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

PHONEKEOPASERTH SOULIVONG

NGHIÊN CỨU VỀ MẬT MÃ HẬU LƯỢNG TỬ

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

PHONEKEOPASERTH SOULIVONG

NGHIÊN CỨU VỀ MẬT MÃ HẬU LƯỢNG TỬ

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

Tôi xin cam đoan luận văn này do chính tôi thực hiện, dưới sự hướng dẫn của TS. Đỗ Thị Bắc. Các kết quả lý thuyết được trình bày trong luận văn là sự tổng hợp từ các kết quả đã được công bố và có trích dẫn đầy đủ, kết quả của chương trình thực nghiệm trong luận văn này được tác giả thực hiện là hoàn toàn trung thực, nếu sai tôi hoàn toàn chịu trách nhiệm.

Thái Nguyên, tháng 8 năm 2023

Học viên

Phonekeopaserth Soulivong

LỜI CẢM ƠN

Lời đầu tiên tôi xin gửi lời cảm ơn sâu sắc tới cô giáo hướng dẫn TS. Đỗ Thị Bắc. Cô đã giao đề tài và tận tình hướng dẫn tôi trong quá trình hoàn thành đề tài luận văn này.

Tôi xin trân trọng cảm ơn Trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên, các thầy cô giáo trong khoa Công nghệ thông tin đã giảng dạy và giúp đỡ tôi trong suốt quá trình học tập tại trường.

Xin chân thành cảm ơn các bạn cùng lớp CH K20A đã đồng hành giúp đỡ tôi trong quá trình học tập.

Cảm ơn gia đình đã hỗ trợ, đồng hành bên tôi trong thời gian tôi đi học để tôi yên tâm học tập nghiên cứu.

Cảm ơn các bạn Việt Nam đã giúp đỡ tôi khi ở đất nước các bạn.

Thái Nguyên, tháng 8 năm 2023

Học viên

Phonekeopaserth Soulivong

MỤC LỤC

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC CHỮ VIẾT TẮT

Chữ viết tắt	Chữ đầy đủ
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AI	Artificial intelligence
AT&T Bell	Bell Telephone Company
BCH	Bitcoin Cash
DES	Data Encryption Standard
DNA	Deoxyribonucleic acid
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ETSI	European Telecommunications Standards Institute
IBM	International Business Machines
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
IoT	Internet of things
MTLT	Máy tính lượng tử (Quantum Computer)
MTTT	Máy tính truyền thống (Classical Computer)
NIST	National Institute of Standards and Technology
NISQ	Noisy Intermediate Scale Quantum
NMR	Nuclear magnetic resonance spectroscopy
NSA	National Security Agency
PQC	Mật mã hậu lượng tử (Post-quantum cryptography)
QCS	Chuẩn hóa mật mã hậu lượng tử (Quantum Crypto-Standard)
RFCs	Request for Comments
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
TLS	Transport Layer Security

MỞ ĐẦU

1. Đặt vấn đề

Ngày nay, máy tính lượng tử (MTLT) và mật mã hậu lượng tử (PQC) đang có vai trò quan trọng và dần đi sâu vào hầu hết các lĩnh vực, ngành nghề khác nhau trong cuộc sống và được sử dụng trong nhiều mục đích: Bảo mật dữ liệu, đảm bảo ẩn danh, đảm bảo tính xác thực của thông tin...[1]-[7]. Một số ví dụ về việc sử dụng mật mã hằng ngày là thương mại điện tử, Chính phủ điện tử, ngân hàng điện tử, thẻ ATM, mật khẩu máy tính, internet [8]-[10]. MTLT hoạt động theo nền tảng khác hoàn toàn. Dùng máy tính cổ điển để giải quyết vấn đề có thể mất cả triệu năm nhưng chỉ cần vài phút hoặc vài giờ để MTLT quy mô đủ lớn làm việc [1]-[5]. Với khả năng ra đời của MTLT sẽ xuất hiện hai xu hướng phát triển của khoa học mật mã, đó là: mật mã lượng tử và mật mã hậu lượng tử.

Mật mã lượng tử thực sự sử dụng các nguyên tắc cơ học lượng tử làm cơ sở an toàn. Bởi vì các hệ thống mật mã này sử dụng các quy luật vật lý thay vì các chứng minh toán học, nên về mặt lý thuyết, đồng thời "không thể phá vỡ" [20]-[23]. Trong khi mật mã lượng tử sử dụng các nguyên tắc lượng tử làm cơ sở của chiến lược an toàn, thì mật mã hậu lượng tử đề cập đến các thuật toán mật mã được cho là vẫn an toàn trước cuộc tấn công của máy tính lượng tử [20], [21].

Mật mã hậu lượng tử (Post-Quantum Cryptography hoặc PQC) là dạng mật mã nhằm chuẩn bị cho kỷ nguyên MTLT bằng cách cập nhật các thuật toán và tiêu chuẩn dựa trên cơ sở toán học hiện có, để nghiên cứu về các phương pháp mã hóa bảo mật chống lại tấn công của MTLT [21], [22], [29]. Các phương pháp mã hóa truyền thống hiện nay dựa trên giả thuyết rằng tính toán được thực hiện bằng các máy tính cổ điển có thể bị giới hạn bởi khả năng tính toán của các máy tính hiện đại. Tuy nhiên, MTLT được cho là có thể giải quyết các bài toán phức tạp về tính toán trong thời gian rất ngắn.

Vì vậy, để đảm bảo tính bảo mật của dữ liệu trước các tấn công từ MTLT, cần phát triển các phương pháp mã hóa mới dựa trên các bài toán mà MTLT khó giải quyết. Các thuật toán và hệ mã hóa được xây dựng trên cơ sở những bài toán này được gọi là mật mã hậu lượng tử.