**ICT Virtual Organization of ASEAN Institutes and NICT (ASEAN IVO)**

**Appendix 2.2**

## Report of International Conference Presentation

| | |
|---|---|
| Name:<br>(Presenter) | Van Phuc Hoang |
| Affiliation: | Institute of System Integration, Le Quy Don Technical University, Vietnam |
| Project Title: | Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH) |
| Name of International Conference:<br>(Link to website) | 2024 IEEE Internatinal Workshop on Technologies for Defense and Security (2024 IEEE TechDefense)<br>Website: https://techdefense.org/ |
| Title of Research Paper: | Enhancing Performance of Deep Learning Based Non-Profiled Side-Channel Attack Using Multi-Output and Transfer Learning |
| Name of all Co-authors (if any) | Ngoc-Tuan Do, Huu Minh Nguyen |

Comments or feedback received at the conference:

There are two comments after presentation including-

- The presentation is very interesting with a novel method. It should be extended with more experimental results.
- The informaion of attack time should be considered as well.

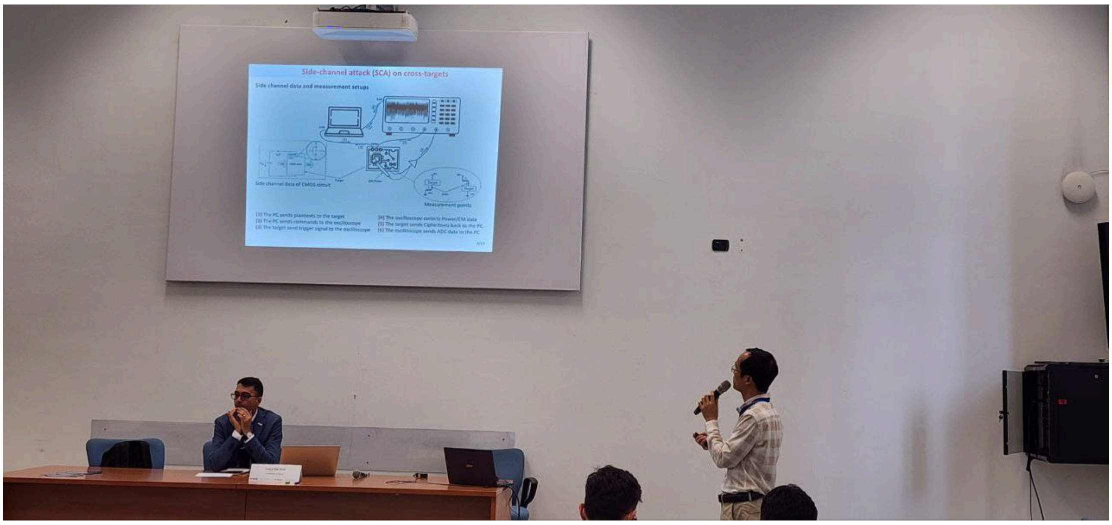
Question: Which cryptographical algorithm to be attacked with the proposed methods?

Answer: The AES cryptography is attacked in this research. However, it can be adapted to other algorithms.

Contribution to the project:

This paper contributes to the project by providing a new side channel analysis (SCA) technique that leverages a multi-output deep learning neural network and transfer learning to enhance the performance of non-profiled SCA on targets with similar properties to the original target. Specifically, we demonstrate the advantage of our method in nonprofiled attacks over power traces collected from AVR XMEGA microcontrollers using ChipWhisperer. The experimental results show that our technique requires only 10% of the power traces compared to the first target to reveal the subbyte key in the second target. Additionally, the attack time for the second target is reduced significantly, approximately by a factor of 5.7, compared to the conventional multi-output deep learning based SCA technique.

Photos


Side-channel attack (SCA) on cross-targets
Side channel data and measurement setups

(Presentation)

THANK YOU FOR YOUR ATTENTION!
Acknowledgement
This publication is the output of the ASEAN IVO project, "Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH)", and financially supported by NICT, Japan.
ASEAN IVO

(Questions and comments)

**[Required Documents]**

A) Presentation Materials (e.g., PPT slides)

B) Final Program of the conference

**Reporter: Van Phuc Hoang**

**Date: November 15, 2024**