On the Impact of the Sampling Rate on the Success of Horizontal DEMA Attack

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

31st Crypto Day, 17/18 October 2019

Side channel analysis (SCA) attacks are nowadays well-known threats for cryptographic implementations. The measurement setup and its settings such as the sampling rate for the measurements of traces significantly influence the success rate of SCA attacks. In [Eisenbarth, Kasper, Moradi, Paar, Salmasizadeh & Shalmani (2008)] authors estimated technical requirements for the SCA attack against AES. They varied the sampling rate used for trace capturing to perform a successful vertical DPA attack and evaluated the number of traces that are necessary to recover the secret key.

In this work we performed a horizontal DEMA attack [Kabin, Dyka, Kreiser & Langendörfer (2018)] against traces of a kP execution captured with different sampling rates of the oscilloscope. As a device under attack we used a development board from Digilent [Arty-Z7 (2018)]. Instantiations of the investigated IHP kP design operating from 4 to 200 MHz clock frequency were ported to the Zynq-7020 system on chip. The measurement setup consists of a Langer MFA-R 0.2-75 near field probe connected to a LeCroy HDO9404-MS oscilloscope. We used sampling rates from 100 MS/s to 40 GS/s to capture traces of the kP execution always at the same measurement position and with the same input data for different operating frequencies. The traces captured with a wide range (from 1 to 10000) measured samples per clock cycle allow us to investigate the influence of the applied sampling rate on the correctness of the key revealed.

To the best of our knowledge, our attack results represent a first attempt to evaluate the impact of the sampling rate of the measurements on the success of horizontal SCA attack against an ECC implementation.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-06

References

ARTY-Z7 (2018). APSoC Zynq-7000 Development Board for Makers and Hobbyists. URL `https://reference.digilentinc.com/reference/programmablelogic/arty-z7/start`.

THOMAS EISENBARTH, TIMO KASPER, AMIR MORADI, CHRISTOF PAAR, MAHMOUD SALMASIZADEH & MOHAMMAD T. MANZURI SHALMANI (2008).

On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *Advances in Cryptology – CRYPTO 2008*, David Wagner, editor, 203–220. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-540-85174-5.

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`.