Is information leakage spilling?

LILIAN BOSSUET, VINCENT GROSSO, CARLOS ANDRES LARA-NINO,

Université Jean Monnet Saint-Etienne, CNRS, Institut d'Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, France

Correlation Power Analysis (CPA) is one of the best known approaches for performing power analysis on cryptographic algorithms. If the implementation is unprotected, a reasonable number of power traces is required to validate the optimal key hypotheses and probably retrieve some part of a secret key. This is achieved by computing a correlation matrix with as many columns as the total number of key guesses and as many rows as the number of samples in the power traces. Then, the correct hypothesis is chosen as the guess with the largest correlation coefficient (or the largest absolute, depending on who you ask). But this ignores the second dimension of the matrix since we assume that a single sample will exhibit the greatest correlation against the model. However, what happens when the correlation "spills" over multiple samples? In this talk we show that in such a case it is possible to use an area estimator to improve the accuracy of selecting the correct hypotheses. We also discuss our impressions on how is this spill can be achieved.

ACKNOWLEDGEMENTS

This work has been supported by the French government through the *Agence Nationale de la Recherche* in the framework of the *France 2030* initiative under project ARSENE with reference ANR-22-PECY-0004.

Author's address: Lilian BOSSUET, Vincent GROSSO, Carlos Andres LARA-NINO,
Université Jean Monnet Saint-Etienne, CNRS, Institut d'Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, 18 rue du Professeur Benoît Lauras 42000, SAINT-ETIENNE, France, carlos.lara@univ-st-etienne.fr.