ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

KHIT BOUNSAVENG

NGHIÊN CỨU CÁC LƯỢC ĐỒ CHỮ KÍ SỐ LƯỢNG TỬ DỰA TRÊN HÀM BĂM

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên – 2023

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

KHIT BOUNSAVENG

NGHIÊN CỨU CÁC LƯỢC ĐỒ CHỮ KÍ SỐ LƯỢNG TỬ DỰA TRÊN HÀM BĂM

NGÀNH KHOA HỌC MÁY TÍNH
Mã số: 8480101

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: TS. Đỗ Thị Bắc

Thái Nguyên – 2023

LỜI CAM ĐOAN

Tên tôi là Khit BOUNSAVENG, học viên lớp cao học K20 – Khoa học máy tính – Trường đại học Công nghệ thông tin và Truyền thông Thái Nguyên. Tôi xin cam đoan đề tài "Nghiên cứu các lược đồ chữ kí số lượng tử dựa trên hàm băm" do cô giáo TS. Đỗ Thị Bắc hướng dẫn, là công trình nghiên cứu do bản thân tôi thực hiện, dựa trên sự hướng dẫn của cô giáo hướng dẫn khoa học và các tài liệu tham khảo đã trích dẫn.

Tôi xin chịu trách nhiệm với lời cam đoan của mình.

Thái Nguyên, năm 2023

Học viên

KHIT BOUNSAVENG

LỜI CẢM ƠN

Để hoàn thành luận văn này, trong suốt quá trình thực hiện đề tài nghiên cứu, tôi luôn nhận được sự quan tâm giúp đỡ của: Cô giáo hướng dẫn trực tiếp TS. Đỗ Thị Bắc, đã giúp đỡ tận tình về phương hướng và phương pháp nghiên cứu cũng như hoàn thiện luận văn.

Các thầy, cô giáo trong khoa Công nghệ thông tin, Trường đại học Công nghệ thông tin và Truyền thông – Đại học Thái Nguyên đã tạo điều kiện về thời gian, địa điểm nghiên cứu, phương tiện vật chất cho tác giả.

Tôi xin bày tỏ lời cảm ơn chân thành đến tất cả những sự giúp đỡ quý báu đó.

Thái Nguyên, năm 2023

Học viên

KHIT BOUNSAVENG

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CẢM ƠN ii
MỤC LỤC iii
DANH MỤC CÁC BẢNG BIỂU v
DANH MỤC CÁC HÌNH VẼ vi
DANH MỤC CÁC CHỮ VIẾT TẮT vii
MỞ ĐẦU 1
CHƯƠNG 1. TỔNG QUAN VỀ VỀ MÁY TÍNH LƯỢNG TỬ VÀ SỰ PHÁT TRIỂN CỦA CÁC LƯỢC ĐỒ CHỮ KÍ SỐ KHÁNG LƯỢNG TỬ DỰA TRÊN HÀM BĂM 3
1.1. Tổng quan về máy tính lượng tử 3
1.1.1. Sự ra đời của máy tính lượng tử 3
1.1.2. Tiến trình phát triển của MTLT 4
1.1.3. Các thành tựu đáng chú ý của các công ty và tập đoàn 5
1.1.4. So sánh giữa MTLT và MTTT 5
1.1.5. Các nguyên tắc hoạt động của MTLT 7
1.1.6. Các thành phần cấu tạo của MTLT 7
1.1.7 Ứng dụng của MTLT 8
1.1.8. Ưu điểm và nhược điểm của máy tính lượng tử 10
1.1.9. Những khó khăn và hướng phát triển của máy tính lượng tử 10
1.2. Giới thiệu tổng quan về chữ ký số 11
1.2.1. Các khái niệm và định nghĩa 12
1.2.2. Các mức độ tấn công và các khả năng thành công 13
1.2.3. Khái niệm về độ an toàn của lược đồ ký điện tử và ROM 14
1.2.4. Chứng minh quyền sở hữu khóa bí mật 15
1.2.5. Chữ ký số dựa trên hàm băm 15
1.3. Tiểu kết chương 1 18
CHƯƠNG 2. CÁC LƯỢC ĐỒ CHỮ KÍ SỐ LƯỢNG TỬ DỰA TRÊN HÀM BĂM 19
2.1. Khái quát về sự phát triển chữ ký số lượng tử dựa trên hàm băm 19
2.2. Mô hình hoạt động của các lược đồ chữ ký số dựa trên hàm băm 27
2.2.1. Lược đồ chữ kí số Lamport 27

2.2.2. Lược đồ chữ ký số Merkle 28
2.2.3. Lược đồ chữ ký số HORS 30
2.2.4. Lược đồ chữ ký số SPHINCS+: 32
2.2.5. Lược đồ chữ ký số Picnic 34
2.3. Tiểu kết chương 2 35
CHƯƠNG 3. XÂY DỰNG PHƯƠNG ÁN VÀ KẾT QUẢ ĐÁNH GIÁ 36
3.1. Dự án án tiêu chuẩn hóa mật mã hậu lượng tử của NIST 36
3.2. Lựa chọn thuật toán 37
3.3. Phương án tiếp cận việc đánh giá và so sánh 39
3.3.1. Độ phức tạp thuật toán 39
3.3.2. Hiệu suất và độ tin cậy 39
3.3.3. Thực thi trên cùng phần mềm, phần cứng 40
3.4. Phân tích những hạn chế của các thuật toán và đề xuất các giải pháp để cải thiện hiệu quả và khả năng ứng dụng của chúng 41
3.5. Đánh giá khả năng ứng dụng của các thuật toán chữ ký số kháng lượng tử dựa trên hàm băm 42
3.6. Tiểu kết chương 3 42
KẾT LUẬN 44
TÀI LIỆU THAM KHẢO 46
PHỤ LỤC 48

DANH MỤC CÁC BẢNG BIỂU

Bảng 1.1: So sánh sự khác biệt giữa MTLT và MTTT 6
Bảng 1.2: So sánh các lược đồ chữ ký dựa trên hàm băm với các chuẩn chữ ký số hiện tại (kích thước được tính theo byte) 18
Bảng 3.1: Tổng hợp độ phúc tạp tính toán của các thuật toán. 39
Bảng 3.2: Tổng hợp thông số về hiệu suất và độ tin cậy của các thuật toán. 40
Bảng 3.3: Tổng hợp số phép tính của các thuật toán trong các phương án đề xuất. 40

DANH MỤC CÁC HÌNH VẼ

Hình 1.1: Máy tính lượng tử.....4
Hình 1.2: So sánh sự khác biệt giữa MTLT và MTTT 6
Hình 2.1: Một cây Merkle với 23 cặp khóa.....21
Hình 2.2: Ví dụ về đường dẫn xác thực cây Merkle. 23
Hình 2.3: Minh họa về sự khác biệt giữa MSS (ở bên trái) và SPR-MSS (ở bên.....25
phải, trong đó H là hàm băm có khóa, k là khóa và mặt nạ bit v 0 và v1).....25
Hình 2.4: Lược đồ chữ ký của Lamport. Ở đây, m = 1011 được sử dụng như một thông
điệp ví dụ và các nút màu xám chỉ ra những bí mật được tiết lộ. 28
Hình 2.5: Minh họa cây băm nhị phân với p = 16.....28
Hình 2.6: Cấu trúc của lược đồ chữ ký số nhiều lần SPHINCS.....33
Hình 3.1: Sơ đồ dòng thời gian PQC của dự án NIST. 37

DANH MỤC CÁC CHỮ VIẾT TẮT

Chữ viết tắt	Chữ đầy đủ
API	Application Programming Interface
DNA	Deoxyribonucleic acid
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMSS	Emergency Medical Services System
HORST	Hierarchical Off-line Recomputable Signature Trees
IBM	International Business Machines
MTLT	Máy Tính Lượng Tử
MTT	Máy Tính Truyền Thông
MD5	Message Digest Algorithm 5
MSS	Managed Security Services
NIST	National Institute of Standards and Technology
NIST PQC	Elliptic Curve Digital Signature Algorithm
OTS	One-Time Signature
OPS	Operations Per Second
PRF	Pseudorandom Function
QKD	Quantum Key Distribution
RSA	Rivest Shamir Adleman
RFC	Request for Comments
ROM	Read-Only Memory
SHA	Secure Hash Algorithm
SPHINS	Post-Quantum Cryptographic Signature Scheme
SPR-MSS	Signature-Based Packet Routing with Multiple Sinks
WOTS	Winternitz One-Time Signature
XMSS	eXtended Merkle Signature Scheme

MỞ ĐẦU

Trong các năm gần đây, với sự phát triển của máy tính lượng tử, các phương pháp truyền thống trong việc bảo mật thông tin như thuật toán chữ ký số dựa trên RSA hay ECC đang dần trở nên không an toàn và cần được thay thế bằng các giải pháp mới khác [1-5]. Một trong những giải pháp đó là sử dụng các thuật toán chữ ký số kháng lượng tử (hậu lượng tử) dựa trên hàm băm [6-10].

Các thuật toán chữ ký số kháng lượng tử dựa trên hàm băm đã được đề xuất từ khá lâu và được chứng minh đạt được độ bảo mật tốt hơn so với các thuật toán chữ ký số truyền thống [1, 10-16]. Các thuật toán chữ ký số này được phát triển dựa trên kỹ thuật chữ ký số một lần và sử dụng hàm băm để tạo ra khóa [7-9, 17-19].

Đến năm 2016, Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ (National Institute of Standards and Technology - NIST) đã kêu gọi các cá nhân và các tổ chức đề xuất thuật toán được cho là có khả năng kháng lượng tử với thời hạn một năm đến tháng 11 năm 2017 [21]. Tháng 1 năm 2018, NIST đã công bố kết quả của vòng đầu tiên. Đã có 82 thuật toán được đề xuất (gồm cả mã hóa, trao đổi khóa và chữ ký số). Trong đó 23 trong số chúng là các lược đồ chữ ký và chỉ 4 là các lược đồ chữ ký dựa trên hàm băm (nhưng chỉ có 2 trong số đó được xuất bản). Vào tháng 4 năm 2018, NIST đã tổ chức một hội thảo, nơi người đề xuất trình bày các giải pháp của họ. Tiếp theo là giai đoạn phân tích từ 3 đến 5 năm với báo cáo về các đánh giá. Dự kiến, từ năm 2023 đến năm 2025, một bản thảo chuẩn hóa cho mật mã hậu lượng tử [21] sẽ sẵn sàng. NIST nhấn mạnh rằng đây không phải là một cuộc thi và một số ứng viên có thể được chấp thuận cho một ứng dụng/mục đích duy nhất.

Mật mã hậu lượng tử là một lĩnh vực khoa học còn rất mới và là không gian mở đối với các nhà khoa học trên cả thế giới và ở Việt Nam. Hiện tại máy tính lượng tử chưa được sử dụng phổ biến mới chỉ được nghiên cứu và sử dụng trong các phòng thí nghiệm của các tập đoàn lớn trên thế giới nên việc nghiên cứu về mật mã kháng lượng tử hay nhỏ hơn là chữ ký số kháng lượng tử là rất thời sự và cấp thiết.

Trong luận văn này, sẽ giới thiệu về các thuật toán chữ ký số kháng lượng tử dựa trên hàm băm, bao gồm các thuật toán chính như Lamport, Merkle, HORS, Picnic và SPHINCS+ [21]. Đây là các thuật toán được đánh giá cao về khả năng ứng dụng và trong đó có các thuật toán lọt vào vòng 2 hoặc vòng 3 của cuộc thi tìm chuẩn mã hóa do NIST tổ chức đã nêu trên và sẽ trình bày về cấu trúc, cách thức hoạt động của từng