Deep Learning for Side Channel Attack

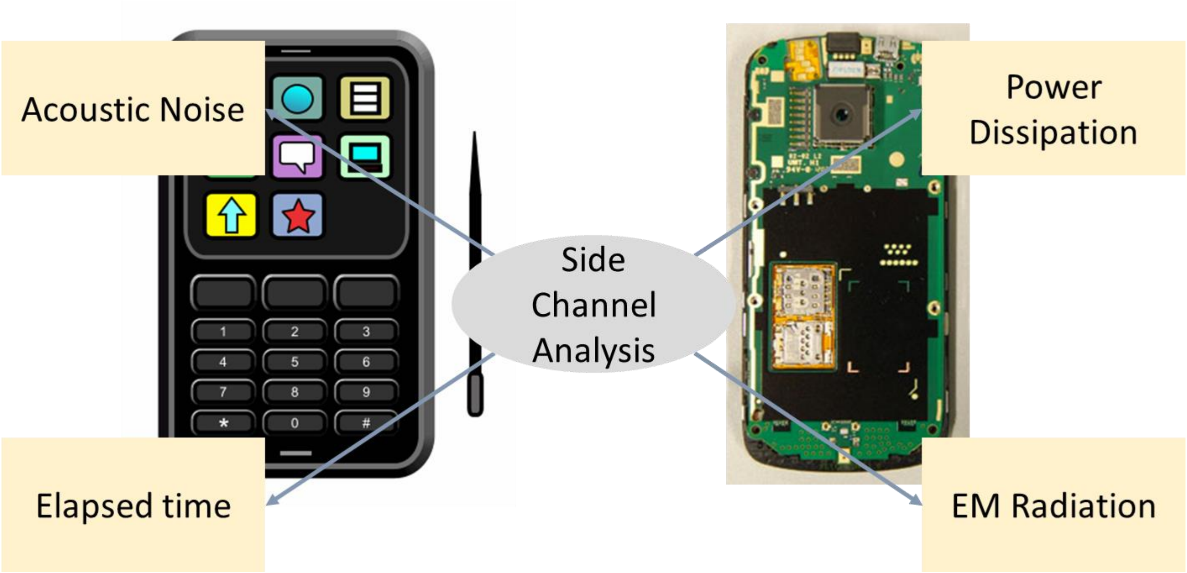
Group 19
E/17/038
E/17/101
E/17/292

Contents

- What is SCA?
- Side Channel Attacks
- Countermeasures
- What is RFTC?
- Why RFTC?
- Our Aim
- Summary of literature
- Methodology
- Current work done
- Work plan
- Expected outcomes and impacts

What is SCA?

- Attack that exploits information leaked through the physical implementation

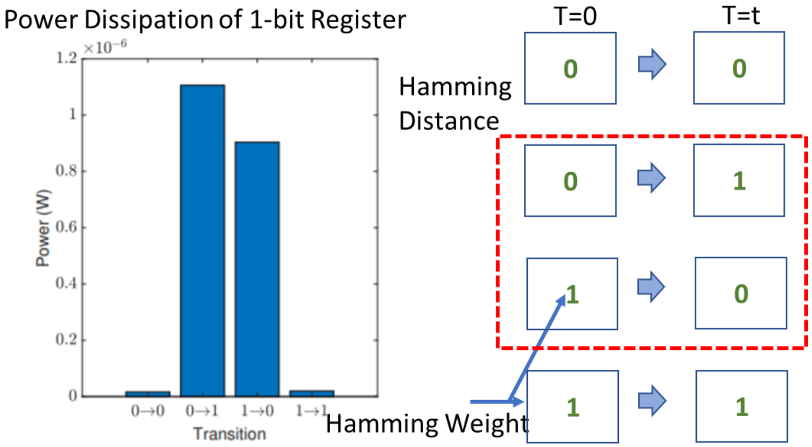


Side Channel Attacks

- Power Analysis Attacks
- Differential Power Analysis (DPA)
- Simple Power Analysis (SPA)
- Timing Attacks
- Electromagnetic Radiation Analysis (e.g., Van Eck phreaking)
- Acoustic Cryptanalysis

Power Analysis Attack

- Revealing the secret information via the power dissipation of the device (proposed by Paul Kocher in 1999)
- Why?
  - CMOS gates are the most popular building blocks of IC manufacturing
  - Power dissipation of CMOS gates depend on inputs



Countermeasures

- Masking : randomizing or masking the sensitive data during cryptographic operations
- Noise Injections: introduces additional noise in the side-channel signals
- Random Delay Insertion (RDI): inserts random delays into the execution of instructions.
- Random Clock Dummy Data (RCDD): inserts random dummy data into the clock signal.

What is RFTC?

- **R**andom **F**requency **T**uning **C**ountermeasure
- Introduces random frequency variations in the clock signal during the execution of cryptographic operations
- Instead of using a fixed clock frequency, RFTC dynamically changes the clock frequency at different phases of the operation.
- For example, during the key generation phase, the clock frequency might be set to 800 kHz, and during the encryption phase, it might be set to 1.2 MHz.

Why RFTC?

- None of the countermeasures were tested and proven to be secure against Correlation Power Analysis (CPA) based attacks (Preprocessed methodologies):
  - Dynamic Time Warping based CPA attacks (DTW-CPA)
  - Principal Component Analysis based CPA attacks (PCA-CPA)
  - Fast Fourier Transform based CPA attacks (FFT-CPA)
- RFTC is tested against all three attacks and shown to be secure for up to four million encryptions.
- But not tested against ML attacks

Project - Our Aim

- Testing RFTC against Machine Learning models using AISY framework
- Improving MLP and CNN models to attack RFTC

Summary Of Literature Review

- What are the countermeasures taken already
- RFTC what and why
- template and deep learning approaches
- AISY

Template and Deep Learning Approach

Template Attack

- requires a pre-computation phase
- performs statistical analysis on the new set of side-channel power traces from the target device
- Issues: in high-dimensional spaces, making it difficult to estimate accurate statistical models or capture meaningful patterns

Template and Deep Learning Approach

Deep Learning Approach

- Choice of algorithm depends on the nature of the problem or issue and the characteristics of the data
- Eg: Recurrent Neural Networks (RNNs), Long Short Term Memory (LSTM), Generative Adversarial Networks (GANs), Reinforcement Learning (RL), Deep neural networks (DNNs), Convolutional neural networks (CNNs),multilayer perceptron (MLP)
- CNN and MLP has played a major role

AISY framework

- a deep learning-based framework for profiling side-channel analysis
- brings state of-the-art deep learning-based side-channel attacks
- enables the users to run the analyses and report the results efficiently
- offers all commonly used settings and allows users to extend the framework according to their needs easily.
- comes with the option to store all analysis results in an SQLite database
- web application provides a user-friendly way to visualize analysis, plots, results, and tables
- user can generate the full script used to produce results stored in the web application database

Methodology

- Create custom dataset with available traces
- Convert that to .h5 file format
- Test various models and find best ML architecture to attack unprotected AES
- Use that model to attack AES protected with RFTC (use available traces)
- Find a better model if previous model was not able to break AES protected with RFTC
- Compare the results with previous works

Current work done

- Literature Review
- Going through more papers regarding RFTC countermeasure
- Following tutorials to learn more about MLP and CNN
- Going through AISY framework code structure

Work Plan

Semester 7

Week	1	2	3	4	5	6	7	8
Finalize topic	■							
Literature Search		■	■	■	■	■		
Study AISY framework		■	■	■	■	■	■	■
Project Proposal					■	■	■	
Make .h5 format dataset								■
Report writing			■	■	■	■	■	■

Work Plan

Semester 8

Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Attack unprotected AES using MLP	🟥	🟥													
Attack unprotected AES using CNN			🟥	🟥											
Attack AES protected with RFTC using MLP			🟥	🟥	🟥	🟥	🟥								
Attack AES protected with RFTC using CNN					🟪	🟪	🟪	🟪	🟪	🟪					
Evaluation		🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪	🟪			
Report Writing	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥		
Finalize report														🟪	🟪

Expected Outcome & Impacts

- Find best ML architecture to work with RFTC
- Models and parameters
- Results of attacks
- Github repository regarding AISY

Thank You

Q & A