Effect of Power Trace Set Properties to Differential Power Analysis

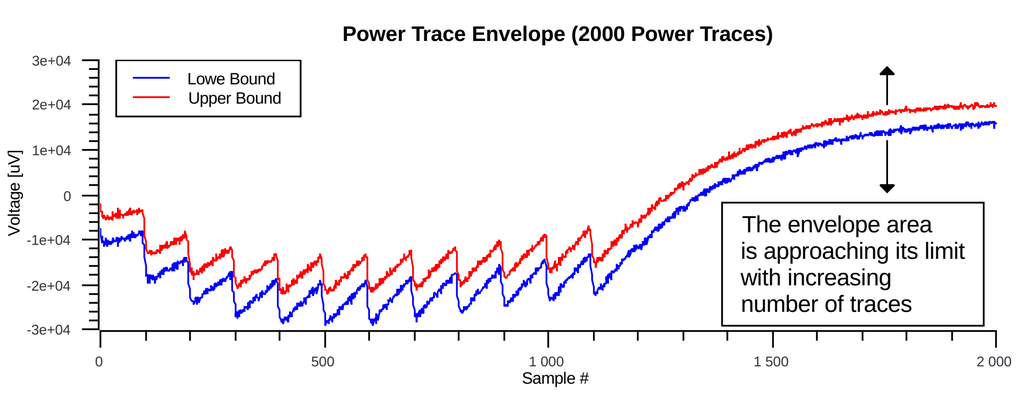
Motivation

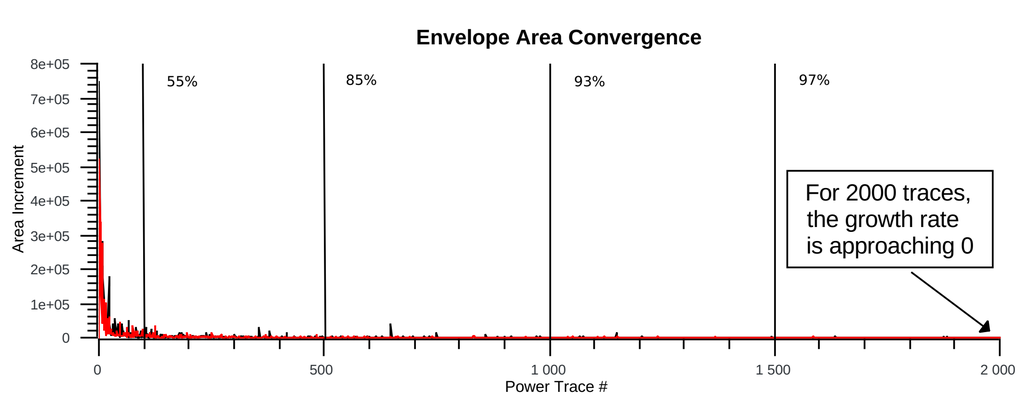
- The properties of power traces widely used for side-channel attack execution were not systematically studied
- Evaluation of power traces used by side channel differential power analysis attacks (DPA) in general offers the opportunity to evaluate circuit vulnerabilities, the efficiency of countermeasures or even identify unknown vulnerabilities

Method

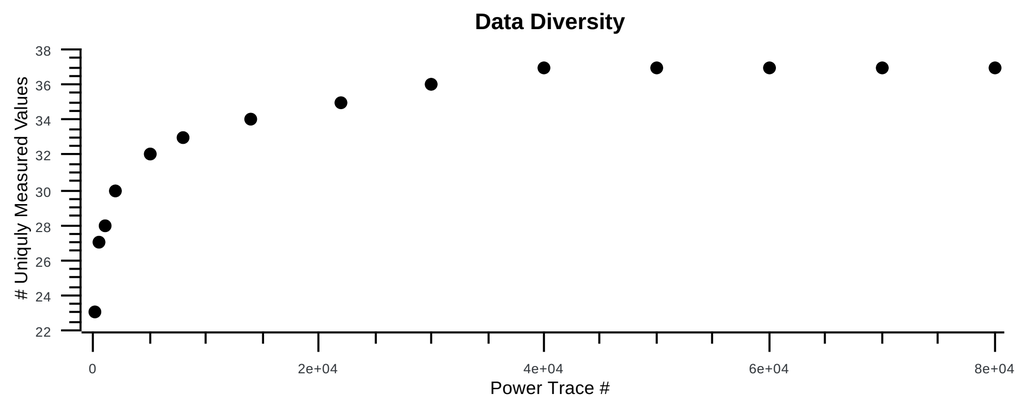
- The in-data variation/data diversity is examined
- Comparison with Principal Component Analysis (PCA) is provided
- The Difference of Means principle was used for evaluation because of:
  - → no power model is used, thus no model inaccuracy is introduced
  - → it is well suited for data under evaluation
  - → extracting groups of power traces distinguished by Hamming Weight (from the dataset) is simple to implement and simple to evaluate

Dataset Characterization – The Geometrical Approach



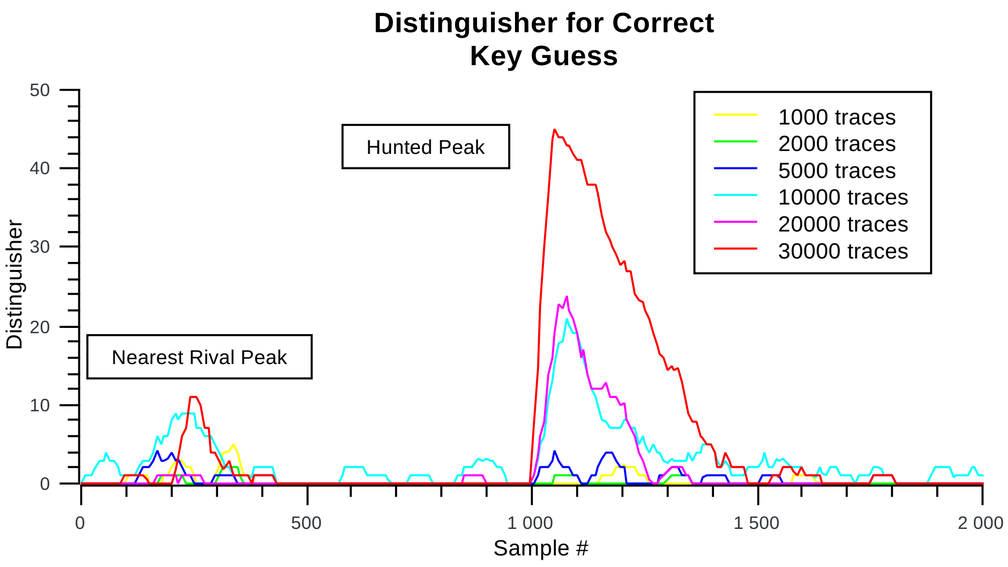


- A dataset (power traces) for AES @ Artix7 FPGA implementation
- Values in the Power Trace Envelope (PTE) are ≈ normally distributed
- The size of the PTE characterizes the in-trace variability – is the computation well balanced?
- The Data Diversity limit characterizes the vertical DC accuracy of the measuring equipment
- The variance in Power Trace Envelope is ≈ uniformly distributed

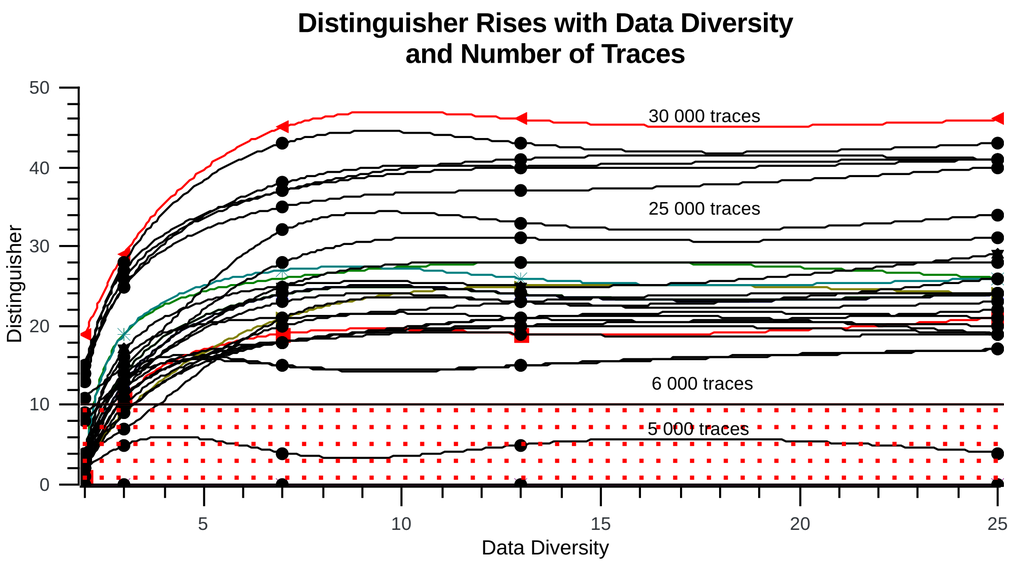


Principal Component Analysis (PCA) gives similar results as the geometric approach – 100 (randomly selected) traces express the dataset variance accurately and the variance is distributed almost uniformly for all sample IDs across the dataset

Difference of Means – The Distinguisher



- The dataset under evaluation is split into two chunks according to the Hamming Weight (HW) of the processed data
- Mean values for both chunks are computed for each sample ID: the difference of means is significant in particular samples, where data of interest are processed
- The binary output of Welch's t-test (quantile = 0,99) is summarized inside sliding-window of size 1/2 of clock cycle for neighbouring sample IDs → The Distinguisher



- The dataset diversity has been reduced to evaluate the influence of measurement accuracy (nearest points with equal sample IDs – in all traces – were merged)
- The distinguisher recognizes the hunted peak well:
  - → for more than 5k traces for diversities about 5
  - → for at least 25k traces even for data diversity 2 (lower limit)
- The diversity above 5 is sufficient and its further increasing has no significant influence on distinguisher quality

Outcomes

- Dataset variance cannot be used for vulnerability estimation or for selection of the moment (sample), where an attack likely succeeds
- Attacker concentrates on in-data information (e.g. Hamming Weight of processed data), which does not have relation to in-trace variance
- For diversities between 2 and 5: when the data diversity is increased by factor 2, the distinguisher quality is increased (at least) by factor 1.5
- The ability to distinguish two values only inside Power Trace Envelope is sufficient for successful attack but the number of power traces must be significantly high

Acknowledgements

The dataset (100k power traces) was provided by Vojtěch Miškovský from CTU in Prague.

The author highly appreciates the consultation related to statistical hypothesis testing provided by Zdeněk Kobeda from UWB in Pilsen.

This research has been partially supported by the grant GA16-05179S of the Czech Grant Agency and by CTU grant SGS17/213/OHK3/3T/18.

Computational resources were provided by the CESNET LM2015042 and the CERIT Scientific Cloud LM2015085, provided under the programme "Projects of Large Research, Development, and Innovations Infrastructures".

Jan Bělohoubek, Petr Fišer, Jan Schmidt

{jan.belohoubek, petr.fiser, jan.schmidt}@fit.cvut.cz

Faculty of Information Technology, Czech Technical University in Prague

FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE