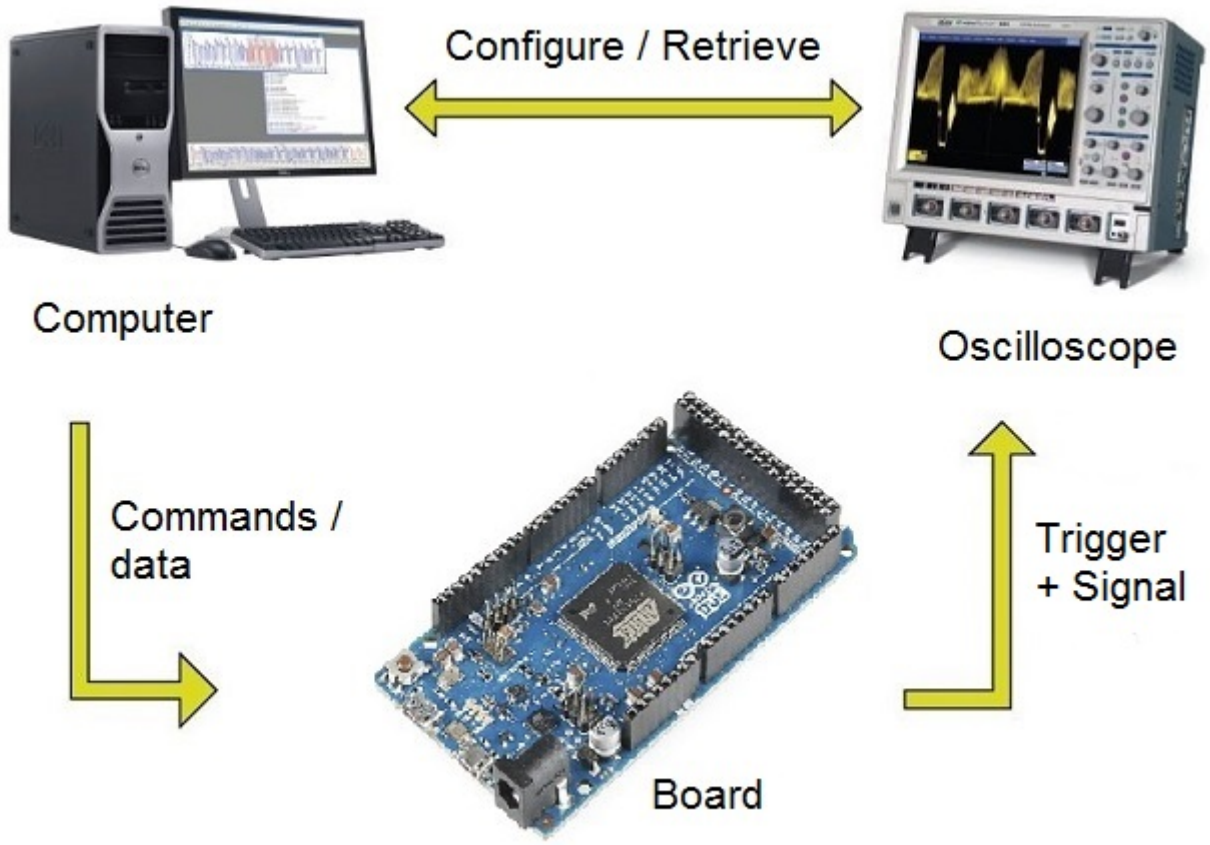

Figure 1: Attack bench scheme

3.3 Main result obtained during this mission

Our aim was to find a new vulnerability in the McEliece cryptosystem, namely one related to information leakages via a power consumption analysis. We studied possible hardware attacks to recover the private key. Attacks against private key are stronger than ones against message. It appeared that the first step in the McEliece decryption could be vulnerable against power consumption analysis. The first thing to do was then to implement this step on an embedded device. We worked with a ARM Cortex-M3 microprocessor. After that, we tried to make the attack described in [4] using the bench in Figure 1.

We used into the bench schematically described in Figure 1 a computer to configure the oscilloscope and to send commands with data to the board. The syndrome computation (critical part) was implemented on a microcontroller on the board. After trigger signal reception, the oscilloscope saved power consumption of the board sending thanks to probes during the syndrome computation. Finally, data from the oscilloscope was retrieved by the computer and analyzed.

Our target was the secret permutation used as a part of the private key in the McEliece cryptosystem. We sent a ciphertext as one-hot (the word composed by one bit equals to one and all other bits equal to zero). We shifted the one into the word and observed the running time during the syndrome computation. Result with a toy example of lenght 8 is given in Figure 2.

In Figure 2, we represented with big red dots bits equal to one into the original permutation matrix and with small blue dots bits equal to one that we found after analysis. That means we correctly discovered the secret permutation in this example. With a realistic example, i.e.

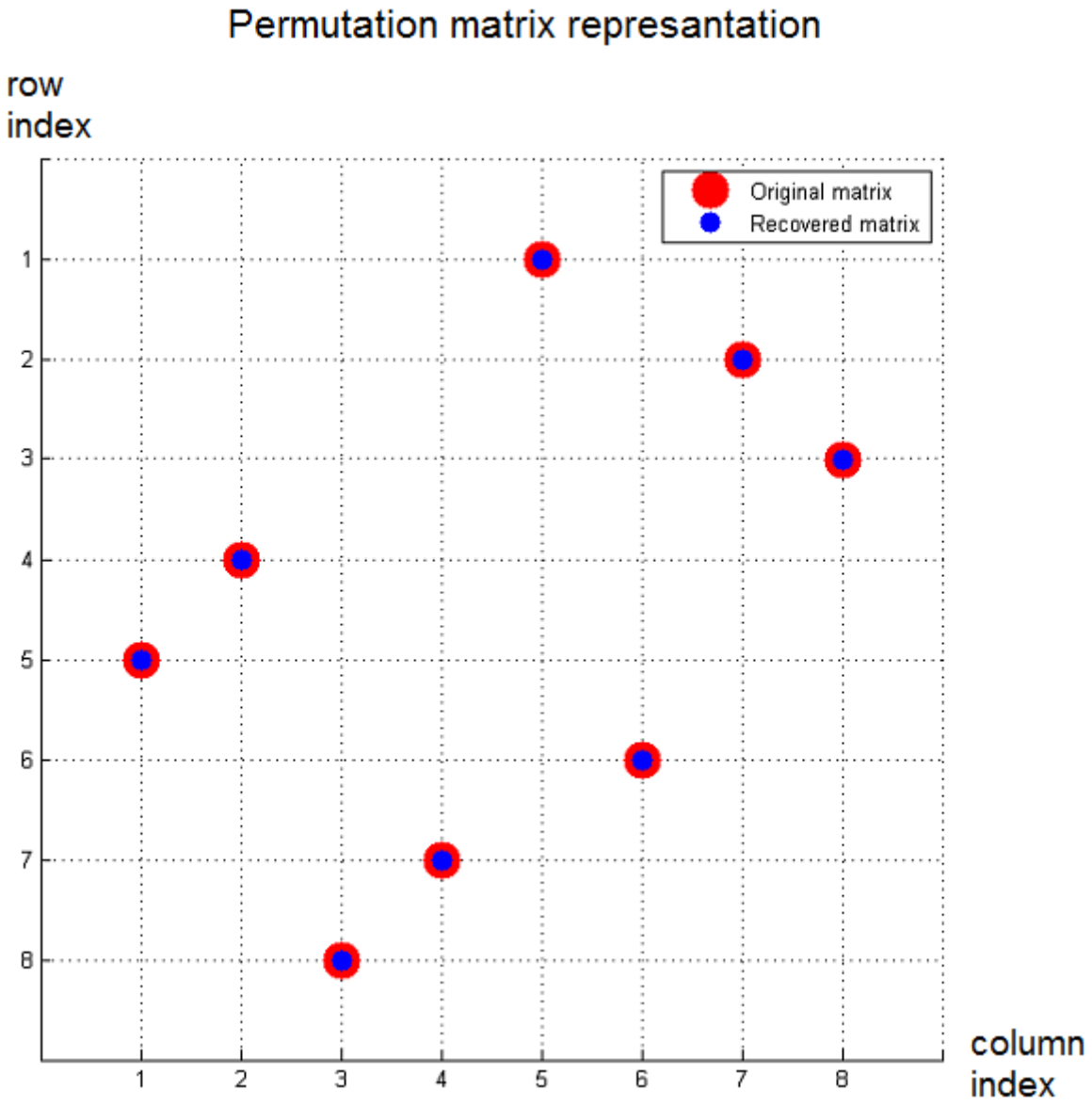

Figure 2: Recovering via timing attack the 8-bit permutation matrix used in the toy example

with a 1024-bit permutation matrix, we succeed with 100% almost all time (99.98% correct one-positions are recovered in worst case).

We made a similar attack with simple power analysis. We got an idea for a countermeasure detailed in [11]. One countermeasure was proposed in [17]. But after measurements with a realistic example, we showed that our countermeasure is better [10]. Clearly, timing attack and simple power analysis are not possible using our countermeasure.

3.4 Publications and conclusion

The main result detailed in the previous section was accepted as a short presentation for the workshop TRUDEVICE 2015. I will present it on March 13th, 2015 [11]. We are also writing an extended version with improvements for the international conference MAREW 2015 [10]. Results obtained during this mission will be integrated into my Ph.D. dissertation and will be very helpful for my thesis.

To conclude about the McEliece cryptosystem implementation on embedded devices, every part of the private key have to be well stored and protected during computations. In the context of the mission, objectives were achieved. Study of hardware attacks on cryptographic protocols based on error-correcting codes was done. In the context of the COST action, the one-hot word can be seen mathematically as a method of a fault injection attack. We also modified existing algorithms in order to make them more resistant to selected attacks providing a new countermeasure. Experience in the host team about embedded devices and power analysis was very helpful to achieve this work.

3.5 Collaboration perspectives

I plan to continue my collaboration with Martin Petrvalský in the first half year at the Hubert Curien Laboratory in order to propose our attack against an hardware implementation on Field-Programmable Gate Array (FPGA). We are also investigating how to perform a differential power analysis on our implementation.

References

[1] Roberto M. Avanzi, Simon Hoerder, Dan Page, and Michael Tunstall. Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. *Journal of Cryptographic Engineering*, 1(4):271–281, November 2011.

[2] 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.

[3] Valerii Denisovich Goppa. A new class of linear error-correcting codes. *Problemy Peredachi Informatsii*, 6(3):24–30, September 1970.

[4] 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.

[5] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Neal Koblitz, editor, *Advances in Cryptology (CRYPTO'96)*, volume 1109 of *Lecture Notes in Computer Science (LNCS)*, pages 104–113, Berlin, Heidelberg, 1996. Springer.

[6] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. North-Holland, 2006.

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

[8] H. Gregor Molter, Marc Stöttinger, Abdulhadi Shoufan, and Falko Strenzke. A simple power analysis attack on a McEliece cryptoprocessor. *Journal of Cryptographic Engineering*, 1(1):29–36, April 2011.

[9] Nicholas J. Patterson. The algebraic decoding of Goppa codes. *IEEE Transactions on Information Theory*, 21(2):203–207, March 1975.

[10] Martin Petrvalský, Tania Richmond, and Miloš Drutarovský. Countermeasure against SPA implementation of an embedded McEliece cryptosystem. Prepared to submission to MAREW 2015.

[11] Tania Richmond, Martin Petrvalský, and Miloš Drutarovský. A side-channel attack against the secret permutation on an embedded McEliece cryptosystem. Accepted in TRUDEVICE, 2015.

[12] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, November 1994.

[13] Abdulhadi Shoufan, Falko Strenzke, H. Gregor Molter, and Marc Stöttinger. A timing attack against Patterson algorithm in the McEliece PKC. In Donghoon Lee and Seokhie Hong, editors, *Proceedings of the 12th International Conference on Information, Security and Cryptology (ICISC 2009)*, volume 5984 of *Lecture Notes in Computer Science (LNCS)*, pages 161–175. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[14] Falko Strenzke. A timing attack against the secret permutation in the McEliece PKC. 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 95–107. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[15] Falko Strenzke. Message-aimed side channel and fault attacks against public key cryptosystems with homomorphic properties. *Journal of Cryptographic Engineering*, 1(4):283–292, 2011.

[16] Falko Strenzke. Timing attacks against the syndrome inversion in code-based cryptosystems. In Philippe Gaborit, editor, *The 5th International Workshop on Post-Quantum Cryptography (PQCrypto 2013)*, volume 7932 of *Lecture Notes in Computer Science (LNCS)*, pages 217–230. Springer, Berlin Heidelberg, 2013. `http://eprint.iacr.org/2011/683`.

[17] Falko Strenzke, Erik Tews, H. Gregor Molter, Raphael Overbeck, and Abdulhadi Shoufan. Side channels in the McEliece PKC. In Johannes Buchmann and Jintai Ding, editors, *The Second International Workshop on Post-Quantum Cryptography (PQCrypto 2008)*, volume 5299 of *Lecture Notes in Computer Science (LNCS)*, pages 216–229. Springer, Berlin Heidelberg, October 2008.