THUYẾT MINH ĐỊNH HƯỚNG NGHIÊN CỨU CHIẾN LƯỢC VỀ LƯỢNG TỬ TRONG AN TOÀN THÔNG TIN (2025-2035)

# TÓM TẮT TỔNG QUAN

Với sự phát triển mạnh mẽ của công nghệ điện toán lượng tử, các hệ thống mã hóa truyền thống như RSA, ECC đang đối mặt với nguy cơ bị phá vỡ trong tương lai gần. Thuyết minh này đề xuất chiến lược nghiên cứu toàn diện về công nghệ lượng tử trong an toàn thông tin, tập trung chính vào **mã hóa sau lượng tử (Post-Quantum Cryptography - PQC)** nhằm xây dựng nền tảng bảo mật thông tin chống lại các cuộc tấn công từ máy tính lượng tử.

**Mục tiêu tổng quát**: Phát triển và triển khai hệ sinh thái mã hóa sau lượng tử hoàn chỉnh, đảm bảo an toàn thông tin trong kỷ nguyên điện toán lượng tử.

# PHÂN TÍCH HIỆN TRẠNG VÀ NHU CẦU

## Thách thức từ điện toán lượng tử

- Thuật toán Shor có thể tấn công phá mã RSA, ECC trong thời gian đa thức

- Thuật toán Grover làm giảm một nửa độ bảo mật của mã hóa đối xứng

- Dự báo máy tính lượng tử với khả năng tính toán lớn (10000 – 100000 qubits) xuất hiện trong 10-15 năm tới

## Nhu cầu cấp thiết

- Chuyển đổi hệ thống mã hóa hiện tại sang PQC

- Đảm bảo tính tương thích ngược và khả năng triển khai

- Xây dựng tiêu chuẩn và quy trình đánh giá bảo mật

- Xây dựng cơ sở về truyền tin lượng tử

# ĐỊNH HƯỚNG NGHIÊN CỨU THEO GIAI ĐOẠN

## GIAI ĐOẠN 1: NỀN TẢNG LÝ THUYẾT VÀ THUẬT TOÁN CƠ BẢN PQC (2025-2027)

### Mục tiêu chính

- Nghiên cứu sâu các họ thuật toán PQC cốt lõi

- Phát triển nền tảng toán học và lý thuyết

- Xây dựng khung đánh giá bảo mật chuẩn

### Nội dung nghiên cứu chi tiết

#### Nghiên cứu các họ thuật toán PQC:

**- Mã hóa dựa trên lưới (Lattice-based)**: CRYSTALS KYBER, CRYSTALS DILITHIUM, FALCON

**- Mã hóa dựa trên mã sửa lỗi (Code-based)**: Classic McEliece, BIKE, HQC

**- Mã hóa đa biến (Multivariate)**: Rainbow, GeMSS

**- Mã hóa đồng cấu (Isogeny-based)**: SIKE

**- Mã hóa dựa trên hàm băm (Hash-based)**: SPHINCS+, XMSS

#### Phát triển nền tảng toán học:

Lý thuyết về độ phức tạp của các bài toán tạo nên các hệ mã hoá, khả năng chống chịu trước tấn công lượng tử, các hướng tấn công và phòng thủ mới.

#### Xây dựng framework đánh giá:

Xây dựng các bộ tiêu chuẩn đánh giá, từ đó phát triển các bộ công cụ, phương pháp đo lường, phân tích và mô phỏng

#### Kết quả mong đợi

- Hệ mã hoá PQC cho môi trường Việt Nam nói chung và các hoạt động quân sự nói riêng.

- Bộ tiêu chuẩn và công cụ đánh giá

- Bài báo khoa học quốc tế

## GIAI ĐOẠN 2: TRIỂN KHAI VÀ TỐI ƯU HÓA PQC (2027-2030)

### Mục tiêu chính

- Phát triển các hệ mã thực tế, tối ưu hóa hiệu suất và bảo mật

- Xây dựng nguyên mẫu cho hệ thống nói trên

### Nội dung nghiên cứu chi tiết

#### Tối ưu hóa

- Tối ưu cho các nền tảng khác nhau (x86, ARM, nhúng)

- Kỹ thuật tăng tốc phần cứng (FPGA, ASIC)

- Bảo vệ chống tấn công kênh bên (side-channel attacks)

#### Phát triển hệ thống hybrid:

- Kết hợp PQC với mã hóa cổ điển

- Nghiên cứu phương pháp chuyển đổi các hệ mã hoá trước lượng tử hiện có sang PQC

- Quản lý khóa trong môi trường hỗn hợp

#### Xây dựng prototype:

- Hệ thống PKI dựa trên PQC

- Giao thức bảo mật mạng (TLS, VPN)

- Ứng dụng trong IoT và blockchain

#### Kết quả mong đợi

- Thư viện PQC tối ưu hoàn chỉnh

- 3-5 prototype hệ thống thực tế

- Bài báo khoa học quốc tế

## GIAI ĐOẠN 3: NGHIÊN CỨU VÀ PHÁT TRIỂN TRUYỀN TIN LƯỢNG TỬ (2030-2032)

### Mục tiêu chính

- Xây dựng nền tảng lý thuyết hoàn chỉnh cho truyền tin lượng tử

- Phát triển và chuẩn hóa các giao thức truyền tin lượng tử

- Thiết kế kiến trúc hệ thống quantum communication networks

### Nội dung nghiên cứu chi tiết

#### Xây dựng nền tảng lý thuyết truyền tin lượng tử

**- Lý thuyết thông tin lượng tử cơ bản**: Quantum entropy, quantum channel capacity, quantum error correction

**- Quantum entanglement theory**: Entanglement distillation và purification protocols

**- Quantum no-cloning theorem**: Ứng dụng trong bảo mật và detection of eavesdropping

**- Information-theoretic security**: Chứng minh tính bảo mật tuyệt đối của quantum cryptography

**- Quantum channel modeling**: Mô hình hóa noise, loss và decoherence trong môi trường thực

#### Phát triển giao thức truyền tin lượng tử tiên tiến:

**- Giao thức Quantum Key Distribution (QKD)**: BB84, SARG04, Decoy State, Continuous Variable QKD

**- Quantum Secure Direct Communication (QSDC)**: Deterministic QSDC protocols, Quantum dialogue protocols

**- Quantum Network Protocols**: Quantum repeater protocols, Quantum internet protocols

**- Hybrid Classical-Quantum Protocols**: QKD + Classical encryption, Post-quantum + Quantum hybrid

#### Thiết kế kiến trúc hệ thống quantum communication:

Thiết kế kiến trúc theo từng lớp cho mạng lượng tử, giao thức giữa truyền tin cổ điển và lượng tử, quản lý tài nguyên cho mô hình.

#### Kết quả mong đợi

- Bộ giao thức truyền tin lượng tử hoàn chỉnh cho môi trường Việt Nam

- Framework thiết kế quantum communication networks

- Bài báo khoa học quốc tế về quantum communication

## GIAI ĐOẠN 3: CHUẨN HÓA, HOÀN THIỆN VÀ MỞ RỘNG (2032-2035)

### Mục tiêu chính

- Phát triển tiêu chuẩn quốc gia

- Hợp tác quốc tế và đào tạo nhân lực chuyên môn

- Sản phẩm ứng dụng

### Nội dung nghiên cứu chi tiết

#### Phát triển tiêu chuẩn quốc gia

- Xây dựng bộ tiêu chuẩn kỹ thuật quốc gia TCVN về PQC

- Thiết lập quy trình chứng nhận (certification) và đánh giá tuân thủ sản phẩm PQC

- Thiết lập cơ chế cập nhật và bảo trì tiêu chuẩn theo xu hướng công nghệ

#### Hợp tác quốc tế và đào tạo nhân lực chuyên môn

- Thiết lập mối quan hệ hợp tác quốc tế về lượng tử trong an toàn thông tin.

- Phát triển chương trình đào tạo

- Tổ chức các hội thảo quốc tế thường niên về nghiên cứu lượng tử và PQC

#### Sản phẩm ứng dụng

- Các sản phẩm phục vụ cho bảo mật thông tin của chính phủ và quân đội

#### Kết quả mong đợi

- Tiêu chuẩn quốc gia về PQC được quốc tế công nhận

- Nhân lực đại học và sau đại học về PQC

- Bộ mã hoá PQC trong mạng truyền thông quân sự

# NGUỒN LỰC VÀ TỔ CHỨC THỰC HIỆN

## Nhân lực

- Trung tâm nghiên cứu xuất sắc về an toàn thông tin

## Cơ sở vật chất

- Phòng thí nghiệm điện toán hiệu năng cao

- Cơ sở đào tạo và hội thảo

# KẾT LUẬN VÀ KHUYẾN NGHỊ

Nghiên cứu mã hóa sau lượng tử là nhiệm vụ cấp bách và có ý nghĩa chiến lược quốc gia. Thông qua lộ trình 10 năm được đề xuất, Việt Nam có thể:

**- Chủ động** trong việc bảo vệ an toàn thông tin trước thời đại lượng tử

**- Dẫn đầu** khu vực về công nghệ PQC

**- Đảm bảo** an ninh mạng quốc gia trong dài hạn

**Khuyến nghị triển khai**:

Khởi động ngay từ năm 2025 với các nghiên cứu nền tảng, đầu tư mạnh vào đào tạo nhân lực chất lượng cao, thiết lập mối quan hệ hợp tác nghiên cứu quốc tế, xây dựng chính sách hỗ trợ.