Activity report NATO project

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

May, 2-7 2015

Team members involved:

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

Works done:

- Development of the Side Channel Attack (SCA) tools
- Security analysis of authentication protocols based on error correcting codes
- Enhancement of authentication protocols based on error correcting codes
- Proposition of a Simple power analysis (SPA) side channel attack (SCA) on McEliece decryption
- Countermeasure against proposed SPA side channel attack
- Design of FPGA-based evaluation boards dedicated to SCA using (Microsemi Smart Fusion 2 and Altera Cyclone V SoC FPGA)

Recent publications:

1. **Weaknesses in Two RFID Authentication Protocols**
   N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed
   Proceedings of C2SI 2015, to appear, LNCS xxxx, 2015

2. **Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem**
   M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer
   Poster in MAREW 2015, IEEE, 2015

3. **Improved RFID Authentication Protocol based on Randomized McEliece Cryptosystem**
   N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed
   International Journal of Network Security, to appear, 2015

1. **Weaknesses in Two RFID Authentication Protocols**
   N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed
   Proceedings of C2SI 2015, to appear, LNCS xxxx, 2015

Abstract : *One of the most important challenges related to Radio Frequency Identification (RFID) systems is security. In this paper, we analyze the security and performance of two recent RFID authentication protocols based on two diffeerent code-based cryptography schemes. The first one, proposed by Malek and Miri, is based on randomized McEliece cryptosystem. The second one, proposed by Li et al., is based on Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) McEliece cryptosystem. We provide enough evidence to prove that these two RFID authentication protocols are not secure. Furthermore, we propose an improved protocol that eliminates existing weaknesses in studied protocols.*

❷ **Countermeasure against the SPA Attack on an Embedded McEliece Cryptosystem**
M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel and V. Fischer
Poster in MAREW 2015, IEEE, 2015

Abstract : *[...] a novel countermeasure against a simple power analysis based side channel attack on a software implementation of the McEliece public key cryptosystem. [...] we attack a straightforward C implementation [...] on an ARM Cortex-M3 microprocessor. Next, we demonstrate on a realistic example that using a "chosen ciphertext attack" method, it is possible to recover the complete secret permutation matrix. We show that this matrix can be completely recovered [...]. Then, we estimate the brute-force attack complexity reduction depending on the knowledge of the permutation matrix. Finally, we propose an efficient software countermeasure having low computational complexity. Of course, we provide all the necessary details regarding the attack implementation and all the consequences of the proposed countermeasure especially in terms of power consumption.*
(Will be presented in the next talk in more details.)

❸ **Improved RFID Authentication Protocol based on Randomized McEliece Cryptosystem**
N. Chikouche, F. Cherif, P.-L. Cayrel and M. Benmohammed
International Journal of Network Security, to appear, 2015

Abstract : *[...] This paper proposes a new mutual authentication protocol in RFID systems based on the randomized McEliece cryptosystem. Our work includes a comparison between the new protocol and different existing protocols based on error-correcting codes in terms of security and performance. We prove the security and privacy properties. The performance of the proposed authentication protocol is analyzed in terms of storage requirement, communicational cost and computational cost.*

Perspectives:

- Acquire power traces from McEliece decryption and their analysis
- Go on towards Differential Power Analysis (DPA) on McEliece decryption and error correcting code-based decryption in general
- Propose efficient countermeasures against proposed attacks

Questions?