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

Appendix 2.2

Report of International Conference Presentation

Name: (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: (Link to website)	The 16th IEEE International Symposium on Embedded Multicore/ Many-core Systems-on-Chip (MCSoC-2023) https://mcsoc-forum.org
Title of Research Paper:	Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks
Name of all Co-authors (if any)	Van-Phuc Hoang, Ngoc-Tuan Do, Trong-Thuc Hoang and Cong-Kha Pham

Comments or feedback received at the conference:

There are two comments after presentation including-

- The presentation is interesting with much useful information. It should be applied to data in social media since today there are a lot of data on social media. In fact, it is possible if we can extract metadata from the social media platform.
- The method should be improved for the implementation with low resource embedded devices.

Contribution to the project:

This paper contributes to the project by providing a method for a deep learning based security evaluation of cryptographic algorithm in IoT based smart healthcare systems. A new metric based on the inversion of exponential rank (IER) is proposed to enhance the performance of non-profiled side channel analysis. The experimental results show that the proposed technique could reveal the secret subkey even if the partial success rate percentage is only 10% in the ASCAD dataset. Furthermore, when utilizing minimally tuned models and IER metric to execute attacks on the CHES-CTF 2018 data, there is a substantial increase in the percentage of correctly revealed bytes, rising from 62.5% to 93.75%. Other papers of this session presents the software/hardware implementations of emrging secure solutions for IoT systems such as quantum cryptography and open ISA based RISC-V processors.

Photos	Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks 16th IEEE International Symposium on Embedded Multicore/Many-core Systems-on-Chip IEEE

[Required Documents]

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

B) Final Program of the conference

Reporter: Van Phuc Hoang

Date: December 25, 2023