（別紙様式６）

専攻分野及び研究計画

Field of Study and Research Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name in full,  in your native language | พนาวัฒนกุล |  | ภาคิน |  |
| （姓名（自国語）） | , |
|  | (Surname) |  | (Given name) | (Middle name) |
| Name in Roman capital letters | PANAWATTANAKUL |  | PAKIN |  |
| (姓名（ローマ字）) | , |
|  | (Surname) |  | (Given name) | (Middle name) |
|  |  |  |  |  |
| Nationality | Thai | | | |
| （国　籍） |

Proposed study program in Japan (Outline your field of study on this side and the specific of your study program on the reverse side of this sheet. This section is one of the most important references for selection. The statement must be typewritten or written in block letters. Additional sheets of paper may be attached if necessary. If plagiarism or fraud is discovered after selection, the selection will be cancelled retroactively.)

（日本での研究計画；この研究計画は，選考の重要な参考となるので，表面に専攻分野の概要を，裏面に研究計画の詳細を具体に記入すること。記入はタイプ又は楷書によるものとし，必要な場合は別紙を追加してもよい。なお、採用後に不正、盗用等が判明した場合は遡って採用を取り消す。）

If you have Japanese language ability, write in Japanese. （相当の日本語能力を有する者は，日本語により記入すること｡）

　１　Present field of study（現在の専攻分野）

I am currently in my fourth year of studying Computer Engineering at Mahidol University International College. The curriculum provides a broad foundation in the computer field, covering programming, electronic circuits, networking, and computer system design. My academic interests focus on digital circuit design, computer architecture, operating systems, and FPGA design. I am also currently working on my senior project “Design and Evaluation of Cryptography Accelerator on FPGAs”, additionally I am going to work on this topic during internship at JAIST in the next January, which we aim to understand and successfully built a fast and resource efficient cryptography accelerator. This inspires me pursue research in FPGA design in my master’s degree.

　２　Your research topic in Japan: Describe articulately the research you wish to carry out in Japan.

（渡日後の研究テーマ：日本においてどういった研究がしたいかを明確に記入すること）

My research topic will focus on hardware acceleration of post-quantum cryptography on FPGAs. Currently, I am working on my senior project, which involves implementing a cryptographic accelerator on FPGA. Building on this experience, I aim to deepen my knowledge and focus on advanced algorithms such as post-quantum cryptography, for example, Kyber.

Through my research in Japan, I intend to design, implement, and evaluate FPGA-based accelerators for post-quantum key exchange mechanisms. The goal is to contribute to both theoretical understanding and practical applications, particularly in the field of secure embedded systems and future communication networks.

３　Study program in Japan: (Describe in detail and with specifics - particularly concerning the ultimate goal(s) of your research in Japan)

（研究計画：詳細かつ具体に記入し、特に研究の最終目標について具体的に記入すること。）

**FPGA-based Post-Quantum Cryptography Accelerator**

The inspiration of this study is the advancement of quantum computing in the past few years. Since quantum computers will be able to bypass current cryptography algorithms such as RSA and ECC, which rely on the hardness of the integer factorization problem, the discrete logarithm problem, or the elliptic-curve discrete logarithm problem, there is a growing concern for the security of modern communication systems. To address this, researchers are developing post-quantum cryptographic (PQC) algorithms that can resist attacks from quantum computers. The U.S. National Institute of Standards and Technology (NIST) has selected CRYSTAL-Kyber for key encapsulation as part of post-quantum cryptography standards.

At the same time, hardware acceleration has become increasingly important for cryptography, especially post-quantum cryptography, which requires complex computation such as polynomial multiplication and division. In embedded systems, or IoT devices, where computation resources are limited, pure software implementations often cannot meet the performance and energy efficiency requirements. Which leads to Field Programmable Gate Arrays (FPGAs), which are a suitable platform because of reconfigurability and the ability to achieve high throughput and low latency through parallelization.

My research at JAIST will focus on implementing an FPGA-based accelerator for CRYSTAL-Kyber on FPGA. There are 3 main aspects that need to be considered when designing an FPGA, including computation time, efficient use of FPGA resources, and power consumption. Achieving this requires careful consideration and deep understanding about both cryptography and FPGA design, which I plan to improve through the time at JAIST before finally implementing the accelerator on simulation and FPGA boards.

Regarding evaluation methods, to ensure that the accelerator can accurately encapsulate and decapsulate. The known answer vectors from NIST will be used to compare the input/output of the algorithms. On the other hand, the performance of the accelerator can be evaluated by comparing FPGA-based implementation against implementation on software or hybrid implementation, as well as comparing to other FPGA implementations by other researchers. Many of the evaluation matrixes can be obtained from simulations and fabrication processes on FPGA design suites such as Vivado.

I have planned my master’s study program at JAIST into eight phases.

1. Acquiring fundamental knowledge about FPGA which will be done in the first four months at JAIST
2. Conducting a literature review about post-quantum cryptography to get a better understanding of the algorithm and find suitable optimization methods.
3. There are several optimization techniques that can be used to speed up computation. In this phase I will study and choose suitable technique that can utilize FPGAs characteristic such as parallelization.
4. Start designing each module separately, and test for correctness and performance of each module
5. Integrate modules together creating working system including the process of designing control unit
6. Testing and evaluate of accelerator both on simulation result and FPGA board implementations
7. Finalize information and then writing research paper finishing master program

**Research timeline 2026 – 2028**



Finally, the ultimate goal of this research is to successfully build a fast, efficient, and scalable FPGA-based accelerator for post-quantum cryptography. Such an accelerator would contribute to secure deployment of PQC in embedded systems, IoT devices, and large-scale infrastructures, supporting the global transition to quantum-resistant security.