MACHINE LEARNING BASED POWER ANALYSIS Attacks

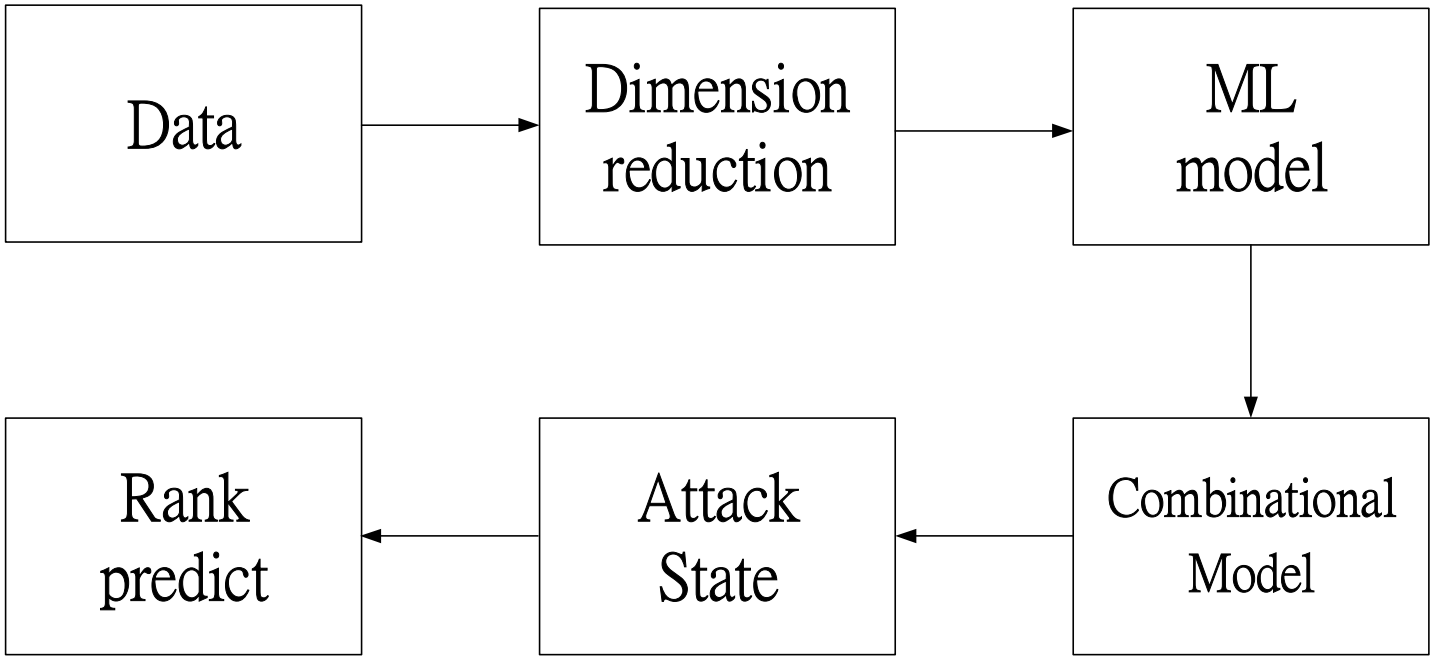
Presenter: Yun-Wen Lu

Advisor: Chen-Yi Lee Hsie-Chia Chang

Motivation

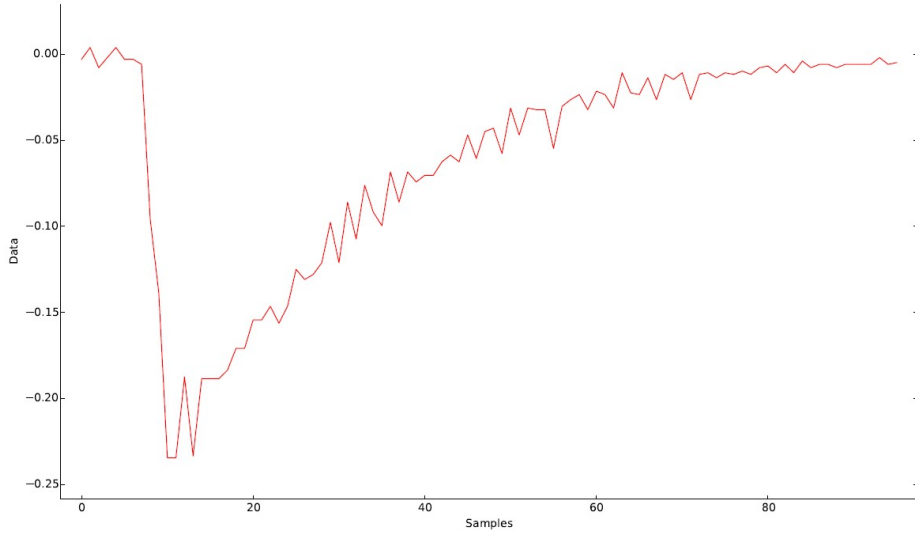
- Power analysis and machine learning have natural similarity.
- Need an alternative method for non-optimal profiling .

structure


Data
Dimension reduction
ML model
Combinational Model
Attack State
Rank predict

Attack aes

- Attack round key of single round (16 byte of round key)
- Attack first round
- Attack each subkey separately (8 bits a subkey)
- Need Pre-processing ?



Conclusion & Future Work

- Conclusion: ML-based side channel attack provides good methods to choose points of interest and increase robustness when encounters non optimal profiling.

- Future work:Try to implement the state of the art ML-based side channel attack method at pre-processing module or distinguisher module.