

Daniel is a security engineer, and he has a got a project for side-channel analysis of an AES hardware implementation. He has already collected power traces for that AES implementation with a 128-bit key 'K' and have stored the traces in "traces_AES.csv" file. The first column in the csv file indicates the plaintext, the second column indicates the ciphertext and rest of the columns indicates the sample points. Now Daniel has to analyse the power traces and will have to find the AES key using Correlation Power Analysis (CPA). Help Daniel to perform the CPA attack.