



HAL
open science

Countermeasure against the SPA attack on an embedded mceliece cryptosystem

Martin Petrvalsky, Tania Richmond, Miloš Drutarovský, Pierre-Louis Cayrel,
Viktor Fischer

► **To cite this version:**

Martin Petrvalsky, Tania Richmond, Miloš Drutarovský, Pierre-Louis Cayrel, Viktor Fischer. Countermeasure against the SPA attack on an embedded mceliece cryptosystem. Microwave and Radio Electronics Week (MAREW) 2015, Apr 2015, Pardubice, Czech Republic. hal-02019991

HAL Id: hal-02019991

<https://inria.hal.science/hal-02019991>

Submitted on 14 Feb 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Martin Petrvalský¹, Tania Richmond², Miloš Drutarovský¹,
Pierre-Louis Cayrel² and Viktor Fischer²

¹Department of Electronics & Multimedia Communications, Technical University of Kosice

e-mail: {martin.petrvalsky, milos.drutarovsky}@tuke.sk

²Hubert Curien Laboratory, Jean Monnet University

e-mail: {tania.richmond, pierre.louis.cayrel, fischer}@univ-st-etienne.fr

INTRODUCTION

The code-based cryptosystems are very attractive because of their robustness regarding attacks based on the use of quantum computers. The first code-based cryptosystem was proposed by R. McEliece in 1978 [1]. However, it appeared that the code-based cryptosystems are as vulnerable to side channel attacks (SCA) proposed by Kocher in 1996 [2] as other cryptosystems. The first known SCA against the McEliece public key cryptosystem (PKC) appeared in 2008 [3].

MCELIECE PKC

Encryption:

→ Encode message m using generator matrix G : $\bar{c} = m \cdot SGP$

→ Add error vector e to produce ciphertext c : $c = \bar{c} + e$

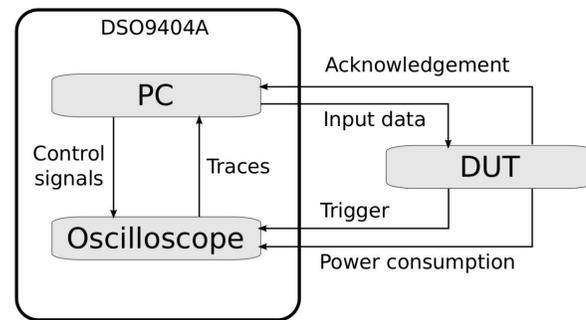
Decryption:

→ *Permute ciphertext c using permutation matrix P^{-1} : $\hat{c} = c \cdot P^{-1}$

→ *Use decoding algorithm: $\hat{m} = DEC(\hat{c})$

→ Unscramble message using scrambling matrix S^{-1} : $m = \hat{m} \cdot S^{-1}$

WORKPLACE & MEASUREMENT



Attacked HW:
ARM Cortex-M3 based
STM32F103 MCU

Oscilloscope:
Agilent Technologies
DSO9404A

PERMUTATION MATRIX REVELATION

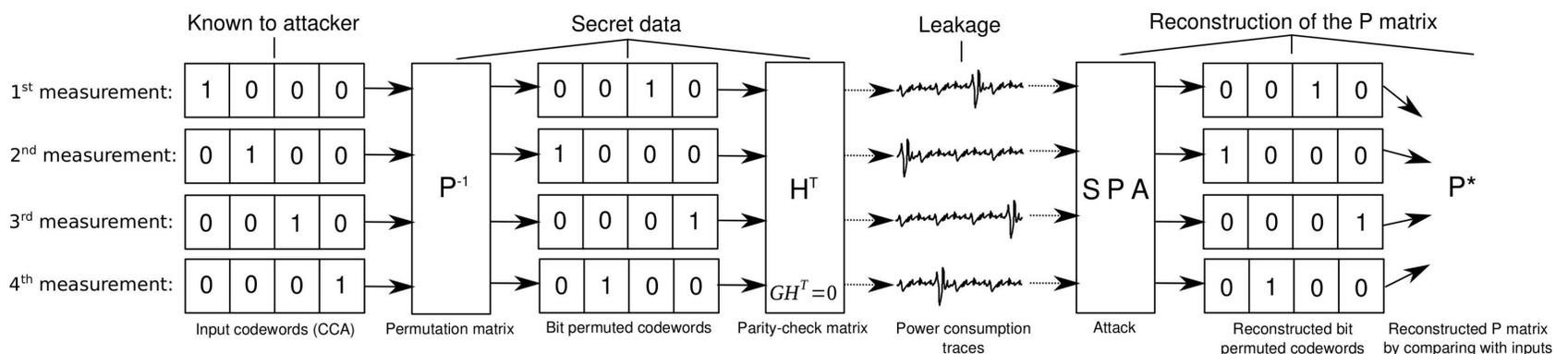
→ Quantification of a threat that poses revealed P matrix to an attacker – is it a complete breakdown of the encryption?

→ Using parameters: $n = 1024$ $m = 10$

→ Complexity of the attack: $m^2(n^3 + n^2)$

→ Complexity decreases from 2^{62} to 2^{37} binary operations

HOW DOES SIMPLE POWER ANALYSIS USING CHOSEN CIPHERTEXT ATTACK WORK?

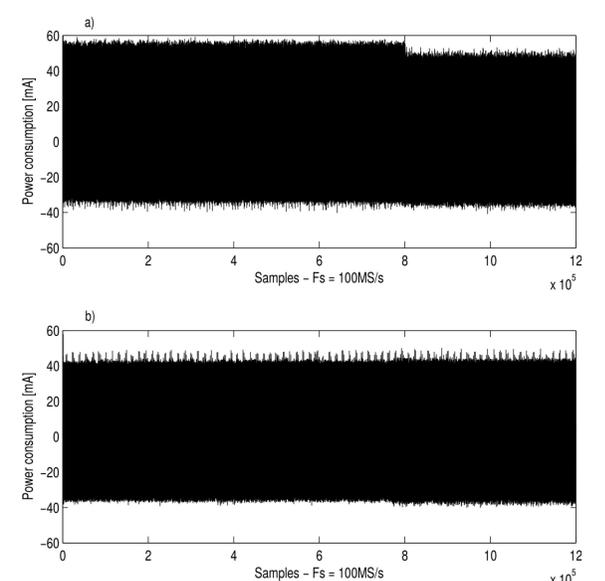
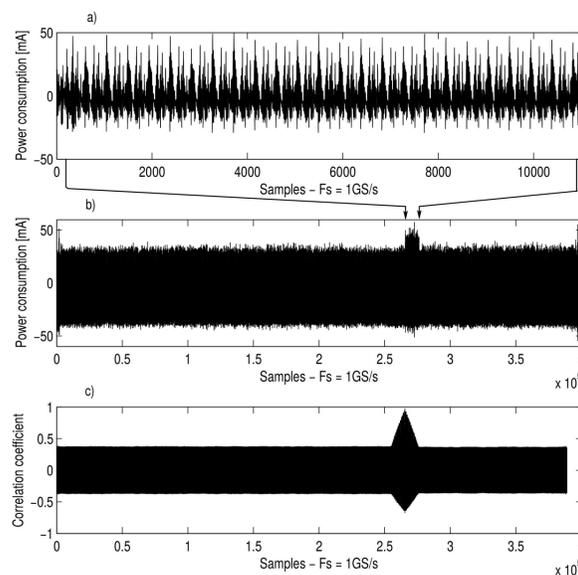


RESULTS & CONCLUSION

- Recreation of the SPA attack
- Quantification of the threat: $2^{62} \rightarrow 2^{37}$ operations
- Application of the software countermeasure based on avoiding conditional statements and creating time and instruction constant software
- Countermeasure 3x slower on average
- Advantage of the linear complexity
- Problem with initialization of variables
- Test of the SPA resistant implementation

• Future steps:

- a) DPA attack on the secure implementation
- b) Attack on an FPGA implementation



ACKNOWLEDGEMENT



The authors would also like to thank Alain Couvreur for his helpful advices.

REFERENCES

- [1] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," California Inst. Technol., Pasadena, CA, Tech. Rep. 44, January 1978.
- [2] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in Advances in Cryptology (CRYPTO'96), ser. LNCS, N. Koblitz, Ed., vol. 1109. Springer, 1996, pp. 104–113.
- [3] F. Strenzke, E. Tews, H. G. Molter, R. Overbeck, and A. Shoufan, "Side channels in the McEliece PKC," in The Second International Workshop on Post-Quantum Cryptography (PQCrypto 2008), ser. LNCS, J. Buchmann and J. Ding, Eds. Springer, October 2008, vol. 5299, no. 5299/2008, pp. 216–229.