Lab 3 – Countermeasures

Stjepan Picek
s.picek@tudelft.nl

Delft University of Technology, The Netherlands

June 3, 2018

- Implement RSA with square-and-multiply, square-and-multiply-always, and Montgomery ladder technique.
- Explain the difference between techniques.
- There is no need to implement any support for big integers for this assignment. Normal numbers (e.g., 32-bit values) are OK.

- Implement AES-128 and record measurements in the Hamming distance model.
- Consider S-box output where a register stores values. In the initial moment the register is pre-charged to 0.
- Use CPA to attack the AES implementation, report results.
- Add a random delay countermeasure to AES.
- For each value to be measured (S-box output) store either:
  1. S-box output with some Gaussian noise, or
  2. Random value
- Decide which value to use uniformly at random.
- Report on results, which dataset is more difficult to attack. Why?

Report

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