Power and Electromagnetic Analysis for Template Attacks

Margaux Dugardin, Louiza Papachristodoulou, Zakaria Najm, Lejla Batina, Jean-Christophe Courrège, Jean-Luc Danger, Sylvain Guilley

Power and Electromagnetic Analysis for Template Attacks

Margaux Dugardin[1,3], Louiza Papachristodoulou[2], Zakaria Najm[3]

Lejla Batina[2], Jean-Christophe Courrège[1], Jean-Luc Danger[3,4], Sylvain Guilley[3,4]

[1] Thales Communications & Security, firstname.lastname@thalesgroup.com

[2] Radboud University Nijmegen, Digital Security Group, lejla@cs.ru.nl, louiza@cryptologio.org

[3] TELECOM ParisTech, COMELEC, firstname.lastname@telecom-paristech.fr

[4] Secure - IC, firstname.lastname@secure-ic.com

Abstract

This work presents side-channel attacks with power and electromagnetic side-channels during scalar-multiplication on an elliptic curve, in order to compare the efficiency of those methods in horizontal variations of template attacks. More precisely, we perform Online Template Attack, an efficient attack technique applied to regular scalar-multiplication algorithms, on a target device where an attacker has limited control over. Our target device uses the double-and-add-always algorithm on a twisted Edwards curve running on a smart-card with an ATmega163 CPU. We show that the attack is feasible in both power and electromagnetic attack scenarios, but power analysis gives better templates for key recovery in this setting.

Smart card Implementation

The smart card implementation is a regular scalar multiplication (double-and-add-always) from Michael Hutter and Peter Schwabe [2] over the twisted Edward curve Ed25519.
The equation from the curve is :

$$E(\mathbb{F}_p) : -x^2 + y^2 = 1 + dx^2y^2 \text{ over finite field } \mathbb{F}_p \text{ where : } \begin{cases} p = 2^{255} - 19 \\ d = (121665/121666) \mod p \end{cases}$$

Traces Before Pre-processing

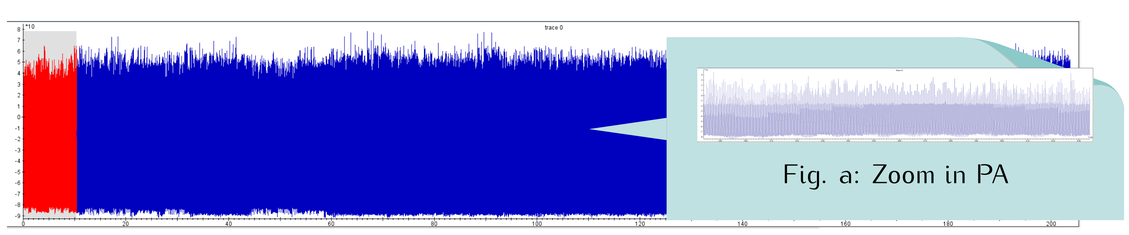

Fig. a: Zoom in PA

Fig. 1: Power consumption trace

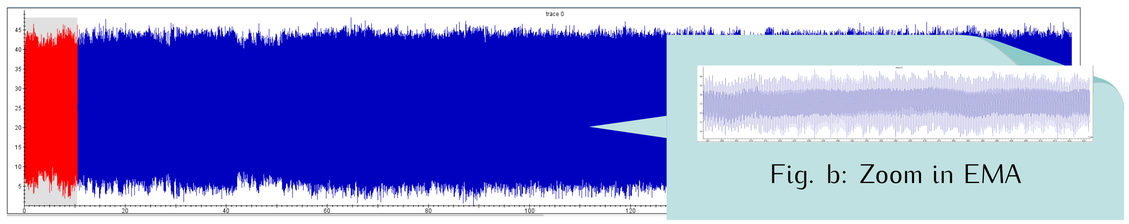

Fig. b: Zoom in EMA

Fig. 2: Electromagnetic Emanation trace

Online Template Attack

Online Template Attacks (OTA) are introduced by Batina et al. in [1].

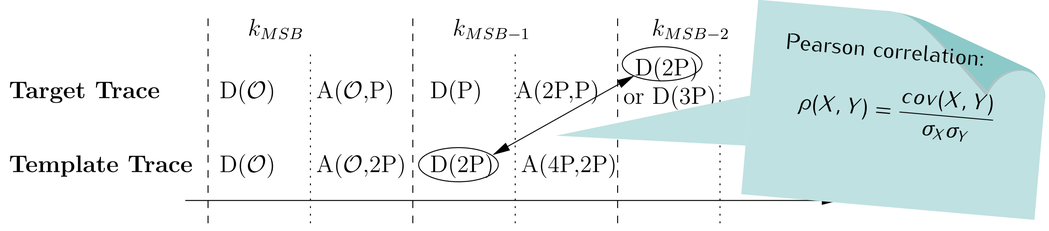

Fig. 3: Example to find the second MSB in the target trace with the template trace of **2P**

To find each key bit, we compute the Pearson correlation between the target trace and the template trace.

Analysis

In both cases we can correctly retrieve the corresponding key-bit of the exponent.

Analysis	correct guess	bad guess	difference between two guess
EMA	0.72	0.56	low
PA	0.67	0.30	high

Tab 1. Result of the pattern matching between the target and template trace.

EM signals apart from more information, contain also more noise, or "fake" peaks due to aliasing of the magnetic and current fields. In practice, we observe that EMA needs more preprocessing of the original trace compared to PA, in order to achieve the desired results in a template side-channel analysis scenario. However, more preprocessing destroys our original signal due to interpolation, and as a result the templates are not so accurate as in current traces.

Measurement Set-up

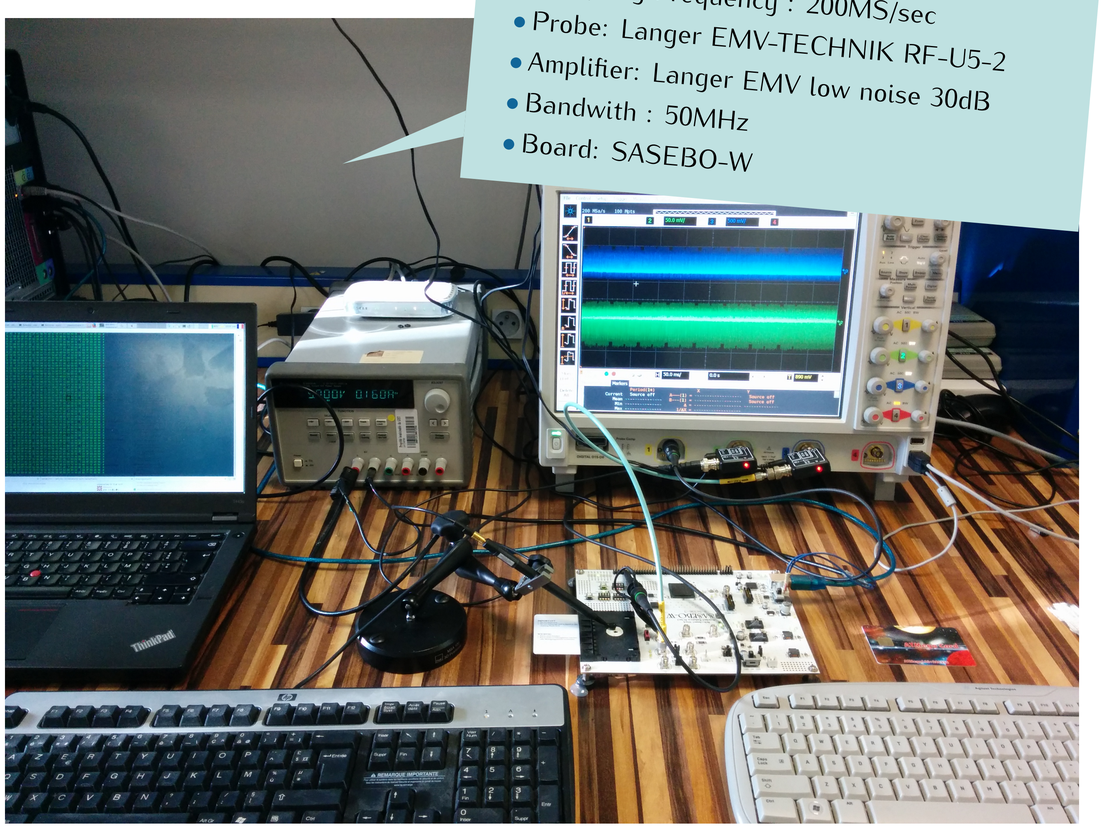

Fig. 4: Lab Set-up

Results

The results of the correlation between the target and the template traces are depicted. As correlation metric we used the Pearson's correlation coefficient and we compared the pattern of the beginning of the computation of **2P** and **3P** with the whole target trace of **P**. We expect to see the highest correlation for the correct key guess at the end of the second iteration of the double-and-add algorithm.

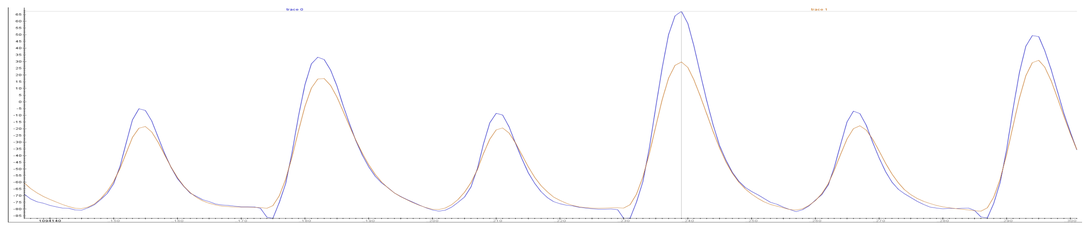

Fig. 5: PA pattern matching between **P2P** and **P3P**

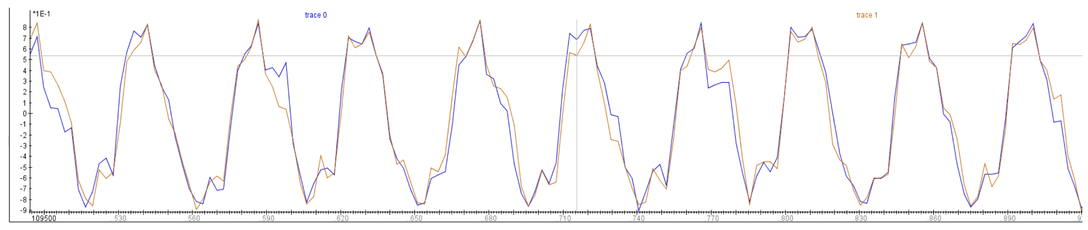

Fig. 6: EMA pattern matching between **P2P** and **P3P**

Conclusion

We conclude that PA can give more successful results for horizontal variations of template matching, such as OTA. This could be due the nature of the noise; the noise in PA is suitable for horizontal analysis, while the noise during EM acquisitions can be easier cancelled out by averaging a number of traces in vertical attack scenarios.

Bibliography

1. Lejla Batina, Lukasz Chmielewski, Louiza Papachristodoulou, Peter Schwabe, and Michael Tunstall. Online template attacks. In Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings, pages 21-36, 2014.
2. Michael Hutter and Peter Schwabe. NaCl on 8-bit AVR microcontrollers. In Amr Youssef and Abderrahmane Nitaj,editors, Progress in Cryptology - AFRICACRYPT 2013, volume 7918 of LNCS, pages 156-172, 2013.