Placement of Gates in ECC Designs

Christian Wittke, Zoya Dyka, Peter Langendoerfer
IHP
Im Technologiepark 25
Frankfurt (Oder), Germany

29th Crypto Day, 6/7 September 2018

In Heyszl (2013) a localized Electromagnetic Analysis (EMA) attack against an FPGA implementation of an Elliptic Curve (EC) point multiplication was introduced. The attacked design is an implementation of the Montgomery kP algorithm using projective López-Dahab coordinates for the NIST EC *B-163*. The Montgomery kP algorithm is a bitwise processing of the scalar k, whereby the activity of registers depends on the processed bit value of the scalar k. Thus, the scalar k can be revealed due to the physical placement of the registers in a hardware implementation. To prevent this kind of attacks a randomized placement of flip flops of all registers was proposed in Heyszl (2013). This randomization leads to an equal distribution of flip flops in the chip area and can increase the vulnerability of designs against other side channel analysis attacks. Isolated placed flip flops can be attacked more precisely using optical fault injection attacks. Furthermore interconnects of isolated placed flip flops can be significant longer than interconnects of flip flops placed close to each other. These interconnects can be a strong leakage source that increases the success of EMA attacks, for example horizontal bus and address bit DEMA attacks.

Thus, the designer needs a methodology for an intelligent placement of gates. This work describes our first experiments for the development of an intelligent placement of logic gates and register flip flops in the layout.

References

Johann Heyszl (2013). *Impact of Localized Electromagnetic Field Measurements on Implementations of Asymmetric Cryptography.* Ph.D. thesis, Technische Universität München.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-10