Project Review Report

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 RA and 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.

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)

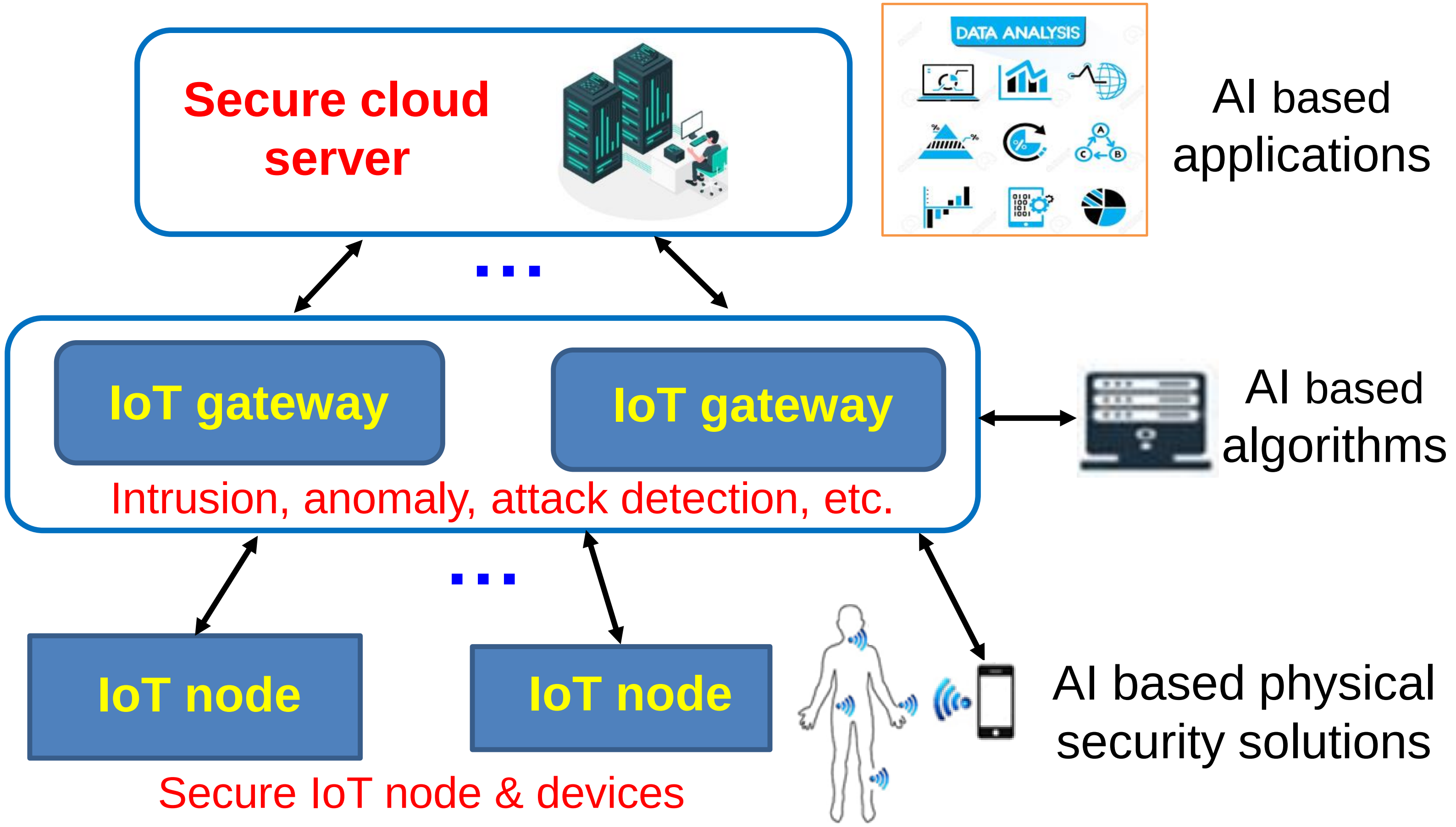
Van Trung Nguyen (LQDTU, Vietnam)
Quang Kien Trinh (LQDTU, Vietnam)
Nga Dao Thi (LQDTU, Vietnam)
Van Tuan Luu (LQDTU, Vietnam)
Ngoc Tuan Do (LQDTU, Vietnam)

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 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

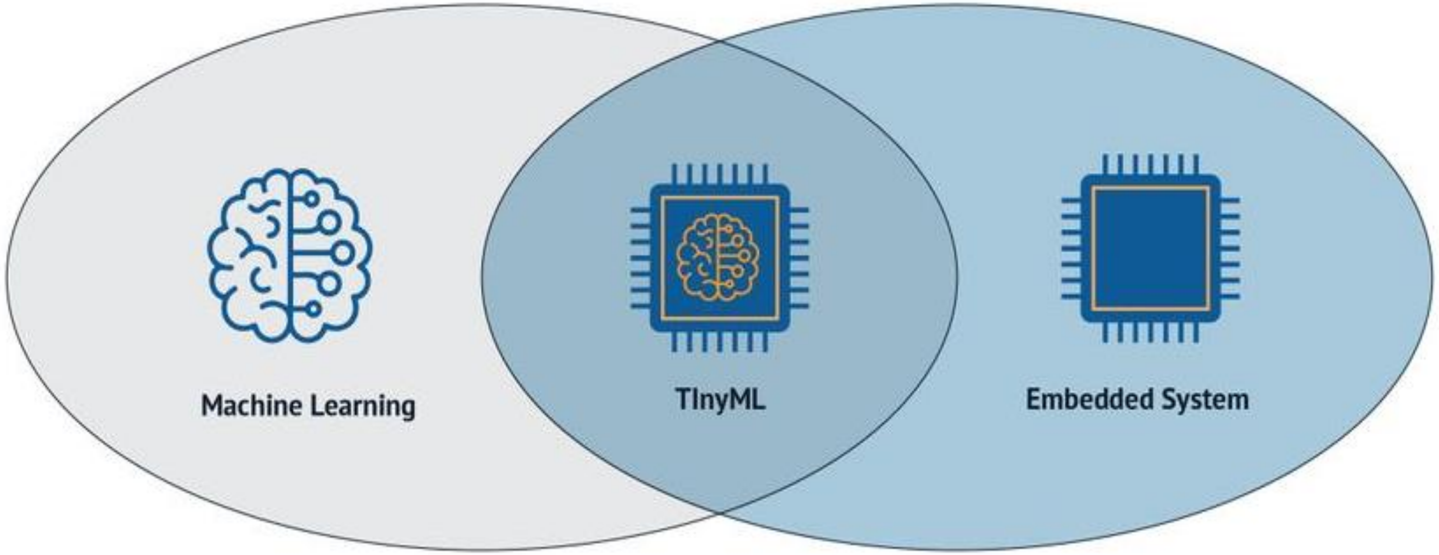
AI based physical security solutions

Project activities:

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

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

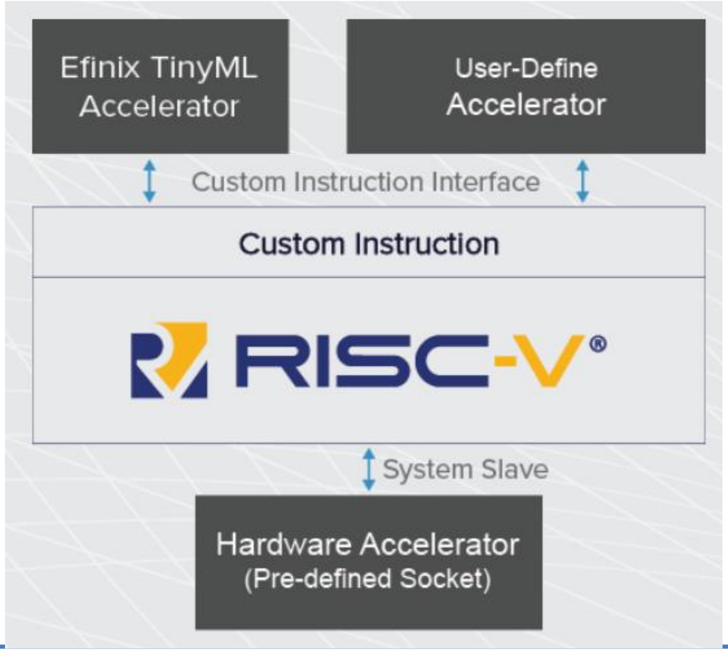
1. The combination of Embedded machine learning and open source hardware in Healthcare systems



- 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.

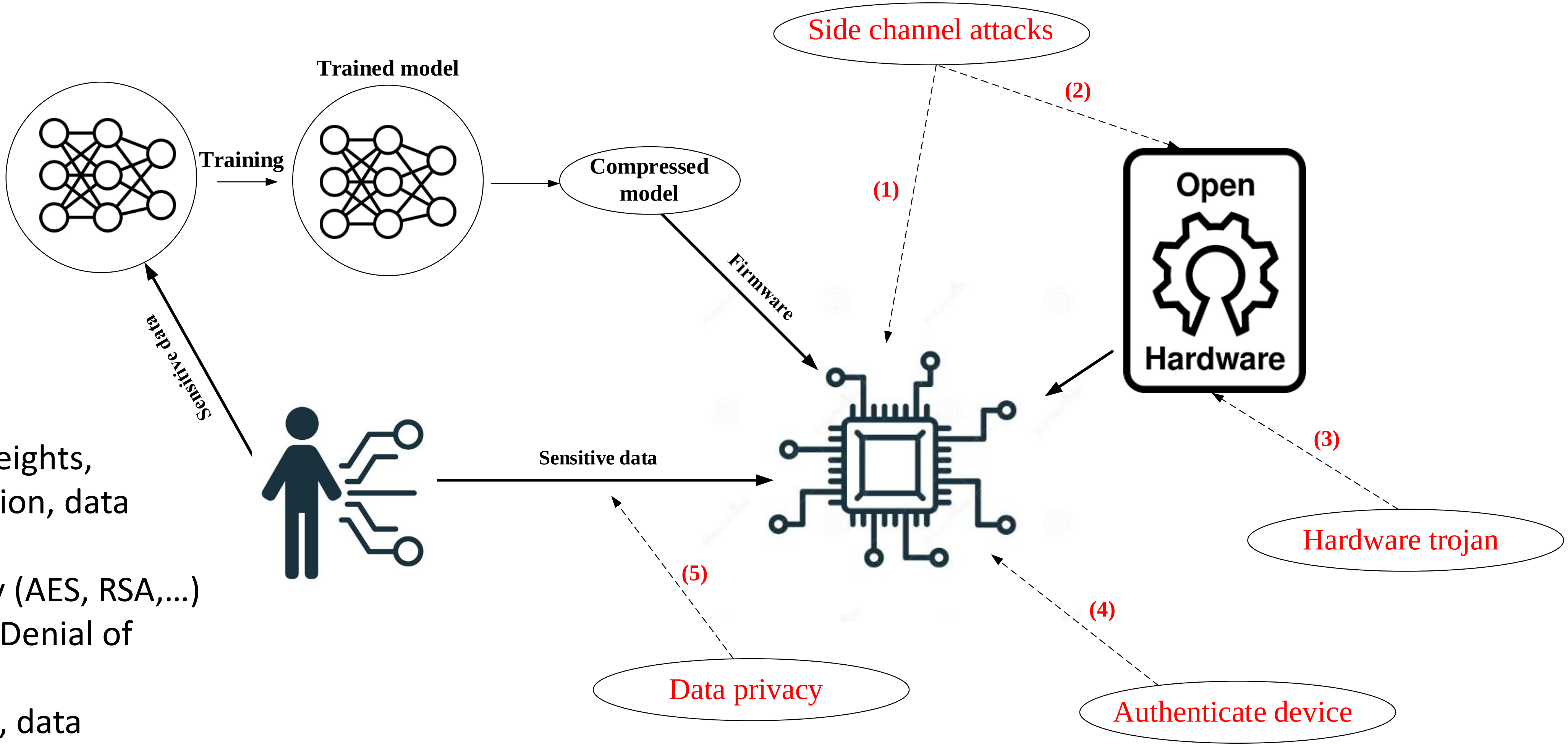
Main issue: The lack of research on security and potential threats


Efinix TinyML Accelerator
User-Define Accelerator
Custom Instruction Interface
Custom Instruction
RISC-V®
System Slave
Hardware Accelerator (Pre-defined Socket)

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

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

2. Potential threats:



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

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

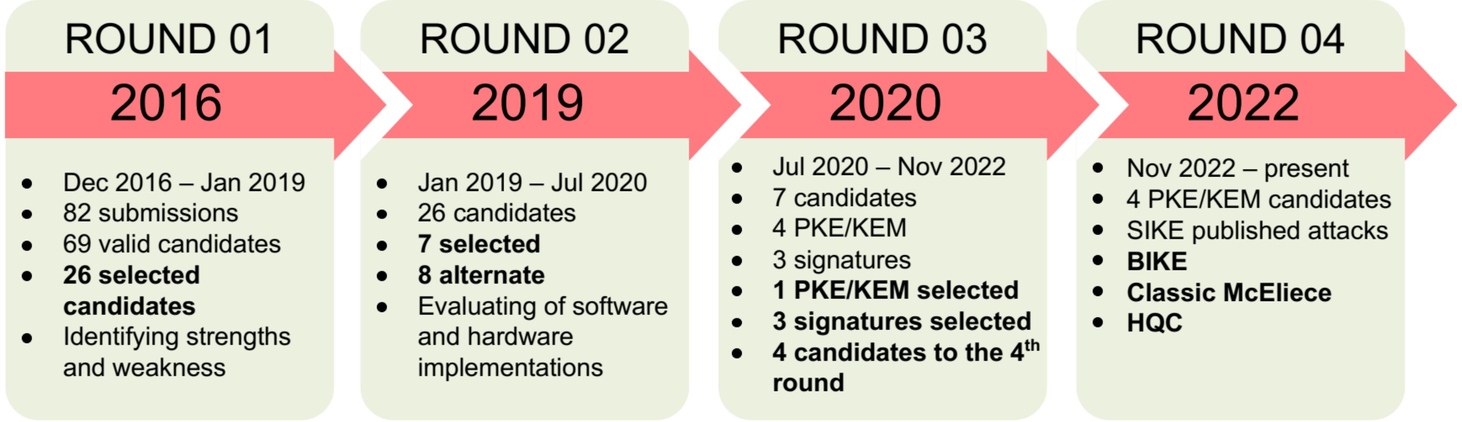
(3) Malicious functions, Denial of services,…

(4) Unauthorized access, data integrity, …

(5) Accessing the sensitive data

Activity 2: Survey on Post-Quantum Cryptography 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

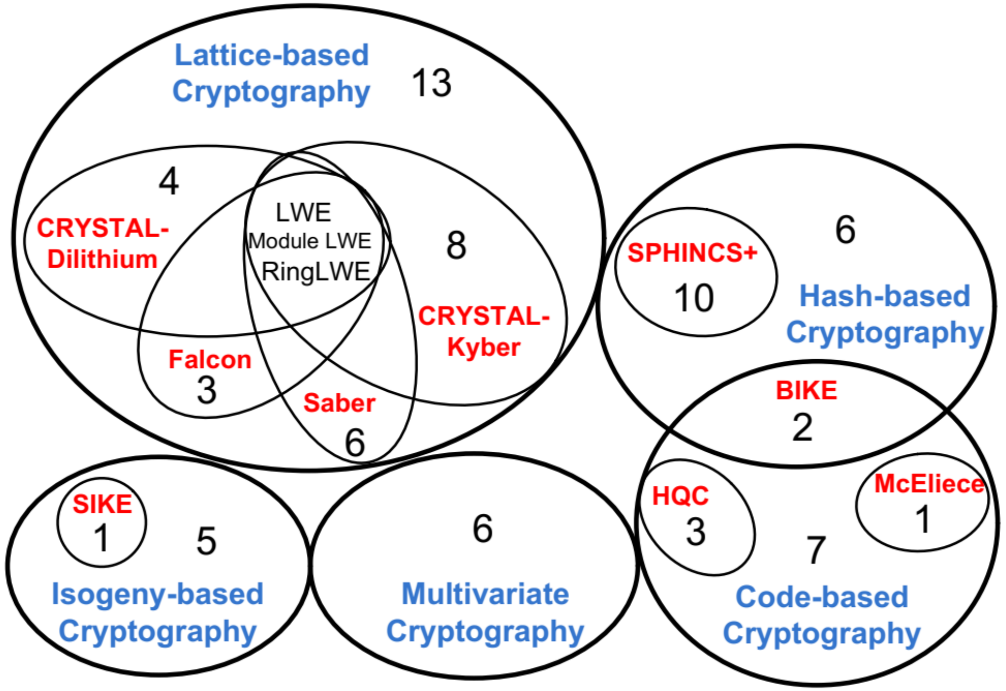
ROUND 03
2020

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

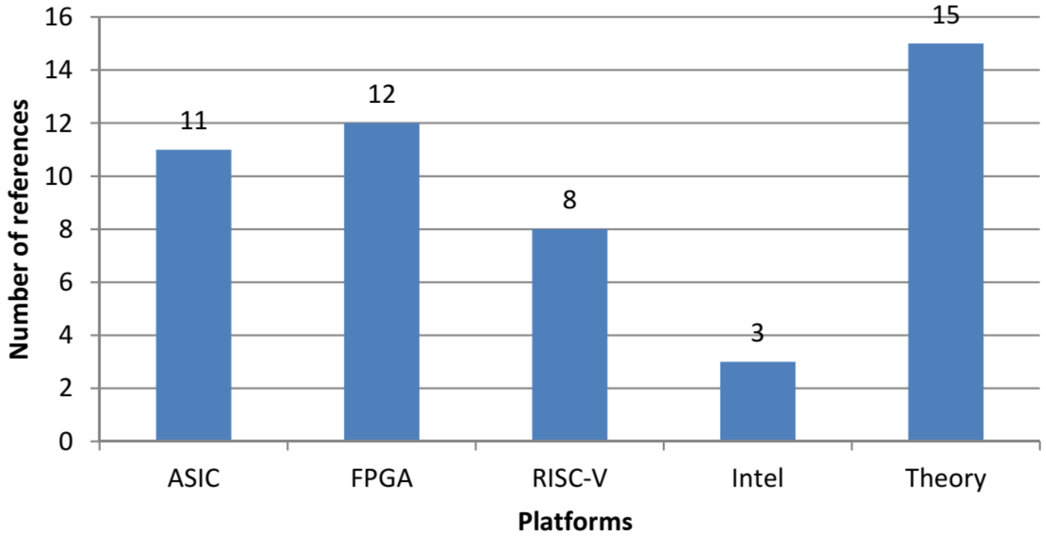
ROUND 04
2022

- 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:

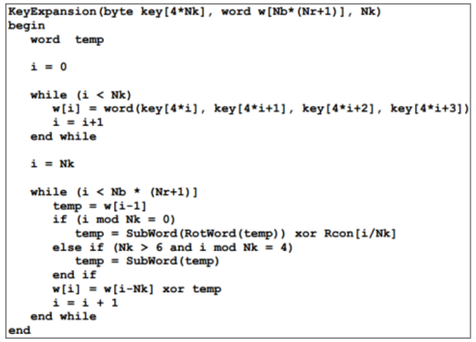


Number of references implemented on different platforms:



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

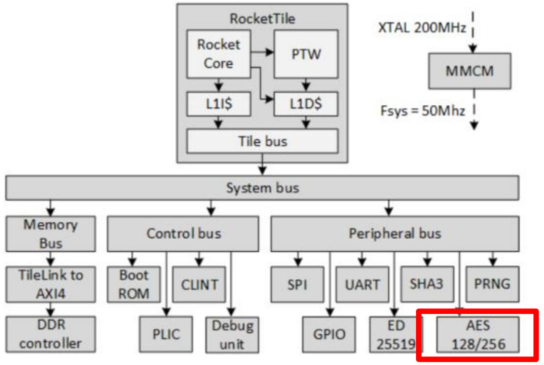
Activity 3: Deep Learning-Based Side Channel Attacks for Security Evaluation in SHs



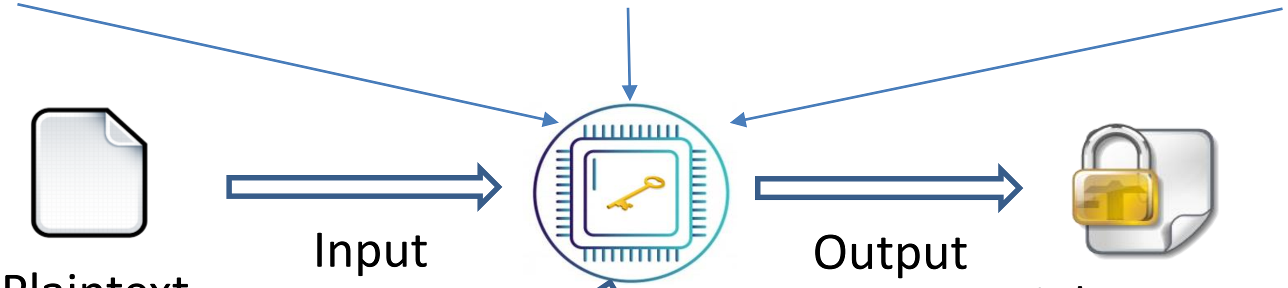
```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
   word  temp

   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



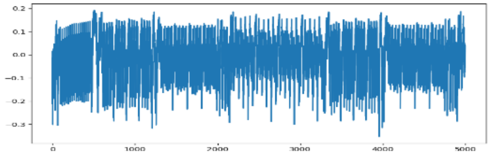
Plaintext

Input

Output

Ciphertext

- Power consumption
- Electromagnetic Radiation
- Temperature variation
- …



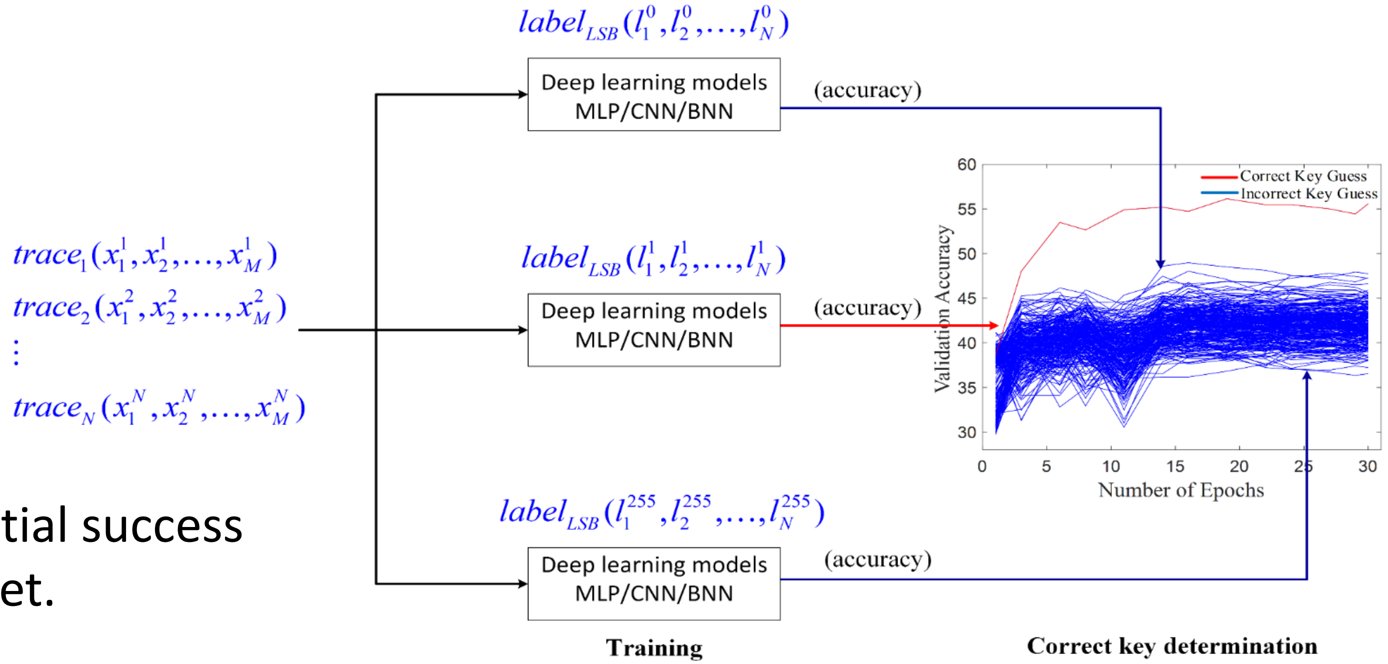
Side channel analysis

Secret key

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

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.



$trace_1(x_1^1, x_2^1, \ldots, x_M^1)$
$trace_2(x_1^2, x_2^2, \ldots, x_M^2)$
⋮
$trace_N(x_1^N, x_2^N, \ldots, x_M^N)$
$label_{LSB}(l_1^0, l_2^0, \ldots, l_N^0)$
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)
Correct Key Guess
Incorrect Key Guess
Validation Accuracy
60
55
50
45
40
35
30
0
5
10
15
20
25
30
Number of Epochs
Training
Correct key determination

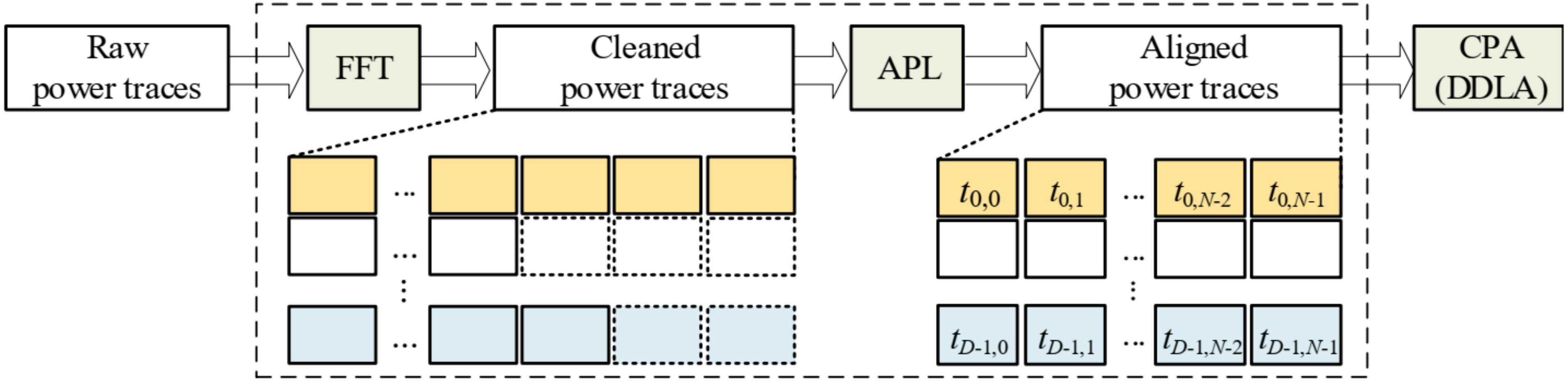
- ➢ It could reveal the secret subkey even if the partial success rate percentage is only 10% in the ASCAD dataset.

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 ($\alpha = 1.3$)			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗

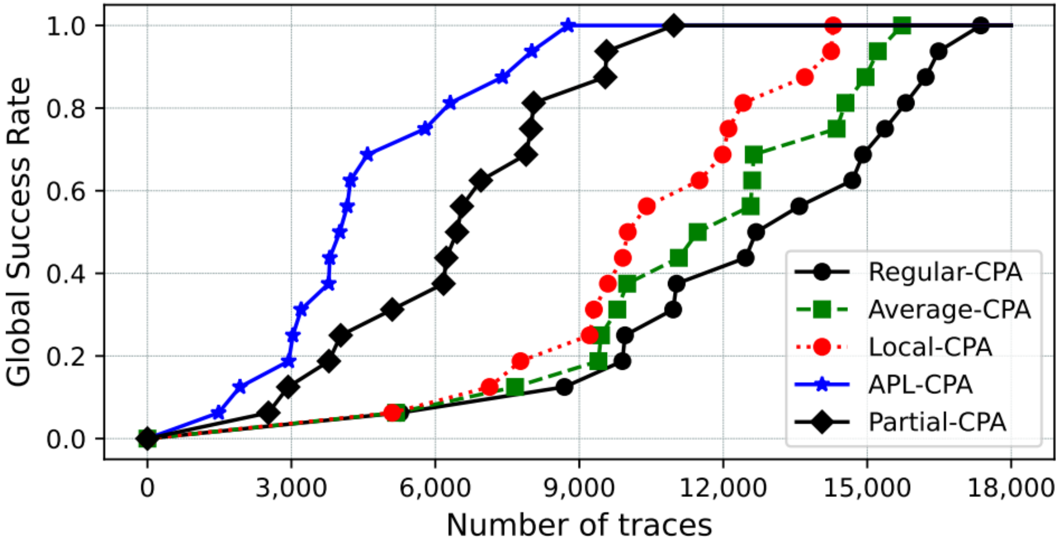
✓: Successful revealing secret key

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 (accepted).

Activity 4: Security Evaluation by Compacting Side-Channel Measurements



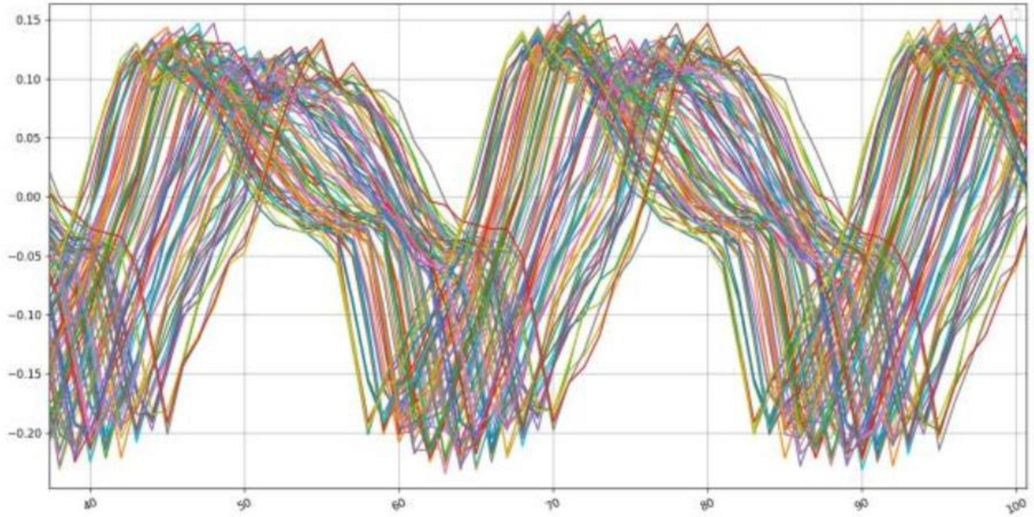
Main idea: We propose a new technique to reduce the computation time by extracting the Point of Interest (POI) with an interpolation method. The proposal uses the local extreme value and two adjacent samples around it to interpolate the real peak amplitude. Compared to the conventional CPA, the execution 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.



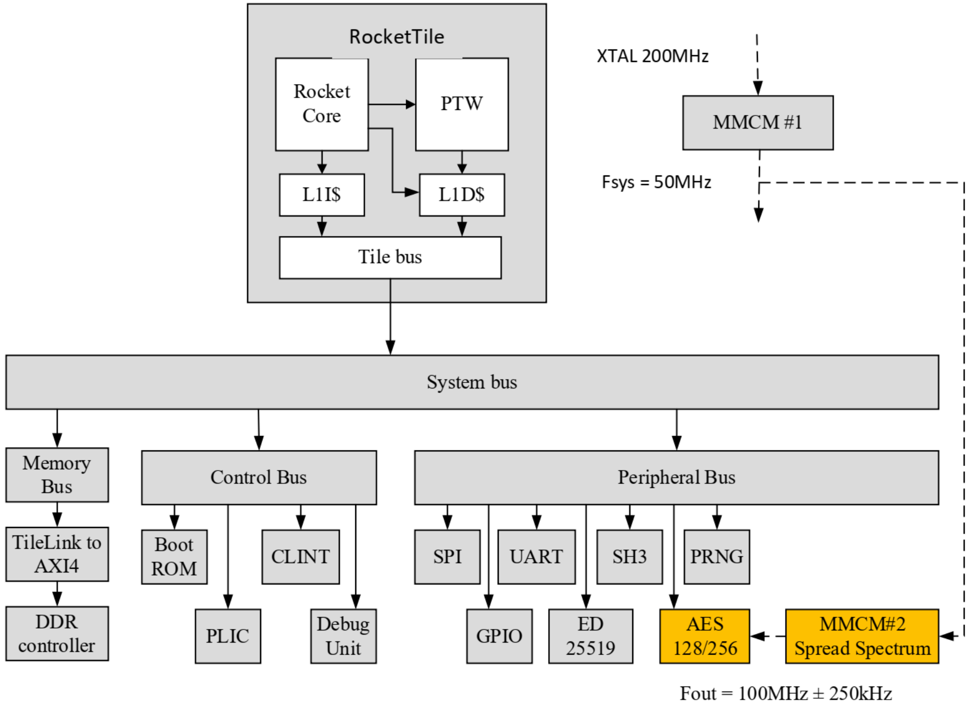
Thai-Ha Tran, Duc-Thuan Dam, Ba-Anh Dao, Van-Phuc Hoang, Cong-Kha Pham, and Trong-Thuc Hoang, “Compacting Side-Channel Measurements with Amplitude Peak Location Algorithm,” submitted to IEEE Transactions on VLSI Systems, 2023.

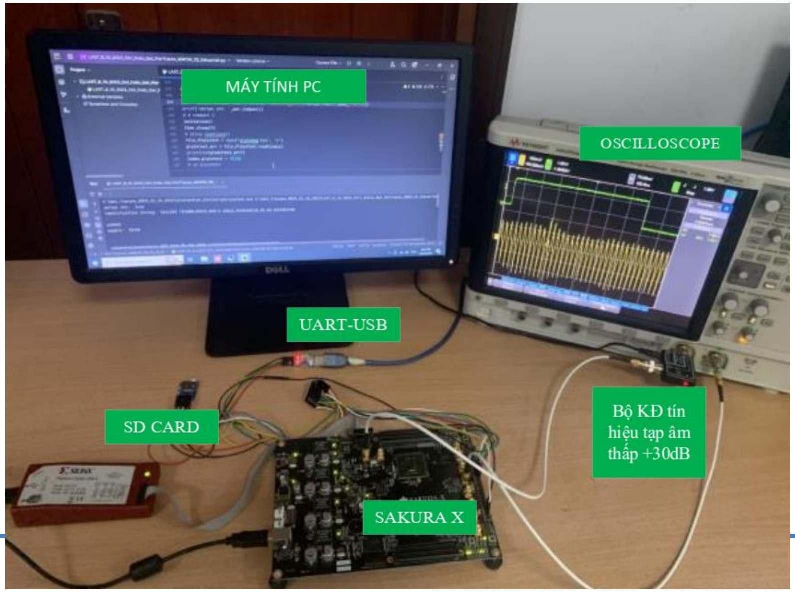
Activity 5: Countermeasures against side-channel attacks for RISC-V processors

- ➢ 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.



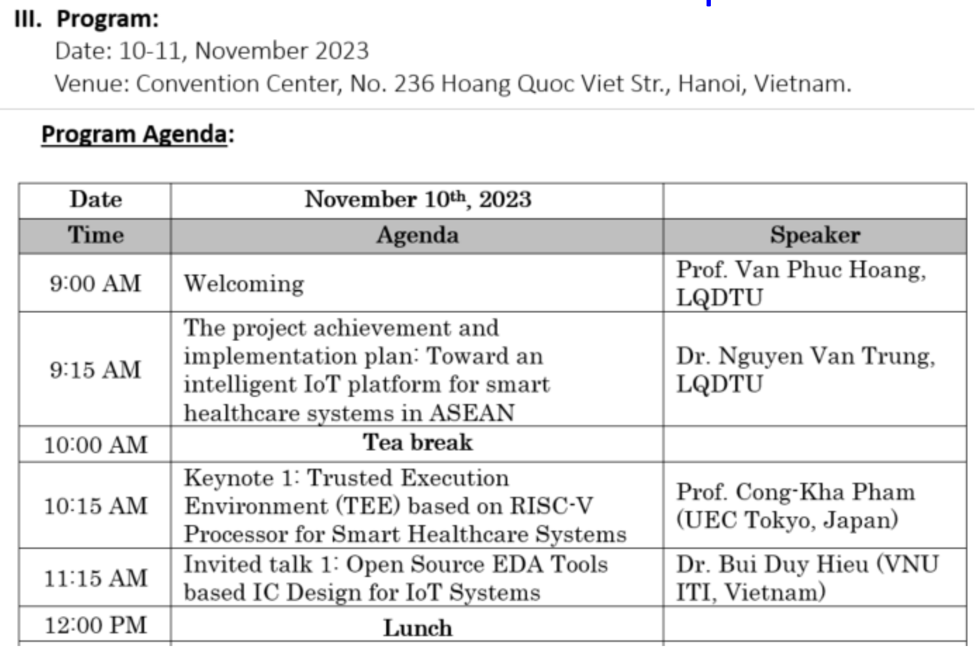


Luu Van Tuan, Trinh Quang Kien, Hoang Van Phuc et. al., “Countermeasures against side-channel attacks for RISC-V processors with integrated AES-128 core,” REV-ECIT conference 2023 (submitted).

Activity 6: Organizing Meetings and Workshops

- Project kick-off meeting: Online meeting, 12 participants.
- Open technical workshop entitled *"Advanced Cyber-security Solutions for IoT Systems"* organized in Hanoi, Vietnam: 16-presentation session and panel discussion.
- We plan for more workshops in the next year.

Application for workshop organization on Nov. 10-11 was accepted!



III. Program:

Date: 10-11, November 2023

Venue: Convention Center, No. 236 Hoang Quoc Viet Str., Hanoi, Vietnam.

Program Agenda:

Date	November 10th, 2023	
Time	**Agenda**	**Speaker**
9:00 AM	Welcoming	Prof. Van Phuc Hoang, LQDTU
9:15 AM	The project achievement and implementation plan: Toward an intelligent IoT platform for smart healthcare systems in ASEAN	Dr. Nguyen Van Trung, LQDTU
10:00 AM	**Tea break**	
10:15 AM	Keynote 1: Trusted Execution Environment (TEE) based on RISC-V Processor for Smart Healthcare Systems	Prof. Cong-Kha Pham (UEC Tokyo, Japan)
11:15 AM	Invited talk 1: Open Source EDA Tools based IC Design for IoT Systems	Dr. Bui Duy Hieu (VNU ITI, Vietnam)
12:00 PM	**Lunch**	

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)	The 16th IEEE International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC-2023)	18-21/12/2023 (accepted)	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 (submitted)	Hanoi, Vietnam

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	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 (Vietnam) and UEC (Japan)	IEEE Transactions on VLSI Systems	IEEE	2023 (submitted)

Budget Plan for 2023 Fiscal Year (Tentative)

Date	Item	Amount (USD)	Notes
Nov. 2023	2-day workshop organizing in Hanoi	9,828	
Nov. 2023	Attend ASEAN IVO Forum in Vientiane, Laos (project report)	600	
Dec. 2023	Purchase embedded machine learning, FPGA, laptop	8,729	
Dec. 2023	Attend IEEE MCSoC 2023 conference in Singapore	1,813	
Jan. 2024	Purchase EM probes, oscilloscope, LoRa Kit, PC	7,191	
Feb. 2024	One-month internship at NICT, Japan	3,600	
Mar. 2024	2-day workshop organizing in Hanoi	8,239	
	Total	**40,000**	

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:**
  - — With only 4 months from June 2023, the project team has achieved encouraging results.
  - — We have completed the survey and some techniques for cyber-security assurance in IoT-based SH systems.
  - — 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 hospital and patient sites.