ANalysis of Variance and CPA in SCA

S. Tiran, D. Aboulkassimi, G. Reymond,
J.-B. Rigaud, G. Ducharme, P. Maurine

Abstract

Since the Differential Power Analysis (DPA) by Paul C. Kocher, new Side Channel Attacks (SCA) or techniques to increase their efficiency have been proposed in the literature. E. Brier, C. Clavier and F. Olivier proposed the use of Pearson correlation, the so called Correlation Power Analysis is now one of the most used attack in this context. Few attention has been paid to the ANalysis Of VAriance (ANOVA). Its first used in the context of SCA was introduced by F. Standaert, B. Gierlichs [1], and further analyzed in [2]. However, it was found that CPA and ANOVA gave the same results. We propose to analyse more deeply the use of ANOVA, and to show that it can perform similar or much better results than CPA in all cases, maintaining the same ease of use and the same speed. Indeed, this distinguisher is able to detect even non linear leakages contrary to Pearson correlation.

[1] François-Xavier Standaert, Benedikt Gierlichs, and Ingrid Verbauwhede. Partition vs. comparison side-channel distinguishers: An empirical evaluation of statistical tests for univariate side-channel attacks against two unprotected cmos devices.

[2] Lejla Batina, Benedikt Gierlichs, and Kerstin Lemke-Rust. Differential cluster analysis.