Horizontal SCA Attack using Machine Learning Algorithms

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

30th Crypto Day, 28/29 March 2019

Machine learning becomes popular way of data analysis nowadays. It provides many useful tools that may be applied to Side Channel Analysis by finding relationships in datasets without prior knowledge of the key. The first attempt to apply unsupervised cluster classification algorithms for an attack on an ECC implementation was described in [Heyszl, Ibing, Mangard, Santis & Sigl (2013)].

The *K-means* [Bock (2008)] algorithm is capable to cluster linearly separable data sets and is often used due to its simplicity. In this work we use the *k-means* algorithm to conduct several types of horizontal attacks against our two *kP* designs with and without countermeasures. We provide a comparison of these attacks with a traditional approach based on a Pearson correlation coefficient analysis and *the difference of the mean* [Kabin, Dyka, Kreiser & Langendörfer (2018)] attack. In the end we evaluate a success rate of the attack for each investigated case.

References

Hans-Hermann Bock (2008). Origins and extensions of the k-means algorithm in cluster analysis. *Journal for History of Probability and Statistics (JEHPS)* **vol. 4**. URL `http://www.jehps.net/Decembre2008/Bock.pdf`.

Johann Heyszl, Andreas Ibing, Stefan Mangard, Fabrizio De Santis & Georg Sigl (2013). Clustering Algorithms for Non-profiled Single-Execution Attacks on Exponentiations. In *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*, 79–93. URL `https://doi.org/10.1007/978-3-319-08302-5_6`.

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`.

crypto day matters 30 (2019)
Beiträge vom 30. Kryptotag, 28.-29.03.2019, Mozilla, Berlin.
doi:10.18420/cdm-2019-30-05