VIETNAM NATIONAL UNIVERSITY, HANOI
VNU UNIVERSITY OF ENGINEERING AND TECHNOLOGY

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom – Happiness

INFORMATION ON DOCTORAL THESIS

1. Full name: Đào Mạnh Hiệp ..... 2. Gender: Male.....

3. Date of birth: 19th July, 1995 ..... 4. Place of birth: Hanoi, Vietnam.....

5. Admission decision number: 1344/QĐ-CTSV signed on 25th November 2019 by Principal of VNU University of Engineering and Technology .....

6. Changes in academic process: ....

(List the forms of change and corresponding times)

7. Official thesis title: Security Lightweight RFID tag with Elliptic Curve Cryptography

8. Major: Electronics Engineering .....9. Code: 9520203

10. Supervisors: .....

- Prof. Trần Xuân Tú, VNU Information Technology Institute
- Prof. Vincent Beroulle, University Grenoble Alpes, France

11. Summary of the contributions of the thesis:

Radio frequency identification (RFID) technology has made a breakthrough in the field of wireless authentication with many applications. Unlike active RFID tags that use a separate internal feed source, passive tags convert the electromagnetic energy provided by the reader into electricity to supply the system running on the card. The removal of the internal battery makes the device more compact and cost-effective. Therefore, passive RFID cards play an important role in handheld applications such as electronic passports, citizen ID cards, or contactless payment cards.

However, passive RFID tags face a variety of security vulnerabilities, including wireless and hardware attacks. In order to mitigate risks, the integration of ciphers such as the Elliptic Curve Encryption (ECC) algorithm into passive RFID tags is a key element for data protection. However, the implementation of ECC on passive RFID tags faces the following challenges:

- Physical resource limitations: Passive RFID tags are subject to strict constraints on energy consumption, area, and latency by the ISO/IEC-14443 standard.
- Security requirements: Passive RFID card protection measures against wireless and hardware attacks increase processing complexity. As a result, the cost of implementing the system has increased significantly.

In addition, the design process to implement the authentication protocol using the ECC curve encryption algorithm goes through many layers of design with a series of choices in system architecture and implementation algorithms. This complicates the design space of the system, increasing the time-to-market and product development costs.

Therefore, these issues motivate our researches to develop a new design process that helps designers balance the cost of execution and the security of the system by simultaneously evaluating both of these factors at each design stage. In addition, the new design process also needs to reduce design time to optimize product research and development costs.

In order to address these issues, the study has proposed the following key contributions:

- A cost-effective and low-power BEC hardware architecture with a physical area of 21.68 kGates logic has been proposed and synthesized using TSMC 65nm CMOS technology, according to the traditional top-down design method. The recommended hardware architecture consumes 126μW of power at 10MHz, which is estimated using the Synopsys PrimeTime tool. The hardware implementation results show that our proposed system is cost-effective in terms of deployment and energy consumption when compared to other buildings. Besides, the TVLA review proves that the proposal is resistant to the side channel security vulnerability.
- Propose EEMitM (Early Evaluation Meet-in-the-Middle) design methodology to help optimize multiple objectives in a large design space. By using a database of reference security principals, designers can model the selected system without creating a prototype. The proposed framework allows for rapid modeling in the software environment, which in turn significantly reduces the time to market. Experiments show that, when applying this proposal, the product development time is reduced by 480 times compared to the traditional design process. In terms of accuracy in estimating the cost of implementation, experiments show a latency error of only 1.2%. In the case of the worst power consumption estimate, the accuracy remains at an acceptable error of 22.6%.

12. Practical applicability, if any:

- Applications in passive RFID authentication, encryption card applications such as e-Civil Identification cards, contactless payment cards, or e-passports.
- The proposed EEMitM design methodology initially addresses some of the key challenges in exploring the design space for authentication protocols using Elliptic Curve Cryptography algorithms for passive RFID cards, initiating many open research directions that can continue to be developed.

13. Further research directions, if any:

- Security evaluation of the proposed hardware design of Binary Edward Curves with particular hardware vulnerabilities, including Correlation Power Analysis (CPA) or Differential Power Analysis (DPA).
- Develop design methodologies into automated design tools (EDAs) with graphical user interfaces (GUIs).
- Expand application databases for many specific applications

14. Thesis-related publications: .....

- **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, and Xuan-Tu Tran. "How to Develop ECC-Based Low-Cost RFID Tags Robust Against Side-Channel Attacks." In International Conference on Industrial Networks and Intelligent Systems, pp. 433-447. Cham: Springer International Publishing, 2021.
- Souhir Gabsi, Vincent Beroulle, Yann Kieffer, **Manh-Hiep Dao**, Yassin Kortli, and Belgacem Hamdi. "Survey: Vulnerability analysis of low-cost ECC-based RFID protocols against wireless and side-channel attacks." Sensors 21, no. 17 (2021): 5824.
- **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, and Xuan-Tu Tran (2023). "Secure-by-Design methodology using Meet-in-the-Middle design flow for hardware implementations of ECC-based passive RFID tags". In ICWMC 2023, The Nineteenth International Conference on Wireless and Mobile Communications. IARIA (pp. 14-19).
- **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, Xuan-Tu Tran, and Duy-Hieu Bui. "Low-cost Low-Power Implementation of Binary Edwards Curve for Secure Passive RFID Tags." In 2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), pp. 494-500. IEEE, 2023