Side-Channel Leakage: A Case Study of GIFT-COFB

Rogelio Calvillo, Brisbane Ovilla, Cuauhtemoc Mancillasi
CINVESTAV-IPN, Mexico

Abstract

Side channel attacks represent a category of attacks against implementations of hardware or software of cryptography algorithms. These attacks aim to recover the secret key or the encrypted data as plain text, totally or partially, through the information leaked by devices unintentionally.
We propose to make a detailed study on the security of a software implementation of the GIFT-COFB algorithm against attacks focused on Correlational Power Analysis, which is a side-channel attack that exploits power consumption during the execution of the cryptographic operation. In particular, the ChipWisperer-lite board captures the power consumption traces on target devices. In work, we propose looking out for powers consumption models that, together with the execution of a plaintext-chosen attack, allow obtaining the cryptographic key by relating the encrypted texts with the consumption traces obtained from each execution on the target device. The purpose of carrying out these attacks is to find vulnerabilities in the GIFT-COFB implementations and propose concrete countermeasures to make these implementations resistant to such attacks. Our results will improve the security of software implementations of the GIFT-COFB lightweight cryptography algorithm.