PhaseSCA: Exploiting Phase-Modulated Emanations in Side Channels

Pierre Ayoub (1), Aurélien Hernandez (1), Romain Cayre (1), Aurélien Francillon (1), Clémentine Maurice (2)

(1) EURECOM, Sophia Antipolis, France

(2) Univ. Lille, CNRS, Inria

Abstract

In recent years, the limits of electromagnetic side-channel attacks have been significantly expanded. However, while there is a growing literature on increasing attack distance or performance, the discovery of new phenomenons about compromising electromagnetic emanations remains limited.

In this work, we identify a novel form of modulation produced by unintentional electromagnetic emanations: phase-modulated emanations. This observation allows us to extract a side-channel leakage that can be exploited to reveal secret cryptographic material. We introduce a technique allowing us to exploit this side-channel in order to perform a full AES key recovery, using cheap and common hardware equipment like a software-defined radio. Moreover, we demonstrate that the exploitation of this new phase leakage can be combined with traditional amplitude leakage to significantly increase attack performance. While investigating the underlying phenomenon causing this unintentional modulation, we identified several prior works that have approached similar exploitation - without being aware of each other. Creating a bridge between older and recent work, we unveil the relationship between digital jitter and signal phase shift in the context of side-channel attacks and fill the gap between prior works from various research fields.