Design for Security: Assignment 2

March 28, 2023

Mutual Information Analysis

A trace file called "AES_TRACE_FILE" has been uploaded to the Hello IITK Portal. Your job is to find out the entire last round 128-bit AES Key using mutual information analysis. Your intermediate target variable should be the 9th round AES S-Box output. You are free to choose the leakage model. Please note that as the traces are obtained from an FPGA implementation of AES, Hamming weight leakage model may be a sub-optimal choice.

Signal to Noise Ratio Computation

Compute the signal-to-noise ratio of the given power trace where the target variable is 9th round AES S-Box output.