Breaking of an Open Source Fully Balanced Elliptic Curve Design Using Automated Simple SCA

Ievgen Kabin[1], Zoya Dyka[1], Dan Klann[1] and Peter Langendörfer[1,2]
{kabin, dyka, klann, langendoerfer}@ihp-microelectronics.com

[1]IHP - Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany

[2]BTU Cottbus-Senftenberg
Cottbus, Germany

32nd Crypto Day, 15. January 2021

The main operation in Elliptic Curve Cryptography (ECC) is the multiplication of an elliptic curve (EC) point P with a long binary scalar k, denoted as kP. The goal of attackers is to reveal the scalar k (further denoted as *key* k). This is often possible by analysing measured power or electromagnetic traces of kP executions, or other side channel effects.

The Montgomery ladder is the algorithm most often used for implementing the kP calculation. This algorithm is reported in the literature as resistant against simple Side Channel Analysis (SCA) attacks due to the fact that it is a balanced algorithm, i.e. the processing of each bit value of the scalar k is done in the same sequence of operations, namely one EC point addition and one EC point doubling. But the use of registers in the Montgomery ladder depends on the key and by that makes it vulnerable to vertical data bit and horizontal address bit attacks. One of the known countermeasures is to randomize the sequence of the EC point operations – addition and doubling – per iteration of the main loop of the algorithm. The randomization makes sense only if the sequence of the field operations calculating an EC point addition is the same as the one for calculating an EC point doubling, for example if an unified EC point addition formula is applied.

[4] reports on a fully balanced ASIC Coprocessor implementing complete addition formulas on Weierstrass Elliptic Curves. The design is open source and the VHDL code is available at the GitHub repository [3]. We synthesized this open source design for the IHP 250 nm cell library and simulated the power traces of a kP execution using the basis point of EC *secp256k1* as the input point P corresponding to the original testbench.

We experimented with differently long scalars k. We simulated the power traces for keys of about 20 bits, as well as of about 200 bit and performed

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-23

an SPA using each single power trace. In all cases we are able to reveal scalars successfully. The analysis was automated as described in [1]. More details about the performed attacks and their results can be found in [2].

References

[1] Ievgen Kabin, Zoya Dyka, Marcin Aftowicz, Dan Klann & Peter Langendoerfer (2020a). Resistance of the Montgomery kP Algorithm against Simple SCA: Theory and Practice. In *2020 IEEE Latin-American Test Symposium (LATS)*, 1–6. ISSN: 2373-0862.

[2] Ievgen Kabin, Zoya Dyka, Dan Klann, Nele Mentens, Lejla Batina & Peter Langendoerfer (2020b). Breaking a fully Balanced ASIC Coprocessor Implementing Complete Addition Formulas on Weierstrass Elliptic Curves. In *2020 23rd Euromicro Conference on Digital System Design (DSD)*, 270–276.

[3] Niels Pirotte (2018). VHDL design of ASIC implementation for ECC with complete formulae. Master Thesis. URL `https://github.com/NielsPirotte/MasterThesis_Niels_Pirotte`.

[4] Niels Pirotte, Jo Vliegen, Lejla Batina & Nele Mentens (2018). Design of a Fully Balanced ASIC Coprocessor Implementing Complete Addition Formulas on Weierstrass Elliptic Curves. In *2018 21st Euromicro Conference on Digital System Design (DSD)*, 545–552.