# Investigation of horizontal type side-channel attacks on practical setups

January 4, 2015

## 1 Project

ICT COST Action IC1204: Trustworthy Manufacturing & Utilization of Secure Devices. This project is aligned to COST working group 5 (Validation, Evaluation, and Fault Injection). This document constitutes the project report for the Short Term Scientific Mission (STSM) of Louiza Papachristodoulou to TELECOM-ParisTech.

## 2 Involved Institutions

Visitor: Louiza Papachristodoulou, University Nijmegen, The Netherlands

Host institution: Prof. Dr. Sylvain Guilley, TELECOM-ParisTech, Paris, France

## 3 Planned Research

Implementing security protocols for embedded devices is a constant challenge for the cryptographic community due to the development of new and powerful side-channel attack techniques. By measuring the power consumption or the electromagnetic emanation of a device during the execution of a cryptographic algorithm, it is possible to derive secret data with a single or multiple traces.

Elliptic curve cryptography (ECC) offers a great variety of fast and efficient algorithms that can be applied for cryptographic protocols. However, ECC, as most of cryptographic primitives, is prone to physical attacks, such as side-channel and fault injection analyses. Thus, many protections have been put forward to thwart those attacks. It is usual in theoretical analyses of such attacks and countermeasures to consider that traces are noisy in vertical scale, but not in the horizontal scale. Said differently, it is implicitely assumed that the traces are well synchronized. However, in practice, even without "dealignment" protections, making the same computation twice (with the same "masks", if any), does not yield the same trace. This is due to many factors, such as the caching of code and of data, interrupts of some slave devices on the bus (e.g., serial ports), the state of the memory (e.g., a "malloc" function behaves differently

depending on the number of previous "malloc"s), etc. Such non-deterministic behavior complicates the attacks, and symmetrically helps to defend the circuit. The purpose of the study (visit at TELECOM-ParisTech) is to understand better to which extent the non-determinism of software execution deters the attacks.

The visitor, Louiza Papachristodoulou, has been investigating various collision and template attacks on elliptic curves, analyzing their efficiency in real-world software implementations and trying to perform them with as few traces as possible. The results of this research led to the development of a new attack technique, namely the Online Template Attack (OTA), which needs one trace per key bit to retrieve the secret scalar during a scalar-multiplication. The corresponding paper appears in LNCS proceedings of Indocrypt 2014 [1].

During the research visit, the plan was to combine the existing knowledge on ECC related attacks with the side-channel leakage expertise of TELECOM-ParisTech; TELECOM-ParisTech shared its platform, equipped to run C/ASM code of various types of ECC (coordinates representation, ECSM algorithms, type of curve, etc.) on a state-of-the-art ARM Cortex-M4, with caches activated or deactivated. Besides, side-channel capture is done locally by accurate electromagnetic probes, and analysed with various filtering and signal processing platforms [2].

# 4 Detailed work during STSM

During the visit in ParisTech institute, we investigated the various leakage factors that affect the dealignment of traces during the execution of an elliptic curve algorithm in a horizontal attack setting. More precisely, we focused on regular algorithms such as the double-and-add-always and the Montgomery ladder, which are in principle used to protect the scalar multiplication from simple side-channel attacks. We used the implementation of double-and-add-always for three different curves, namely the Edwards curve used for Ed25519 signatures [4], the Brainpool curve BP256r1 [3] and the NIST curve SecP256r1 [5], in order to compare and analyze the reasons that this regular algorithm leaks in different curve implementations. One implementation was readily available, while two implementations needed a slight modification of an existing library.

For a more detailed description on our practical work in the lab, we used an ARM Cortex-M4 microcontroller on a STM32f4 platform provided by ParisTech to perform our experiments. Running on the target device were the PolarSSL implementations of the Brainpool curve BP256r1 and the NIST curve SecP256r1. For the acquisition of traces, we used a Lecroy Wave Runner 6100A oscilloscope and a Langer EMV-TECHNIK RF-U5-2 near field probe.

With this setup, we performed the OTA [1] attack taking advantage of the electromagnetic (EM) emanations for side-channel analysis. During our research, we found an interesting path to investigate further, namely comparing the results from Power and EM analysis, in order to find out which one gives clearer traces, higher correlation values for our expected key guesses, more details in the leakage traces with lower sample frequency, and other factors that affect our experiments. At ParisTech a combination of

side-channel attacks was already proposed; for instance combining commonly used distinguishers or combinations of different measurements corresponding to the same activity [6]. Initiated by this paper, we also investigated the results of combining and comparing power and EM analysis on the different platforms (the ATMega 168 microcontroller running on a SASEBO-W board and the STM32f4 Cortex-M4 microcontroller).

The results of our research are as follows:

- EM signals are in general more noisy, but we can perform EM measurements in embedded devices, where power measurements cannot be performed. However, the OTA technique still works in this context.
- OTA is also applicable to the widely deployed Weierstrass curves, for instance TLS versions that use NIST curves are affected by our attack. We extracted the 256-bit key used for each of those curves with 257 traces, a result which shows the applicability and generalization of the OTA technique to various implementations.
- We showed that OTA works with different distinguishers, Pearson and Cross-Correlation coefficients. The Cross-Correlation gave higher success rate for our attack scenario, which can be due to the fact that there is a significant amount of misaligned (vertically and horizontally) traces during the acquisition with the EM probe.

Blinding the secret scalar is a common countermeasure used in this context, but it does not protect against our attack. However, point blinding and random field isomorphisms can efficiently thwart our attack.

Concluding, the results of this research helped us to understand the leakage factors of ECC implementations in horizontal attack scenarios and investigate efficient countermeasures to prevent similar attacks. Through the analysis of real measurements, we were able to adjust and fine-tune the parameters that give the optimal results for our setup, in order to perform the attack successfully on different curves.

As future work, we plan to investigate more on the parameters that are responsible for noisy traces and link those parameters to the probability of success of horizontal type of attacks that we got from our experiments. This is quite challenging to achieve when using different platforms, since it is time-consuming to fix the parameters that fit better in every setup. Determining those parameters in a general scale will give us a possibility to develop techniques to realign noisy traces and obtain higher success rate probabilities. Moreover, the experience obtained through working with different platforms and especially the SASEBO-W will help building a similar setup in our lab in Radboud. Thus, we will be able to extend our knowledge to different algorithms and their security against horizontal type of attacks.

# 5 Publications

The results of our research during the STSM at ParisTech are summarized in the following two papers:

- Margaux Dugardin, Louiza Papachristodoulou, Zakaria Najm, Lejla Batina, Jean-Luc Danger, Sylvain Guilley, Jean-Christophe Courrge, Anne-Sophie Rivemale, Carine Therond. Power and Electromagnetic Analysis for Online Template Attacks. *poster presentation for TRUDEVICE 2015 WORKSHOP (2-4 pages paper).*

- Margaux Dugardin, Louiza Papachristodoulou, Zakaria Najm, Lejla Batina, Jean-Luc Danger, Sylvain Guilley. EM Online Template Attacks are practical. *submitted to COSADE 2015*

## References

[1] Lejla Batina, Lukasz Chmielewski, Louiza Papachristodoulou, Peter Schwabe, and Michael Tunstall. Online Template Attacks. In Debdeep Mukhopadhyay Willi Meier, editor, *Indocrypt 2014*, 2014.

[2] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm. Side-channel leakage and trace compression using normalized inter-class variance. In Ruby B. Lee and Weidong Shi, editors, *HASP 2014, Hardware and Architectural Support for Security and Privacy, Minneapolis, MN, USA, June 15, 2014*, page 7. ACM, 2014.

[3] BSI. RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Technical report, Bundesamt fr Sicherheit in der Informationstechnik (BSI), 2010.

[4] 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, pages 156–172, 2013.

[5] NIST. FIPS publication 186-4 - Digital Signature standard (DSS). Technical report, National Institute of Standards and Technology (NIST), July 2013.

[6] Youssef Souissi, Shivam Bhasin, Sylvain Guilley, Maxime Nassar, and Jean-Luc Danger. Towards different flavors of combined side channel attacks. In Orr Dunkelman, editor, *Topics in Cryptology - CT-RSA 2012 - The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 - March 2, 2012. Proceedings*, volume 7178 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 2012.