Low-Cost Countermeasure against Horizontal Bus and Address-Bit SCA

Ievgen Kabin, Zoya Dyka, Dan Kreiser and Peter Langendoerfer

IHP

Frankfurt (Oder), Germany

Implementing cryptographic algorithms in a really tamperproof way is an extremely challenging task. The addressing of blocks in hardware implementations has been reported as a significant problem in the past. The addressing of logic blocks and registers may be exploited to reveal the key. Vertical and horizontal attacks against Elliptic Curve Cryptography designs exploiting the addressing of registers in Montgomery kP implementations are described in [1] and [2] respectively. The vulnerability of cryptographic implementations due to the activity of the bus was discussed in [2], [3]. Each *write-to-* or *read-from-* a register (or a block) operation consists of two steps: addressing the register (block) and the reading/storing of the data. The exchange of data between logic blocks is done via a bus which is often a muxer. The energy consumption of the bus depends on the address of the logic blocks. The selection of the block to be addressed depends on the scalar k, that is the secret (key). Thus, the processed scalar k can be revealed by SCA attacks that exploit the addressing of the selected logic blocks.

Since the key dependent addressing of blocks is the main leakage source in our implementation of the Montgomery kP algorithm [2] we developed a regular schedule in which the blocks are addressed that helps to reduce the leakage significantly. In total for 21 of 54 clock cycles the addressing can be changed without affecting the functionality of the design We verified the feasibility of our approach analysing simulated power traces for the IHP [4] 250 nm technology as well as power and electromagnetic traces measured on a Xilinx Spartan-6 FPGA [5]. The number of clock cycles in which key candidates were extracted with a correctness of more than 90 per cent was reduced from 14 to zero attacking the FPGA power trace and from 21 to 5 attacking the electromagnetic trace. The proposed solution can be helpful when designing SCA resistant implementation of Montgomery kP operation for FPGAs as well as for ASICs.

References

[1] Itoh, K., Izu, T., Takenaka, M., *Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA.*, In: Cryptographic Hardware and Embedded Systems - CHES 2002. pp. 129-143. Springer, Berlin, Heidelberg (2002).

[2] I. Kabin, Z. Dyka, D. Kreiser, and P. Langendoerfer, *Horizontal Address-Bit DEMA against ECDSA*, in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1-7.

[3] Messerges, T.S., Dabbish, E.A., Sloan, R.H., *Power Analysis Attacks of Modular Exponentiation in Smartcards*, In: Cryptographic Hardware and Embedded Systems. pp. 144157. Springer, Berlin, Heidelberg (1999).

[4] IHP - Innovations for High Performance Microelectronics, *https://www.ihp-microelectronics.com/en/start.html*.

[5] Xilinx Inc.. Spartan-6 Family Overview, Product Specification. DS160 (v2.0) October 25, 2011, *https://www.xilinx.com/support/documentation/data_sheets/ds160.pdf*.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-09