# Project Title: Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH)

**Background:**

Recent attacks against IoT devices have posed serious security and privacy issues. As the developing countries, the vulnerability of the supply chain in ASEAN countries can cause damage and disruption since it is extremely difficult to secure the supply chain due to the vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain.

**Targets:**

- Propose a comprehensive cyber-security platform with artificial intelligence (AI) empowered hardware-software oriented solutions for IoT-based SHs, including: 1) secure IoT nodes using security oriented RISC-V processor and ML attack resistant PUF designs for lightweight device authentication and crypto key generation; 2) integrated DL based hardware Trojan detector; 3) DL assisted security side channel attack (SCA) evaluation tools; 4) verified remote attestation (RA) and proof of execution (PoX) for IoT devices integrated with modern ML techniques; 5) efficient and accuracy DNN based tools for attacks and threats detection including malware, ransomware, intrusion detection and DoS, especially for early attack detection;
- Develop existing links and establish new links for researchers from ASEAN and Japan in the areas of cyber-security for IoT-based SHs;
- Deliver both international leading-edge research and uniquely skilled researchers in the area of AI powered hardware/software oriented cyber-security for IoT-based SHs.

➡ Toward a platform for comprehensive IoT cyber-security solutions in ASEAN

Speaker: Van Tuan Luu (LQDTU, Vietnam)

# Project Members

Van Phuc Hoang (LQDTU, Vietnam)
Cong-Kha Pham (UEC, Japan)
Kazuo Sakiyama (UEC, Japan)
Hoang Trong Thuc (UEC, Japan)
Thai Ha Tran (UEC, Japan)
Takeshi Takahashi (NICT, Japan)

Bah Hwee Gwee (NTU, Singapore)
Norrathep Rattanavipanon (PSU, Thailand)
Kuljaree Tantayakul (PSU, Thailand)
Kong Phutphalla (CADT, Cambodia)
Lay Vathna (CADT, Cambodia)
Lay Puthineath (CADT, Cambodia)

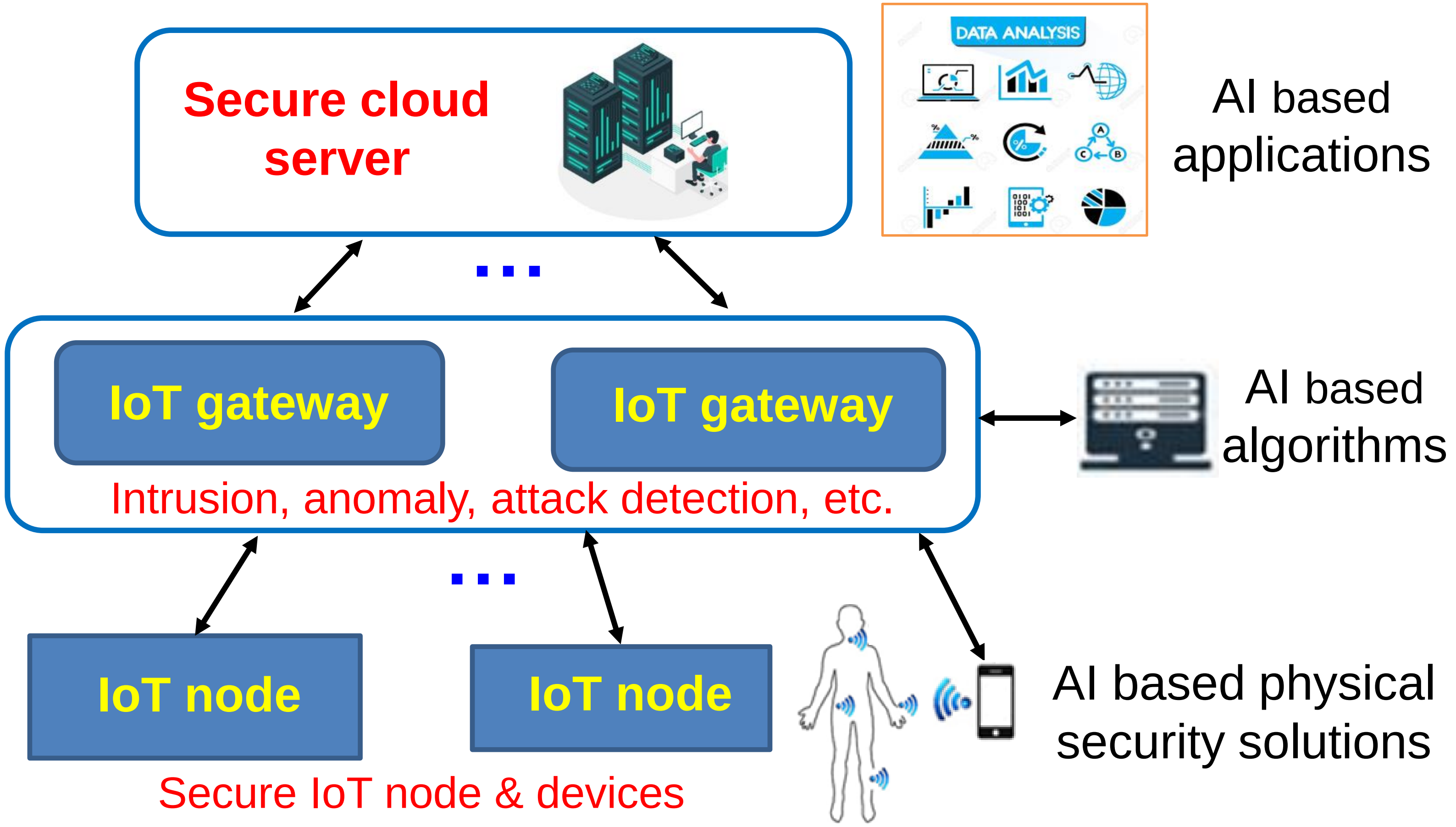
Van Trung Nguyen (LQDTU, Vietnam)
Quang Kien Trinh (LQDTU, Vietnam)
Nga Dao Thi (LQDTU, Vietnam)
Van Tuan Luu (LQDTU, Vietnam)
Ngoc Tuan Do (LQDTU, Vietnam)

**Leader:** Prof. Van Phuc Hoang (LQDTU, Vietnam)

**Project Duration:** From June 01, 2023 to March 31, 2025

**Project Budget:** 80,00 USD

# Proposed Architecture for AI Powered Comprehensive Cyber-Security Solution in Smart Healthcare (SH) Systems



Secure cloud server

AI based applications

...

IoT gateway

IoT gateway

Intrusion, anomaly, attack detection, etc.

AI based algorithms

...

IoT node

IoT node

Secure IoT node & devices

AI based physical security solutions

**Project activities:**

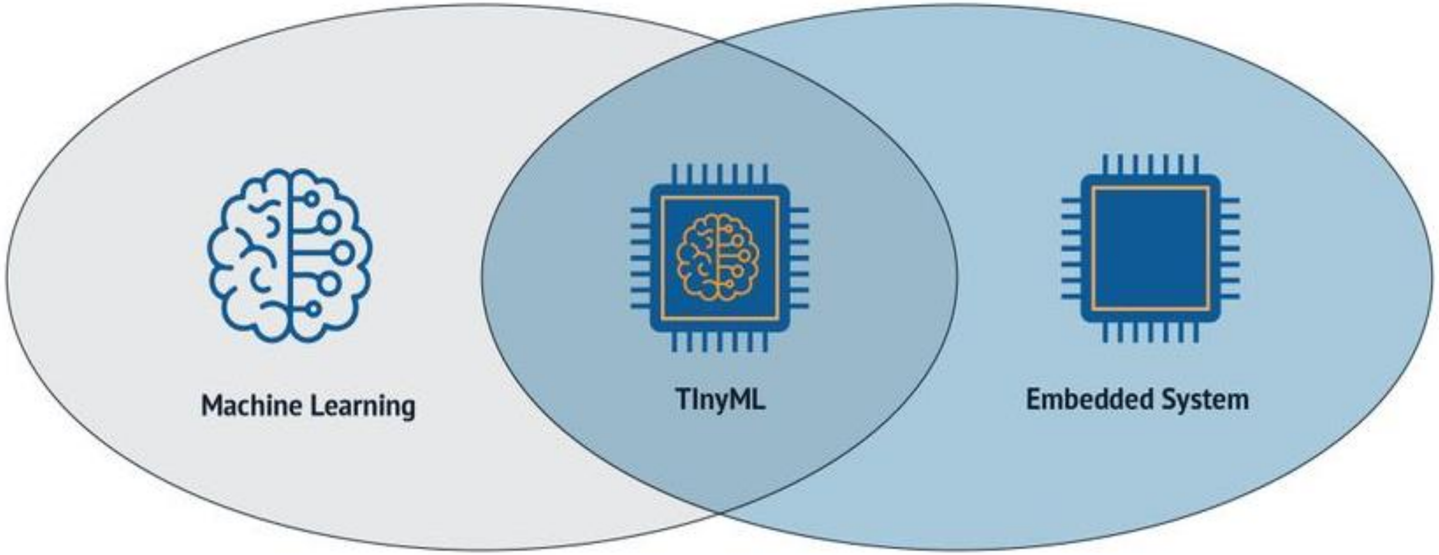
1. Scientific contributions
2. Technological development
3. Experiments
4. Meetings & Workshops

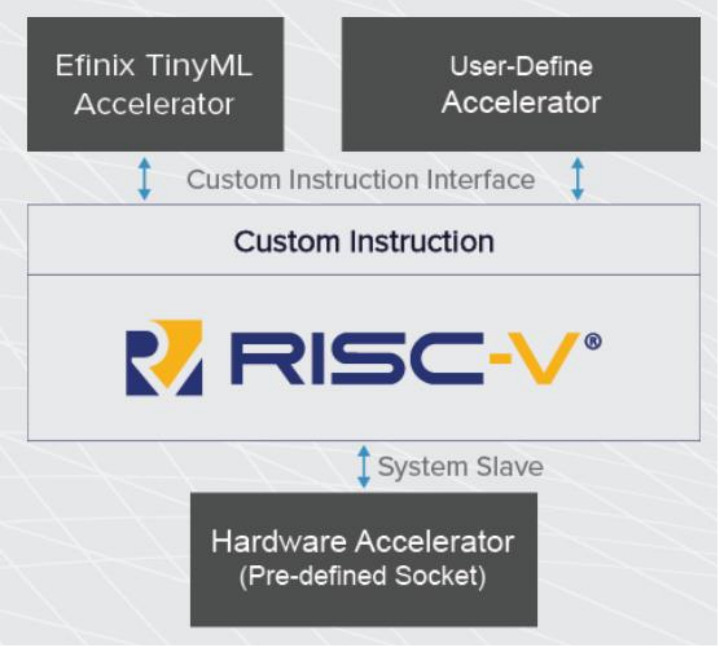
# Activity 1: Survey on applications and security of embedded ML for SHs

## 1. Combination of embedded machine learning and open source hardware in healthcare systems

- The objective of the Embedded machine learning (EML) framework developed for smart healthcare systems is to ensure efficient utilization of bandwidth, minimize latency, enhance privacy, ensure the security of patients' sensitive information, and reduce expenses.

- The combination of EML and OSH bring many advantages for smart health care system: Cost-effectiveness; Flexibility and customizability; Innovation.





Efinix TinyML Accelerator

User-Define Accelerator

Custom Instruction Interface

Custom Instruction

RISC-V®

System Slave

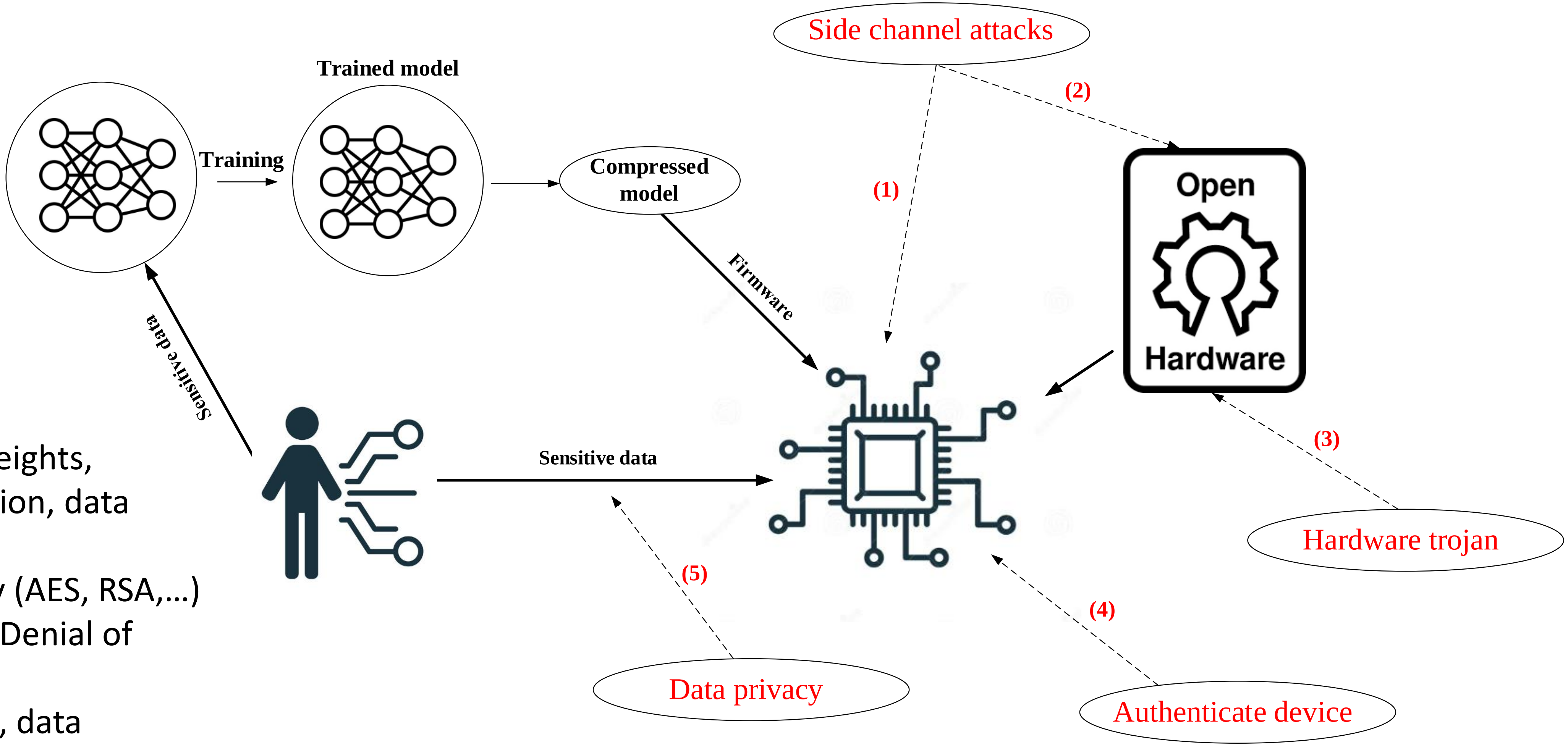
Hardware Accelerator (Pre-defined Socket)

**Main issue: The lack of research on security and potential threats**

[*] https://www.efinixinc.com/solutions-tinyml.html

# Activity 1: Survey on applications and security of embedded ML for SHs (cont.)

## 2. Potential threats:



**(1)** Reverse engineer (weights, neuron, activation function, data input)

**(2)** Reveal the secret key (AES, RSA,…)

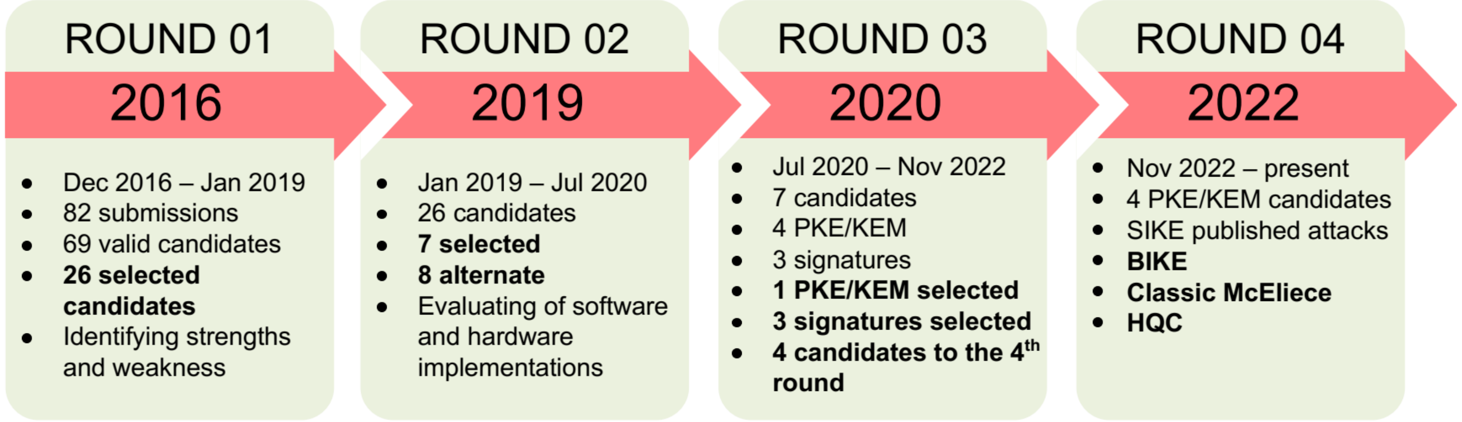
**(3)** Malicious functions, Denial of services,…

**(4)** Unauthorized access, data integrity, …

**(5)** Accessing the sensitive data

# Activity 2: Survey on Post-Quantum Cryptography (PQC) for Secure, Smart Systems

**PQC the standardization process of NIST:**



ROUND 01
2016

- Dec 2016 – Jan 2019
- 82 submissions
- 69 valid candidates
- **26 selected candidates**
- Identifying strengths and weakness

ROUND 02
2019

- Jan 2019 – Jul 2020
- 26 candidates
- **7 selected**
- **8 alternate**
- Evaluating of software and hardware implementations

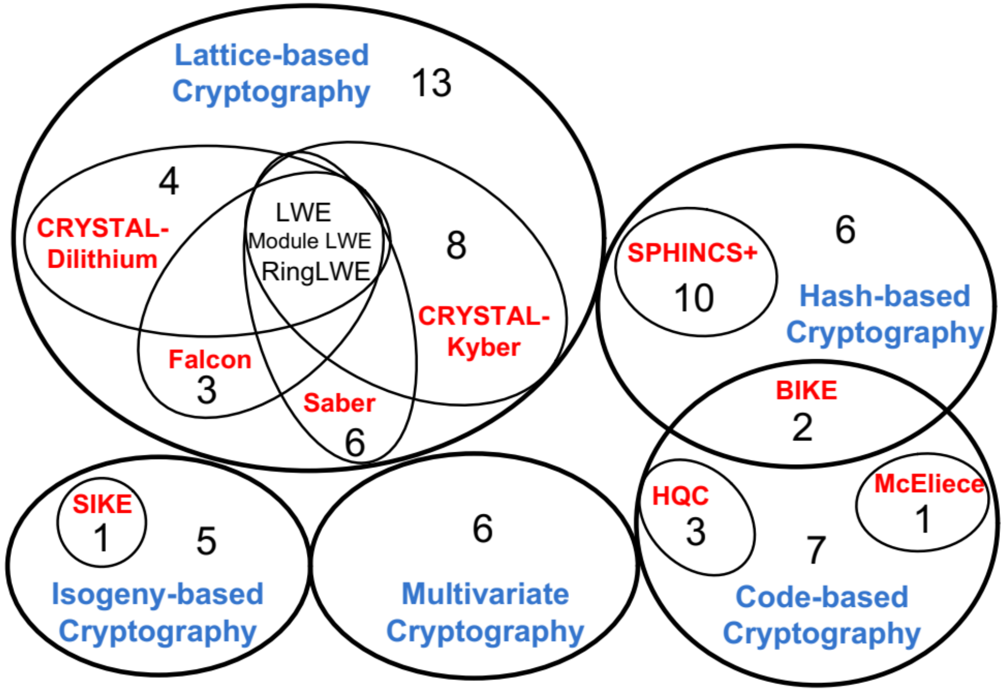
ROUND 03
2020

- Jul 2020 – Nov 2022
- 7 candidates
- 4 PKE/KEM
- 3 signatures
- **1 PKE/KEM selected**
- **3 signatures selected**
- **4 candidates to the 4th round**

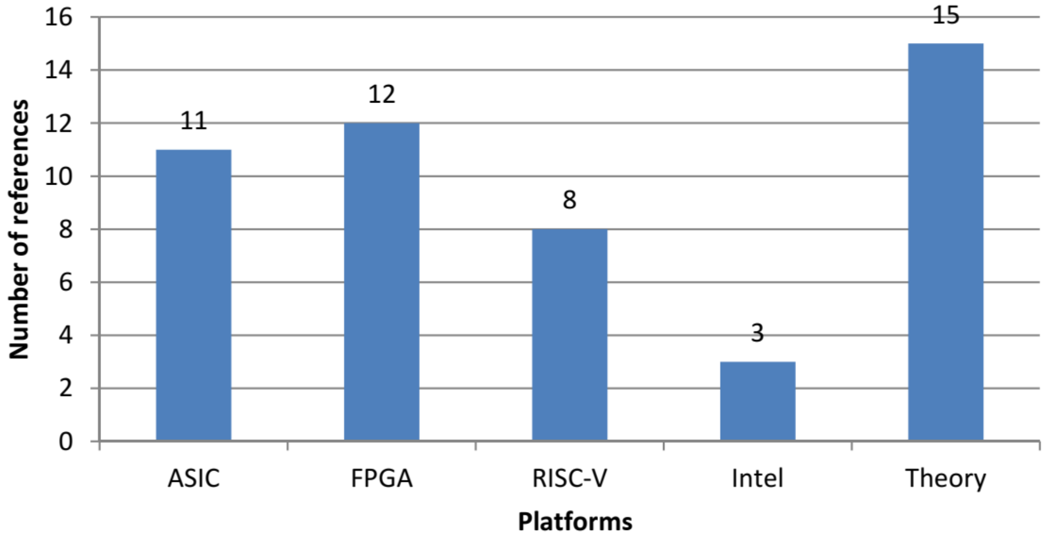
ROUND 04
2022

- Nov 2022 – present
- 4 PKE/KEM candidates
- SIKE published attacks
- **BIKE**
- **Classic McEliece**
- **HQC**

**Venn diagram describes the fields of PQC research related to the references:**

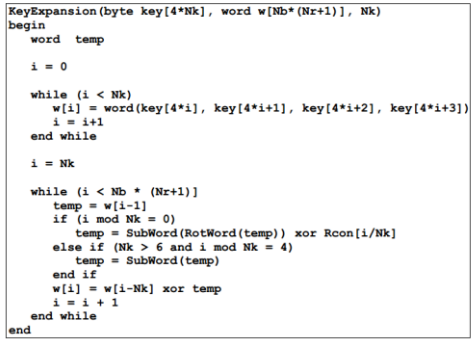


Number of references implemented on different platforms:



Duc-Thuan Dam, Thai-Ha Tran, Van-Phuc Hoang, Cong-Kha Pham, Trong-Thuc Hoang, “A Survey of Post-Quantum Cryptography: Start of a New Race,” Cryptography 2023, 7, 40. https://doi.org/10.3390/ cryptography7030040

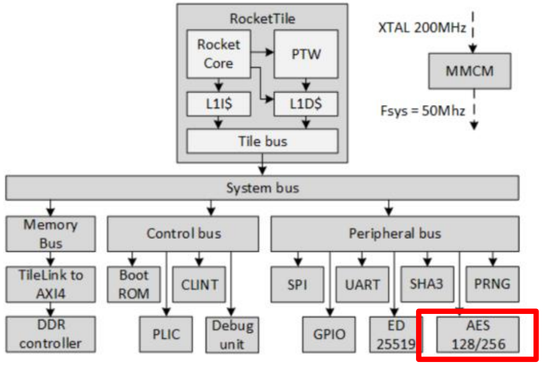
# Activity 3: Deep Learning-Based Side Channel Attacks for Security Evaluation in SHs



```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
   word  temp

   i = 0

   while (i < Nk)
      w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
      i = i+1
   end while

   i = Nk

   while (i < Nb * (Nr+1)]
      temp = w[i-1]
      if (i mod Nk = 0)
         temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
      else if (Nk > 6 and i mod Nk = 4)
         temp = SubWord(temp)
      end if
      w[i] = w[i-Nk] xor temp
      i = i + 1
   end while
end
```

Software implementation

Application Specific Integrated Circuit



A built-in accelerator

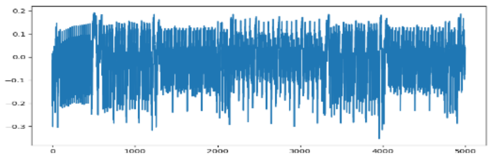
Plaintext

Input

Output

Ciphertext

- Power consumption
- Electromagnetic Radiation
- Temperature variation
- …



Side channel analysis

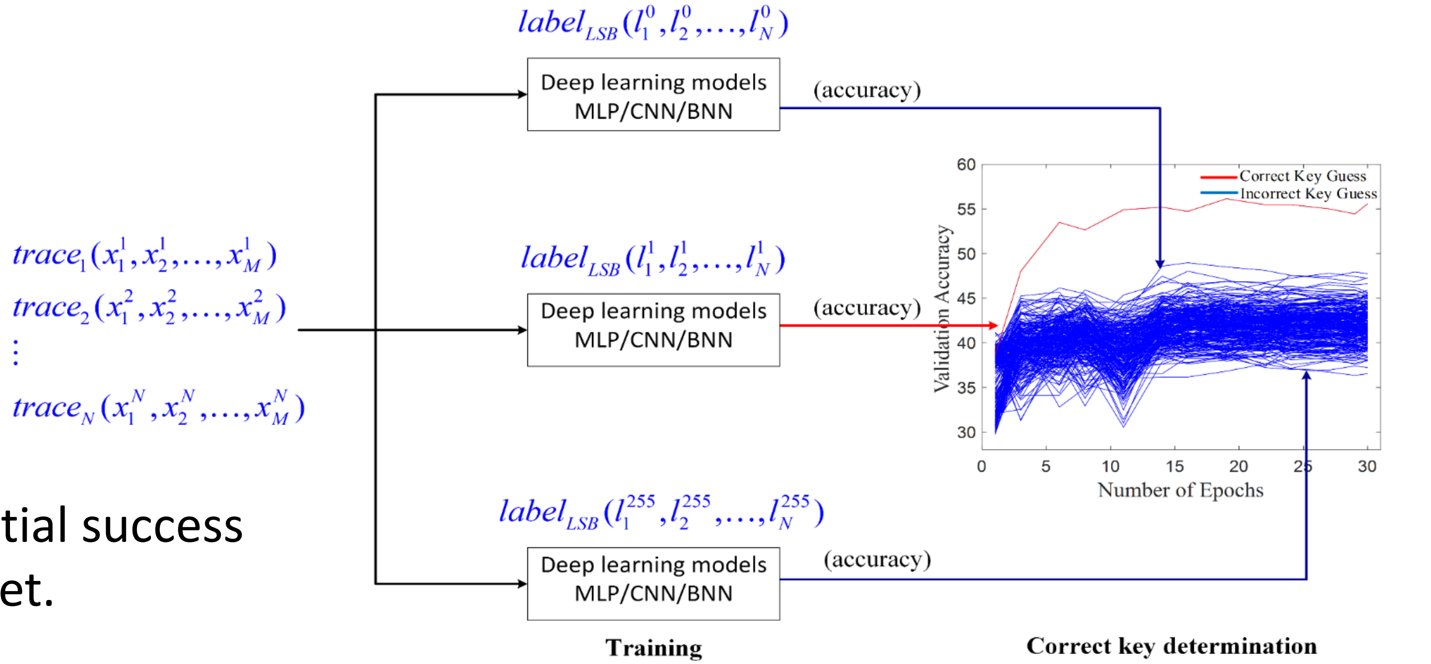
Secret key

# Activity 3: Deep Learning-Based SCA for Security Evaluation in SHs (cont.)

## Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks:

- We propose a new metric based on the inversion of exponential rank (IER) to enhance the performance of deep learning-based SCA.

- It could reveal the secret subkey even if the partial success rate percentage is only 10% in the ASCAD dataset.



$trace_1(x_1^1, x_2^1, \ldots, x_M^1)$
$trace_2(x_1^2, x_2^2, \ldots, x_M^2)$
$\vdots$
$trace_N(x_1^N, x_2^N, \ldots, x_M^N)$

$label_{LSB}(l_1^0, l_2^0, \ldots, l_N^0)$
Deep learning models MLP/CNN/BNN
(accuracy)

$label_{LSB}(l_1^1, l_2^1, \ldots, l_N^1)$
Deep learning models MLP/CNN/BNN
(accuracy)

$label_{LSB}(l_1^{255}, l_2^{255}, \ldots, l_N^{255})$
Deep learning models MLP/CNN/BNN
(accuracy)

Training

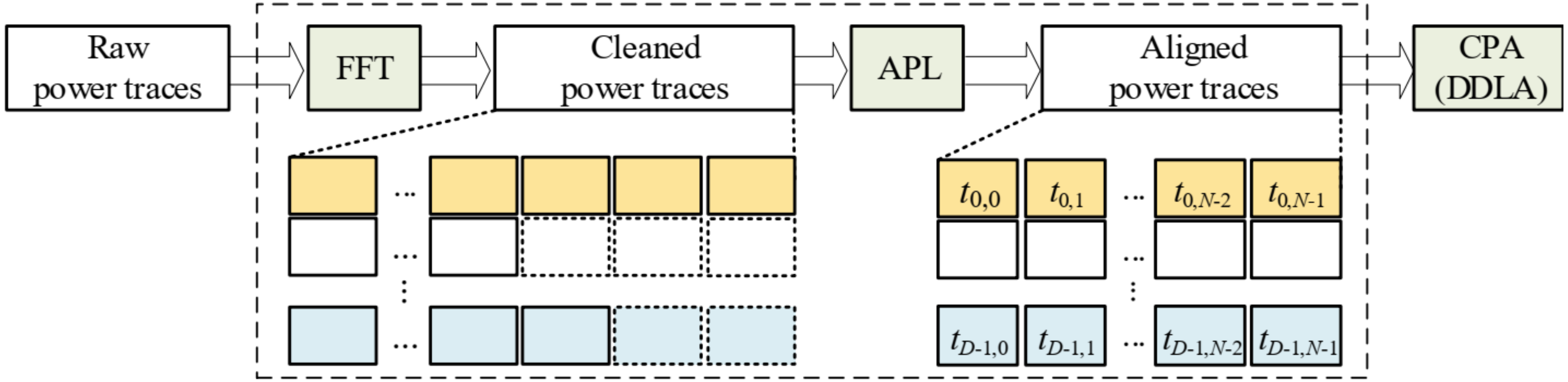
Correct key determination

| Attack | No. of epochs | Results | Byte | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| MOR [6] | 15 | SR (%) | 96.67 | **3.33** | **26.67** | 93.33 | 100 | 60 | 86.67 | **36.67** | 73.33 | 60 | 70 | **36.67** | 70 | 73.33 | **10** | **0** |
| MOR+IER ($\alpha = 1.3$) | | | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| MOR [6] | 20 | SR (%) | - | **20** | **53.33** | - | - | - | - | **90** | - | - | **-** | **60** | - | - | **60** | **0** |
| MOR+IER ($\alpha = 1.3$) | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |

✓: Successful revealing secret key

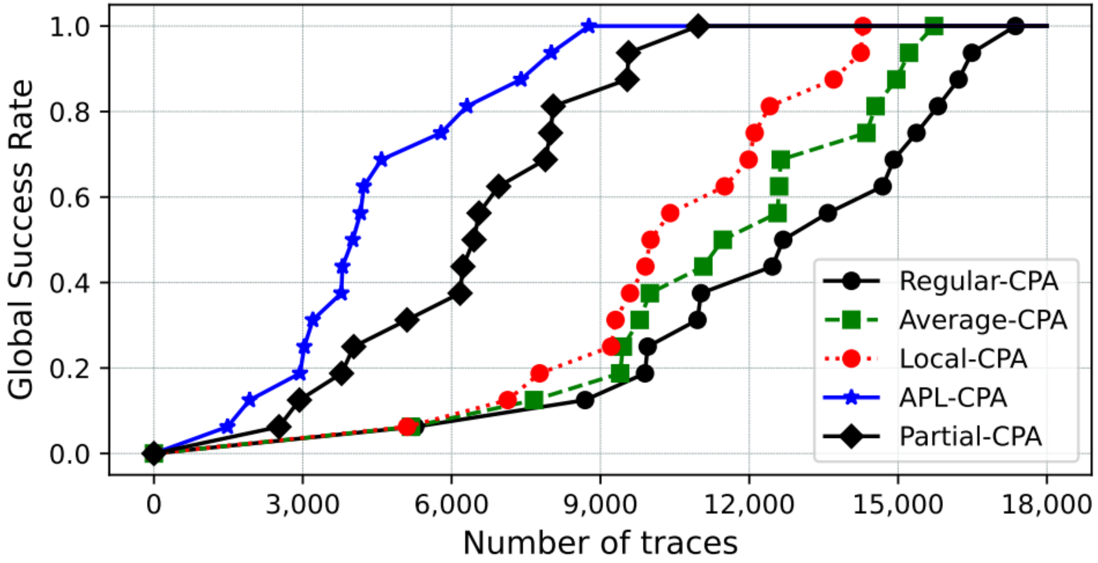
Van-Phuc Hoang, Ngoc-Tuan Do, Trong-Thuc Hoang and Cong-Kha Pham, “Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks,” IEEE MCSoC 2023 conference.

# Activity 4: Security Evaluation by Compacting Side-Channel Measurements



Raw power traces → FFT → Cleaned power traces → APL → Aligned power traces → CPA (DDLA)

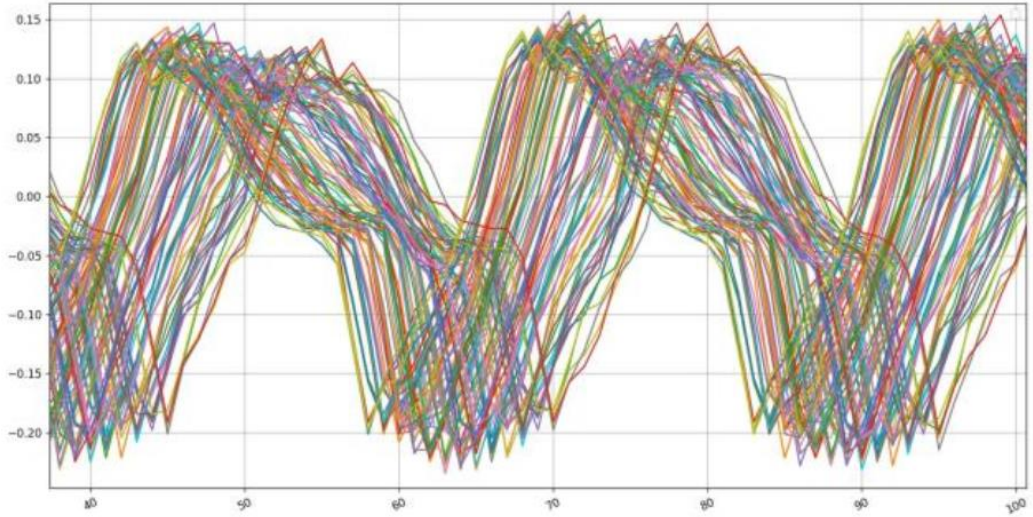
**Main idea:** We propose a new technique to reduce the computation time by extracting the Point of Interest (POI) with an interpolation method. The proposal uses the local extreme value and two adjacent samples around it to interpolate the real peak amplitude. Compared to the conventional CPA, the execution time in our solution is decreased by approximately 9.55 times, with only 53.32% of the given power traces used for attacking the masking design.



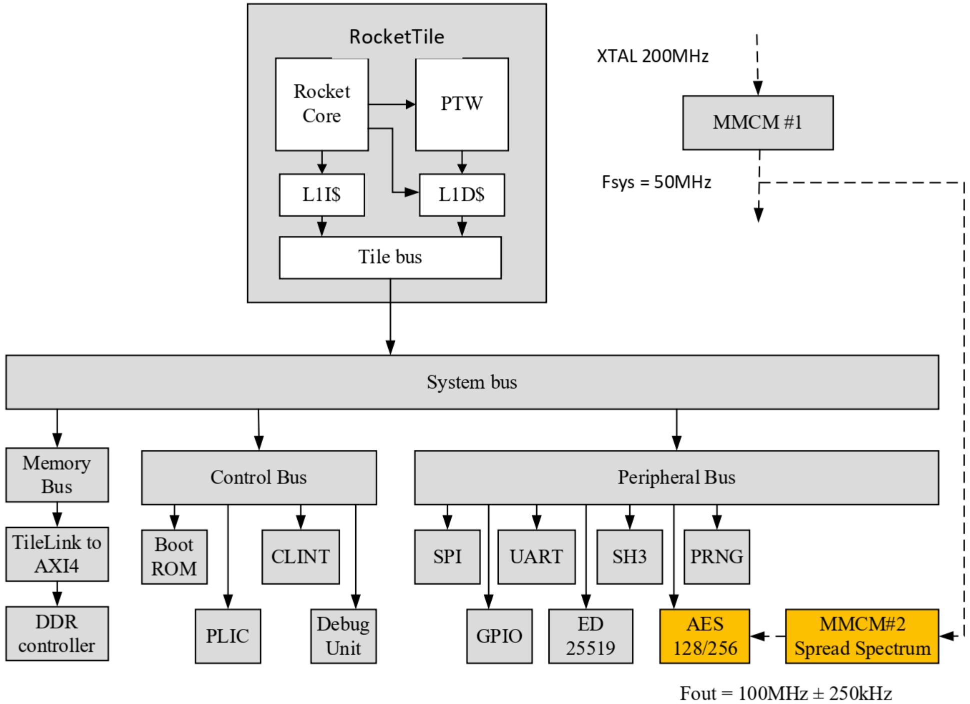
T. -H. Tran, D. -T. Dam, B. -A. Dao, V. -P. Hoang, C. -K. Pham and T. -T. Hoang, "Compacting Side-Channel Measurements with Amplitude Peak Location Algorithm," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 32, no. 3, pp. 573-586, March 2024, doi: 10.1109/TVLSI.2023.3339810.

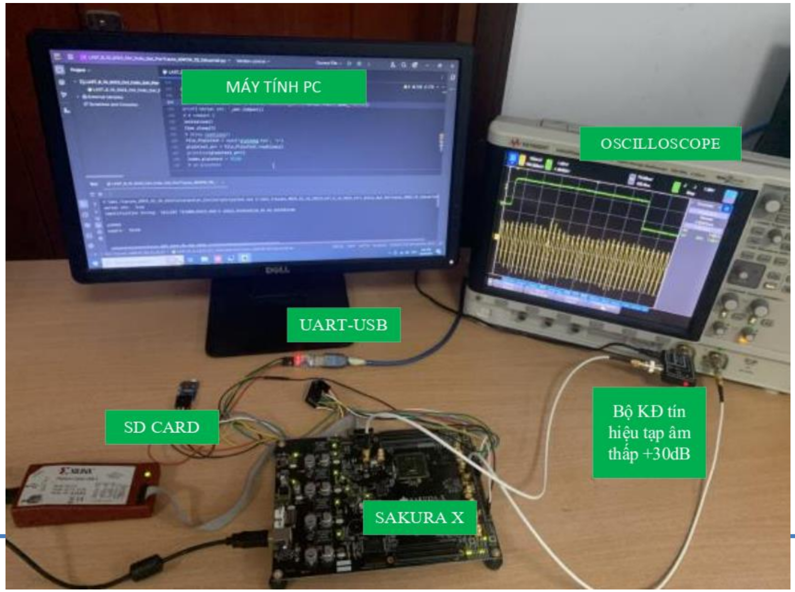
# Activity 5: Countermeasures against side-channel attacks for RISC-V processors

- ➢ Countermeasures against side-channel attacks for RISC-V processors with integrated AES-128 core by using Spread-Spectrum Clock Generation:



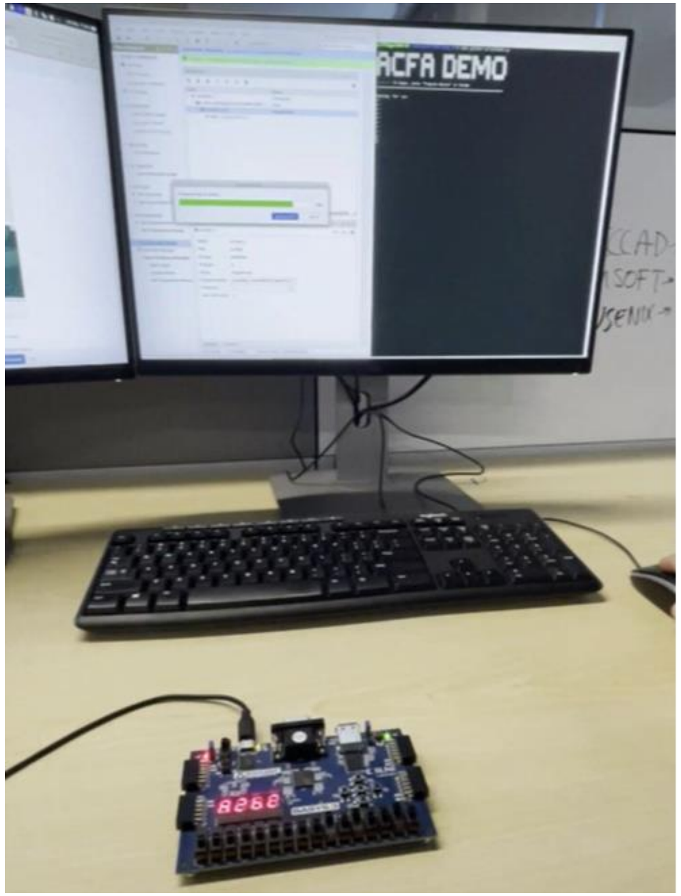
- ➢ The level of information leakage is reduced by 182 times.

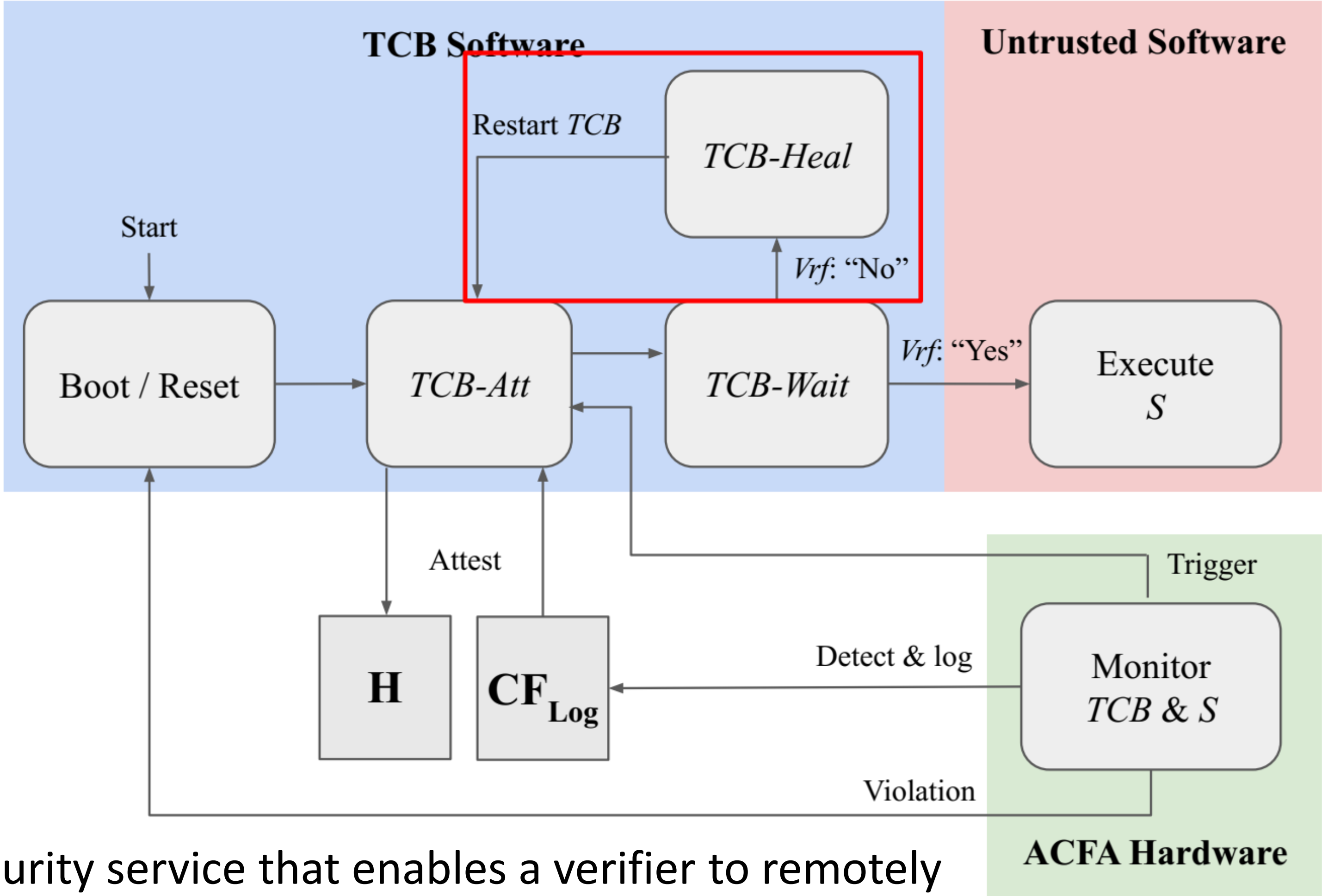




Luu Van Tuan, Trinh Quang Kien, Hoang Van Phuc et. al., "Countermeasures against side-channel attacks for RISC-V processors with integrated AES-128 core," REV-ECIT conference, Dec. 2023.

# Activity 6: Secure Runtime Auditing & Guaranteed Device Healing via Active Control Flow Attestation (ACFA)





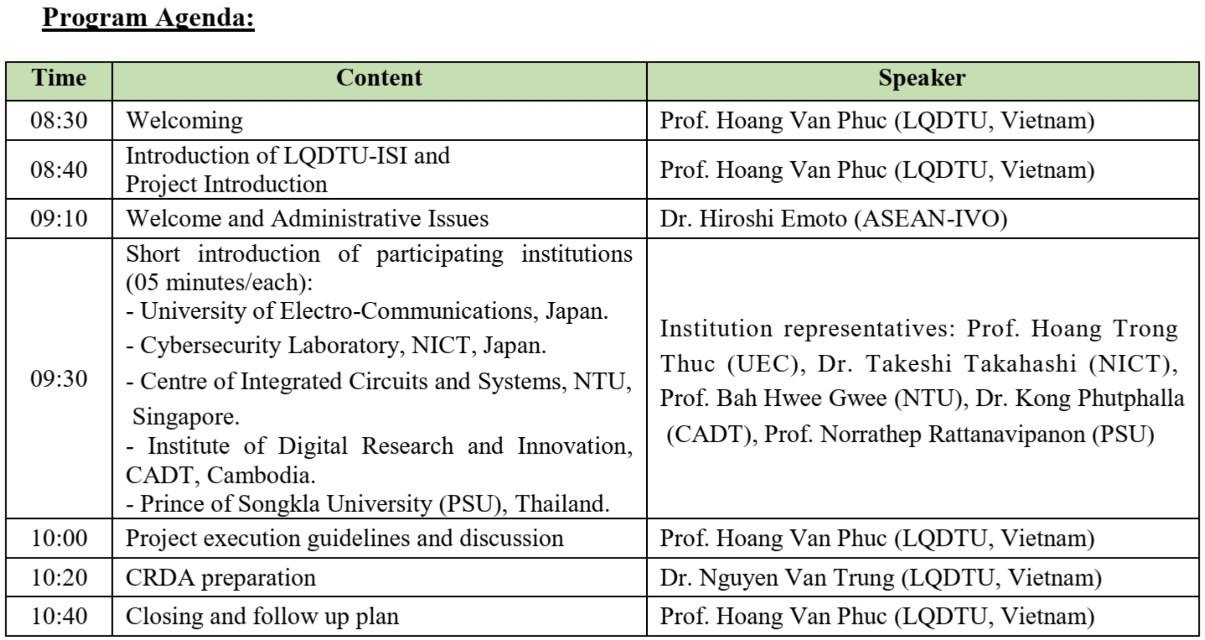
- ➢ Remote Attestation (*RA*) is an inexpensive security service that enables a verifier to remotely detect illegal modifications to the software binary installed on a prover MCU
- ➢ Hardware Cost of proposed ACFA: 275 LUTs, 202 FFs (5.8x less LUTs, 10.5x less FFs than LiteHAX)

Caulfield Adam, Norrathep Rattanavipanon, and Ivan De Oliveira Nunes, "ACFA: Secure Runtime Auditing & Guaranteed Device Healing via Active Control Flow Attestation", In 32nd USENIX Security Symposium (USENIX Security 23), 2023.

# Activity 7: Organizing Meetings and Workshops

- Project kick-off meeting on 10 August, 2023: Online meeting, 12 participants.
- Introduce about project members.
- Discuss the research tasks, plan and contributions of each member.
- Clarify the rules for using project budget.

**Kick-off meeting on 10 August, 2023**
**(online via Zoom)**



**Program Agenda:**

| Time | Content | Speaker |
|---|---|---|
| 08:30 | Welcoming | Prof. Hoang Van Phuc (LQDTU, Vietnam) |
| 08:40 | Introduction of LQDTU-ISI and Project Introduction | Prof. Hoang Van Phuc (LQDTU, Vietnam) |
| 09:10 | Welcome and Administrative Issues | Dr. Hiroshi Emoto (ASEAN-IVO) |
| 09:30 | Short introduction of participating institutions (05 minutes/each):<br>- University of Electro-Communications, Japan.<br>- Cybersecurity Laboratory, NICT, Japan.<br>- Centre of Integrated Circuits and Systems, NTU, Singapore.<br>- Institute of Digital Research and Innovation, CADT, Cambodia.<br>- Prince of Songkla University (PSU), Thailand. | Institution representatives: Prof. Hoang Trong Thuc (UEC), Dr. Takeshi Takahashi (NICT), Prof. Bah Hwee Gwee (NTU), Dr. Kong Phutphalla (CADT), Prof. Norrathep Rattanavipanon (PSU) |
| 10:00 | Project execution guidelines and discussion | Prof. Hoang Van Phuc (LQDTU, Vietnam) |
| 10:20 | CRDA preparation | Dr. Nguyen Van Trung (LQDTU, Vietnam) |
| 10:40 | Closing and follow up plan | Prof. Hoang Van Phuc (LQDTU, Vietnam) |

# Activity 7: Organizing Meetings and Workshops (cont.)

- Open technical workshop entitled *"Advanced Cyber-security Solutions for IoT Systems"* organized in Hanoi, Vietnam on 10-11 November, 2023: 16-presentation session and panel discussion.
  - ➢ Present and discuss the research issues and status of the project.
  - ➢ Exchange of ideas and latest research results in advanced cyber-security techniques and solutions for IoT-based smart healthcare systems.
  - ➢ Define the detailed tasks and the project plan.

Project Review
Project Title: Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH)
IVO
NICT
IVO Project: Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH)
International Workshop on Advanced Cyber-security Solutions for IoT Systems
Hanoi, Vietnam
November

IoT
• Ubiquitous, remote, wireless
• Widely adopted in
• Smart home applications
• Smart cities and industrial automation
• Smart healthcare
• Functionality: Sensors, actuators, or control units
• Attractive targets for attacks and malware (e.g., Stuxnet, Mirai Botnet)
IVO
NICT
IVO Project: Artificial Intelligence Po
Comprehensive Cyber-Security for
Healthcare Systems (AIPOSH
International Workshop o
Advanced Cyber-securit Solu
for IoT Syste
Vietna
ember 10-11,

NICT
IVO Project: Artificial Intelligence Powered Comprehensive Cyber-Security for Smart Healthcare Systems (AIPOSH)
International Workshop on Advanced Cyber-security Solutions for IoT Systems

# Activity 7: Organizing Meetings and Workshops (cont.)

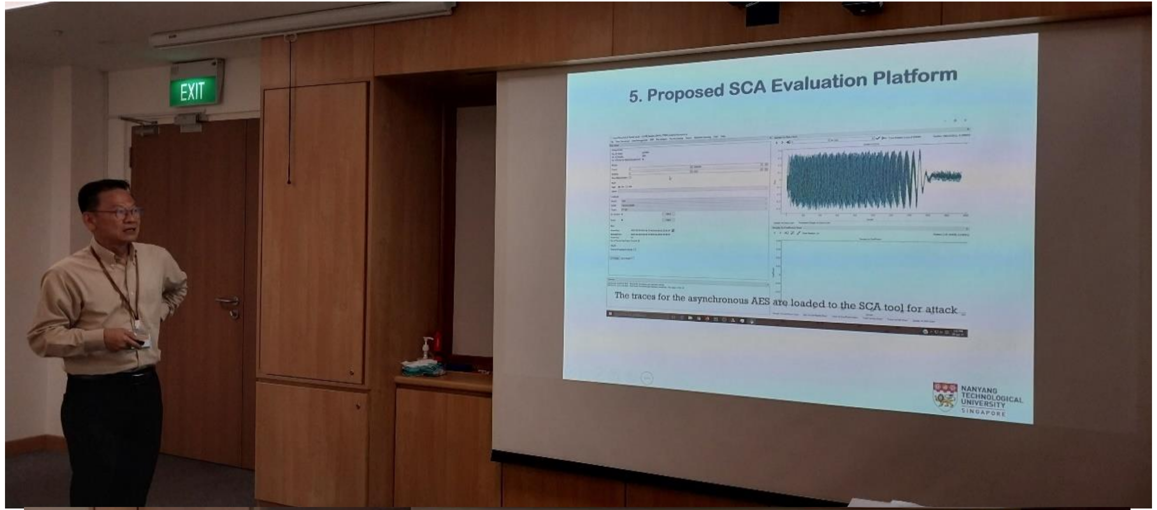
- Open technical workshop entitled *"Intelligent Edge Computing and Machine Learning Solutions for Internet of Things Systems"* organized in Hanoi, Vietnam on 04-05 June, 2024: 14-presentation session and panel discussion.
  - ➢ Present and discuss the research issues and status of the project.
  - ➢ Exchange of ideas and latest research results in advanced cyber-security techniques and solutions for IoT-based smart healthcare systems.
  - ➢ Define the detailed tasks and the project plan.

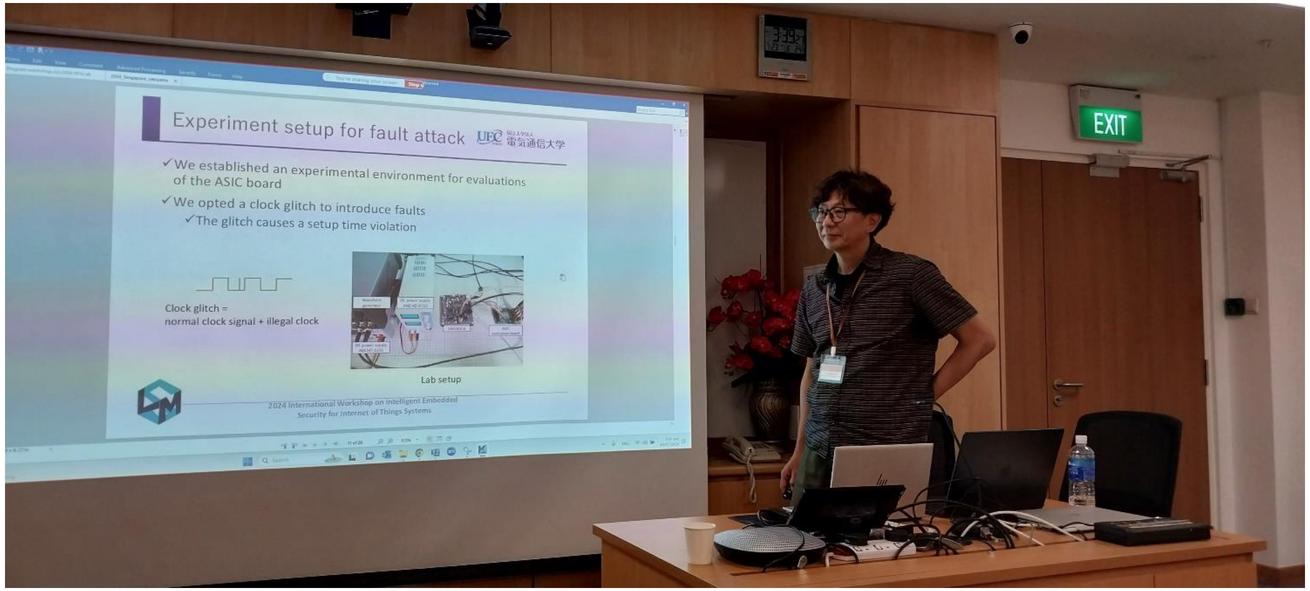
Background and motivations
Power Consumption VS Battery
International Workshop on Secure, Efficient IC Design and Intelligent ... Solutions for IoT Systems

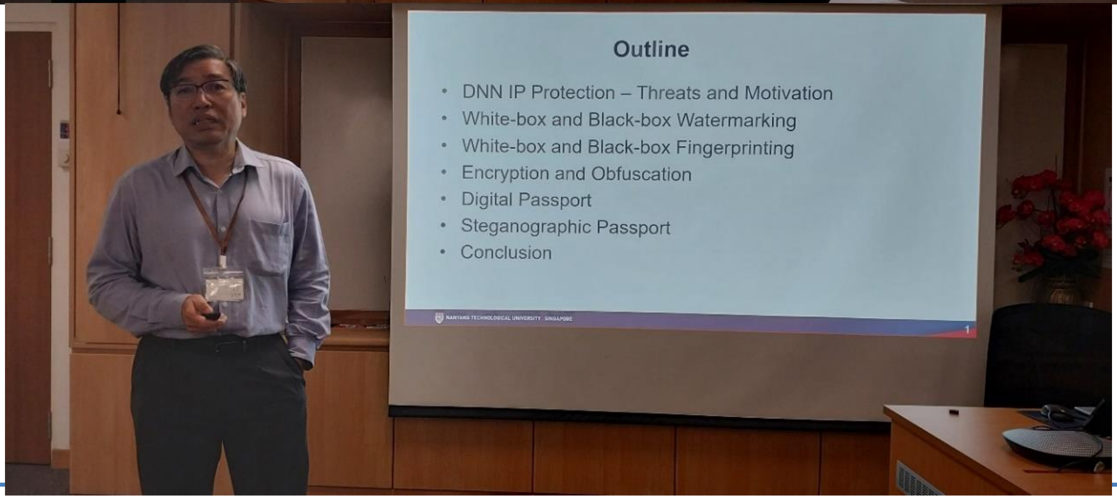
Implementation of TinyML on Edge computing
Essential stages within the TinyML workflow are:
2024 International Workshop on Secure, Energy Efficient IC Design and Intelligent Edge Computing Solutions for IoT Systems

# Activity 7: Organizing Meetings and Workshops (cont.)

- Open technical workshop entitled “Intelligent Embedded Security for Internet of Things Systems” organized in NTU (Singapore) on 22-0524 July, 2024: 17-presentation session and panel discussion.
  - Present and discuss the research issues and status of the project.
  - Exchange of ideas and latest research results in intelligent embedded security solutions for IoT-based smart healthcare systems.
  - Lab tour at NUS and NTU.
  - Define the detailed tasks and the project plan.


EXIT
5. Proposed SCA Evaluation Platform
The traces for the asynchronous AES are loaded to the SCA tool for attack
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE


Experiment setup for fault attack
UEC 電気通信大学
✓We established an experimental environment for evaluations of the ASIC board
✓We opted a clock glitch to introduce faults
✓The glitch causes a setup time violation
Clock glitch = normal clock signal + illegal clock
Lab setup
2024 International Workshop on Intelligent Embedded Security for Internet of Things Systems
EXIT


Outline
DNN IP Protection – Threats and Motivation
White-box and Black-box Watermarking
White-box and Black-box Fingerprinting
Encryption and Obfuscation
Digital Passport
Steganographic Passport
Conclusion

# Summary of Scientific Contribution - Presentations at International Conferences

| No | Paper title: | Author names | Affiliation | Conference name | Conference date | Conference venue |
|---|---|---|---|---|---|---|
| 1 | Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks | Van-Phuc Hoang, Ngoc-Tuan Do, Trong-Thuc Hoang, Cong-Kha Pham | LQDTU (Vietnam) and UEC (Japan) | 16th IEEE MCSoC 2023 | 18-21/12/2023 | Singapore |
| 2 | Countermeasures against side-channel attacks for RISC-V processors with integrated AES-128 core | Luu Van Tuan, Trinh Quang Kien, Hoang Van Phuc et. al. | LQDTU (Vietnam) | National Conference on Electronics, Communications and Information Technology – (REV-ECIT 2023) | 16/12/2023 | Hanoi, Vietnam |
| 3 | An Efficient Hiding Countermeasure with Xilinx MMCM Primitive in Spread Mode | Thai-Ha Tran, Van-Phuc Hoang, Duc-Hung Le, Trong-Thuc Hoang, Cong-Kha Pham | UEC (Japan), LQDTU (Vietnam), HCMUS (Vietnam) | IEEE ISCAS2024 | 19-22/5/2024 | Singapore |
| 4 | Enhancing Performance of Deep Learning Based Non-Profiled Side-Channel Attack Using Multi-Output and Transfer Learning | Van-Phuc Hoang, Ngoc-Tuan Do, Huu Minh Nguyen | LQDTU (Vietnam) | 2024 IEEE TechDefense | 11-13/11/2024 | Italy |
| 5 | Improving Efficiency of Non-Profiled Side-Channel Attack on AES-128 Algorithm Using Transfer Learning | Le Thanh, Huu Minh Nguyen, Ngoc-Tuan Do, Van-Phuc Hoang | LQDTU (Vietnam) | National Conference on Electronics, Communications and Information Technology – (REV-ECIT 2024) | 14/12/2024 | Hanoi, Vietnam |

# Summary of Scientific Contribution - Presentations at International Conferences (cont.)

| No | Paper title: | Author names | Affiliation | Conference name | Conference date | Conference venue |
|---|---|---|---|---|---|---|
| 6 | Improving Accuracy of Voice Digit Recognition Using TinyML and Iterative Reasoning | Ngoc-Tuan Do, Van-Phuc Hoang | LQDTU (Vietnam) | The fifth International Conference on Intelligent Systems & Networks (ICISN 2025) | 22-23/3/2025 (submitted) | Hanoi, Vietnam |
| 7 | ACFA: Secure Runtime Auditing & Guaranteed Device Healing via Active Control Flow Attestation | Caulfield Adam, Norrathep Rattanavipanon, Ivan De Oliveira Nunes | PSU (Thailand), RIT (USA) | 32nd USENIX Security Symposium (USENIX Security 23) | 9-11/8/2023 | CA, USA |
| 8 | TRACES: TEE-based Runtime Auditing for Commodity Embedded Systems | Caulfield Adam, Antonio Joia Neto, Norrathep Rattanavipanon, Ivan De Oliveira Nunes | PSU (Thailand), RIT (USA) | Annual Computer Security Applications Conference (ACSAC) | 9-13/12/2024 (accepted) | Hawaii, USA |
| 9 | PEARTS: Provable Execution in Real-time Embedded Systems | Joia Neto, Antonio, Norrathep Rattanavipanon, Ivan De Oliveira Nunes | PSU (Thailand), RIT (USA) | 46th IEEE Symposium on Security and Privacy (S&P) | 12-14/5/2025 (accepted) | CA, USA |

# Summary of Scientific Contribution (cont.) - Published Journal Papers

| No | Paper title: | Author names | Affiliation | Journal name | Journal publisher | Volume no. & pages |
|---|---|---|---|---|---|---|
| 1 | A Survey of Post-Quantum Cryptography: Start of a New Race | Duc-Thuan Dam, Thai-Ha Tran, Van-Phuc Hoang, Cong-Kha Pham, Trong-Thuc Hoang | LQDTU (Vietnam) and UEC (Japan) | Cryptography | MDPI | Vol. 4, No. 40, p1-18, Aug. 2023 |
| 2 | Performance Analysis of Gradient Inversion Attack in Federated Learning with Healthcare Systems | Thi-Nga Dao, Phat Tien Nguyen | LQDTU (Vietnam) | REV Journal on Electronics and Communications | REV | vol. 14, no. 3, Sept. 2024 |
| 3 | Compacting Side-Channel Measurements with Amplitude Peak Location Algorithm | Thai-Ha Tran, Duc-Thuan Dam, Ba-Anh Dao, Van-Phuc Hoang, Cong-Kha Pham, Trong-Thuc Hoang | LQDTU, ACT (Vietnam) and UEC (Japan) | IEEE Transactions on VLSI Systems | IEEE | vol. 32, no. 3, pp. 573-586, Mar. 2024 |
| 4 | Vital Sign Monitoring with Machine Learning Techniques | Hoang Thi Yen, Van Phuc Hoang, Quang Sun | LQDTU (Vietnam) and UEC (Japan) | REV Journal on Electronics and Communications | REV | vol. 14, no. 3, Sept. 2024 |
| 5 | Spread Spectrum-based Countermeasures for Cryptographic RISC-V | Thai-Ha Tran, Ba-Anh Dao, Duc-Hung Le, Van Phuc Hoang, Trong-Thuc Hoang, and Cong-Kha Pham | LQDTU, ACT (Vietnam), VNU HCM and UEC (Japan) | IEEE Transactions on VLSI Systems | IEEE | 2024 |

# Societal Impact

- **The societal impact of the project is as follows:**
  - For the community, thanks to this proposed system, the security assurance can be improved for IoT based SHs.
  - For the government organizations, the developed system will provide an efficient tool for information security management and decision making processes.
  - Since the SH system is designed for low power consumption, it is environmental friendly.
  - The outcome of this project is to raise the awareness amongst policy makers, business and industries, people in ASEAN on the comprehensively secure IoT systems as a management tool and possible roles that they should take in tackling the problems of not only ICT but also human life, business, transportation, industry and others.

# Conclusions and Future Works

- **Conclusions:**
  - — The project team has achieved encouraging results.
  - — We have completed the survey and some techniques for cyber-security assurance in IoT-based SH systems using machine learning and deep learning techniques.
  - — Perform laboratory experiments for essential components in the proposed systems.
  - — Ready to propose and implement the overall system.

- **Future works:**
  - — Organize the workshop and more meetings to exchange ideas and research results.
  - — Purchase equipment for R&D activities.
  - — Perform more experiments for other essential components in the proposed systems.
  - — Build the application for field experiments in healthcare systems.