ĐẠI HỌC QUỐC GIA TP. HCM

**TRƯỜNG ĐẠI HỌC BÁCH KHOA**

--------------------

**NGUYỄN TUẤN HÙNG**

#### THIẾT KẾ BỘ XỬ LÝ NTT VÀ INTT CHO MÃ HOÁ LƯỢNG TỬ CRYSTALS-KYBER

Chuyên ngành : Điện Tử

Mã số:………………

**LUẬN VĂN THẠC SĨ**

TP. HỒ CHÍ MINH, tháng 01 năm 2022

CÔNG TRÌNH ĐƯỢC HOÀN THÀNH TẠI

TRƯỜNG ĐẠI HỌC BÁCH KHOA –ĐHQG -HCM

Cán bộ hướng dẫn khoa học :

(Ghi rõ họ, tên, học hàm, học vị và chữ ký)

Cán bộ chấm nhận xét 1 :

(Ghi rõ họ, tên, học hàm, học vị và chữ ký)

Cán bộ chấm nhận xét 2 :

(Ghi rõ họ, tên, học hàm, học vị và chữ ký)

Luận văn thạc sĩ được bảo vệ tại Trường Đại học Bách Khoa, ĐHQG Tp. HCM ngày . . . . . tháng . . . . năm . . . . .

Thành phần Hội đồng đánh giá luận văn thạc sĩ gồm:

(Ghi rõ họ, tên, học hàm, học vị của Hội đồng chấm bảo vệ luận văn thạc sĩ)

1.

2.

3.

4.

5.

Xác nhận của Chủ tịch Hội đồng đánh giá LV và Trưởng Khoa quản lý chuyên ngành sau khi luận văn đã được sửa chữa (nếu có).

**CHỦ TỊCH HỘI ĐỒNG TRƯỞNG KHOA**

**- Trang 3:** Tờ nhiệm vụ luận văn thạc sĩ

**- Trang 4:**  Lời cám ơn

**- Trang 5:** Tóm tắt luận văn thạc sĩ (Tiếng Việt và Tiếng Anh).

- **Trang 6**: Lời cam đoan của tác giả LV

**- Mục lục**

**- Toàn bộ nội dung luận văn (thực hiện theo đề cương đã bảo vệ)**

**- Tài liệu tham khảo**

**- Phụ lục** (nếu có)

**PHẦN LÝ LỊCH TRÍCH NGANG**

Họ và tên: Nguyễn Tuấn Hùng

Ngày, tháng, năm sinh: 11/06/1997 Nơi sinh: TP. Hồ Chí Minh

Địa chỉ liên lạc: 110/44/22 Tô Hiệu, P. Hiệp Tân, Q. Tân Phú, TP. HCM

##### QUÁ TRÌNH ĐÀO TẠO

2015 – 2019 :

##### QUÁ TRÌNH CÔNG TÁC

2018 – 2019:

***LỜI CẢM ƠN***

*Tp. Hồ Chí Minh, ngày 05 tháng 12 năm 2021.*

**Sinh viên**

**TÓM TẮT LUẬN VĂN**

Luận văn này trình bày về …

**MỤC LỤC**

[1. MỞ ĐẦU 1](#_Toc90907030)

[1.1 Lý do chọn đề tài 1](#_Toc90907031)

[1.2 Mục đích 1](#_Toc90907032)

[1.3 Đối tượng và phạm vi nghiên cứu 1](#_Toc90907033)

[1.4 Ý nghĩa khoa học và thực tiễn của đề tài nghiên cứu 1](#_Toc90907034)

[2. TỔNG QUAN 2](#_Toc90907035)

[2.1 Tình hình nghiên cứu trong và ngoài nước 2](#_Toc90907036)

[2.2 Nhiệm vụ đề tài 2](#_Toc90907037)

[3. NHỮNG NGHIÊN CỨU LÝ THUYẾT 2](#_Toc90907038)

[3.1 Lý thuyết về CRYSTALS-Kyber 2](#_Toc90907039)

[3.2 Lý thuyết về Number Theoretic Transform (NTT) 2](#_Toc90907040)

[3.3 Lý thuyết về phép toán rút gọn modulo Exact-KRED 2](#_Toc90907041)

[3.4 Lý thuyết về bộ nhớ BRAM M10K trên FPGA Cyclone V 2](#_Toc90907042)

[3.5 Xử lý tính toán lý thuyết trên phần mềm máy tính 2](#_Toc90907043)

[4. TRÌNH BÀY, ĐÁNH GIÁ VÀ BÀN LUẬN KẾT QUẢ 2](#_Toc90907044)

[4.1 Thiết kế phần cứng xử lý NTT và INTT cho CRYSTALS-Kyber 2](#_Toc90907045)

[4.2 Kết quả tổng hợp và mô phỏng 2](#_Toc90907046)

[4.3 Đánh giá, bàn luận và so sánh kết quả 2](#_Toc90907047)

[5. KẾT LUẬN VÀ KIẾN NGHỊ NHỮNG NGHIÊN CỨU TIẾP THEO 2](#_Toc90907048)

[5.1 Các hướng tối ưu thiết kế phần cứng xử lý NTT và INTT 2](#_Toc90907049)

[5.2 Thiết kế phần cứng xử lý CRYSTALS-Kyber 3](#_Toc90907050)

[5.3 Thiết kế lõi phần cứng xử lý bảo mật chung cho hệ thống 3](#_Toc90907051)

[6. DANH MỤC CÔNG TRÌNH CÔNG BỐ CỦA TÁC GIẢ 3](#_Toc90907052)

[7. DANH MỤC TÀI LIỆU THAM KHẢO 3](#_Toc90907053)

[8. PHỤ LỤC 5](#_Toc90907054)

[8.1 Các phần tối ưu cần lưu ý ở phần mềm Quartus 5](#_Toc90907055)

[8.2 Sơ đồ thiết kế chính theo Quartus 5](#_Toc90907056)

[8.3 Các phần thiết kế chính trên Verilog 5](#_Toc90907057)

[8.4 Các công thức Excel chính đã sử dụng 5](#_Toc90907058)

DANH SÁCH HÌNH MINH HỌA

[Hình 5‑1 Kết quả thi công 3](#_Toc310380287)

[Hình 5‑2 Kết quả mô phỏng 3](#_Toc310380288)

**DANH SÁCH BẢNG SỐ LIỆU**

[Bảng 1 Thông số hệ thống 3](#_Toc310380293)

# MỞ ĐẦU

## Lý do chọn đề tài

Tổ chức National Institute of Standards and Technology (NIST) đã tổ chức thực hiện quy trình chuẩn hoá mã hoá sau lượng tử (Post-Quantumn Cryptography hay PQC) hay mã hoá lượng tử từ 2016 [1].

NIST mô tả lý do thực hiện chuẩn hoá của họ là để tìm ra một loại mã hoá mới an toàn trước sự phát triển tương lai của máy tính lượng tử. Điều này dựa trên các nghiên cứu gần đây cho thấy mã hoá hiện đại (ECDSA, RSA, …) đang được sử dụng sẽ không còn an toàn trước máy tính lượng tử. Các thông tin đang được mã hoá sẽ không còn bí mật trong tương lai gần. Nhu cầu phát triển chuẩn mã hoá để sử dụng cho thời kỳ hậu lượng tử hoá là rất cấp thiết.

Cho đến vòng 3 của quy trình chuẩn hoá mã hoá lượng tử, có 5 ứng cử viên được lựa chọn cho vòng tiếp theo. Trong đó bao gồm 4 ứng cử viên thuộc dòng mã hoá lattice-based và 1 ứng cử viên thuộc dòng mã hoá code-based. Dòng mã hoá lattice-based đang chứng tỏ mình là một trong những dòng mã hoá của tương lai với khả năng bảo mật trước máy tính lượng tử và hiệu quả tính toán rất khả thi.

Trong 4 ứng cử viên mã hoá lattice-based, CRYSTALS-Kyber hay Kyber là ứng cử viên đầu tiên và được đánh giá rất triển vọng để được chuẩn hoá trong tương lai [2]. Kyber đòi hỏi nỗ lực tính toán nghiêm túc, chủ yếu là phép nhân các đa thức trên một vành đa thức có kích thước không đổi. Dạng mã hoá trên mạng mô-đun (module lattice) này mang lại sự cân bằng tốt giữa hiệu quả và bảo mật. Tuy nhiên, quá trình tạo, mã hóa và giải mã khóa có thể chiếm một tỷ lệ lớn trong khả năng tính toán và chu kỳ đồng hồ của bộ vi xử lý. Kyber sử dụng một kỹ thuật hỗ trợ tốc độ phép tinh nhân có tên là Number-Theoretic Transform (NTT) và chọn các tham số để hỗ trợ kỹ thuật này. Để triển khai Kyber một cách hiệu quả, việc tối ưu hóa NTT và NTT nghịch đảo (INTT) là rất quan trọng.

Nhiều nhà nghiên cứu triển khai mã hoá lattice-based trên phần mềm để chứng minh khái niệm cho nghiên cứu của họ và cũng một phần thể hiện tốc độ tính toán của giải thuật được nghiên cứu. Tuy vậy, khi có một dòng mã hoá được chuẩn hoá, các ứng dụng thực tế thường được tối ưu khi triển khai diện rộng bằng phần cứng. Tiêu biểu có thể kể đến AES-NI, RSA co-processor,…

## Mục đích

## Đối tượng và phạm vi nghiên cứu

Xem xét nghiên cứu nhiều

## Ý nghĩa khoa học và thực tiễn của đề tài nghiên cứu

Mô tả các nhiệm vụ của đề tài bao gồm yêu cầu, kết quả cần đạt và giới hạn đề tài. Trong từng nội dung sinh viên cũng cần trình bày thêm cách tiếp cận cũng như ý tưởng thực hiện.

(Ví dụ)

Nội dung 1: Tìm hiểu lý thuyết về …

Nội dung 2: Tìm hiểu về Kit …

Nội dung 3: Thiết kế bộ điều khiển … sử dụng giải thuật …

# TỔNG QUAN

# Tình hình nghiên cứu trong và ngoài nước

# Nhiệm vụ đề tài

# NHỮNG NGHIÊN CỨU LÝ THUYẾT

# Lý thuyết về CRYSTALS-Kyber

# Lý thuyết về Number Theoretic Transform (NTT)

# Lý thuyết về phép toán rút gọn modulo Exact-KRED

# Lý thuyết về bộ nhớ BRAM M10K trên FPGA Cyclone V

# Xử lý tính toán lý thuyết trên phần mềm máy tính

# TRÌNH BÀY, ĐÁNH GIÁ VÀ BÀN LUẬN KẾT QUẢ

# Thiết kế phần cứng xử lý NTT và INTT cho CRYSTALS-Kyber

# Kết quả tổng hợp và mô phỏng

# Đánh giá, bàn luận và so sánh kết quả

# KẾT LUẬN VÀ KIẾN NGHỊ NHỮNG NGHIÊN CỨU TIẾP THEO

# Các hướng tối ưu thiết kế phần cứng xử lý NTT và INTT

# Thiết kế phần cứng xử lý CRYSTALS-Kyber

# Thiết kế lõi phần cứng xử lý bảo mật chung cho hệ thống

# DANH MỤC CÔNG TRÌNH CÔNG BỐ CỦA TÁC GIẢ

TCAM, NTT

# DANH MỤC TÀI LIỆU THAM KHẢO

1. NIST, “Post-Quantum Cryptography Standardization”, csrc.nist.gov, https://csrc.nist.gov/Projects/post-quantum-cryptography.
2. Bos, Joppe, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé, "CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM." In 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 353-367. IEEE, 2018, doi: 10.1109/EuroSP.2018.00032.
3. Andrzejczak, Michal, Farnoud Farahmand, and Kris Gaj, "Full Hardware Implementation of the Post-Quantum Public-Key Cryptography Scheme Round5." In 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), pp. 1-2. IEEE, 2019, doi: 10.1109/ReConFig48160.2019.8994765.
4. Huang, Yiming, Miaoqing Huang, Zhongkui Lei, and Jiaxuan Wu, "A pure hardware implementation of crystals-kyber PQC algorithm through resource reuse." IEICE Electronics Express (2020) ID: 17-20200234, doi: 10.1587/elex.17.20200234.
5. Botros, Leon, Matthias J. Kannwischer, and Peter Schwabe, "Memory-efficient high-speed implementation of Kyber on Cortex-M4." In International Conference on Cryptology in Africa, pp. 209-228. Springer, Cham, 2019, doi: 10.1007/978-3-030-23696-0\_11.
6. Jati, Arpan, Naina Gupta, Anupam Chattopadhyay, and Somitra Kumar Sanadhya, "A Configurable Crystals-Kyber Hardware Implementation with Side-Channel Protection." Cryptology ePrint Archive (2021).
7. Zhao, Yixuan, Zhiteng Chao, Jing Ye, Wen Wang, Yuan Cao, Shuai Chen, Xiaowei Li, and Huawei Li, "Optimization Space Exploration of Hardware Design for CRYSTALS-KYBER." In 2020 IEEE 29th Asian Test Symposium (ATS), pp. 1-6. IEEE, 2020. doi: 10.1109/ATS49688.2020.9301498.
8. Albrecht, Martin R., Christian Hanser, Andrea Hoeller, Thomas Pöppelmann, Fernando Virdia, and Andreas Wallner, "Implementing RLWE-based schemes using an RSA co-processor." Cryptology ePrint Archive (2018).
9. Sanal, Pakize, Emrah Karagoz, Hwajeong Seo, Reza Azarderakhsh, and Mehran Mozaffari-Kermani. "Kyber on ARM64: Compact Implementations of Kyber on 64-bit ARM Cortex-A Processors." Cryptology ePrint Archive (2021).
10. Seo, Hwa-jeong, Hyeok-dong Kwon, Kyoung-bae Jang, and Hyunjun Kim, "Optimized implementation of scalable multi-precision multiplication method on RISC-V processor for high-speed computation of post-quantum cryptography." Journal of the Korea Institute of Information Security & Cryptology 31, no. 3 (2021): 473-480, doi: 10.13089/JKIISC.2021.31.3.473.
11. Xing, Yufei, and Shuguo Li, "A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 328-356, doi: 10.46586/tches.v2021.i2.328-356.
12. Guo, Wenbo, Shuguo Li, and Liang Kong, "An Efficient Implementation of KYBER." IEEE Transactions on Circuits and Systems II: Express Briefs (2021), doi: 10.1109/TCSII.2021.3103184.
13. Bisheh-Niasar, Mojtaba, Reza Azarderakhsh, and Mehran Mozaffari-Kermani, "High-Speed NTT-based Polynomial Multiplication Accelerator for CRYSTALS-Kyber Post-Quantum Cryptography." Cryptol. ePrint Arch., Tech. Rep 563 (2021): 2021.
14. Yarman, Ferhat, Ahmet Can Mert, Erdinç Öztürk, and Erkay Savaş, "A hardware accelerator for polynomial multiplication operation of CRYSTALS-KYBER PQC scheme." In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1020-1025. IEEE, 2021, doi: 10.23919/DATE51398.2021.9474139
15. Chen, Zhaohui, Yuan Ma, Tianyu Chen, Jingqiang Lin, and Jiwu Jing, "Towards efficient Kyber on FPGAs: A processor for vector of polynomials." In 2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 247-252. IEEE, 2020, doi: 10.1109/ASP-DAC47756.2020.9045459.
16. Zhang, Cong, Dongsheng Liu, Xingjie Liu, Xuecheng Zou, Guangda Niu, Bo Liu, and Quming Jiang, "Towards Efficient Hardware Implementation of NTT for Kyber on FPGAs." In 2021 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-5. IEEE, 2021, doi: 10.1109/ISCAS51556.2021.9401170.
17. Pöppelmann, Thomas, and Tim Güneysu, "Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware." In International conference on cryptology and information security in Latin America, pp. 139-158. Springer, Berlin, Heidelberg, 2012, doi: 10.1007/978-3-642-33481-8\_8
18. Langlois, Adeline, and Damien Stehlé, "Worst-case to average-case reductions for module lattices." Designs, Codes and Cryptography 75, no. 3 (2015): 565-599. Avanzi, Roberto, et al. "CRYSTALS-Kyber algorithm specifications and supporting documentation." *NIST PQC Round* 2.4 (2017), doi: 10.1007/s10623-014-9938-4
19. Avanzi, Roberto, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé, "CRYSTALS-Kyber algorithm specifications and supporting documentation." NIST PQC Round 2, no. 4 (2017).
20. Bisheh-Niasar, Mojtaba, Reza Azarderakhsh, and Mehran Mozaffari-Kermani, "A Monolithic Hardware Implementation of Kyber: Comparing Apples to Apples in PQC Candidates." In International Conference on Cryptology and Information Security in Latin America, pp. 108-126. Springer, Cham, 2021, doi: 10.1007/978-3-030-88238-9\_6.
21. Becker, Hanno, Vincent Hwang, Matthias J. Kannwischer, Bo-Yin Yang, and Shang-Yi Yang, "Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1." Cryptology ePrint Archive (2021).
22. Zhang, Neng, Bohan Yang, Chen Chen, Shouyi Yin, Shaojun Wei, and Leibo Liu, "Highly efficient architecture of NewHope-NIST on FPGA using low-complexity NTT/INTT." IACR Transactions on Cryptographic Hardware and Embedded Systems (2020): 49-72, doi: 10.13154/tches.v2020.i2.49-72.
23. Pöppelmann, Thomas, and Tim Güneysu, "Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware." In International conference on cryptology and information security in Latin America, pp. 139-158. Springer, Berlin, Heidelberg, 2012, doi: 10.1007/978-3-642-33481-8\_8.
24. Longa, Patrick, and Michael Naehrig, "Speeding up the number theoretic transform for faster ideal lattice-based cryptography." In International Conference on Cryptology and Network Security, pp. 124-139. Springer, Cham, 2016, doi: 10.1007/978-3-319-48965-0\_8.
25. Intel, "Cyclone V Device Datasheet," CV-51002 datasheet, Nov. 2019.
26. Nguyen, Duc Tri, Viet B. Dang, and Kris Gaj. "High-Level Synthesis in Implementing and Benchmarking Number Theoretic Transform in Lattice-Based Post-Quantum Cryptography Using Software/Hardware Codesign." In ARC, pp. 247-257. 2020. doi: 10.1007/978-3-030-44534-8\_19.

# PHỤ LỤC

# Các phần tối ưu cần lưu ý ở phần mềm Quartus

# Sơ đồ thiết kế chính theo Quartus

# Các phần thiết kế chính trên Verilog

# Các công thức Excel chính đã sử dụng