HCCA against Montgomery kP Design

Dan Kreiser, Zoya Dyka, Ievgen Kabin and Peter Langendoerfer

IHP

Frankfurt (Oder), Germany

The Montgomery kP algorithm is the most often implemented algorithm for accelerating cryptographic operations for Elliptic Curve Cryptography (ECC), especially for EC over extended binary fields GF(2^n). P is a point of an EC and k is a scalar. The kP operation is performed once for a digital signature generation corresponding to the Elliptic Curve Digital Signature Algorithm (ECDSA) approach [1] and twice for a signature verification. If an attacker can extract the scalar k used for the signature generation, he can reveal the private key of the signers, i.e. kP implementations have to be resistant against Side Channel Analysis (SCA) attacks if attackers can have the physical access to the cryptographic design. The Montgomery kP algorithm is a bitwise processing of the scalar k, whereby the sequence of the operations doesn't depend on the processed bit value of the scalar k. Due to this fact the Montgomery kP algorithm is resistant against simple SCA attacks, but it is vulnerable to vertical and horizontal differential SCA attacks that exploit the addressing of logic blocks and registers to reveal the key [2], [3].

Splitting the measured trace(s) into slots that correspond to the processing of a single bit of the scalar k simplifies if not enables horizontal bus and Address-bit Differential Power Analysis (DPA). Horizontal Collision Correlation Analysis attacks (HCCA) [4], that are normally run against GF(p) implementations, can be used to partition a given trace into slots even for GF(2^n). For the Montgomery kP algorithm the separation of traces into slots can be done due to the fact that a multiplication with EC parameter b or a multiplication with x coordinate of input point P is executed in each slot in the main loop of the Montgomery kP algorithm using Lopez-Dahab projective coordinates.

We run an HCCA attack against our ECDSA design, which supports the NIST EC B-233 and B-283 using a flexible field multiplier. As a result, we can state that even though this attack did not reveal the used scalar k it helps to separate the trace into slots. We assumed that not the field multiplier but other operations performed in parallel to the multiplication cause this effect. To proof this idea we analysed the power and electromagnetic traces of our field multiplier only. The analysis confirmed our assumption. This research has been funded by the Federal Ministry of Education and Research of Germany under grant number 03ZZ052717.

References

[1] D. Johnson, A. Menezes and S. Vanstone, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, in Int. J. Inf. Secur. pp. 144-157. Springer, Berlin, Heidelberg (2001).

[2] K. Itoh, T. Izu, M. Takenaka, *Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA.*, In: Cryptographic Hardware and Embedded Systems - CHES 2002. pp. 129-143. Springer, Berlin, Heidelberg (2002).

[3] I. Kabin, Z. Dyka, D. Kreiser, and P. Langendoerfer, *Horizontal Address-BitDPA against montgomery kP implementation*, in 2017 International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2017, pp. 1-8.

[4] A. Bauer, E. Jaulmes, E. Prouff, J. Wild, *Horizontal Collision Correlation Attack on Elliptic Curves*, In: SAC 2013. pp. 553-570.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-07