Cryptographic ICs: Simulation of Electromagnetic Radiation

Omar A. Sosa[1], Zoya Dyka[1], Ievgen Kabin[1] and Peter Langendoerfer[1,2]
{sosa, dyka, kabin, langendoerfer}@ihp-microelectronics.com

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

[2]BTU Cottbus-Senftenberg
Cottbus, Germany

33rd Crypto Day, 17. September 2021

Cryptographic algorithms implemented in hardware have to be resistant against many physical and side-channel analysis (SCA) attacks. SCA attacks are nowadays well-known threats for cryptographic implementations. Electromagnetic Analysis (EMA) attacks are well-known non-invasive SCA attacks. Especially dangerous are localized EMA attacks. Electromagnetic radiation of a cryptographic chip during the processing of sensitive/secret data can be measured and analysed statistically with the goal to reveal the sensitive/secret data, for example the private key during an authentication process. Detailed knowledge about the electromagnetic radiation of cryptographic chips is necessary for the evaluation of the resistance of the chips against the (localized) EMA attacks during the early design phase, i.e. before the manufacturing and measurements. Therefore, the spatial distribution of electromagnetic radiation of the cryptographic chips needs to be simulated. In this work we discuss the possibility of simulation of electromagnetic traces of hardware accelerators for elliptic curve (EC) cryptography based on the information from the published state-of-art works regarding simulation of EM radiation of cryptographic integrated circuits. Our goal is to be able to evaluate the resistance of EC designs against EMA attacks during the early design phase. Despite the extensive search of the literature we have done, we found only a few publications about the simulation of EM radiation of cryptographic designs. Due to the complex structure of ICs, i.e. several metal layers, huge amount of gates, wires, vias, etc., as well as the complex simulation formulae and long simulation time, the simulation of the EM field of ICs is a challenging task. The simulation time of the electromagnetic radiation of cryptographic chips is an important parameter that depends on many factors: metal layers considered, area simulated, solver method, i.e. EM simulation tool used for it, the attacked cryptographic algorithm and their time window. To reduce the time of the simulation, the following limitation of the simulation conditions are applied in the literature: concentrating only

crypto day matters 33 (2021)
Beiträge vom 33. Kryptotag, 17.09.2021, online.
doi:10.18420/cdm-2021-33-13

on topmost metal layers [Kumar, Scarborough, Yilmaz & Orshansky (2017)], specifying a small area and/or certain time window slot of the cryptographic algorithm implemented [Das, Nath, Chatterjee, Ghosh & Sen (2019)], [Ma, He, Liu, Zhao & Jin (2019)] i.e. concentrating on the operations that are the SCA leakage sources. In our future work we plan to simulate the EM radiation of the IHP ECC designs using limitations of the simulation conditions as proposed in the literature for AES. This task can be more complex than the simulation of the AES designs, due to the big area of EC accelerators and especially due to the long execution time. For example, the IHP accelerator for the EC point multiplication for the NIST EC B-233 needs about 14000 clock cycles. Additionally, the shielding effect of metal fillers has to be simulated. Currently, we did not found publications about the simulation of EM radiation of EC implementations as well as about the influence of the metal fillers on the simulation results. The metal fillers combined with the routing of cryptographic core signal wires in low-level metal layers can reduce the success of EMA attacks. It can be a basis for the development of design rules for the route and placement process as a part of the design methodology for the engineering of resilient systems.

References

D. Das, M. Nath, B. Chatterjee, S. Ghosh & S. Sen (2019). STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*.

A. Kumar, C. Scarborough, A. Yilmaz & M. Orshansky (2017). Efficient simulation of EM side-channel attack resilience. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*.

H. Ma, J. He, Y. Liu, Y. Zhao & Y. Jin (2019). CAD4EM-P: Security-Driven Placement Tools for Electromagnetic Side Channel Protection. In *2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*.