Lab 2 – SCA

Stjepan Picek
s.picek@tudelft.nl

Delft University of Technology, The Netherlands

May 18, 2018

- Implement Correlation Power Analysis.
- Attack datasets from the Non-profiled folder.
- Report results: which dataset is easier to attack (low_noise or high_noise)? Which is easier to use: ciphertext or plaintext? What is the key?
- Implement template attack.
- Attack datasets from profiled folder (traces_HW correspond to model_HW and trace_value to model_value).
- The datasets consists of 50 000 measurements. Use 25 000 for profiling and 25 000 for attacking.
- Report results: which is easier to attack: HW or value model? What are the results? What happens if the profiling set becomes smaller, e.g., 10 000?
- Optional: compare your results for TA with some machine learning technique (not necessary/mandatory but could help you assessing if TA implementation is correct).
- Describe your implementations (CPA and TA).

Report

- All measurements are in Assignment SCA.zip.
- One report per group.
- Keep the report within 10 pages limit, one column.
- Submit your code.
- Reports are due on June 5th, 18:00 (at latest).

Further explanations

- For info on CPA, check https://wiki.newae.com/Correlation_Power_Analysis
- For info on TA, check https://wiki.newae.com/Template_Attacks

Explanation on traces files for Non-profiled folder

- Each row in a file corresponds to a single encryption.
- The values are Hamming weights of round outputs (HW(round output)).
- There are 10 values since there are 10 rounds for AES-128.
- Observe, the values in traces are numbers between 0 and 128 – since the state has 128 bits, max HW can be 128.
- The decimal parts are due to the noise (for instance having a value of 74.32 could mean that your output is 74 (so your round state has Hamming weight 74) and there is noise equal to 0.32).
- Meaning the traces are direct representations of Hamming weights or round outputs (with some noise).
- Row i in traces file corresponds to row i in pt and ct files.

Bonus Assignment

- In some scenarios, template attack will not work good.
- Implement pooled template attack (explanations in Efficient Template Attacks.pdf). Note, here it is also nicely explained template attack.
- Once we obtain our guesses in profiled attacks, we still need some work in order to guess the key. The question is how many traces we actually need in order to guess the key?
- Implement guessing entropy and success rate metrics (explanations in A Unified Framework for the Analysis.pdf).
- Use pooled TA and security metrics to evaluate the profiled dataset (only consider HW model and use 25 000 measurements in the attack phase! You need to use the second half of the measurements for attack). What are the results?
- Submit your code and report up to 10 pages single column.
- Reports are due on June 16th, 18:00 (at latest).