MỤC LỤC

CHƯƠNG 1: TỔNG QUAN VÀ CƠ SỞ LÝ THUYẾT

1.1 Đặt vấn đề

1.2 Lịch sử giải quyết vấn đề

1.3 Phạm vi của đề tài

1.4 Phương pháp nghiên cứu và hướng giải quyết vấn đề

1.5 Cơ sở lý thuyết

1.5.1 Các định nghĩa cơ bản

1.5.2 Đường cong elliptic (Elliptic Curves)

1.5.3 Nhóm cyclic hữu hạn (Finite Cyclic Groups)

1.5.4 Phép ghép cặp song tuyến tính (Bilinear Pairing)

1.5.5 Hàm băm lên đường cong (Hash-to-Curve)

1.5.6 Lược đồ chia sẻ bí mật tuyến tính (Linear Secret Sharing Scheme - LSSS)

1.6 Hệ thống mã hóa CP-ABE

1.6.1 Giới thiệu CP-ABE

1.6.2 Các thuật toán cơ bản trong CP-ABE

1.7 Thư viện RELIC (Reliable Efficient Lightweight Intelligent Cryptographic library)

1.8 Thư viện PBC (Pairing-Based Cryptography library)

1.9 So sánh các hàm sử dụng trong PBC và RELIC

CHƯƠNG 2: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

2.1 Tổng quan quy trình cài đặt hệ thống

2.1.1 Khởi tạo hệ thống (Setup)

2.1.2 Tạo khóa người dùng (Key Generation)

2.1.3 Mã hóa dữ liệu (Encryption)

2.1.4 Giải mã dữ liệu (Decryption)

2.2 Cấu trúc dữ liệu và thuật toán chi tiết

2.3 Các tối ưu hóa và cải tiến khi sử dụng RELIC

2.4 Mô hình kiểm thử và đánh giá hiệu suất

2.5 Các vấn đề gặp phải và hướng xử lý

CHƯƠNG 3: KẾT QUẢ THỰC NGHIỆM VÀ ĐÁNH GIÁ

3.1 Môi trường và công cụ thực nghiệm

3.2 Các bước thực hiện thực nghiệm

3.2.1 Thực hiện khởi tạo (Setup)

3.2.2 Thực hiện tạo khóa (KeyGen)

3.2.3 Thực hiện mã hóa (Encrypt)

3.2.4 Thực hiện giải mã (Decrypt)

3.3 Kết quả thu được và phân tích

3.3.1 Đánh giá thời gian xử lý

3.3.2 Đánh giá độ tương thích hệ thống

3.3.3 So sánh hiệu suất RELIC và PBC

3.4 Đánh giá chung

3.4.1 Ưu điểm

3.4.2 Nhược điểm

3.4.3 Định hướng phát triển

TÀI LIỆU THAM KHẢO