2016 Third International Conference On Artificial Intelligence And Pattern Recognition (AIPR), 19-21 September 2016, Lodz University of Technology

Vulnerability of advanced encryption standard algorithm to differential power analysis attacks implemented on ATmega-128

Kealeboga Mpalane ; Naison Gasela ; B.M Esiefarienrhe ; H.D Tsague

ABSTRACT:

A wide variety of cryptographic embedded devices including smartcards, ASICs and FPGAs must be secure against breaking in. However, these devices are vulnerable to side channel attacks. A side channel attack uses physical attributes such as differences in the power consumption measured from the physical implementation of the cryptosystem while it is performing cryptographic operations to determine the secret key of the device. This paper investigates the vulnerability of 128-bits advanced encryption standard (AES) cryptographic algorithm implementation in a microcontroller crypto-device against differential power analysis (DPA) attacks. ChipWhisperer capture hardware Rev2 tool was used to collect 1000 power traces for DPA. We observed and measured the behaviour of the power consumption of the microcontroller while it was encrypting 1000 randomly generated plaintexts using the same secret key throughout. Our attack was successful in revealing all the 16 bytes (128-bits) of the secret key and the results demonstrated that the AES implementation can be broken using 1000 encryption operations.