Lab 1, Twente, Group 1

Stjepan Picek
s.picek@tudelft.nl

Delft University of Technology, The Netherlands

May 3, 2018

- Implement a PRNG.
- Test PRNG with NIST tests (full set or any subset). It is sufficient to implement some NIST tests and just use those.
- Write a report describing what PRNG is implemented, what tests are used, and what are the statistical results?
- Can you make then results better? How?

- Implement a simulation of an arbiter PUF consisting of 32 stages.
- Use Logistic Regression to attack it.
- Change that implementation into XOR PUF consisting of 2 PUFs, each with 16 stages.
- Use Logistic Regression to attack it.
- Report on the results of both attacks.
- The number of challenge response pairs (CRP) is a user-defined parameter. What happens when there are more CRPs?

Report

- One report per group.
- Keep the report within 5 pages limit, one column.
- Negative results (e.g., unsuccessful attacks, statistical tests that failed) are also results, report on those.
- Reports are due on May 17th, 18:00 (at latest).

Bonus Assignment

- https://security1.win.tue.nl
- Submit the results for phase 1 by June 1st.
- Submit the results for stage 2 by June 25th.
- If you have really good results, win the competition!