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]. Đây là dạng mã hóa mới nhằm thay thế các dạng mã hóa bất đối xứng hiện tại.

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 bất đối xứng 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 lưới (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 [3], RSA/ECC co-processor [4],… Nhiều nghiên cứu về mã hóa lượng tử gần đây cũng được thực hiện trên ASIC, FPGA dưới dạng độc lập hoặc làm bộ xử lý phụ cho các CPU RISC V, ARM, x86,… Trong đó, các chip FPGA là nền tảng tốt để phát triển các nghiên cứu lý thuyết và đánh giá sức mạnh giải thuật.

Để thiết kế phần cứng trên FPGA, ngôn ngữ mô tả phần cứng được sử dụng rất phổ biến. Đây là phương pháp thiết kế mạch kỹ thuật số chính xác, giúp người thiết kế có được phần lớn quyền quyết định các kết quả thiết kế với công cụ từ các nhà phát triển FPGA như Intel hay Xillinx.

Trên đây là tổng quan về các lý do để học viên thực hiện đề tài nghiên cứu thiết kế phần cứng xử lý NTT và INTT trên nền tảng FPGA, bằng ngôn ngữ Verilog, cho mã hóa lượng tử CRYSTALS-Kyber.

## Mục đích

Mục đích nghiên cứu là xây dựng phần cứng xử lý NTT và INTT trên nền tảng FPGA, bằng ngôn ngữ Verilog, cho mã hóa lượng tử CRYSTALS-Kyber. Qua đó, đánh giá và bàn luận các kết quả cũng như bàn luận về các hướng nghiên cứu chuyên sâu để ứng dụng mã hóa lượng tử trên phần cứng.

## Đối tượng và phạm vi nghiên cứu

## Đối tượng nghiên cứu

Đối tượng nghiên cứu của luận văn là thuật toán NTT và INTT với các thông số phù hợp với mã hóa lượng tử CRYSTALS-Kyber, sử dụng ngôn ngữ mô tả phần cứng Verilog và đánh giá trên nền tảng FPGA.

## Phạm vi nghiên cứu

Phạm vi nghiên cứu của luận văn là thuật toán NTT và INTT với các thông số phù hợp với mã hóa lượng tử CRYSTALS-Kyber, tập trung chủ yếu vào việc tối ưu cách áp dụng NTT và INTT trên phần cứng qua ngôn ngữ mô tả phần cứng.

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

## Ý nghĩa khoa học

Đề tài đóng góp về ý nghĩa khoa học trong việc nghiên cứu cách ứng dụng hiệu quả của dạng mã hóa lượng tử lattice-based, vốn đang còn rất mới và vẫn đang được chuẩn hóa.

## Ý nghĩa thực tiễn

Đề tài đóng góp về ý nghĩa thực tiễn trong quá trình chuẩn hóa mã hóa lượng tử để bảo mật thông tin kỹ thuật số trong tương lai. Ngoài ra, đề tài còn giúp đánh giá mức độ khả thi trong việc ứng dụng của mã hóa CRYSTALS-Kyber trên các thiết bị điện tử sau này. Ứng dụng này có thể dưới dạng tích hợp như một phần của vi xử lý chính của các thiết bị đó hoặc dưới dạng một dạng vi xử lý phụ độc lập.

# TỔNG QUAN

## Tình hình nghiên cứu trong và ngoài nước

## Tình hình nghiên cứu ngoài nước

Trong các nghiên cứu trước đây, một trong những triển khai phần cứng hoàn toàn sớm nhất của mã hóa lượng tử [5] là dành cho một dạng mã hóa lượng tử lattice-based có tên Round5. Nghiên cứu này bao gồm thiết kế phần cứng của hàm băm SHA-3 Keccak, AES-GCM và thuật toán Round5. Sự đơn giản từ lợi thế của mô-đun Round5 được sử dụng hiệu quả trên phần cứng, cho thấy tương lai của việc ứng dụng mã hóa lượng tử trên phần cứng. Một phần để tiếp nối việc xử lý mã hóa trên phần cứng như trước đây với mã hóa hiện đại, một phần để giảm tải yêu cầu về tài nguyên xử lý cho các vi xử lý tác vụ chính.

Nghiên cứu [6] trình bày một thiết kế phần cứng đầy đủ tương tự của CRYSTALS-Kyber, giúp tăng tốc hiệu suất 129 lần so với việc triển khai bộ xử lý Cortex-M4 [7]. Trong [8], Jati và cộng sự trình bày thiết kế chống tấn công kênh ngoại (side-channel attack) đầu tiên của CRYSTALS-Kyber trên phần cứng với hiệu suất ấn tượng.

Zhao và cộng sự [9] phân tích mã phần mềm để tối ưu hóa thiết kế của chúng, mang lại kết quả tích cực. Các cách triển khai khác của Kyber khác nhau, từ bộ xử lý lai giữa phần cứng và phần mềm [10] [11] [12] đến phần cứng thuần túy [7] [8] [13] [14]. Các nghiên cứu gần đây về triển khai phần cứng CRYSTALS-Kyber hầu hết tối ưu hóa quá trình xử lý giải thuật NTT và INTT, do các phần còn lại của Kyber đều dựa trên mã hóa hiện đại thuần túy có thể tái sử dụng từ các nghiên cứu trước.

Trong các nghiên cứu đó, nhiều hướng tối ưu khác nhau được trình bày. Nghiên cứu [15] trình bày một kỹ thuật tính số dư modulo mới được gọi là K2-RED cho cấu trúc NTT của họ, giúp cải thiện hiệu suất đáng kể so với cách tính số dư bằng kỹ thuật Barret hay Montgomery. Một kỹ thuật tính số dư modulo khác được sử dụng trong [16], [17] được sửa đổi với các hằng số được tính toán trước.

Zhang và cộng sự [18] trình bày sơ đồ truy cập bộ nhớ kiểu ping-pong để truy cập RAM hiệu quả. Đây cũng là một hướng tối ưu ứng dụng phần cứng của mã hóa lượng tử, giải tắc nghẽn ở phần truy cập bộ nhớ. Bên cạnh đó, Poppelmann và cộng sự [19] giới thiệu cấu trúc chủ-tớ cho nhiều bộ nhân đa thức kết hợp xử lý tính toán cho các phần cần sức mạnh xử lý tính toán lớn.

# Tình hình nghiên cứu trong nước

Nghiên cứu về mã hóa lượng tử trong nước chưa có nhiều trong thời gian này. Tuy vậy, các nghiên cứu về phần cứng ứng dụng trên công nghệ FPGA và các nghiên cứu về thuật toán Fast Fourier Tranform đã phát triển từ nhiều năm trở lại đây.

Nghiên cứu [20] thiết kế hệ thống tính toán Fast Fourier Transform (FFT) 2048 điểm xây dựng trên nền tảng FPGA. Nghiên cứu phù hợp để tham khảo về FFT và cách thực hiện phép nhân hiệu quả trên FPGA. Nghiên cứu [21] cũng sử dụng bộ nhân CORDIC tương tự [20] để tính toán FFT, cấu trúc bộ nhân sử dụng thanh ghi dịch (bộ nhân xoay góc thích nghi) cũng là một hướng tối ưu để tham khảo. Nghiên cứu [22] thể hiện một ứng dụng thực tiễn của việc sử dụng biến đổi Fourier nhanh (FFT). Biến đổi Fourier là một giải thuật quan trọng sử dụng trong nhiều mặt của đời sống, trong xử lý tín hiệu, hình ảnh, … và giờ đây được ứng dụng trong mã hóa lượng tử.

# Nhiệm vụ đề tài

Nhiệm vụ đề tài bao gồm các mục được sau đây, nhằm để thực hiện mục đích đề tài đã đề ra, kết quả cần đạt và giới hạn đề tài. Qua đó trình bày các kết quả nghiên cứu đã được thực hiện.

Nội dung 1: Tìm hiểu lý thuyết mã hóa bất đối xứng, mã hóa lượng tử, NTT, các thành phần toán học cần thiết để thiết kế phần cứng.

Nội dung 2: Xây dựng thiết kế phần cứng xử lý NTT và INTT cho mã hóa lượng tử CRYSTALS-Kyber, tổng hợp thiết kế và mô phỏng kiểm tra.

Nội dung 3: Đánh giá, bàn luận về thiết kế. So sánh kết quả đạt được với các nghiên cứu trước.

Nội dung 4: Bàn luận về hướng phát triển tương lai và kết luận cho nghiên cứu.

Trong đó, phần tiếp theo của luận văn sẽ thể hiện nội dung 1. Phần 4 của luận văn trình bày các phần được nêu trong nội dung 2. Ở phần 4 của luận văn, học viên trình bày nội dung 3. Học viên thực hiện kết luận và bàn luận hướng phát triển theo nội dung 4 ở phần 5 của luận văn. Phần 6 là danh mục các công trình nghiên cứu của học viên. Phần 7 là danh mục tài liệu tham khảo. Phần 8 là phụ lục, gồm các ghi chú về từ ngữ sử dụng trong luận văn và các thông tin thêm.

# NHỮNG NGHIÊN CỨU LÝ THUYẾT

Trong phần này, học viên trình bày các nghiên cứu lý thuyết có liên quan đến đề tài. Qua đó lựa chọn các nền tảng lý thuyết cần để xây dựng phần cứng. Các nghiên cứu lý thuyết đi từ mã hóa bất đối xứng, mã hóa lượng tử CRYSTALS-Kyber, Number Theoretic Transform (NTT) đến các giải thuật chuyên sâu để tối ưu trên phần cứng tốt hơn.

# Lý thuyết về mã hóa bất đối xứng

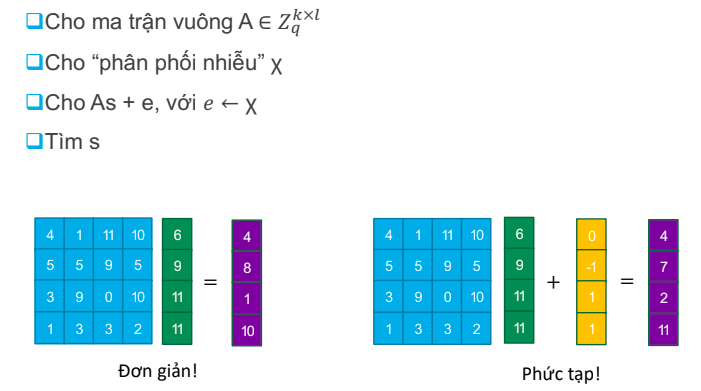
Mã hóa bất đối xứng là dạng mã hóa gồm 2 chìa khóa mã: chìa khóa công khai mà chìa khóa bí mật. Chìa khóa bí mật có thể dùng để mã hóa một văn bản mà chỉ chìa khóa công khai mới xác nhận và giải mã được hoặc một cơ chế tương tự ngược lại. Mã hóa bất đối xứng thường dựa trên một vấn đề toán học phức tạp chỉ có thể giải được một chiều. Có thể lấy ví dụ từ mã hóa RSA dựa trên độ phức tạp của việc phân tích kết quả mã hóa công khai (vốn là một hằng số mũ với chìa khóa bí mật) ra các thừa số để tìm chìa khóa bí mật, độ phức tạp của phép toán logarit. Thông số của các giao tiếp sử dụng mã hóa RSA hiện tại đang ở mức 4096-bit [23]. Bên cạnh đó còn có mã hóa ECDSA, sử dụng độ phức tạp của phép toán logarit rời rạc và ở một mức độ bảo mật cao hơn RSA, tốn ít băng thông hơn [24]. Đây đều là cơ sở để đề ra các giao thức trao đổi khóa, hình thành mã hóa bất đối xứng.

Cả hai dạng mã hóa bất đối xứng nêu trên đều đang có tính bảo mật cao ở thời điểm hiện tại. Đa số các vụ tấn công trên các dạng mã hóa này đều là tấn công lý thuyết. Tuy vậy, để an toàn trước máy tính lượng tử, NIST bắt đầu chuẩn hóa mã hóa lượng tử từ 2016 [1]. Trong các dạng mã hóa đang được chuẩn hóa, CRYSTALS-Kyber có thể là ứng cử viên được dùng để thay thế mã hóa bất đối xứng trong tương lai.

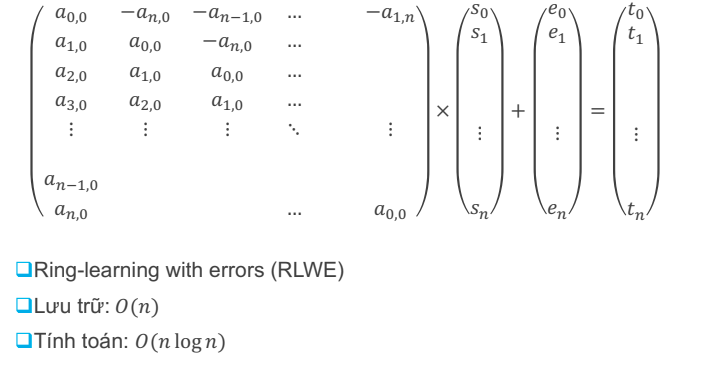
# Lý thuyết về CRYSTALS-Kyber

Lý thuyết về CRYSTALS-Kyber chủ yếu được trình bày bởi tác giả Bos và cộng sự tại [2] và tại trang web của CRYSTALS-Kyber cho những phiên bản mới nhất. Bởi vì CRYSTALS-Kyber là kiểu mã hóa lượng tử chưa chuẩn hóa và vẫn đang cập nhật liên tục. Phiên bản CRYSTALS-Kyber được lựa chọn trong nghiên cứu là phiên bản 3 [2].

CRYSTALS-Kyber là mô hình mật mã dựa trên bài toán Module Learning With Errors (MLWE [24]). Chi tiết về Kyber có thể được tìm thấy trong thông số kỹ thuật cập nhật của nó [24]. Kyber có hai phần: mã hóa công khai chống được phương pháp tấn công chọn văn bản hoặc CPAPKE, cơ chế đóng gói khóa bảo mật hoặc CCAKEM. CPAPKE được bao gồm trong CCAKEM như một bước bắt buộc để tạo mã khóa và mã hóa cũng như giải mã. Trong khi CPAPKE có ba bước khác nhau (tạo khóa, mã hóa và giải mã), cả ba bước đều yêu cầu một bước nhân đa thức lớn có độ phức tạp . Về bản chất, CRYSTALS-Kyber hiểu đơn giản là mã hóa bất đối xứng, bao gồm một phép toán có độ phức tạp lớn (MLWE) và giao thức trao đổi kết quả từ phép toán đó. Hình 1 trình bày độ phức tạp của phép toán trên lưới đã được đơn giản hóa.

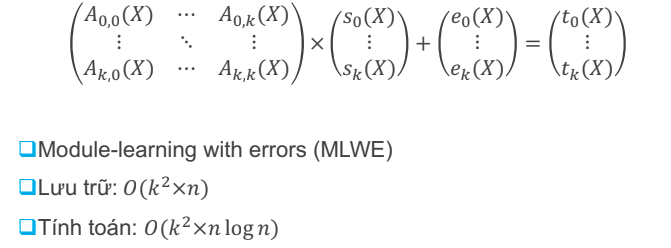


Hình 1 Kyber dựa trên độ phức tạp của phép tính lattice-based (đã đơn giản hóa)



Hình 2 Ring-Learning with errors, tiền đề của MLWE

Hình 2 thể hiện Ring-Learning with errors (RLWE), một cách để giảm lưu trữ phần tử ma trận A. Đây là tiền đề của MLWE của Kyber. Hình 3 là dạng Module-learning with errors mà Kyber sử dụng. Kyber dùng thông số k để nâng độ phức tạp của ma trận A, tăng tính linh hoạt cho giải thuật.



Hình 3 Module-learning with errors (MLWE) được Kyber sử dụng

Cơ chế giao tiếp, đóng gói và chuyển đổi từ văn bản gốc *m* sang văn bản đã được mã hóa *c* cũng được thể hiện trong hình 4. Với Alice và Bob là hai đầu thực hiện giao tiếp mã hóa Kyber. Alice tạo

Một cách rất hiệu quả để xử lý các phép nhân đa thức là Biến đổi lý thuyết số (NTT). Vì lý do đó, NTT được bao gồm trong định nghĩa của Kyber, và các thông số của các phiên bản Kyber được tinh chỉnh để được tính toán hiệu quả với NTT. Bảng 1 thể hiện thông số của từng phiên bản 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. Intel, “Intel® Data Protection Technology with AES-NI and Secure Key”, <https://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard-aes/data-protection-aes-general-technology.html>
4. Eberle, Hans, Nils Gura, Sheueling Chang Shantz, Vipul Gupta, Leonard Rarick, and Shreyas Sundaram. "A public-key cryptographic processor for RSA and ECC." In Proceedings. 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2004., pp. 98-110. IEEE, 2004, doi: [10.1109/ASAP.2004.1342462](https://doi.org/10.1109/ASAP.2004.1342462)
5. 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.
6. 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.
7. 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.
8. Jati, Arpan, Naina Gupta, Anupam Chattopadhyay, and Somitra Kumar Sanadhya, "A Configurable Crystals-Kyber Hardware Implementation with Side-Channel Protection." Cryptology ePrint Archive (2021).
9. 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.
10. 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).
11. 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).
12. 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.
13. 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.
14. 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.
15. 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.
16. 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
17. 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.
18. 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.
19. 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
20. Linh, Đàm & Hoang, Trong-Thuc & Tú, Bùi & Vũ, Đinh. (2014). “Hiện thực và so sánh các thiết kế FFT 2048 điểm xây dựng trên nền tảng FPGA.”
21. Trương Thị Như Quỳnh, Võ Thị Phương Thảo, Hoàng Trọng Thức & Lê Đức Hùng. (2017). “Thiết kế FFT 2048-điểm trên FPGA dựa trên thuật toán CORDIC xoay góc thích nghi với độ chính xác dấu chấm động đơn”
22. Phạm Ngọc Bách, Nguyễn Văn Hiệp. (2018). “Sử dụng biến đổi nhanh fourier (FFT) nghiên cứu cấu trúc bão và sự phát triển xoáy bão trong sơ đồ ban đầu hóa xoáy động lực “
23. RSA (cryptosystem) - <https://en.wikipedia.org/wiki/RSA_(cryptosystem)>
24. Elliptic Curve Digital Signature Algorithm - https://en.wikipedia.org/wiki/Elliptic\_Curve\_Digital\_Signature\_Algorithm
25. 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
26. 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).
27. 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.
28. 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).
29. 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.
30. 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.
31. 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.
32. Intel, "Cyclone V Device Datasheet," CV-51002 datasheet, Nov. 2019.
33. 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

# Các định nghĩa được sử dụng