Side Channel Analysis enhancement: A proposition for measurements resynchronisation

Nicolas Debande, Youssef Souissi, Maxime Nassar
Thanh-ha Le, Sylvain Guilley, Jean-Luc Danger
TELECOM ParisTech, 75 634 PARIS Cedex 13, FRANCE
Morpho, Osny, FRANCE

Abstract

Side Channel Attacks (SCA) have become an increasingly important issue and have posed a real serious practical threat to secure devices since their efficiency to break cryptographic implementations was theoretically and empirically proved. These attacks exploit unintentional physical leakage, such as the power consumption or the radiated magnetic field. In SCA, it seems natural that aligning traces (re-synchronization) is an important pre-processing phase since the deployed analysis are very sensitive to the magnitude of acquired measurements (*i.e.* traces). In the litterature of SCA, only few re-synchronization techniques were presented to the cryptographic community. N.Homma et al. proposed the Phase Only Correlation (POC [2]), which has been recently improved by S.Guilley (Threshold-POC [1]). In an other work, J.Van Woudenberg has used a more generic algorithm, so-called the Dynamic Time Warping (DTW [4]), to align SCA traces. In this paper, we first propose to explore and test the practicability of an interesting signal processing technique based on the high order statistics [3], in the context of SCA. Second, we show the efficiency of our method through a comparative study of existing resynchronisation techniques.

References

[1] Sylvain Guilley, Karim Khalfallah, Victor Lomne, and Jean-Luc Danger. Formal Framework for the Evaluation of Waveform Resynchronization Algorithms. In *WISTP*, June 1 2011.

[2] Naofumi Homma, Sei Nagashima, Yuichi Imai, Takafumi Aoki, and Akashi Satoh. High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching. In *CHES*, pages 187–200, 2006.

[3] Gareth M. James. Curve Alignment by Moments. *Annals of Applied Statistics*, 1:480–501, 2007.

[4] Jasper G. J. van Woudenberg, Marc F. Witteman, and Bram Bakker. Improving Differential Power Analysis by Elastic Alignment. In *CT-RSA*, pages 104–119, 2011.