Successful simple power analysis of GALS ECC design

Zoya Dyka, Frank Vater, Dan Kreiser und Peter Langendoerfer

System dept. IHP
Frankfurt (Oder), Germany

Side channel analysis attacks are significant threat for implementing cryptographic algorithms. A lot of countermeasures based on the randomization of the secret (private) key [1], inputs [1], steps of algorithms [2] or influence of the circuit [3] are published. In [4] the implementation of ECC (Elliptic Curve Cryptography) design as a GALS (Global Asynchronous Locally Synchronous) design was introduced as a possible countermeasure against side channel analysis (SCA) attacks.

We performed a simple power analysis (SPA) attack against the original synchronous IHP ECC design and against its GALS-ified version. In this work we analysed simulated power traces of both ECC designs. To ensure a fair comparison exactly the same manufacturer library of elements, the same inputs, private key and simulation tools were used for obtaining the power traces of both hardware implementations. The private key can be extracted successfully for both designs. This shows clearly that a straight forward GALS-ification of a synchronous ECC design that is vulnerable to SPA is also vulnerable to SPA. Also we explain here why the GALS design is even more vulnerable to other SCA attacks for example to differential power analysis than a synchronous ECC design.

Acknowledgement

The authors would like to thank the Dr. Milos Krstic from System department of IHP for providing the GALS-ified version of IHP ECC design.

References

[1] J. Coron: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. Proceedings of the First International Workshop CHES 1999, August 12-13, 1999, Worcester, MA, USA, LNCS Vol. 1717, pp. 292-302, Springer Berlin Heidelberg, 1999

[2] E. Oswald, M. Aigner: Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks. Proceedings of the Third International Workshop - CHES 2001, May 14-16, 2001, Paris, France, LNCS Vol. 2162, pp. 39-50, Springer Berlin Heidelberg, 2001

[3] Z. Dyka, Ch. Wittke and P. Langendoerfer: Clockwise Randomization of the Observable Behaviour of Crypto ASICs to Counter Side Channel Attacks. Proceedings of Euromicro Conference on Digital System Design (DSD), 26-28 Aug. 2015, pp. 551-554, IEEE,

[4] Xin Fan, S. Peter and M. Krstic: GALS design of ECC against side-channel attacks A comparative study. Proceedings of 24th International Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS), Sept. 29-Oct. 1 2014, pp. 1-6, IEEE,