Deep learning based side channel attack for AES software implementation on RISC-V microcontroller

Ngoc-Tuan Do, Van-Phuc Hoang,
Institute of System Integration (ISI),
Le Quy Don Technical University, Hanoi, Vietnam

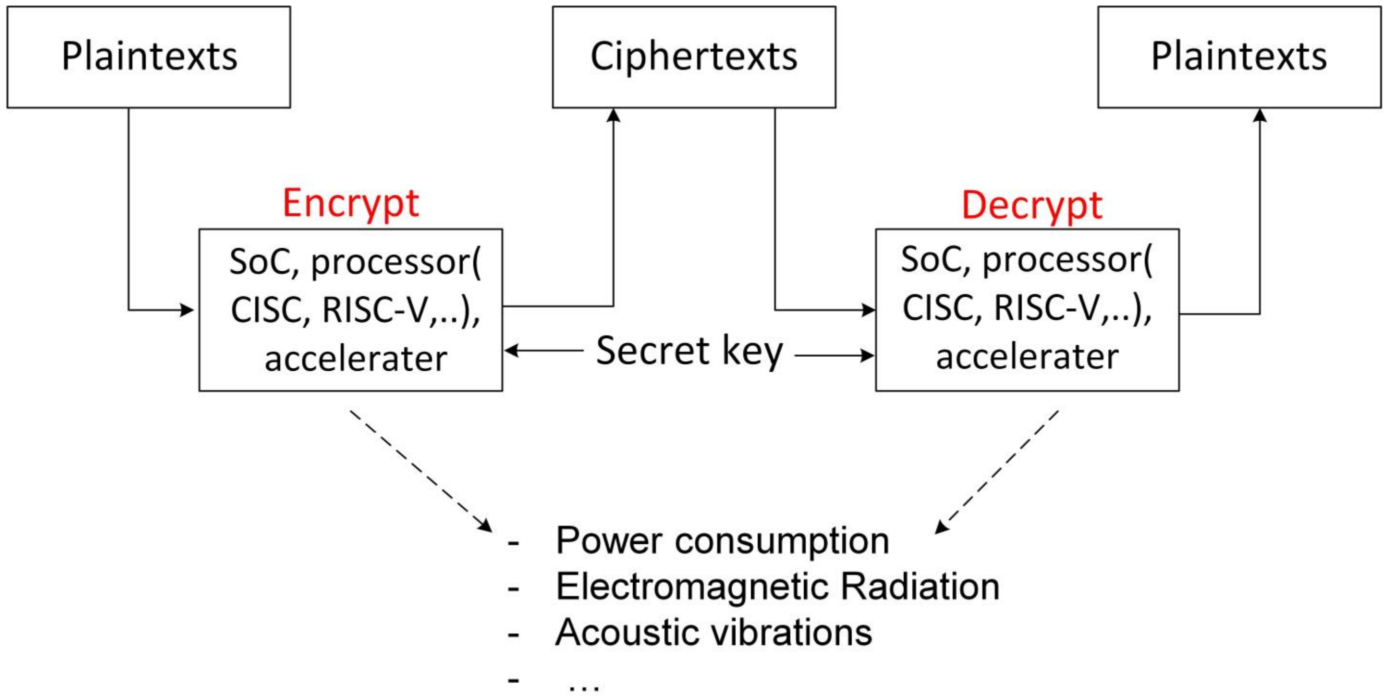
January 2022

Presentation Outline

- Introduction
- RISC-V side channel data preparation
- Deep learning based non-profiled SCA
- Countermeasures
- Conclusions and future works

Introduction

1. Side channel attack



- Side channel attacks can easily break the security of different cryptographic implementations.
- The openness and flexibility of the RISC-V could be exploited for mounting side channel attacks.

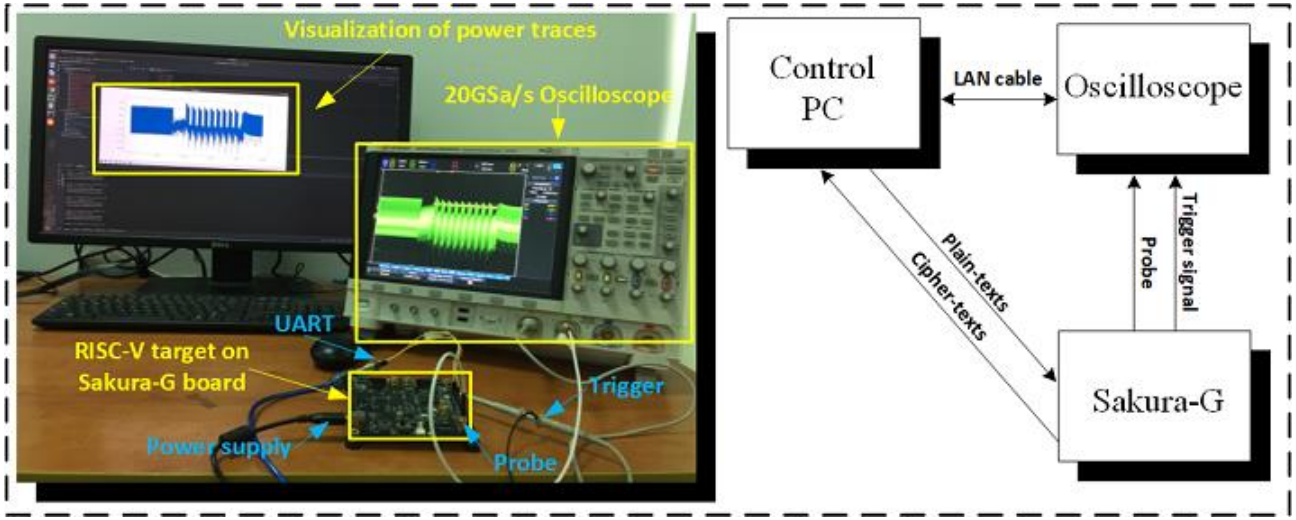
Introduction

2. Side channel attack evaluation

- Assessing the security of an electronic system against SCA is a long, expensive, and complex process.
- Requires various skills and expertise from very different fields (electronics and hardware, signal processing, statistics, cryptography, deep learning, etc.)
- Traditional SCA methods: Correlation power analysis (CPA), Differential power analysis (DPA), Template attacks (TAs) require some preprocessing techniques: traces synchronization, noise filtering, POI selection, dimensionality reduction,…
- Deep learning based SCA methods: they can break conventional SCA countermeasures (masking, misalignment, shuffling) without knowledge of the countermeasures.

RISC-V side channel data prepararion

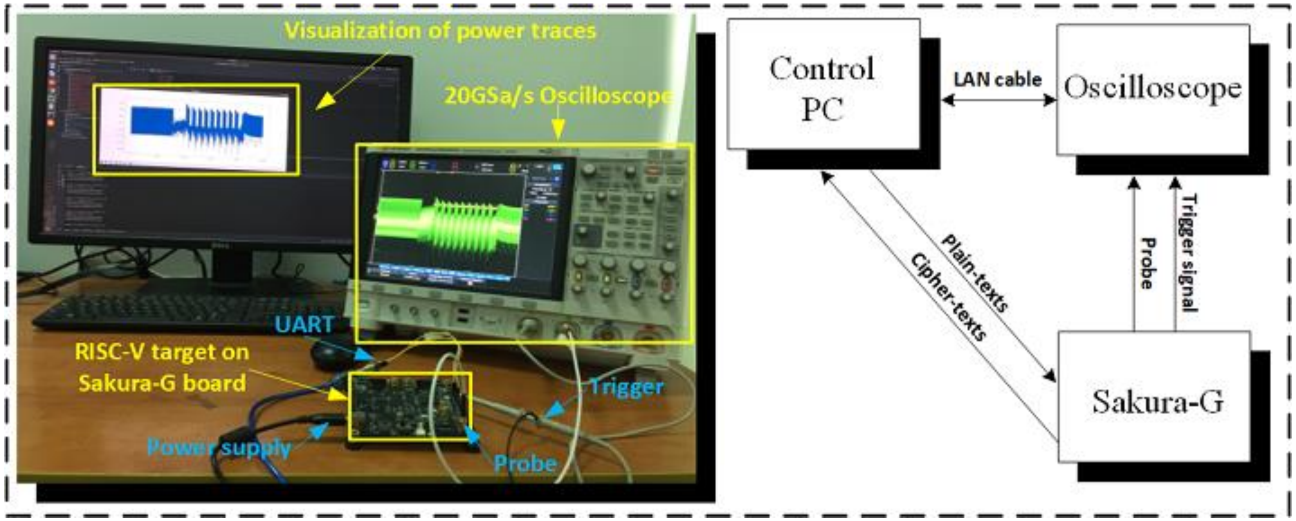
1. Side channel data collecting auto system



- 32-bit Murax RISC-V MCU, 48 Mhz running on Sakura-G board.
- Keysight DSOX6004A Oscilloscope is employed to measure side-channel data when the RISC-V MCU operates the AES-128 encryption.

RISC-V side channel data prepararion

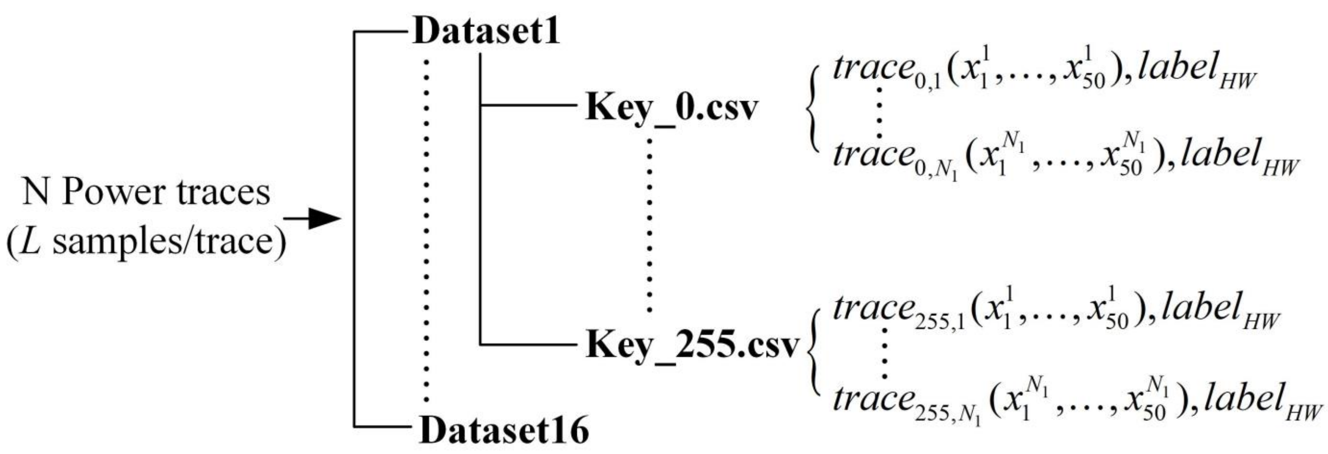
1. Side channel data collecting auto system



- Step 1: Repeatedly sends plaintexts to the RISC-V MCU and commands the oscilloscope to capture the power traces when the MCU executes each encryption.
- Step 2: The control PC receives the measured data from the oscilloscope and corresponding ciphertext from the MCU.
- Step 3: Verifies the ciphertext to ensure that the MCU works correctly. The power traces and the corresponding plaintexts and ciphertexts are saved to NumPy files for creating dataset.

RISC-V side channel data prepararion

2. Dataset reconstruction



- Reduce as ~200-fold compared to original power traces (from 9919 to 50 dimensions).
- Using only three labels HW3, HW4, HW5 for training.

RISC-V side channel data prepararion

2. Dataset reconstruction

- Power consumption model:

$$h_{n,k} = HW\left(Sbox\left(Plaintext_n \oplus k\right)\right)$$

- Pearson correlation coefficient

$$\rho_{k,i} = \frac{\sum_{n=1}^{N}(h_{n,k} - \bar{h}_k)(t_{n,i} - \bar{t}_i)}{\sqrt{\sum_{n=1}^{N}(h_{n,k} - \bar{h}_k)^2 \sum_{n=1}^{N}(t_{n,i} - \bar{t}_i)^2}}$$

- Taking 50 highest values of correlation to deduce 50 positions of power trace
- From 50 positions, create the dataset for all hypothesis keys corresponding to three labels HW3, 4, 5

RISC-V side channel data prepararion

2. Dataset reconstruction

Dataset 1:
+ Unmasked ASCAD
+ 3000 power traces
+ 700 features

Dataset 2:
+ Unmasked ASCAD
+ ~2000 power traces
+ 50 features

Dataset 3:
+ RISC-V SCA data
+ 10000 power traces
+ 50 features

Dataset 4:
+ RISC-V SCA data
+ ~7000 power traces
+ 50 features

Deep learning based non-profiled SCA

➢ **Profiled deep learning based SCA attack**

- Require access to a copy of the target device with full control.
- Need a huge number of power trace to construct a template model.
- Require a DL training for all guess keys.
- Popular architectures: MLP, CNN

➢ **Non-profiled deep learning based SCA attack**

- Do not require a copy of target device.
- Side channel power trace and leakage function are directly used for key extraction.
- Require a DL training for each hypothesis key (256 trainings for AES-128 subkey)
- Popular architectures: MLP, CNN, BNN.

Deep learning based non-profiled SCA

Previous works:

- Differential deep learning analysis (DDLA) is the first DL based SCA technique in non-profiled context [1].
- The dimension of data input determines the complexity of neural network. DDLA requires training process for all hypothesis keys.
- Hamming Weight model cause imbalanced data problem [2]. There are no reports of using HW labeling in non-profiled context.
- The impact of additive noise has been investigated in profiling DL based SCA [3], not in non-profiled context.

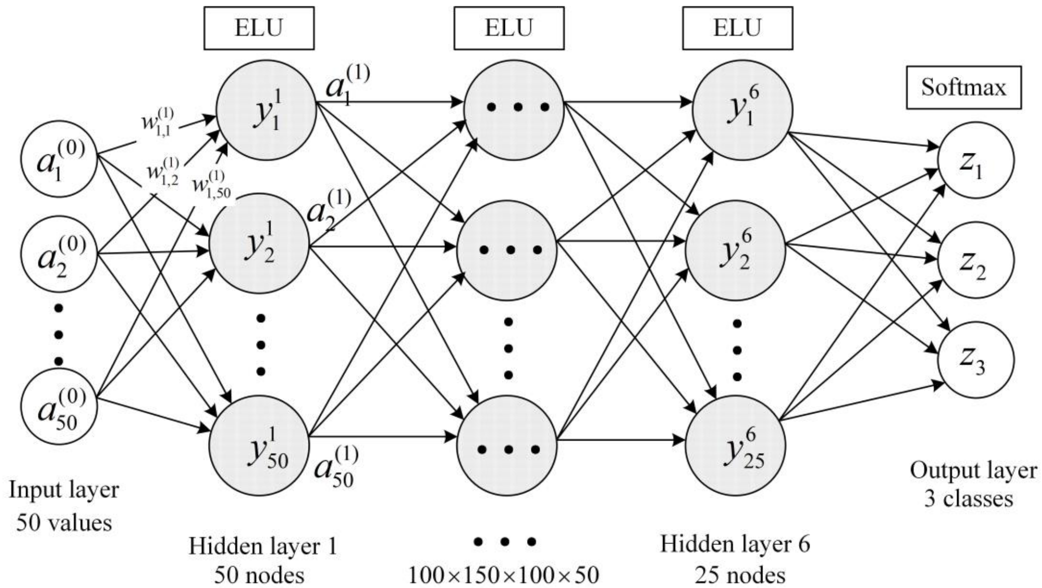
[1] B. Timon, "Non-profiled deep learning-based side-channel attacks," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 196, 2018.

[2] S. Picek, A. Heuser, A. Jovic, S. Bhasin, and F. Regazzoni, "The curse of class imbalance and conflicting metrics with machine learning for sidechannel evaluations," 2018,.

[3] J. Kim, et al. "Make some noise. unleashing the power of convolutional neural networks for profiled sidechannel analysis," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 148–179, 05 2019

Deep learning based non-profiled SCA

MLP architecture:



Proposed MLP for non-profiled side channel attacks [1]

[1] Ngoc-Tuan Do, Van-Phuc Hoang, Van-Sang Doan, "Performance Analysis of Non-profiled Side Channel Attack Based on Multi-Layer Perceptron Using Significant Hamming Weight Labeling," INISCOM 2022 (Accepted).

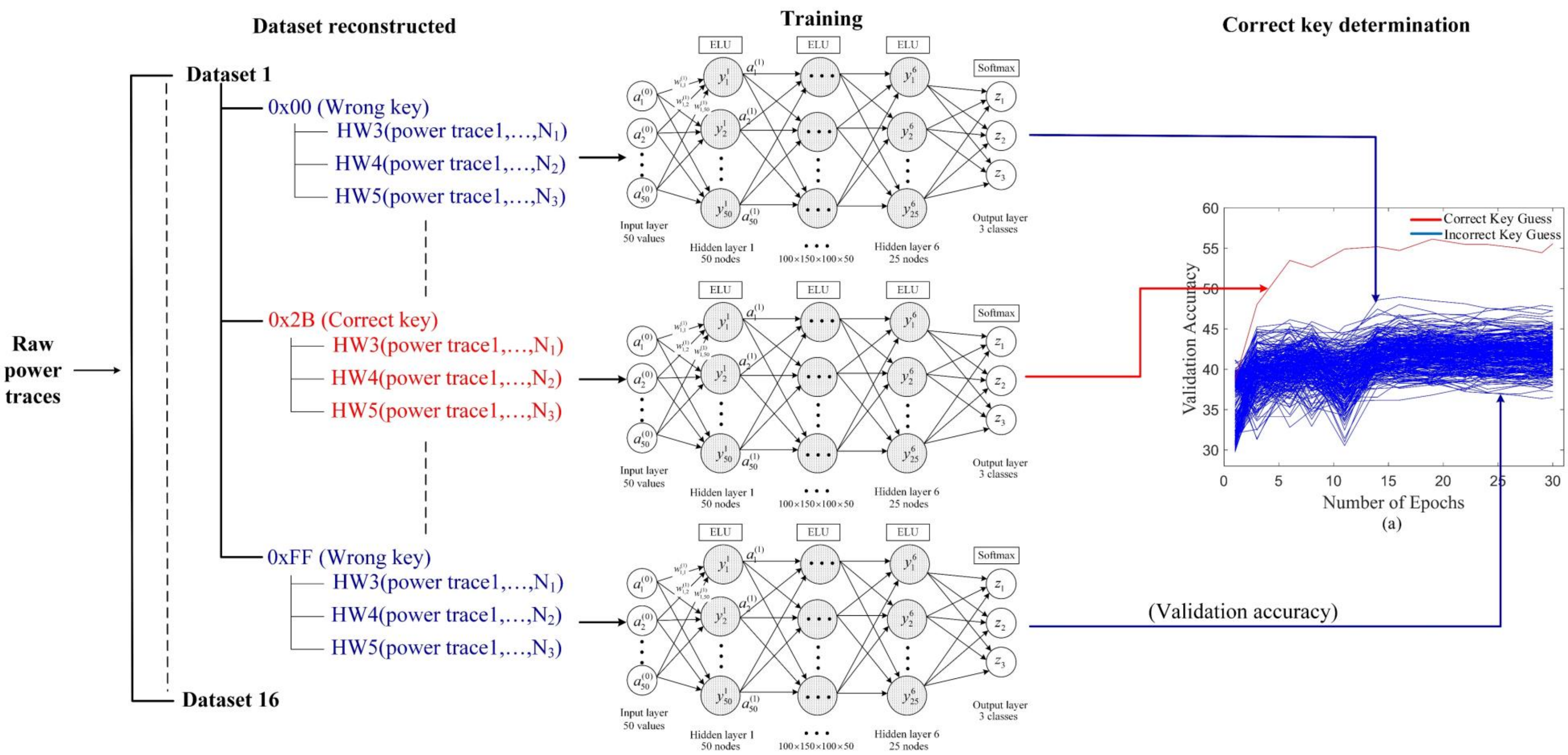
Deep learning based non-profiled SCA

MLP architecture:

- Non-profiled SCA based on multi-layer perceptron with power traces for software AES-128 implementation on RISC-V microprocessor.
- Our proposal uses correlation for reducing the data dimension (ie. From 9919 to 50).
- Using three significant HW values to deal with the imbalance dataset problem.
- The proposed method reduces the number of required power traces (30%).

Deep learning based non-profiled SCA

Deep learning based distinguisher:



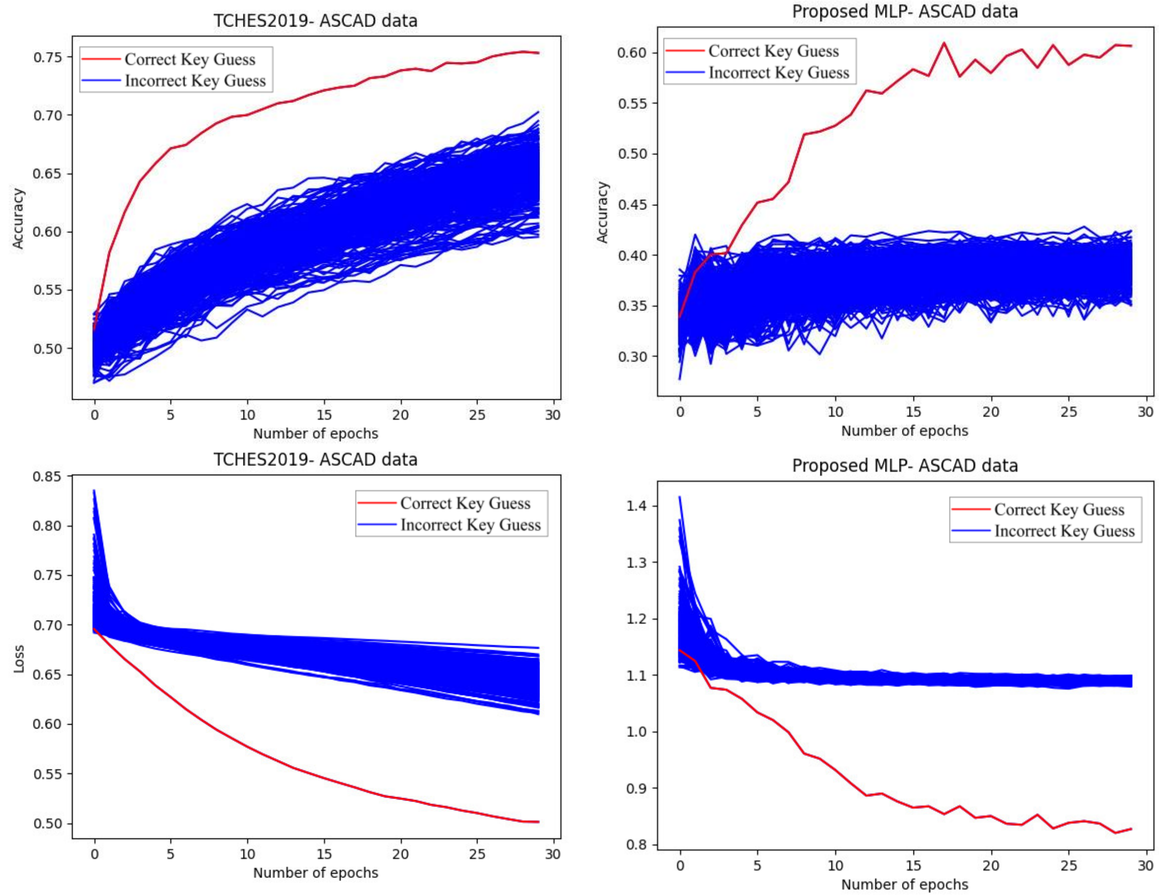
Deep learning based non-profiled SCA

Experimental results:

Dataset 1:
+ Unmasked ASCAD
+ 3000 power traces
+ 700 features

Dataset 2:
+ Unmasked ASCAD
+ ~2000 power traces
+ 50 features

Dataset 1 | Dataset 2



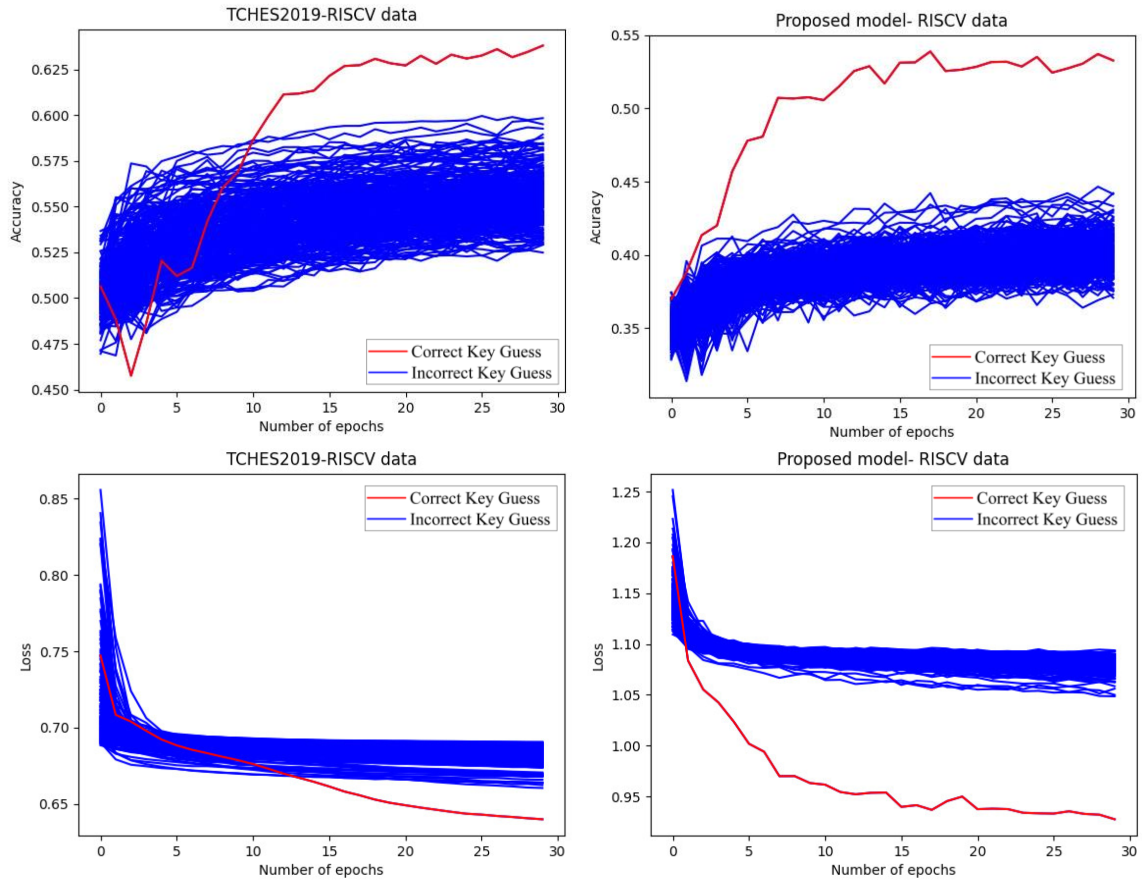
Deep learning based non-profiled SCA

Experimental results:

Dataset 3:
+ RISC-V SCA data
+ 10000 power traces
+ 50 features

Dataset 4:
+ RISC-V SCA data
+ ~7000 power traces
+ 50 features

Dataset 3 | Dataset 4



Countermeasures

- Side-channel analysis countermeasures are categorized into masking and hiding.
- In [1,2], the authors showed that DL based methods can break conventional SCA countermeasures (masking, misalignment, shuffling) without knowledge of the countermeasures in non-profiled context.
- Our experimental results have demonstrated in that DL based non-profiled SCAs are sensitive to additive noise.
- Hiding countermeasures are better methods for preventing deep learning based side-channel attacks.

[1] E. Prouff, R. Strullu, R. Benadjila, E. Cagli, and C. Dumas, “Study of Deep Learning Techniques for Side-Channel Analysis and Introduction to ASCAD Database,” *CoRR*, pp. 1–46, 2018.

[2] B. Timon, “Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis,” *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2019, no. 2, pp. 107–131, 2019, doi: 10.46586/tches.v2019.i2.107-131.

Countermeasures

- Alipour *et al.* [1] showed that a noise-generation-based hiding countermeasure may provide better protection against non-profiling DLSCAs than a masking countermeasure.
- The author in [2,3] presented two hiding methods called RDBB and RDFS against DL based SCA attack on RISC-V processor.

+ RDBB are based on controlling noise levels in measurements and provides better protection against the state-of-the-art non-profiling DLSCA.

+ RDFS generates more than 219,000 distinct frequencies for driving only the cryptographic accelerators.

[1] A. Alipour, A. Papadimitriou, V. Beroulle, E. Aerabi, and D. Hely, “On the Performance of Non-Profiled Differential Deep Learning Attacks against an AES Encryption Algorithm Protected using a Correlated Noise Generation based Hiding Countermeasure,” *Proc. 2020 Des. Autom. Test Eur. Conf. Exhib. DATE 2020*, pp. 614–617, 2020, doi: 10.23919/DATE48585.2020.9116387.

[2] B. A. Dao, T. T. Hoang, A. T. Le, A. Tsukamoto, K. Suzaki, and C. K. Pham, “Exploiting the Back-Gate Biasing Technique as a Countermeasure against Power Analysis Attacks,” *IEEE Access*, vol. 9, pp. 24768–24786, 2021, doi: 10.1109/ACCESS.2021.3057369.

[3] B.-A. Dao, T.-T. Hoang, A.-T. Le, A. Tsukamoto, K. Suzaki, and C.-K. Pham, “Correlation Power Analysis Attack Resisted Cryptographic RISC-V SoC with Random Dynamic Frequency Scaling Countermeasure,” *IEEE Access*, vol. 9, pp. 1–1, 2021, doi: 10.1109/access.2021.3126703.

Conclusions and future works

- Assessing the security of RISC-V processors against SCA is necessary and important.
- DL based methods can provides promising solutions for SCA evaluation process in non-profiled context.
- Preliminary results have clarified the advantages of this approach.
- Experimental results have demonstrated in that DL based non-profiled SCAs are sensitive to additive noise. Hiding countermeasures are suitable for preventing DL based SCA on RISC-V processors.
- New DL models need to be considered to improve the efficiency of evaluation process, such as multi-label learning, multi-task learning.

Thank you for your attention!

Q&A!