Advanced method for power trace alignment in Remote Power Analysis over Heterogeneous SoCs.

ANIS FELLAH-TOUTA, LILIAN BOSSUET, CARLOS ANDRES LARA-NINO,

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

Recent works have demonstrated that it is possible to carry out side-channel attacks on SoC-FPGAs, internally and remotely, without any specialized equipment used in traditional side channel attacks. These advances have highlighted the vulnerability of FPGA-based systems. So far, one of the main limitations of this type of attacks is the problem of remotely determining a stable timing reference point for aligning the traces that correspond to the power consumption of the targeted module. Essentially, because there is no practical way to acquire a trigger signal directly from the architecture under attack since it is, usually, logically isolated. In this work, we propose a stable trigger mechanism based on a frequency-based covert channel, which can be leveraged to improve the feasibility of remote power attacks. We demonstrate this approach by performing a successful key recovery on a hardware implementation of AES-128.

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: Anis FELLAH-TOUTA, Lilian BOSSUET, 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.