CRYPTACUS

ICT COST Action 1403

WG 3: Hardware and Software Security Engineering

Machine Learning and Evolutionary Computation in Cryptology

Stjepan Picek, Domagoj Jakobović, Marin Golub

Sophia-Antipolis, 6.-7. November 2016

What can we do with

- **Machine Learning (ML) techniques?**
  - Regresion.
  - Feature selection.
  - Prototyping.
  - Classification.
  - Clustering.

- **Evolutionary Computation (EC) algorithms?**
  - Optimization.

This work is presented at

- PROOFS 2016

  S. Picek, A. Heuser, S. Guilley
  Template Attack vs. Bayes Classiffier

- SAC 2016

  S. Picek, B. Yang, V. Rozic, N. Mentens
  On the Construction of Hardware-friendly 4x4 and 5x5 S-boxes

Using machine learning techniques for profiled side-channel attacks

- **Side-Channel Attack (SCA)**
  - powerful class of cryptanalysis techniques
  - passive, non-invasive implementation attacks
- **Profiled side-channel attacks**
  - two phases: profiling phase and attack phase
  - Template Attack (TA) is the most powerful attack from the information theoretic point of view
  - some ML techniques also belong to the profiled attacks

Using machine learning techniques for profiled side-channel attacks

- **difficulties**
  - space and time complexity grows significantly with the increase in the number of features or classes (as well as with more complicated ML techniques)
  - profiling and tuning phase is a long process where one cannot be sure in the optimality of the results
- **goal is to explore some simpler ML techniques**
  - for multiclass classification
  - **Naive Bayes**
    - attributes (measurements) are mutually independent
  - **Averaged n-Dependence Estimators**
    - n-dependences

Experimental evaluation

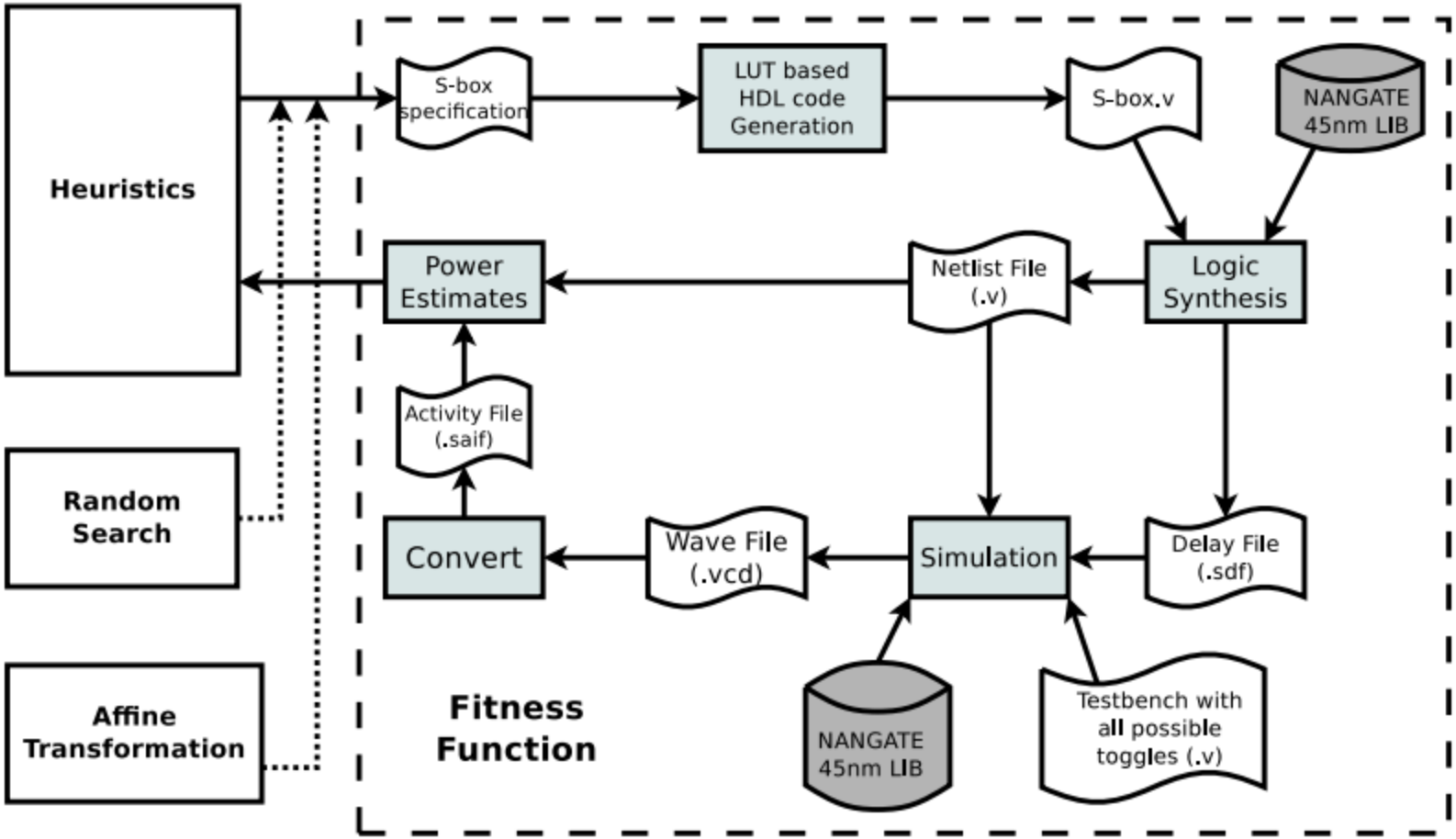
- **datasets**
  - **DPAcontest v2** provides measurements of an AES hardware implementation (noisy)
  - **DPAcontest v4** provides measurements of a masked AES software implementation (noiseless)
- **results are promising**
  - **Naive Bayes** and **A1DE** give competitive results when compared with **TA**
  - **A1DE** is better than **Naive Bayes**

Using evolutionary computation for power consuption minimization of 4x4 S-boxes

- **Static power consumption**
  - caused by subthreshold currents and gate leakage
  - constant over time and does not depend on the clock frequency or the switching activity

- **Dynamic power consumption**
  - originates from the switching activity of the circuit
  - in older technology nodes the dynamic power consumption was dominant in the total power consumption and the static power consumption was negligible
  - with smaller technology nodes, the relative contribution of the static leakage power consumption has increased

Simulation setup for the generation and evaluation of S-boxes



Discussion and experimental evaluation

- results are very good
- two-stage search
  - cryptographic proprties
  - hardware proporties (power consumption, area)
- heuristics is able to find S-boxes with good cryptographic properties that are also small and power effcient