On the First-Order Leakage in Side-Channel Traces of ASCAD Database

Kotaro Saito, Akira Ito, Rei Ueno, Naofumi Homma
Graduate School of Engineering, Tohoku University

Summary

- We report that there is a first-order leakage from the device (i.e., a set of power traces) provided by ASCAD
  - It is mentioned that there is no first-order leakage from the device as a result of calculating SNRs
  - However, the result shows that the 3rd byte of key in variable key database is clearly recovered by first-order Correlation Power Analysis (CPA) .

First-order Correlation Power Analysis (CPA)

- Well-known textbook CPA was used in this report
  - First-order CPA is performed by calculating Pearson's correlation coefficient ρ between hypothetical power consumption $\boldsymbol{p}_k$ and actual traces $\boldsymbol{T}(t)$:

$$\rho = \frac{cov\left(\boldsymbol{p}_k, \boldsymbol{T}(t)\right)}{\sqrt{var(\boldsymbol{p}_k) \cdot var(\boldsymbol{T}(t))}},$$

  where k denotes key candidate and t denotes time. The dimension of vectors is given by the number of data n.
  - Key candidate which gives the highest correlation coefficient is estimated as a recovered key

Power estimation model and datasets

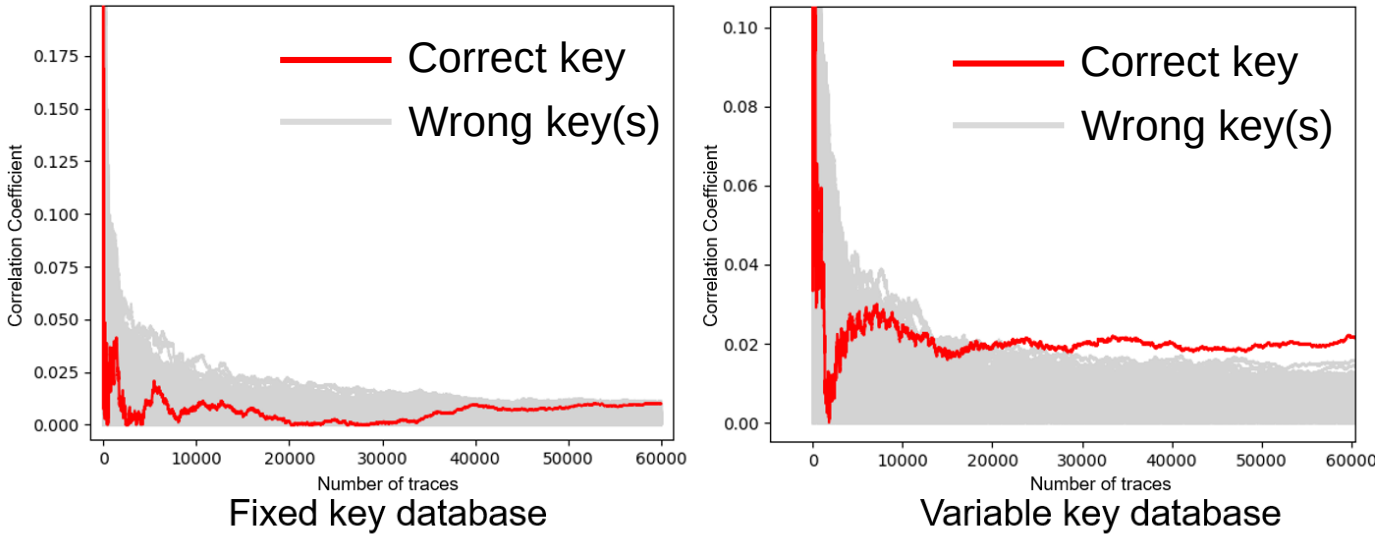
- Hypothetical power consumption of S-box by hamming weight is given by

$$p_k = \mathrm{HW}(\mathrm{Sbox}(\mathrm{plaintext}[3] \oplus \mathrm{key}[3]))$$

- For discussing the existence of first-order leakage, the presence of masking was NOT considered

- Use 2 datasets provided by ASCAD
  - Fixed key database: CPA was performed with both profiling and attack traces because the key value was fixed
  - Variable key database: CPA was performed only with attack traces because the key value was fixed in the traces

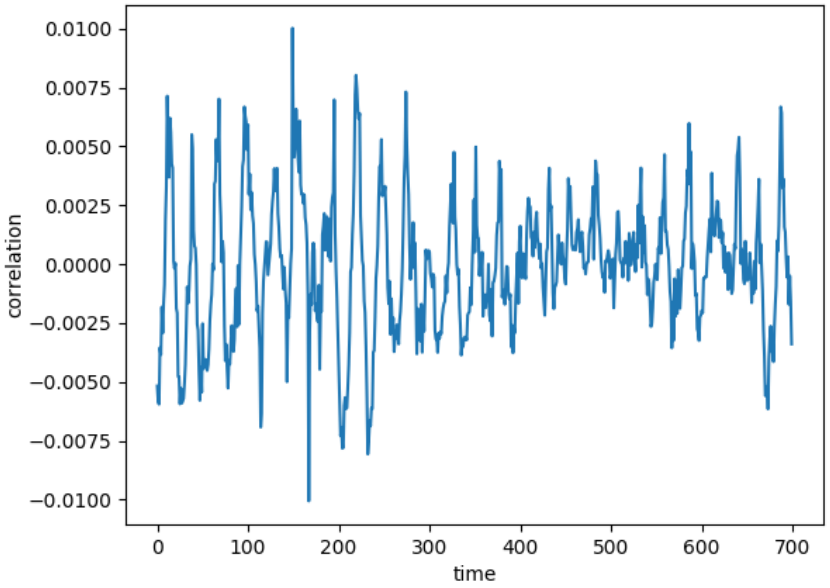
Results of CPAs



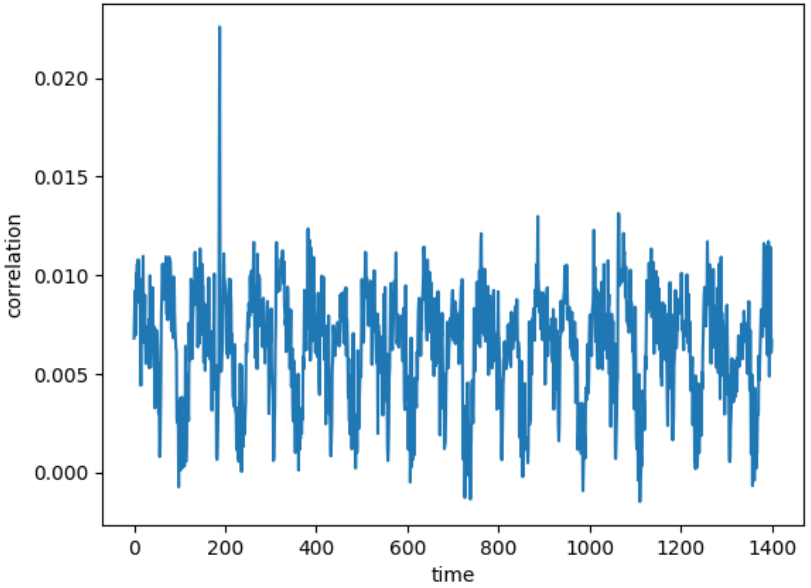
- In variable key database (right), the correct key gave the highest correlation coefficient, which shows there is a first-order leakage from the device

- In fixed key database (left), the rank of correct key was not the first. However, the correlation coefficient given by the correct key is increasing, and there is also a high possibility of first-order leakage

Results of known key analysis



Fixed key database

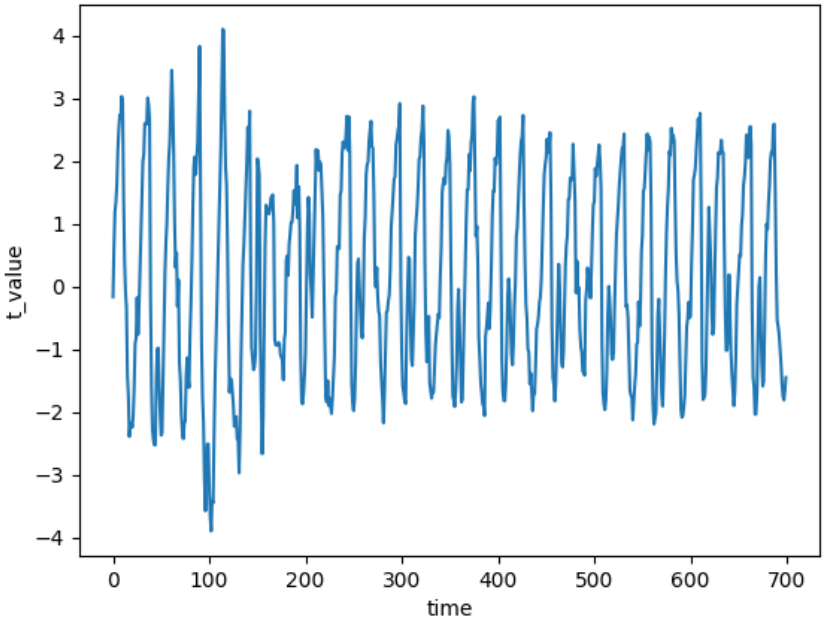


Variable key database

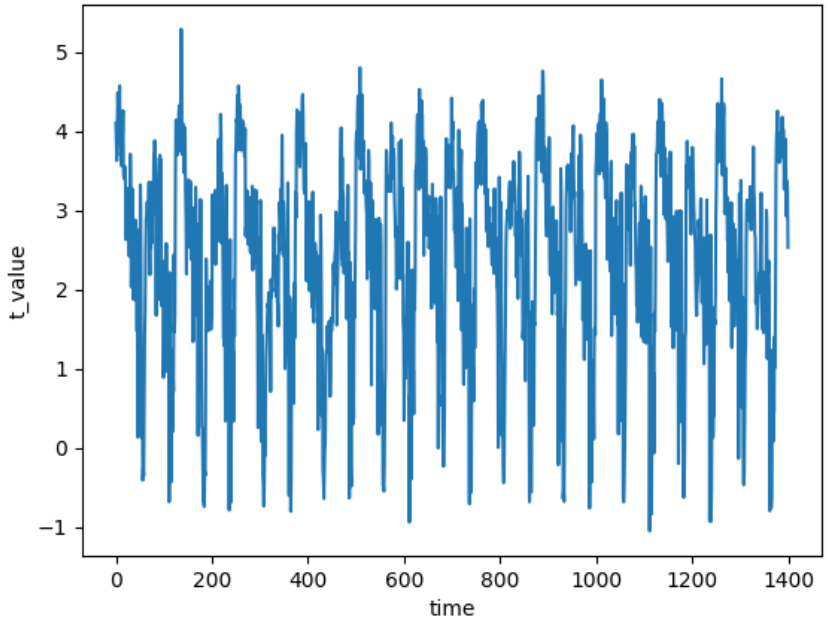
- Calculate time-wise correlation coefficient with the correct key for determining where we should perform CPA

- Highest correlation coefficient was obtained at t = 167 in fixed key database and t = 188 in variable key database

Results of Welch's t-tests



Fixed key database



Variable key database

- Fixed key database: the maximum t value is 4.11
- Variable key database: the maximum t value is 5.29