Activity Report NATO Project SfP 984520

Laboratoire Hubert Curien, UMR CNRS 5516,
Université de Lyon,
Bâtiment F 18 rue du professeur Benoît Lauras
42000 Saint-Etienne
France

Tel Aviv, September, 7-10 2014

Team members involved:

• Viktor Fischer	30%
• Pierre-Louis Cayrel	20%
• Tania Richmond	60%
• Alain Aubert	20%
• Nathalie Bochard	20%
• Lilian Bossuet	10%

Main topics we were working on:

- Preparation of a hardware support
- Preparation of DPA attack tools
- Straightforward implementation of the McEliece encryption algorithm using Goppa codes and Patterson, Berlekamp-Massey and Extended Euclidean decoding algorithms in C
- Implementation of the timing attacks on the McEliece algorithm
- Publications

Preparation of a hardware support – two main activities:

- Verification of the usability of a Socrates-type card for our applications according to our discussion in December 2013
- Preparation of the design of the new card suitable for the DPA

Verification of the usability of a Socrates-type card:

- Memory space – Linux uses only 3 % of the memory space
- Memory requirements – the three parts of our McEliece software implementation (key generation, encryption and decryption) are very small comparing to the available memory space
- Building of our proprietary system on the card – we were able to build our system including new peripherals and run the software
- Accessing our proprietary peripherals – we were able to access registers via a light AXI bus and the internal FPGA memory via standard AXI bus
- Availability of drivers – no additional drivers needed
- General conclusion – hardware and software run correctly on the Socrates card

Preparation of the design of the new card suitable for the DPA:

- Design of the block diagram – based on that of the Socrates card
  - Some peripherals were removed
  - Linear power supplies will be used instead of switching power supplies
- Ordering of the main components – most of main components are already available

Preparation of DPA attack tools:

- Localization of the measurement points (available Micronic FPGA modules dedicated to the DPA were used)
- Development of the remote setup of the oscilloscope using scripts
- Remote control of acquisition of traces (including triggering and delay control)
- Implementation of a DPA attack on a full 128-bit AES (40 thousand traces are needed for the full key recovery)

Straightforward implementation of the McEliece encryption algorithm using Goppa codes and Patterson, Berlekamp-Massey and Extended Euclidean decoding algorithms in C:

- Complete source files and documentation are available at: http://www.cayrel.net/?Implementation-of-Goppa-codes

Recent publications:

1. **Polynomial structures in code-based cryptography**
   V. Dragoi, P.-L. Cayrel, B. Colombier and T. Richmond
   Proceedings of Indocrypt 2013, LNCS 8250, pages 286-296, 2013

2. **Cryptography Based on Error Correcting Codes : A Survey**
   M. Repka and P.-L. Cayrel
   Multidisciplinary Perspectives in Cryptology and Information Security, chapter 5, pages 133-156, 2014

3. **Efficient Software Implementations of Code-based Hash Functions and Stream-Ciphers**
   P.-L. Cayrel, M. Meziani, O. Ndiaye et Q. Santos
   WAIFI 2014, to appear

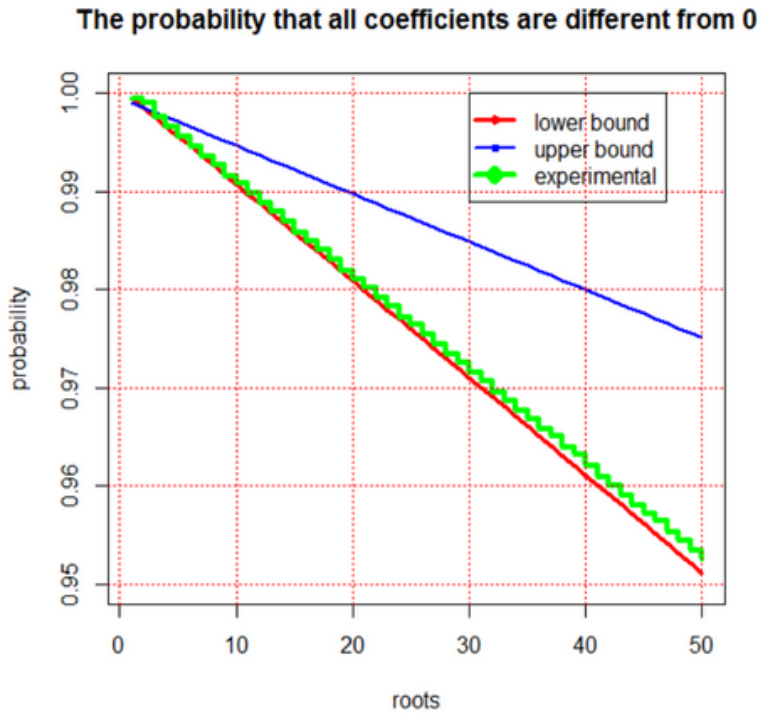
1. **Polynomial structures in code-based cryptography**
   V. Dragoi, P.-L. Cayrel, B. Colombier and T. Richmond
   Proceedings of Indocrypt 2013, LNCS 8250, pages 286-296, 2013

Abstract : *In this article we discuss a probability problem applied in code based cryptography. It is related to the shape of the polynomials with exactly t different roots. We will show that the structure is very dense and the probability that this type of polynomials has at least one coefficient equal to zero is extremelly low. We treated this issue in our research of natural countermeasures to a timing attack against the polynomial evaluation.*

1. **Polynomial structures in code-based cryptography**
   V. Dragoi, P.-L. Cayrel, B. Colombier and T. Richmond
   Proceedings of Indocrypt 2013, LNCS 8250, pages 286-296, 2013

The two bounds:

$$1 + f(n,t) - \left[\frac{t}{n} + (t-1)\mathsf{ub}\right] \leq \mathcal{P}(\bigcap_{i=0}^{t-1} S_i^t \neq 0) \leq 1 + f(n,t) - \left[\frac{t}{n} + (t-1)\mathsf{lb}\right]$$



❷ **Cryptography Based on Error Correcting Codes : A Survey**
M. Repka and P.-L. Cayrel
Multidisciplinary Perspectives in Cryptology and Information Security, chapter 5, pages 133-156, 2014

Abstract : *[...] This chapter surveys the more recent developments in code-based cryptography as well as implementations and side channel attacks. This work also recalls briefly the basic ideas, and provides a roadmap to readers.*

❸ **Efficient Software Implementations of Code-based Hash Functions and Stream-Ciphers**
P.-L. Cayrel, M. Meziani, O. Ndiaye et Q. Santos
WAIFI 2014, to appear

Abstract : *In this work, we present software implementations of two families of cryptographic primitives based on the syndrome decoding problem: hash functions and stream ciphers. We have studied different algorithms, namely, FSB, SFSB, RFSB, SYND, 2SC and XSYND, and improve their performances as software implementations. [...]. We managed to beat the results of the reference implementations when they are available.*

Function	speed in cpb (art.)	speed in cpb (ref.)	speed in cpb (our)	ratio our / art.	ratio our / ref.	Security
FSB-160	257	395.12	110.21	0.43	0.28	100
FSB-224	297	482.51	131.50	0.44	0.27	135
FSB-256	324	528.39	137.41	0.42	0.26	153
FSB-384	423	652.20	203.99	0.48	0.31	215
FSB-512	507	820.87	264.33	0.52	0.32	285
SFSB-160	160	286.20	79.82	0.50	0.28	86
SFSB-224	201	422.91	99.92	0.50	0.24	114
SFSB-384	183	604.19	172.65	0.94	0.29	129
RFSB-509	13.62	22.82	17.26	1.27	0.76	142

Function	speed in cpb (art.)	speed in cpb (ref.)	speed in cpb (our)	ratio our / art.	ratio our / ref	Security
SYND-64	22	-	23.88	1.09	-	71
SYND-96	46	-	29.91	0.65	-	102
SYND-128	27	108.08	30.27	1.12	0.28	131
SYND-192	47	-	53.80	1.14	-	191
SYND-256	53	280.76	41.50	0.78	0.15	252
SYND-512	83	430.36	149.94	1.81	0.35	493
2SC-144	37	298.97	25.18	0.68	0.08	80
2SC-208	47	387.55	33.22	0.71	0.09	170
2SC-352	72	605.61	80.05	1.11	0.13	366
XSYND-509	-	-	15.25	-	-	-

Other realisations :

- Update of the bibliography dealing with code-based cryptography.

- T. Richmond had two talks untitled *Towards a Secure Implementation of a Goppa Decoder* – one at Cryptarchi 2013 and one at JC2S2 2013.