Lab Report - Smartcard

Author: Ali, Muhammad Fateh
Matriculation Number: 03708599
Group: 03

First part: Differential Power Analysis Attack

- **Grooming and Trace Acquisition** **04/05/2019 – 13/05/2019**
  - Reading and understanding of Lab Script with the help of book.
  - Acquisition of traces (400 and 1000) via python script.

- **Implementation of DPA Attack Algorithm** **14/05/2019 – 22/05/2019**
  - Reading data in MATLAB to plot traces.
  - Implementation of equations to get Hypothetical Power Consumption Matrix.
  - Implementation with “corrcoef” function in MATLAB.
  - Implementation of Pearson Correlation formula with vectorization.

- **Testing and Verification of of DPA Attack Algorithm** **23/05/2019 – 24/05/2019**
  - Testing Sample measurement file available on git to generate reference key.
  - Extraction of key for available set of traces to check consistency.
  - Verification of key from online AES encryptor.

- **Improvement to DPA Script and Documentation** **25/05/2019 – 27/05/2019**
  - Trace Compression to analyse speed vs window size trade off.
  - Improvement of overall code structure, variable names, plots etc.
  - Detailed Documentation of DPA script and committing on git.

Second part: Attack on DPA Countermeasures

- **Grooming for attack on countermeasures** **15/06/2019 – 23/06/2019**

- **Attack on Hiding Countermeasures** **24/06/2019 – 04/07/2019**
  - Acquisition of higher number of traces to break hiding countermeasures.
  - Low quality random numbers with higher number traces yield correct key.
  - High quality uniform random numbers and its effects.
  - Improvement in the trace compression as pre-processing to align power traces.
  - Extraction of correct key after attacking shuffling and dummy operations.

- **Implementation of 2nd order DPA** **05/07/2019 – 07/07/2019**
  - Implementation of pre-processing loop for absolute difference.
  - Modification for hypothetical power consumption matrix.
  - Large amount of data handling and memory management for correlation.

- **Efforts to attack Masking countermeasure** **05/07/2019 – 10/07/2019**
  - Lots of traces were acquired in lab with different parameters.
  - In detail, traces were analysed, correlation matrix was analysed to compare differences.
  - Other Pre-Processing Techniques were implemented in efforts to extract correct key.