VIETNAM NATIONAL UNIVERSITY, HANOI
VNU UNIVERSITY OF ENGINEERING AND TECHNOLOGY

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom – Happiness

INFORMATION ON DOCTORAL THESIS

1. Full name : Dong Pham Khoi ..... 2. Sex: Male.....

3. Date of birth: 12/07/1982..... 4. Place of birth: Thanh Hoa province .

5. Admission decision number: 654/QĐ-CTS.. Dated 05/9/2016 .....

6. Changes in academic process: ....

(List the forms of change and corresponding times)

7. Official thesis title: High-performance, low-power AES security hardware architecture for internet of things devices. .....

8. Major: Electronics and Telecommunications Technology…..9. Code: 9510302.01 ....

10. Supervisors: Professor Tran Xuan Tu.....

(Full name, academic title and degree)

11. Summary of the **new findings** of the thesis:

- Propose and implement single-core AES hardware architecture for real-time and high-throughput applications. Parallel architecture and pipeline techniques are used to speed up encoding and reduce latency. The results of hardware implementation on 45nm ASIC technology show that the design achieves high throughput of 111.3 Gbps and low latency (12.6 ns). These results were published at the IEEE ISCIT 2019 Conference (work [C1]).
- Propose and implement a parallel multi-core AES hardware architecture with high encryption throughput. To minimize the cost of area and power consumption, the KeyExpansion block is shared among the AES cores. Hardware performance results demonstrate that the architecture achieves up to 1 Tbps throughput with 10 AES cores on the chip. The results were published at the IEEE APCCAS 2020 Conference (work [C2]) and in the JCSCE Scientific Journal (work [J1]).
- Propose and implement the Spike-MCryptCores hardware architecture with a low-power neural controller that controls the on/off clock of the AES cores (clock gating). Spike-MCryptCores includes software to design, train, and test SNN controllers, and hardware including multiple AES cores and SNN controllers. The SNN controller can help the system reduce energy consumption from 39% to 67%. With Spike-McryptCores, the thesis has introduced a new method to design and control multi-core

systems with small cost, high accuracy and energy saving. These results have been published in the journal Microprocessors and Microsystems (work [J2]).

12. Practical applicability, if any: The results of the thesis can be applied to hardware security with high efficiency and low power consumption for IoT devices.

13. Further research directions, if any:

- Apply the Spike-MCryptCores model to other types of multi-core applications.
- Use Spike-MCryptCores for other low-power techniques such as power-gating or Dynamic Voltage-Frequency Scaling - DVSF.

14. Thesis-related publications:

[C1] Pham-Khoi Dong, H. K. Nguyen, and Xuan-Tu Tran, "A 45nm High-Throughput and Low Latency AES Encryption for Real-Time Applications," in 2019 *19th International Symposium on Communications and Information Technologies* (ISCIT), Sep. 2019, pp. 196–200. doi: 10.1109/ISCIT.2019.8905235.

[C2] Pham-Khoi Dong, H. K. Nguyen, Van-Phuc Hoang, and Xuan-Tu Tran, "Low-Power Implementation of a High-Throughput Multi-core AES Encryption Architecture," in *2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Dec. 2020, pp. 74–77. doi: 10.1109/APCCAS50809.2020.9301668.

[J1] Pham-Khoi Dong, H. K. Nguyen, F. A. Hussin, and Xuan-Tu Tran, "Ultra-High-Throughput Multi-Core AES Encryption Hardware Architecture," *VNU J. Sci. Comput. Sci. Commun. Eng.*, vol. 37, Nov. 2021, doi: 10.25073/2588-1086/vnucsce.290.

[J2] Pham-Khoi Dong, Khanh N. Dang, Duy-Anh Nguyen, and Xuan-Tu Tran, "A light-weight neuromorphic controlling clockgating based multi-core cryptography platform" *Microprocessors and Microsystems*, **resubmitting.**

(List them in chronological order)

Date: ……..	Date: ……..
Signature: ……	Signature: ……
Full name: ……	Full name: ……

*Note: **"Information on Doctoral Thesis"** must be processed on Microsoft Word, font Unicode Times New Roman, letter size 13. " Summary of the new findings of the thesis" should be one-A4 page long.*