Single-Trace Address Bit SCA: Atomicity and Regularity are not Effective Countermeasures

Zoya Dyka[1], Ievgen Kabin[1], Dan Klann[1] and Peter Langendoerfer[1,2]
{dyka, kabin, klann, langendoerfer}@ihp-microelectronics.com

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

[2]BTU Cottbus-Senftenberg
Cottbus, Germany

33th Crypto Day, 17 September 2021

Elliptic Curve Cryptosystems are nowadays widely used as means to implement the security requirements: secret exchange, data confidentiality and integrity, authentication and non-repudiation. Authentication protocols based on the Elliptic Curve (EC) Diffie-Hellman approach and EC digital signature standards (ECDSA) Kerry, Secretary & Director (2013) use different ECs over finite fields, called also Galois fields. The ECs mostly used for authentication are binary curves, i.e. ECs over binary extended finite fields $GF(2^n)$. Authentication is often implemented in hardware as a specialized ASIC. ECDSA protocols specify the ECs over binary finite fields $GF(2^n)$ as well as the ECs over prime finite fields $GF(p)$. Due to the recommendation to the applied key length, i.e. in ECDSA standard Kerry *et al.* (2013) and automotive standard ETSI (2017), the EC P-256 over a prime finite field is often selected for implementations.

The main operation in EC cryptographic protocols is the multiplication of an EC point P with a long binary scalar k. This operation is denoted as kP, takes about 95% of a signature generation time and is sensitive to side-channel analysis (SCA) attacks. SCA attacks are physical attacks based on the measurement and analysis of physical parameters that accompany cryptographic operations: execution time, power consumed, electromagnetic radiation, etc. All these measurable parameters depend on the implemented algorithm, the electrical circuit of the cryptographic chip, the manufacturing technology as well as on the processed input data, i.e. on the coordinates of the point P and on the value of the scalar k. The goal of the attacks is usually to reveal the scalar k. If a single trace of a kP execution is enough for revealing the scalar k, the attack is classified as a horizontal attack. Simple power analysis (SPA) and simple electromagnetic analysis (SEMA) attacks are well-known examples of horizontal attacks.

The kP algorithm implemented in hardware is usually a bitwise processing of the scalar k, i.e. the processing of each bit of the scalar requires a certain time and has its own power (or electromagnetic) profile. If the profiles of '0'-bits are

crypto day matters 33 (2021)
Beiträge vom 33. Kryptotag, 17.09.2021, online.
doi:10.18420/cdm-2021-33-22

distinguishable from the profiles of the ‘1’-bits, the scalar k can be successfully revealed.

Atomicity and regularity principles are well-known methods to prevent the success of single-trace SCA attacks, at least simple power analysis (SPA) and simple electromagnetic analysis (SEMA) attacks. The regularity principle recommends to implement the processing of each bit of the scalar k as the same sequence of operations to make the profiles indistinguishable from each other. The atomicity principle proposes to implement the processing of each bit of the scalar k as multiple sequences of repeatable operations, for example: “multiplication, addition, write-to-register”. We implemented kP algorithms for different ECs i.e. B-233, B-283, P-224 and P-256. We used the Montgomery ladder with Lopez-Dahab projective coordinates Hankerson, López & Menezes (2000) for implementing the kP operation for the binary ECs. This algorithm is a well-known regular algorithm. We used the atomic patterns algorithm Rondepierre (2014) for implementing the kP operation for the prime ECs. We are able to reveal the scalar k completely by analysing a single (simulated) power trace. For the analysis we applied our automatization of SPA. The SCA leakage source is the key dependent addressing of registers and blocks of the kP design. For ‘0’-bits registers/blocks differ from those for ‘1’-bits are addressed for writing/reading the data. Results of our attacks show clearly that regularity as well as atomicity are not effective against single-trace address-bit attacks, at least if “atoms” are as big as proposed in Rondepierre (2014).

References

ETSI (2017). ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites **V**(1.2.1).

Darrel Hankerson, Julio López & Alfred Menezes (2000). Software Implementation of Elliptic Curve Cryptography over Binary Fields. 1–24. ISBN 978-3-540-41455-1.

Cameron F. Kerry, Acting Secretary & Charles Romine Director (2013). FIPS PUB 186-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS).

Franck Rondepierre (2014). Revisiting Atomic Patterns for Scalar Multiplications on Elliptic Curves. 171–186. ISBN 978-3-319-08301-8.