Extended Horizontal SCA Attack Using Clustering Algorithm

Marcin Aftowicz[1], Dan Klann[1], Ievgen Kabin[1], Zoya Dyka[1]
and Peter Langendörfer[1,2]

[1]IHP - Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany
{aftowicz, klann, kabin, dyka, langendoerfer}@ihp-microelectronics.com

[2]BTU Cottbus-Senftenberg
Cottbus, Germany
peter.langendoerfer@b-tu.de

32nd Crypto Day, 15. January 2021

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-25

The ever growing demand on higher communication throughput in the Internet of Things era poses a great threat to information security. Data encryption or authentication algorithms mean higher latency and bigger energy consumption. Hardware acceleration and Elliptic Curve Cryptography (ECC) allow to meet the tight constraints of secure communication, but the hardware needs to be resistant against Side Channel Analysis (SCA) attacks.

In our previous works (Kabin, Dyka, Kreiser & Langendoerfer (2017); Aftowicz, Kabin, Klann, Varabei, Dyka & Langendoerfer (2020)), we have shown that it is possible to extract the secret scalar k (further key) used during an elliptic curve point multiplication (denoted as kP operation) by statistically analysing side channel effects, or by applying machine learning methods. We analysed the current through the chip measured during the kP execution and the electromagnetic emanation of the chip. We attacked our implementation of a modification of the Montgomery ladder. The Montgomery kP algorithm processes the scalar k bit-wise, i.e. one after the other in a loop, from the most significant bit of the scalar k to its least significant bit. The assumption was that the profile of the measured trace, in the part corresponding to the processing of a key bit '1' differs (at least slightly) from the profile of the parts corresponding to the processing of a key bit '0'. We applied the clustering method k-means to extract the scalar k. While successful against a straight forward implementation, the attack failed against a more sophisticated design with pseudo-random addressing of registers. It revealed only 88% of all key bits, leaving space for improvement.

The length of the scalar k processed in the attacked designs was less than 300 bits. In this work we measured traces of many kP executions. Taking into account the countermeasures against vertical attacks proposed by Coron (1999), we are aware that the coordinates of the processed elliptic curve points, as well as the scalars used in the measured kP executions, can be randomized. We gave the clustering algorithm more data to train on, based on the assumption that the key bit ‘0’ profiles can be distinguished from the key bit ‘1’ profiles, i.e. we performed our horizontal attack using an extended number of kP traces. Opposite to the vertical attacks, we did not concentrate on the analysis of the clock cycles that correspond to the key dependent storing of data into registers. Due to this fact, we call our experiments extended horizontal attack. The results of the attack proved again that machine learning algorithms need a substantial amount of data to show its full potential. More traces resulted in a higher success rate of the attack

References

MARCIN AFTOWICZ, IEVGEN KABIN, DAN KLANN, YAUHEN VARABEI, ZOYA DYKA & PETER LANGENDOERFER (2020). Horizontal SCA Attacks against kP Algorithm Using K-Means and PCA. In *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, 1–7. IEEE, Piscataway, NJ. ISBN 978-1-7281-6949-1.

JEAN-SÉBASTIEN CORON (1999). Resistance Against Differential Power Analysis For Elliptic Curve Cryptosystems. In *Cryptographic hardware and embedded systems*, ÇETIN K. KOÇ & CHRISTOF PAAR, editors, volume 1717 of *Lecture Notes in Computer Science*, 292–302. Springer, Berlin and London. ISBN 978-3-540-66646-2.

IEVGEN KABIN, ZOYA DYKA, DAN KREISER & PETER LANGENDOERFER (2017). Horizontal address-bit DPA against Montgomery kP implementation. In *2017 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, 1–8. IEEE, Cancun. ISBN 978-1-5386-3797-5.