Probe comparison for EM-measurement in terms of side channel analysis

Christian Wittke, Zoya Dyka and Peter Langendoerfer

System dept.,
IHP
Frankfurt(Oder), Germany

Side channel analysis is an effective method for attacking cryptographic implementations. The most attacks are based on (statistical) analysis of the power or electromagnetic (EM) traces. These traces are measured while the device is executing cryptographic operations using its private (secret) key. The benefit of electromagnetic analysis attacks (EMA) is the feasibility to do local measurements, i.e. the activity of some blocks of a cryptographic design can be analysed separately. Different EM probes, for example commercial manufactured as well as self-made probes, can be used for measurements. Their size, form, position and orientation influence the shape and the quality of the measured traces significantly. But the focus in scientific publications is usually set on the statistical analysis of already measured traces.

In this work we explain how and why the size, position and orientation of EM probe influence the measurement results. Therefore we compare 7 different EM field probes from Langer [1], Riscure [2] and a self-made probe.

We analysed a hardware accelerator for elliptic curve point multiplication kP for elliptic curve *B-233* [3] over the extended binary Galois field $GF(2^{233})$. The kP operation was implemented using the Montgomery algorithm in projective Lopez-Dahab coordinates as described in [4]. This version of kP design is vulnerable against simple power and electromagnetic analysis attacks [5]. We selected this version since its vulnerabilities can easily be seen, i.e. it is a very helpful example to illustrate the influence of different EM probes on the measured traces. The device under attack, the analysed cryptographic operations and processed inputs are always the same in our experiments. These measurement conditions allow a fair comparison of the probes and show the influence of the probes on the shape of the measured traces.

We performed the measurements of the EM field at two positions on our FPGA Board. First we measured the EM field on the die and second at an interconnect on the PCB. In particular the EM traces measured on the die differ substantially. But also the EM traces measured at the PCB interconnect are different. The measurement results are showing a large difference between the traces of each probe. The impact is much higher for horizontal EM probes than for vertical EM probes. The presented results can be helpful in preparation of electromagnetic analysis attacks, i.e. for choosing the most appropriate EM probe and its orientation at measurement points.

References

[1] LANGER EMV-Technik GmbH, http://www.langer-emv.de/

[2] Riscure Security Lab, https://www.riscure.com/

[3] NIST, "Digital Signature Standard (DSS)," FIPS PUB 186-4, Tech. Rep., July 2013.

[4] S. Peter, "Evaluation of Design Alternatives for Flexible Elliptic Curve Hardware Accelerators," Master's thesis, Brandenburg University of Technology Cottbus, 2006.

[5] IHP Project TAMPRES, from http://www.ihp-microelectronics.com/de/forschung/drahtlose-systeme-und-anwendungen/abgeschlossene-projekte/tampres.html