Security Lab – Introduction to Correlation Power Analysis

for

POULPY CODE-BREAKERS

This laboratory involves hands-on experimentation by making use of Correlation Power Analysis (CPA) techniques on an Advanced Encryption Standard (AES) implementation coded in C, running on a STM32 ARM-based microcontroller.

The main goal will be to study the AES algorithm and the STM32 – Nucleo Printed Circuit Board (PCB) and propose a measurement method. Then power traces will be captured with the use of an Oscilloscope. The attack will be completed by performing CPA on the captured traces.

$$Plaintext: \begin{bmatrix} d_1 \\ \vdots \\ d_D \end{bmatrix} \quad Key\ Hypotheses: [k_1 \quad \dots \quad k_K]$$

$$AES\ Properties: \big(SBOX(data\ xor\ key)\big) \rightarrow V = \begin{bmatrix} v_{1,1} & \cdots & v_{1,K} \\ \vdots & \ddots & \vdots \\ v_{D,1} & \cdots & v_{D,K} \end{bmatrix}$$

$$By\ applying\ a\ hypothetical\ power\ model\ on\ array\ V\ we\ get \rightarrow\ array\ H:$$

$$Hypothetical\ Power\ consumption: H = \begin{bmatrix} h_{1,1} & \cdots & h_{1,K} \\ \vdots & \ddots & \vdots \\ h_{D,1} & \cdots & h_{D,K} \end{bmatrix},$$

$$Measured\ Power\ Traces: \qquad T = \begin{bmatrix} t_{1,1} & \cdots & t_{1,T} \\ \vdots & \ddots & \vdots \\ t_{D,1} & \cdots & t_{D,T} \end{bmatrix}$$

$$By\ performing\ a\ statistical\ analysis\ on\ arrays\ H\ and\ T\ we\ get\ the\ Correlation\ Coefficients:$$

$$R = \begin{bmatrix} r_{1,1} & \cdots & r_{1,T} \\ \vdots & \ddots & \vdots \\ r_{K,1} & \cdots & r_{K,T} \end{bmatrix}$$

$$r_{i,j} = \frac{\sum_{d=1}^{D}\Big(\big(h_{d,i} - \bar{h}_i\big) \cdot \big(t_{d,j} - \bar{t}_j\big)\Big)}{\sqrt{\sum_{d=1}^{D}\big(h_{d,i} - \bar{h}_i\big)^2 \cdot \sum_{d=1}^{D}\big(t_{d,j} - \bar{t}_j\big)^2}}$$

h_i and t_j refer to columns of the corresponding arrays.

Tasks: Complete the Matlab script which perfoms the attack

For MATLAB script go to the following folder and copy in this folder the file "attack_data.mat"
Security_TP\work_handout_code\MATLAB\aes_stm32\attack_folder

1.1. Explain what each of the arrays: D, K, V, H and R represents.

1.2. Complete the missing code in order to perform the Correlation Power Analysis (CPA) attack.

1.3. Concerning the hypothetical power model use Hamming Weight.

1.4. Perform the CPA attack and try to find only some bytes of the key according to the instructor directions. Include in your report the key you have found.

1.5. What is the maximum correlation?

1.6. Explain in your report why, in your opinion, Hamming Weight can be used as a hypothetical power model.

1.7. Include in your report all the files found in the attack folder after performing the CPA attack, besides the two files: "attack_data.mat" and "constants.mat".

1.8. Explain the content of the file "attack_data.mat" in detail.

1.9. Why is array R of size KxT ?

1.10. What is the minimum number of traces necessary to find one byte of the key with each hypothetical power model?

1.11. Find the Matlab function which implements equation.

1.12. Shortly explain ways (minimum two ways) with which you can increase the security of the AES, either the Tiny-AES or any AES in general, against CPA attacks.