ECC Based Secure Authentication Solutions

Ievgen Kabin, Zoya Dyka, Dan Klann and Peter Langendoerfer
IHP – Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25
Frankfurt (Oder), Germany

30th Crypto Day, 28/29 March 2019

Product counterfeiting becomes a significant problem worldwide. It can affect not only a company's reputation and its financial benefits but also personal safety and security of the end-users or customers. Authentication approaches based on Elliptic Curve Cryptography (ECC) are preferable as they can easily fit into requirements of low cost applications where computational costs, execution time and therefore power consumption are critical.

Many world known manufacturers such as NXP or Infineon offer their low cost ECC-based anticounterfeiting integrated circuits for an authentication process [NXP-Semiconductors (2016)], [Infineon-Technologies (2017)]. These devices typically use authentication protocols based on NIST elliptic curves (EC) [NIST-FIPS (2013)] over binary fields as they are more suitable for an efficient hardware implementation compared to EC over prime fields. Each authentication chip has a unique identifier, a random-number generator and a hardware cryptographic-acceleration engine. Additionally, each authentication chip has a certificate (with a public key) and the private key of the chip, inserted into a block of non-volatile memory during production flow for secure storage.

In this work we provide a comparison of the NXP A1006 Secure Authenticator which uses B-163 elliptic curve and Infineon Optiga Trust B solution (131 bits, probably B-131) based on publicly available information with our own implementation for the B-233 EC, running on a Digilent's Cmod S7 board equipped with a Spartan-7 FPGA [Digilent-Inc. (2018)]. We demonstrate power traces as well as electromagnetic traces measured during the authentication process and discuss the possibility to perform horizontal differential side channel analysis attacks [Kabin, Dyka, Kreiser & Langendörfer (2018)] against the used EC point multiplication algorithm.

References

Digilent-Inc. (2018). Cmod S7: Breadboardable Spartan-7 FPGA Module. URL `https://reference.digilentinc.com/reference/programmable-logic/cmod-s7/start`.

Infineon-Technologies (2017). OPTIGA Trust B SLE95250: Authentication solution for improved security and reduced system costs. URL `https://www.infineon.com/cms/de/product/`

crypto day matters 30 (2019)
Beiträge vom 30. Kryptotag, 28.-29.03.2019, Mozilla, Berlin.
doi:10.18420/cdm-2019-30-21

security-smart-card-solutions/optiga-embedded-security-solutions/optiga-trust/optiga-trust-b-sle-95250/.

Ievgen Kabin, Zoya Dyka, Dan Kreiser & Peter Langendörfer (2018). Horizontal Address-Bit DEMA against ECDSA. In *9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018, Paris, France, February 26-28, 2018*, 1–7. URL https://doi.org/10.1109/NTMS.2018.8328695.

NIST-FIPS (2013). FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 186-4 Digital Signature Standard (DSS). URL http://dx.doi.org/10.6028/NIST.FIPS.186-4.

NXP-Semiconductors (2016). A1006 Secure tamper-resistant authenticator IC. URL https://www.nxp.com/products/identification-and-security/authentication/secure-authenticator-ic-embedded-security-platform:A1006.