Evaluation of the ECDSA IHP Hardware Accelerator

Marcin Aftowicz, Dan Klann, Ievgen Kabin, Zoya Dyka
and Peter Langendörfer
IHP - Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany

31st Crypto Day, 17./18. October 2019

An untapped gold mine for forward thinking industries or the next logical step in the evolution of technology, the Internet of Things poses both - an opportunity and a challenge for commercial and scientific world. While expanding the information throughput and equipping all possible devices with an access to the net, we excise the limits of communication with no regard towards its security, allowing low cost products to leak the sensitive information to anyone listening.

In advent of self driving cars and smart cities, the necessity of secure information flow with very low latency is indisputable and can nowadays be only achieved using high-end processors. The established ITS security standards mandate the use of digital signatures to achieve the authenticity of messages.

In order to bring that ability to the embedded systems we implemented an ECDSA hardware accelerator, allowing over 2500 signature generations and 1200 signature verifications per second for B-233 elliptic curves. We have integrated the accelerator into an OpenSSL toolkit and run tests to uncover possible bottlenecks. The results of those measurement are the subject of this work.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-04