Correlation Electromagnetic Attack on PRESENT Lightweight Block Cipher

Nilupulee A. Gunathilake, Ahmed Al-Dubai, William J. Buchanan and Owen Lo

School of Computing, Edinburgh Napier University

Abstract

Side-channel attacks are an unavoidable risk factor in cryptography. Therefore, continuous observations over physical leakages are essential in order to verify the strengths of recommended ciphers. PRESENT is an ultra-lightweight block cipher which is promising to be applied on IoT devices in the near future. Our preliminary reviews of literature showed unavailability of a correlation electromagnetic analysis (CEMA) of it. Hence, in an effort to fill in this research gap, we opted to investigate the capabilities of CEMA against the PRESENT algorithm. This work aims to determine the probability of secret key leakage with a minimum number of EM waves possible. The process initially started from a simple EMA (SEMA) and gradually enhanced up to a CEMA. The current results indicate a probability of leaking seven bytes of the encryption key out of ten. The work still continues towards an optimisation of the attack.