INFORMATION OF THE DOCTORAL THESIS

Title of thesis:

Researching lightweight cryptography based on polynomial rings applied to devices with limited resources

Specified field of study: **Electrical Engineering**

Code of specialty: **9.52.02.03**

Name of PhD. candidate: **Hoang Manh Thang**

Scientific supervisors: **Prof. Dr. Nguyen Binh**

Academic institution: **Posts and Telecommunications Institute of Technology**

NEW FINDINGS OF THE THESIS

1. The CBC-QRHE cryptosystem has been constructed, utilizing residue quadratic residue residue of degree two and composite elements of even polynomial rings capable of resisting pre-chosen plaintext attacks (CPA). With its resistance against CPA, the CBC-QRHE system is considered to provide security assurance. Furthermore, from a theoretical standpoint, the decryption and encryption algorithms of the CBC-QRHE cryptographic system have a computational complexity of $O(n)$, and practically, the modules of the system have been implemented on resource-constrained devices, demonstrating greater efficiency than the original cryptographic system. Therefore, the CBC-QRHE system is deemed suitable for resource-constrained devices..
2. The OM-CA cryptosystem has been developed, employing the Omura-Massey system on a polynomial ring with two adjacent layers of Cyclic codes with reception capabilities. Although the OM-CA system has not yet been tested on actual devices, theoretically, both the decryption and encryption algorithms exhibit a computational complexity of $O(n)$, indicating the system's potential suitability for resource-constrained devices. Moreover, during the construction of the OM-CA system, the author proposed four additional methods to enhance the reception capabilities in polynomial ring-based cryptographic systems.
3. The OM-PI cryptosystem has been constructed, implementing the Omura-Massey system on a polynomial ring with two primitive root twin elements. Similar to the OM-CA system, OM-PI has not undergone testing on actual devices. However, in theoretical terms, the computational complexity of the OM-PI system is f $O(n)$, suggesting its suitability for resource-constrained devices. One of the significant outcomes achieved during the development of the OM-PI system was elucidating the isomorphic relationship between the polynomial ring with two primitive root twin elements and the finite field f $GF(p)$. This mathematical foundation forms the basis for constructing the OM-PI cryptographic system.

APPLICATIONS, PRACTICAL APPLICABILITY AND MATTES NEED FURTHER STUDIES

In terms of theory, the research methods employed in the dissertation can be applied to further explore and develop lightweight cryptographic systems in two approaches as follows: first, using polynomial rings to enhance existing cryptographic systems into lightweight ones; second, employing polynomial rings to construct new lightweight cryptographic systems. On the practical side, the three cryptographic systems in the dissertation need additional research steps to demonstrate performance, compatibility, and feasibility before being applied in real-world scenarios.

So, there are some open issues that require further investigation, as follows:

1. Expand and refine the theory regarding the application of polynomial rings in cryptography in general, and lightweight cryptography in particular. Specifically, explore the applications of primitive root twin polynomial rings in enhancing and constructing new lightweight cryptographic systems.
2. Implement and evaluate the CBC-QRHE, OM-CA, OM-PI cryptographic systems on commonly available resource-constrained devices in the market with diverse structures such as FPGA, ASIC.
3. Integrate the CBC-QRHE, OM-CA, OM-PI cryptographic systems into practical applications, ensuring secure information exchange functionality between IoT devices to guarantee data security in real-world scenarios.

Faculty of Electronic	**PhD. Candidate**
Deputy of responsible Faculty	
Dr. Nguyen Trung Hieu	**Hoang Manh Thang**