

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:

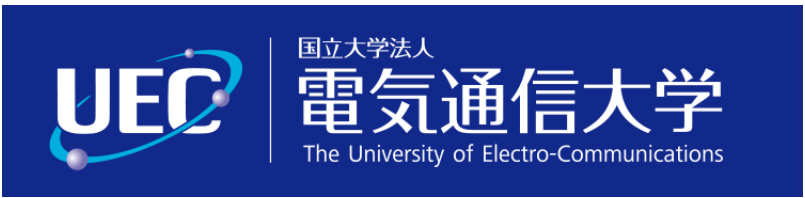
- Propose a comprehensive cyber-security platform with artificial intelligence (AI) empowered hardware-software oriented solutions for IoT-based smart healthcare (SH) Systems;
- Develop existing links and establish new links for researchers from ASEAN and Japan in the areas of cyber-security for IoT-based 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 Phuc Hoang (LQDTU, Vietnam)

Project Members

- | | | |
|---------------------------------|--|-----------------------------------|
| Van Phuc Hoang (LQDTU, Vietnam) | Bah Hwee Gwee (NTU, Singapore) | Van Trung Nguyen (LQDTU, Vietnam) |
| Cong-Kha Pham (UEC, Japan) | Norrathep Rattanavipanon (PSU, Thailand) | Quang Kien Trinh (LQDTU, Vietnam) |
| Kazuo Sakiyama (UEC, Japan) | Kuljaree Tantayakul (PSU, Thailand) | Nga Dao Thi (LQDTU, Vietnam) |
| Hoang Trong Thuc (UEC, Japan) | Kong Phutphalla (CADT, Cambodia) | Van Tuan Luu (LQDTU, Vietnam) |
| Thai Ha Tran (UEC, Japan) | Lay Vathna (CADT, Cambodia) | Ngoc Tuan Do (LQDTU, Vietnam) |
| Takeshi Takahashi (NICT, Japan) | Lay Puthineath (CADT, Cambodia) | |



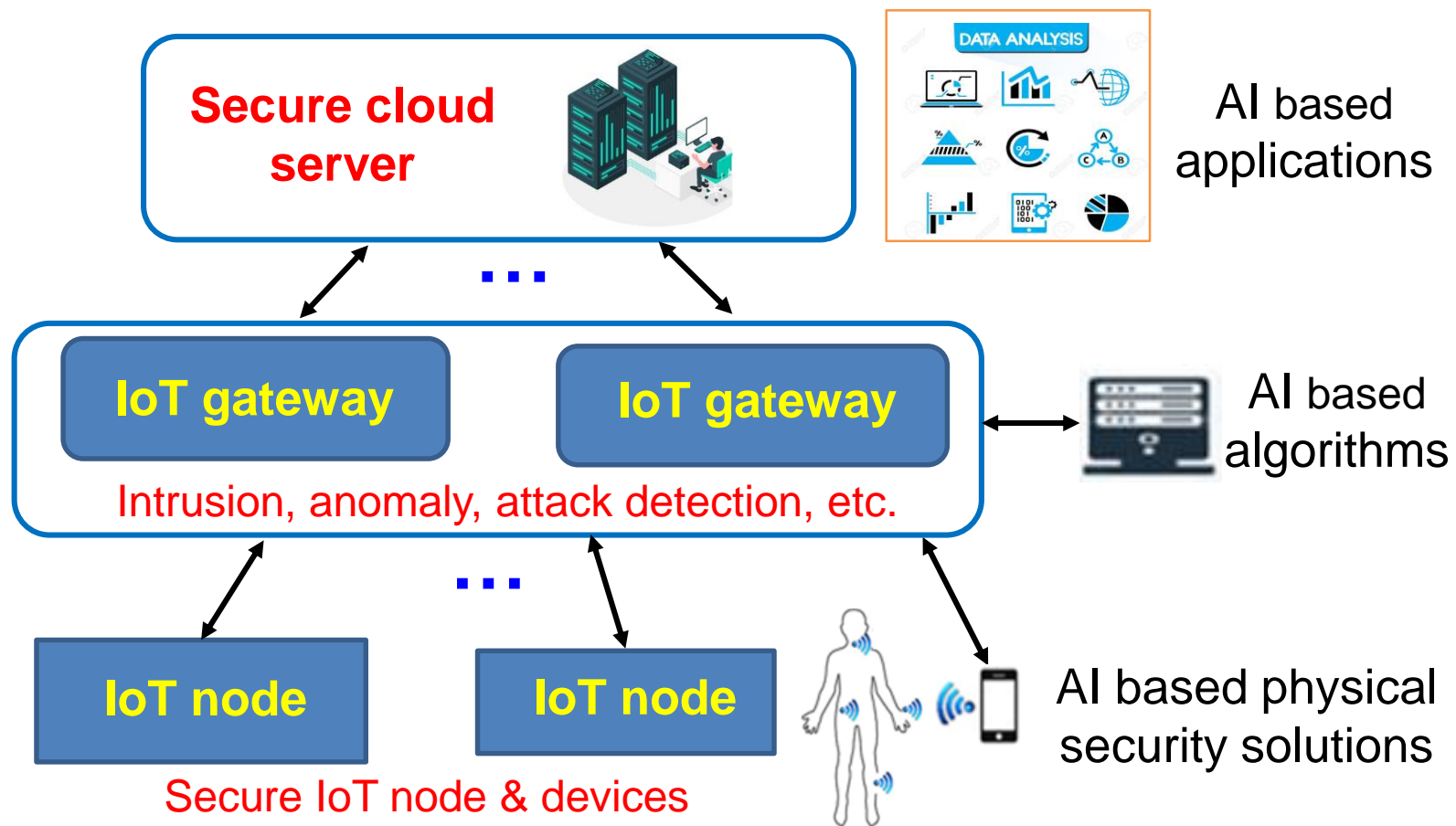
Leader: Prof. Van Phuc Hoang (LQDTU, Vietnam)

Project Duration: From June 01, 2023 to March 31, 2026

Project Budget: 80,000 USD



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



Project activities:

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

Activity 1: Survey on security of embedded ML & Post-Quantum Cryptography (PQC)

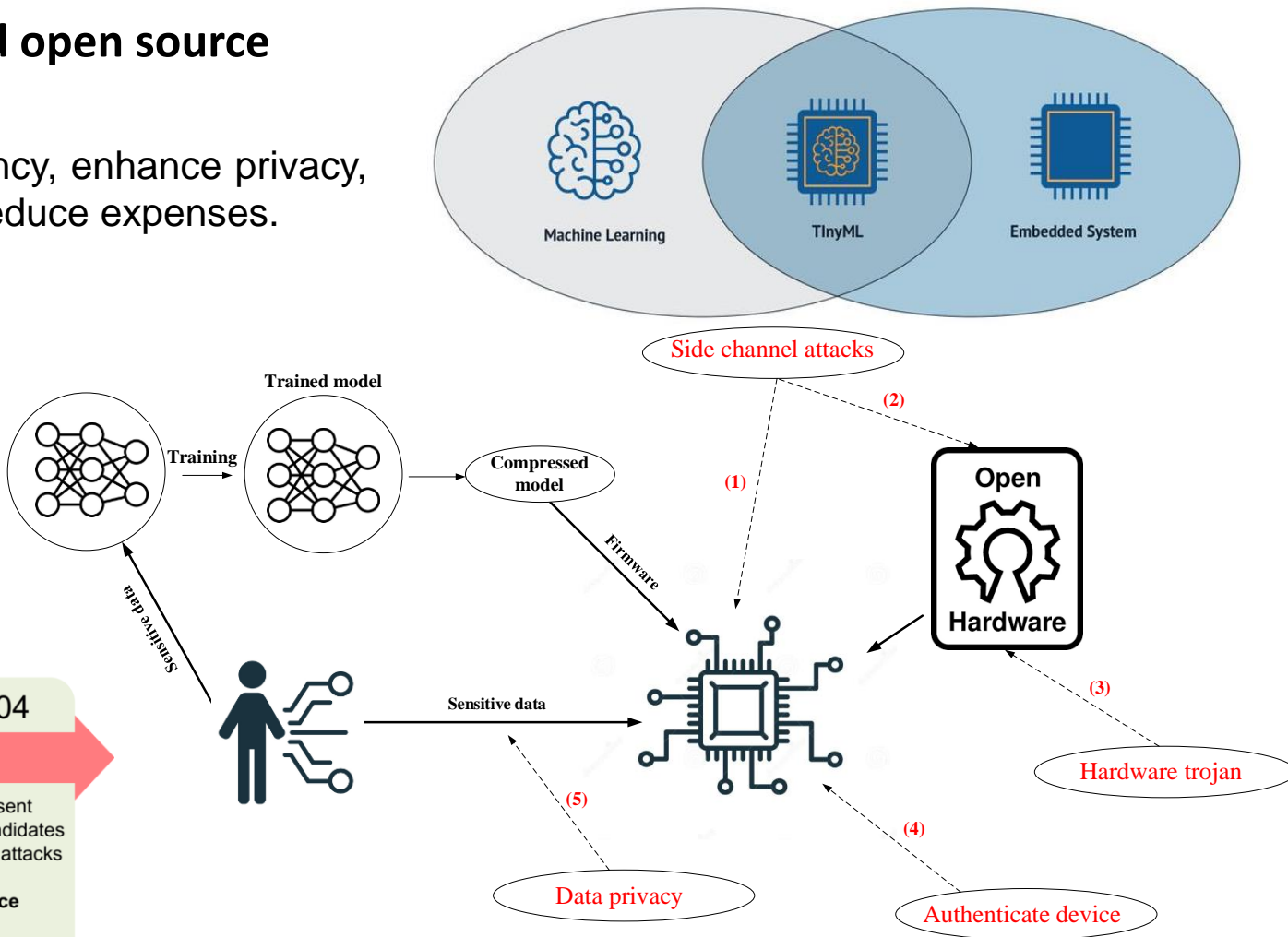
1. Combination of embedded machine learning and open source hardware (OSH) in healthcare systems

- To ensure efficient utilization of bandwidth, minimize latency, enhance privacy, ensure the security of patients' sensitive information, and reduce expenses.

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

3. PQC:

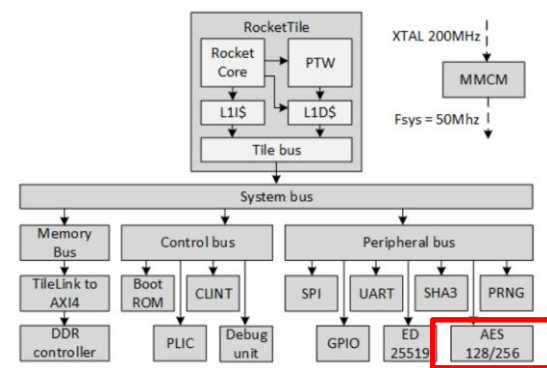


Duc-Thuan Dam, Thai-Ha Tran, Van-Phuc Hoang, Cong-Kha Pham, Trong-Thuc Hoang, "A Survey of Post-Quantum Cryptography: Start of a New Race," Cryptography 2023, 7, 40. <https://doi.org/10.3390/cryptography7030040>

Activity 2: Deep Learning-Based Side Channel Attacks for Security Evaluation in SHs

```

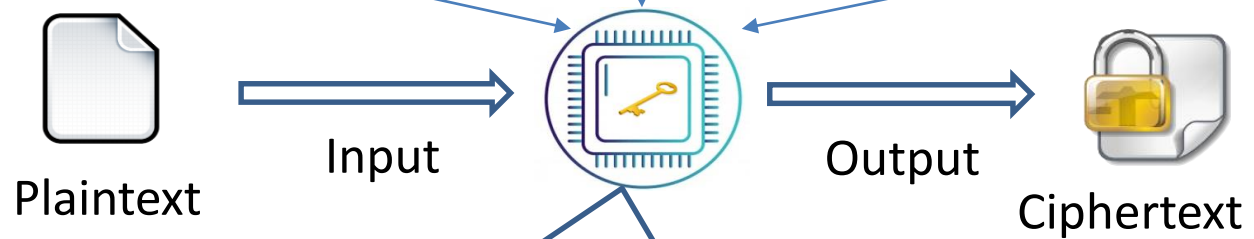
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nr, Nk)
begin
  word temp
  i = 0
  while (i < Nr)
    w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
    i = i+1
  end while
  i = Nr
  while (i < Nb * (Nr+1))
    temp = w[i-1]
    if (i mod Nk = 0)
      temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
    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
  
```



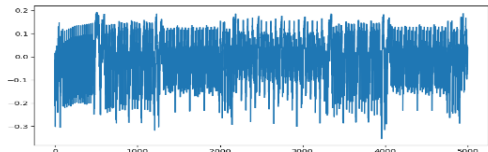
Software implementation

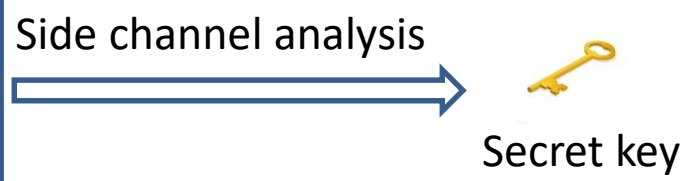
Application Specific Integrated Circuit

A built-in accelerator



- Power consumption
- Electromagnetic Radiation
- Temperature variation
- ...

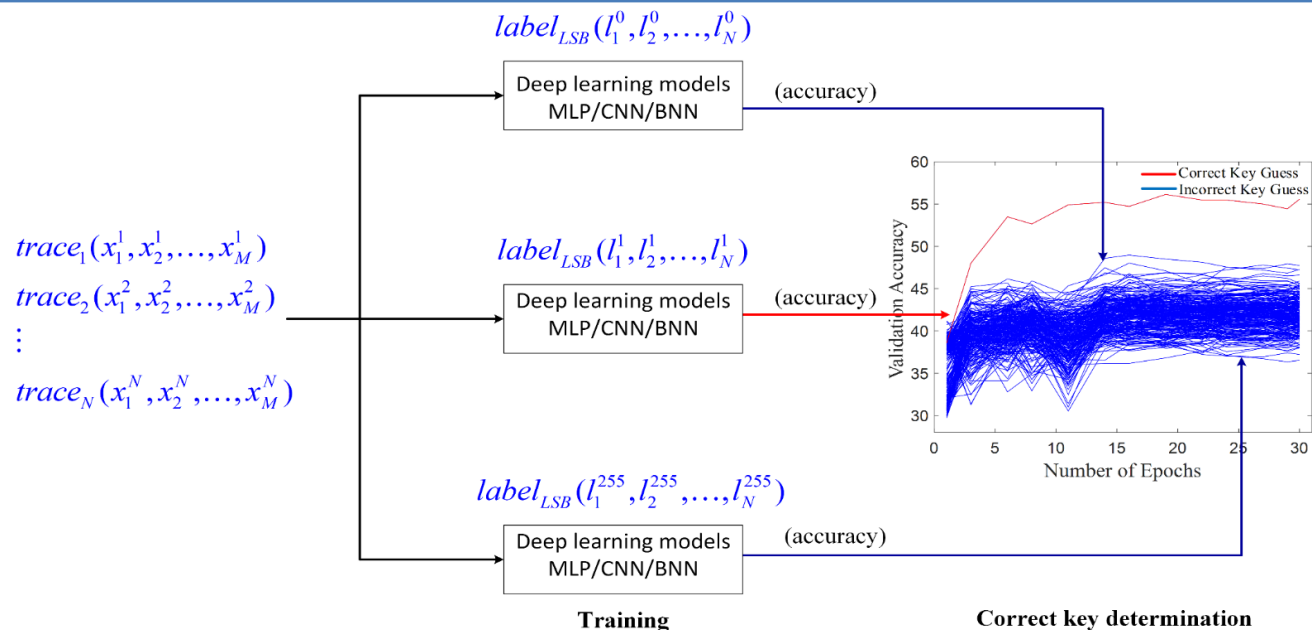




Activity 2: Deep Learning Based SCA for Security Evaluation in SHs (cont.)

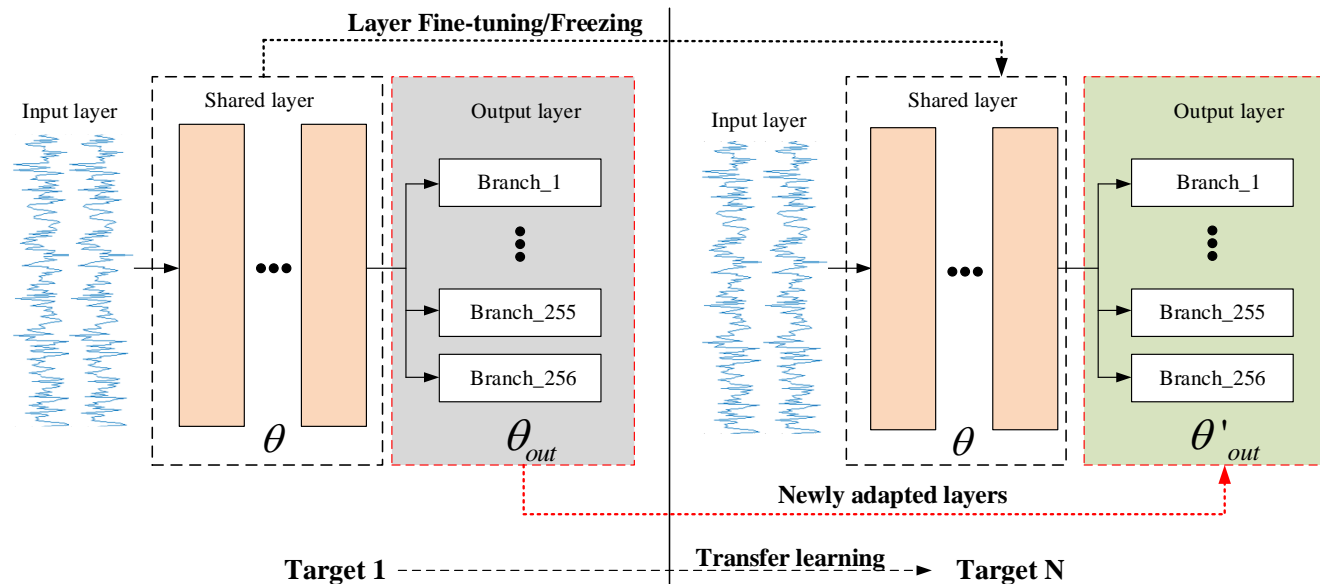
Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks:

- 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 partial success rate percentage is only 10% in the ASCAD dataset.

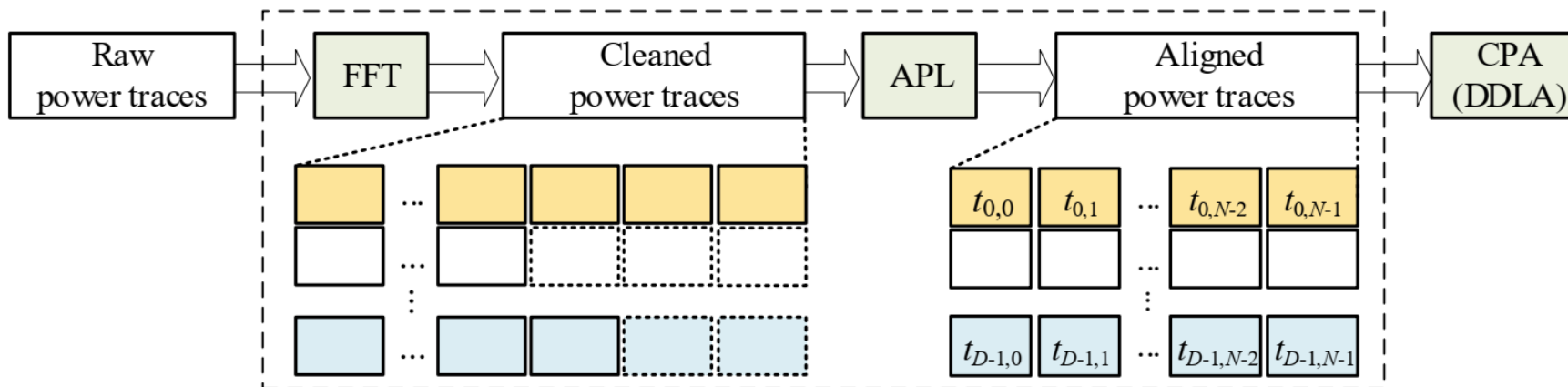


Enhancing Performance of Deep Learning Based Non-Profiled Side-Channel Attack Using Multi-Output and Transfer Learning:

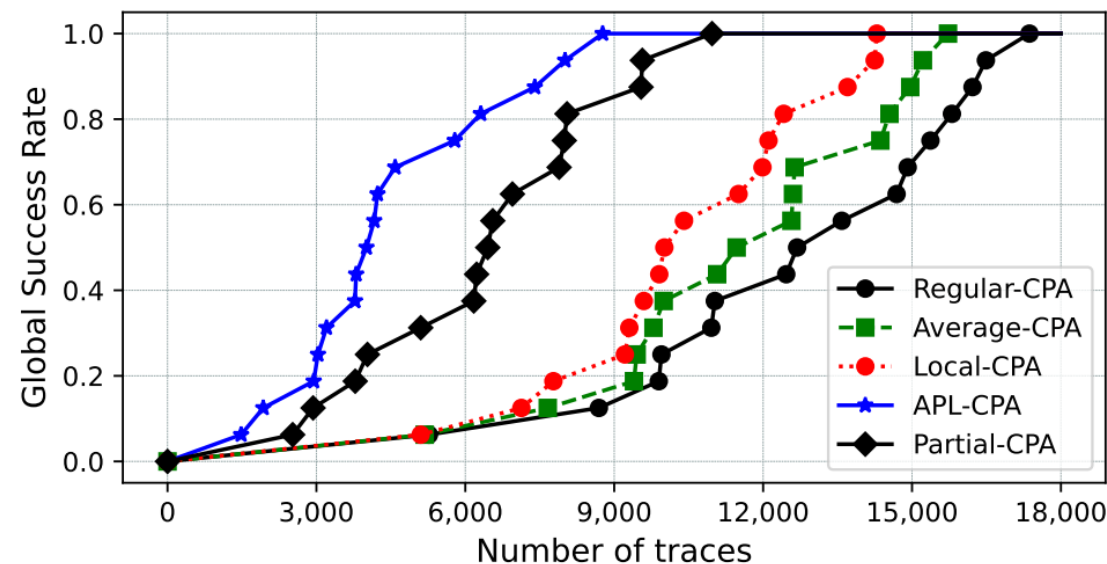
- Van-Phuc Hoang et. al, "Revealing Secret Key from Low Success Rate Deep Learning-Based Side Channel Attacks," IEEE MCSoc 2023 conference.
- Van-Phuc Hoang et, al, "Enhancing Performance of Deep Learning Based Non-Profiled Side-Channel Attack Using Multi-Output and Transfer Learning," 2024 IEEE TechDefense.



Activity 3: Security Evaluation by Compacting Side-Channel Measurements



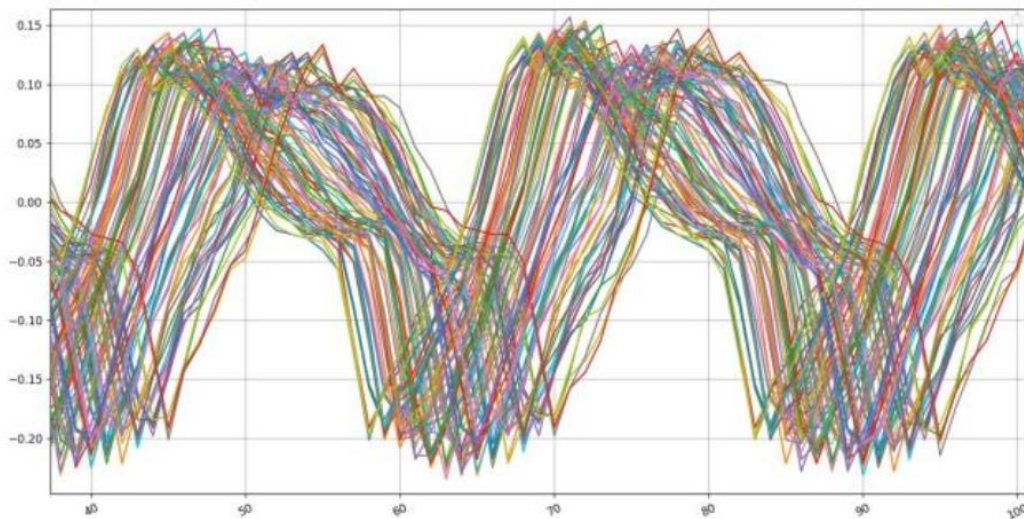
Main idea: We propose a new technique to reduce the computation time by extracting the Point of Interest (POI) with an interpolation method. The proposal uses the local extreme value and two adjacent samples around it to interpolate the real peak amplitude. Compared to the conventional CPA, the execution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



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.

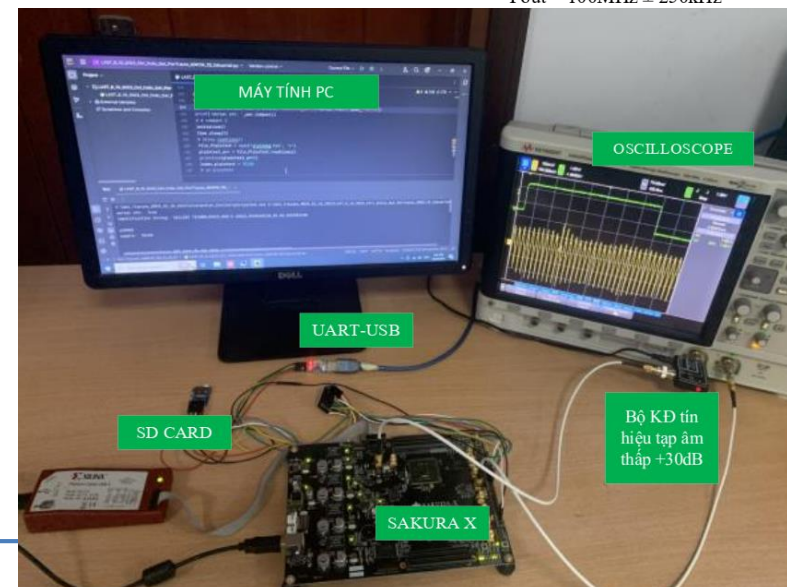
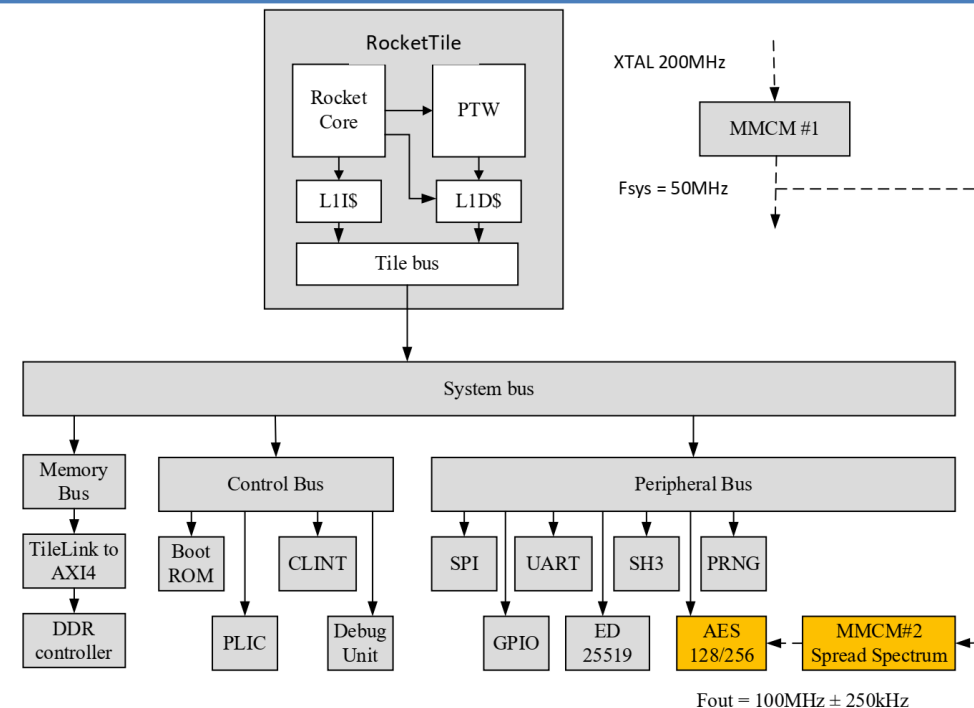
Activity 4: Countermeasures against side-channel attacks for RISC-V processors

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

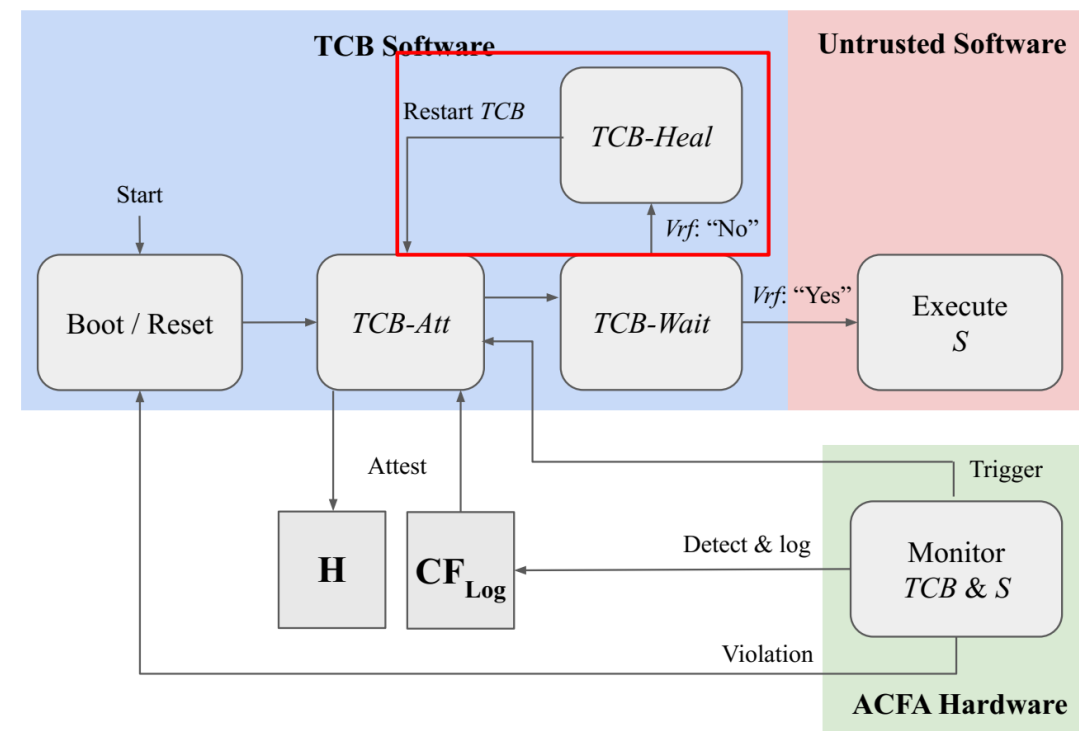
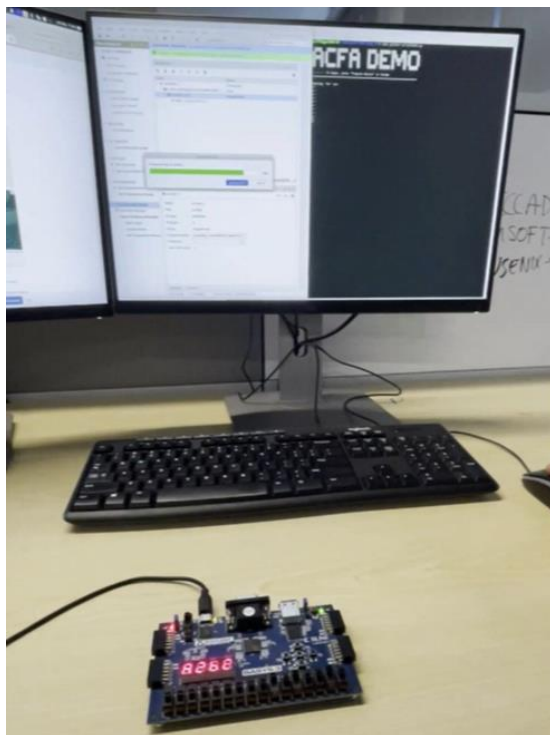


- The level of information leakage is reduced by 182 times.

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.

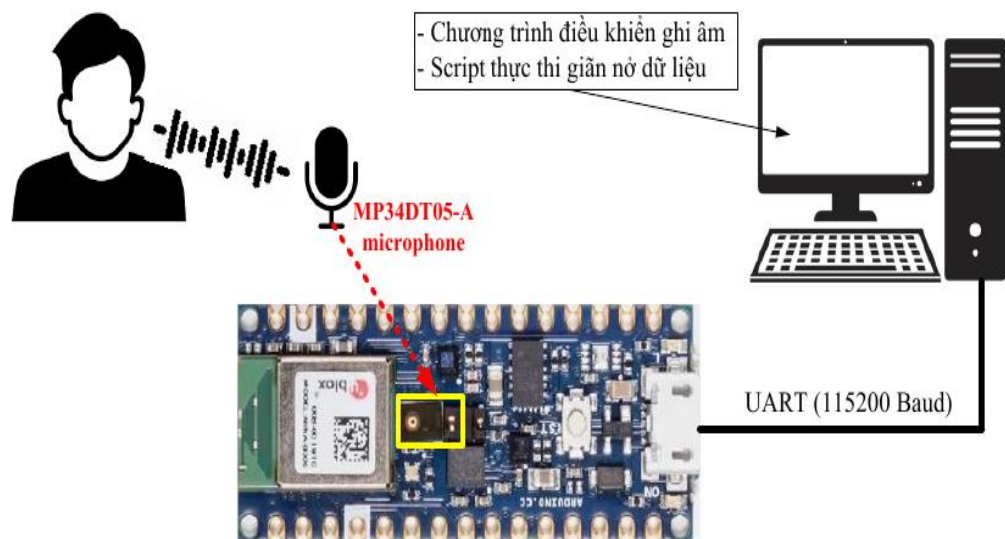


Activity 5: Secure Runtime Auditing, Guaranteed Device Healing via Active Control Flow Attestation (ACFA) & TEE-based Runtime Auditing

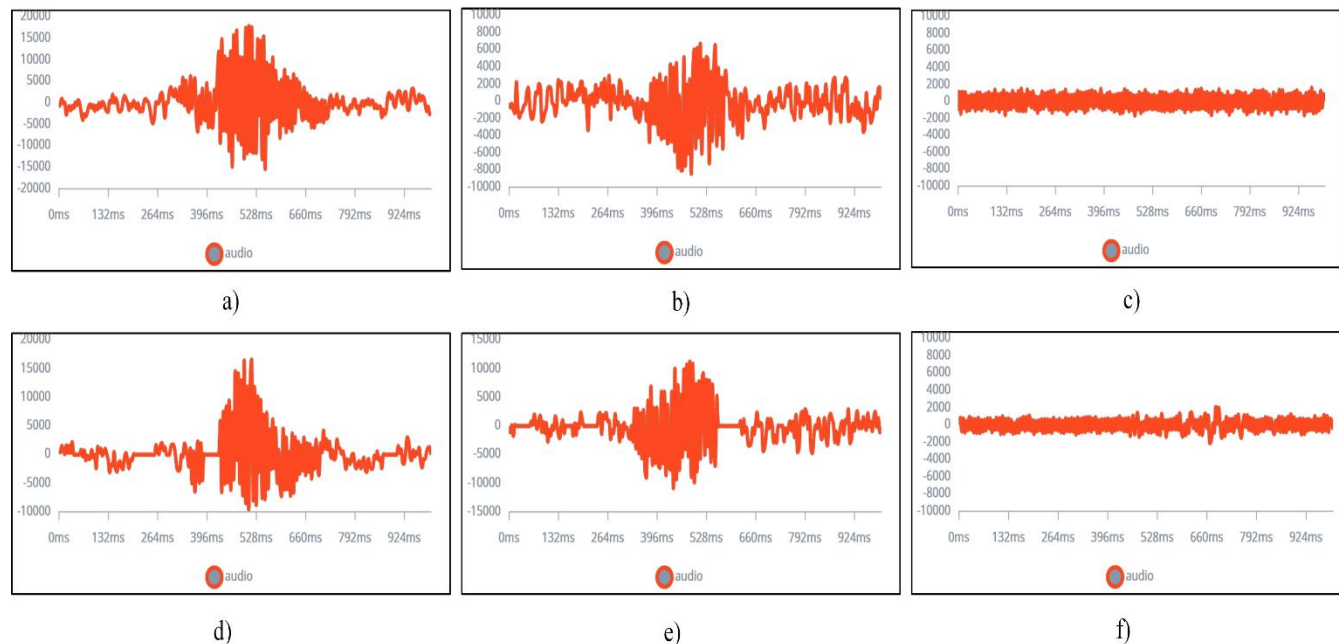


- Remote Attestation (RA) is an inexpensive security service that enables a verifier to remotely detect illegal modifications to the software binary installed on a prover MCU
- Hardware Cost of proposed ACFA: 275 LUTs, 202 FFs (5.8x less LUTs, 10.5x less FFs than LiteHAX)
 - Caulfield Adam, Norrathep Rattanaivanon, 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.
 - A. Caulfield, A. J. Neto, N. Rattanaivanon and I. De Oliveira Nunes, "TRACES: TEE-based Runtime Auditing for Commodity Embedded Systems," 2024 Annual Computer Security Applications Conference (ACSAC), USA, 2024, pp. 257-270, doi: 10.1109/ACSAC63791.2024.00035.

Activity 6: Tiny ML for Elder People Assistance in SH (On-going Work)



a) Experimental setup for recording keyword sounds

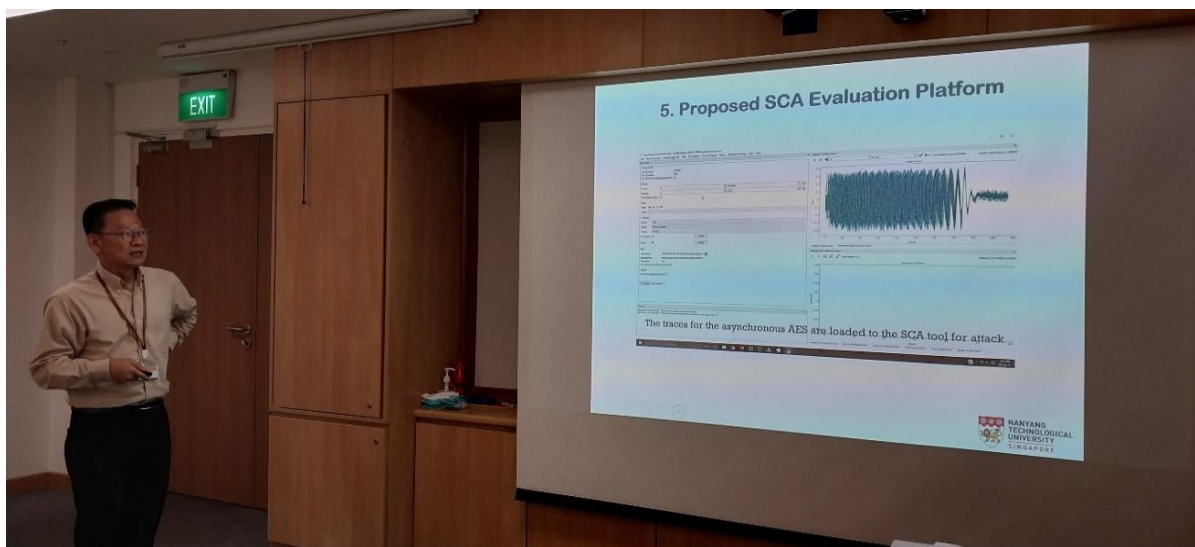


b) Examples of audio signals recorded from Arduino Nano 33 BLE development board

- Tiny ML: Implement ML in resource constrained hardware devices.
- A native recording application and a custom data-collection script running on host PC controlling Arduino board and synchronized the captured signals.
- Representative waveforms illustrate variations in amplitude and temporal structure across different spoken digits and background conditions.

Activity 7: Organizing Meetings and Workshops

- Project kick-off meeting on 10 August, 2023: Online meeting, 12 participants.
- 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.
- 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.
- Open technical workshop entitled *“Intelligent Embedded Security for Internet of Things Systems”* organized in NTU (Singapore) on 22-24 July, 2024: 17-presentation session and panel discussion.
- Open technical workshop entitled *“”* organized in Hanoi, July, 2025: 17-presentation session and panel discussion.



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, 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 Huy 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

No	Paper title:	Author names	Affiliation	Conference name	Conference date	Conference venue
6	ACFA: Secure Runtime Auditing & Guaranteed Device Healing via Active Control Flow Attestation	Caulfield Adam, Norrathep Rattanaivanon, Ivan De Oliveira Nunes	PSU (Thailand), RIT (USA)	32nd USENIX Security Symposium (USENIX Security 23)	9-11/8/2023	CA, USA
7	TRACES: TEE-based Runtime Auditing for Commodity Embedded Systems	Caulfield Adam, Antonio Joia Neto, N. Rattanaivanon, Ivan De Oliveira Nunes	PSU (Thailand), RIT (USA)	Annual Computer Security Applications Conference (ACSAC)	9-13/12/2024	Hawaii, USA
8	PEARTS: Provable Execution in Real-time Embedded Systems	Joia Neto, Antonio, N. Rattanaivanon, Ivan De Oliveira Nunes	PSU (Thailand), RIT (USA)	46th IEEE Symposium on Security and Privacy (S&P)	12-14/5/2025	CA, USA
9	Correlation Power Analysis of Pipelined and Multi-Threaded Coarse-Grained Reconfigurable Cryptographic Accelerator	Van-Tuan Luu et al.	LQDTU (Vietnam) , NAIST (Japan)	10th IEEE International Conference on Integrated Circuits, Design, and Verification (ICDV)	16-17/6/2025	HCMC, Vietnam



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 et al.	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, VNU HCM (Vietnam) and UEC (Japan)	IEEE Transactions on VLSI Systems	IEEE	2024
6	Non-Contact Pulse Rate Estimation from Remote Photoplethysmography using Wavelet Transform Filter and Convolutional Neural Network	Hoang Thi Yen, Doan Van Sang, Van-Phuc Hoang, Guanghao Sun	LQDTU (Vietnam) and UEC (Japan)	International Journal of Biomedical Engineering and Technology	Indersci.	2025
7	Efficient non-profiled side-channel attack using multi-output deep learning neural network and transfer learning	Le Huy Thanh, Ngoc-Tuan Do, Van-Phuc Hoang, Huu Minh Nguyen	LQDTU (Vietnam)	Internet of Things	Elsevier	2025 (submitted)

- **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:**

- The project team has achieved encouraging results with many publications.
- We have completed the survey and innovative techniques for cyber-security assurance in IoT-based smart healthcare systems using machine learning and deep learning techniques.
- Perform laboratory experiments for essential components in the proposed systems.
- AI can be exploited for: Security evaluation, elder assistance, system protection, etc.
- Ready to propose and implement the overall system.

- **Future works:**

- Perform more experiments for other essential components in the proposed systems.
- Complete the work on Tiny ML implementation for elder people assistance in smart healthcare systems.
- Build the application for field experiments in healthcare systems.