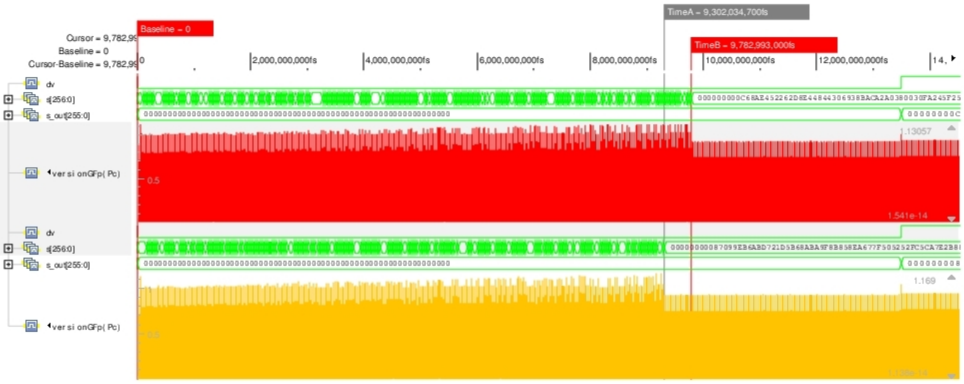
Comments On: Constant Time Modular Inversion

Ievgen Kabin, Zoya Dyka, Dan Kreiser and Peter Langendoerfer

IHP
Frankfurt (Oder), Germany

Modular inversion is a challenge for cryptographic implementations as it is one of the most time consuming field operations in the ECC calculations. Basically it is performed by using of the Fermats little theorem, Extended Euclidean algorithm or any of its binary variants based on the Montgomery modular inverse algorithm [1]. A typical implementation of an Extended Euclidean algorithm for modular inversion can be the source of information leakage. It happens due to the fact that these algorithms have an input-centric sequence of conditional branches and therefore the time for calculating the result depends on the inputs. In [2] a constant time modification of the Montgomery modular inverse algorithm was proposed that can prevent Simple Power Analysis attacks. The main idea in [2] is to calculate an inverse by performing always the same number of constant time iterations. This algorithm for inverse calculculation is also very fast. It requires for example only 4(224 - 1) iterations, i.e. 892 clock cycles, for calculation of an inverse elment of *GF(p)* for the NIST EC P-224. Due to this fact we implemented this modular inverse algorithm in VHDL according to the Algorithm 2 as it is given in [2]. We tested the functionality of our design using Cadence SimVision and we simulated its power traces for different inputs using Synopsys PrimeTime for the IHP 250nm technology. Despite the fact that author of [2] claims a constant calculation time for any inversion, it can be easily seen that after several numbers of iterations dependent on the processed input the values of intermediate variables are not changing anymore and the power consumption of the design is reduced significantly. Thus, the execution time of each inverse calculation can be easy estimated analysing the measured power trace, i.e. the algorithm proposed in [2] cannot prevent time and power analysis attacks.



Acknowledgement: This research has been funded by the Federal Ministry of Education and Research of Germany under grant number 03ZZ052717.

References

[1] B. S. Kaliski, *The Montgomery inverse and its applications*, IEEE Transactions on Computers, vol. 44, no. 8, pp. 1064-1065, Aug. 1995.

[2] J. W. Bos, *Constant time modular inversion*, J Cryptogr Eng, vol. 4, no. 4, pp. 275-281, Nov. 2014.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-08