Intelligent Clustering as a Means to Improve K-means Based Horizontal Attacks

(The best paper award in The First International Workshop on Machine Learning for Security and Cryptography held in conjunction with IEEE PIMRC 2019)

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

31st Crypto Day, 17/18 October 2019

Machine learning approaches have a high potential for improving the success rate of side channel analysis attacks. In this paper we present horizontal side channel analysis attacks against three crypto-implementations suffering from different levels of leakage using a single power and a single electromagnetic trace. We show the effectivity of attacks using k-means as analysis tool. In addition we introduce a new approach that we call intelligent clustering that enables attackers to select the start centroids in such a way that the ability of k-means to extract the key bits is increased up to 38.56 % compared to k-means starting the farthest neighbors centroids and up to 66.66 % compared to the mean correctness for k-means starting with random centroids.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-10