HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Nguyễn Sơn Lâm

NGHIÊN CỨU VÀ ĐÁNH GIÁ CÁC MÔ HÌNH KÝ SỐ ĐA BÊN HẬU LƯỢNG TỬ TRÊN NỀN THUẬT TOÁN CRYSTALS-DILITHIUM

CHUYÊN NGÀNH: HỆ THỐNG THÔNG TIN

MÃ SỐ: 8.48.01.04

TÓM TẮT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI - 2025

Đề án tốt nghiệp được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. ĐẶNG MINH TUẤN và PSG.TS. TRẦN QUANG ANH

Phản biện 1: .....

Phản biện 2: .....

Đề án tốt nghiệp sẽ được bảo vệ trước Hội đồng chấm đề án tốt nghiệp thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng ..... năm .....

Có thể tìm hiểu đề án tốt nghiệp tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

PHẦN MỞ ĐẦU

Chữ ký số đóng vai trò then chốt trong việc đảm bảo an toàn thông tin và giá trị pháp lý cho các giao dịch điện tử, từ ký kết hợp đồng, hóa đơn điện tử, phê duyệt báo cáo nội bộ cho đến các ứng dụng trong hệ thống phân tán và công nghệ blockchain. Trong nhiều thập kỷ qua, các thuật toán mật mã khóa công khai như RSA và ECDSA đã được sử dụng rộng rãi và trở thành nền tảng cho hầu hết các hệ thống chữ ký số hiện nay. Tuy nhiên, sự phát triển nhanh chóng của máy tính lượng tử, cùng với sự ra đời của thuật toán Shor, đã đặt ra mối đe dọa nghiêm trọng đối với các hệ mật mã truyền thống, khi chúng có thể bị phá vỡ trong thời gian đa thức trên máy tính lượng tử, làm suy giảm đáng kể mức độ an toàn của chữ ký số hiện hành.[1], [2]

Trước bối cảnh đó, mật mã hậu lượng tử (Post-Quantum Cryptography – PQC)[3] đã trở thành một hướng nghiên cứu quan trọng nhằm xây dựng các thuật toán mật mã có khả năng chống lại cả các cuộc tấn công từ máy tính cổ điển và máy tính lượng tử. Khác với RSA và ECDSA vốn dựa trên các bài toán toán học dễ bị giải bởi thuật toán lượng tử Shor, các thuật toán hậu lượng tử được xây dựng dựa trên những bài toán được cho là khó giải ngay cả đối với máy tính lượng tử, tiêu biểu như bài toán mạng (lattice-based), bài toán mã hóa (code-based) và bài toán dựa trên hàm băm (hash-based). Trong số đó, CRYSTALS-Dilithium là một thuật toán chữ ký số tiêu biểu thuộc nhóm lattice-based và đã được Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) chính thức lựa chọn làm tiêu chuẩn chữ ký số hậu lượng tử. Việc chuẩn hóa này mở ra cơ hội quan trọng cho nghiên cứu, đánh giá và triển khai các hệ thống chữ ký số an toàn trong kỷ nguyên hậu lượng tử.

Song song với quá trình chuẩn hóa chữ ký hậu lượng tử, nhu cầu ký số đa bên – trong đó nhiều thực thể cùng tham gia ký và xác thực một tài liệu – ngày càng gia tăng trong các lĩnh vực như quản lý văn bản điện tử, hợp đồng số, tài chính – kế toán và các hệ thống phân tán như blockchain. Mô hình ký đa bên không chỉ nâng cao tính minh bạch và độ tin cậy, mà còn giúp phân tán quyền kiểm soát và giảm thiểu rủi ro từ một thực thể đơn lẻ. Tuy nhiên, phần lớn các nghiên cứu hiện nay về chữ ký số hậu

lượng tử vẫn chủ yếu tập trung vào mô hình ký đơn. Các nghiên cứu về ký số đa bên dựa trên CRYSTALS-Dilithium mới chỉ dừng lại ở mức đề xuất lý thuyết hoặc thử nghiệm giới hạn, và đặc biệt, nhiều công trình chưa công bố mã nguồn triển khai, gây khó khăn cho việc kiểm chứng, đánh giá độc lập và ứng dụng thực tiễn.

Xuất phát từ khoảng trống nghiên cứu nêu trên, đề tài "Nghiên cứu và đánh giá các mô hình ký số đa bên hậu lượng tử trên nền CRYSTALS-Dilithium" được thực hiện nhằm tái hiện và triển khai thử nghiệm các mô hình ký số đa bên dựa trên Dilithium, đồng thời tiến hành đo đạc và phân tích các chỉ số hiệu năng quan trọng như thời gian sinh khóa, kích thước khóa, thời gian ký, thời gian xác minh, kích thước chữ ký, dung lượng dữ liệu trao đổi và khả năng mở rộng theo số lượng bên tham gia. Kết quả nghiên cứu kỳ vọng sẽ cung cấp dữ liệu thực nghiệm có giá trị, góp phần đánh giá tiềm năng ứng dụng và đề xuất các hướng cải tiến kỹ thuật cho các hệ thống chữ ký số đa bên hậu lượng tử trong tương lai.

Chương 1.CƠ SỞ LÝ THUYẾT VÀ TỔNG QUAN NGHIÊN CỨU

1.1.Khái quát về chữ ký số

Chữ ký số (*Digital Signature*) là một cơ chế mật mã được sử dụng nhằm xác thực nguồn gốc, đảm bảo tính toàn vẹn của dữ liệu điện tử và cung cấp khả năng chống chối bỏ cho người ký. Không giống như chữ ký tay truyền thống, chữ ký số dựa trên các thuật toán toán học và cặp khóa mật mã để thiết lập niềm tin trong môi trường số.

Một hệ thống chữ ký số an toàn phải thỏa mãn ba đặc tính an ninh cơ bản:

Tính toàn vẹn (Integrity): Đảm bảo rằng nội dung dữ liệu không bị thay đổi sau khi được ký; mọi chỉnh sửa dù nhỏ nhất đều dẫn đến việc chữ ký không còn hợp lệ.

- Tính xác thực (Authenticity): Xác nhận danh tính của người ký, đảm bảo chữ ký được tạo ra bởi chủ sở hữu hợp pháp của khóa bí mật tương ứng.
- Tính chống chối bỏ (Non-repudiation): Ngăn chặn người ký phủ nhận hành vi ký của mình, do chỉ họ mới có quyền truy cập và sử dụng khóa bí mật để tạo chữ ký.
- Ba đặc tính này là nền tảng để chữ ký số được công nhận giá trị pháp lý và an ninh trong các hệ thống điện tử.

Về mặt kỹ thuật, một lược đồ chữ ký số tiêu chuẩn bao gồm ba thuật toán chính:

- Sinh khóa (Key Generation – KeyGen): Là thuật toán xác suất nhận tham số an toàn làm đầu vào để sinh ra một cặp khóa gồm khóa công khai (*public key – pk*) và khóa bí mật (*secret key – sk*). Khóa công khai được phân phối rộng rãi, trong khi khóa bí mật được giữ kín bởi người ký.

- Ký (Signing – Sign): Thuật toán sử dụng khóa bí mật (*sk*) và thông điệp cần ký (*M*) để tạo ra chữ ký số (σ).
- Xác minh (Verification – Verify): Thuật toán nhận đầu vào là khóa công khai (*pk*), thông điệp (*M*) và chữ ký (σ), sau đó đưa ra kết quả xác minh hợp lệ hoặc không hợp lệ.

Một hệ thống chữ ký số phải đảm bảo tính đúng đắn (correctness), nghĩa là mọi chữ ký được tạo hợp lệ bởi thuật toán *Sign* đều phải được thuật toán *Verify* chấp nhận.

Chữ ký số cung cấp mức độ đảm bảo an ninh phi vật lý tương đương, thậm chí vượt trội so với chữ ký tay, và đóng vai trò then chốt trong nhiều lĩnh vực của xã hội số:

- Tài chính – ngân hàng: Được sử dụng để xác thực giao dịch, hợp đồng điện tử và các hoạt động chuyển tiền, giúp giảm thiểu gian lận và loại bỏ quy trình giấy tờ thủ công.
- An ninh mạng: Là nền tảng của hạ tầng khóa công khai (PKI), ứng dụng trong chứng chỉ số X.509, giao thức TLS/SSL và ký phần mềm (*code signing*).
- Blockchain và tiền mã hóa: Đóng vai trò trung tâm trong việc chứng minh quyền sở hữu tài sản và xác thực giao dịch mà không cần bên trung gian đáng tin cậy.
- Chính phủ điện tử: Hỗ trợ triển khai các dịch vụ công trực tuyến như khai thuế, đăng ký kinh doanh và bảo đảm giá trị pháp lý cho văn bản điện tử.

1.2.Hệ thống hóa các mô hình ký số đa bên

1.2.1. Ký Ngưỡng (Threshold Signatures – TS)

Ký ngưỡng là mô hình tập trung vào việc bảo vệ khóa bí mật và phân tán rủi ro, bằng cách không cho bất kỳ cá nhân nào nắm giữ toàn bộ khóa ký.

Nguyên lý: Khóa bí mật (sk) được chia thành n mảnh thông qua sơ đồ chia sẻ bí mật (ví dụ Shamir Secret Sharing). Một chữ ký hợp lệ chỉ có thể được tạo khi có ít nhất t mảnh khóa (với t là ngưỡng) cùng tham gia.

Quy trình:Mỗi bên ký cục bộ bằng phần khóa của mình để tạo ra mảnh chữ ký. Các mảnh này sau đó được một nút tổng hợp (Combiner) kết hợp thành một chữ ký cuối cùng. Bên xác minh chỉ cần sử dụng một khóa công khai duy nhất mà không cần biết chính xác những ai đã tham gia ký.

Ưu điểm: Không tồn tại điểm lỗi đơn lẻ (single point of failure). Tạo ra một chữ ký duy nhất, giúp tiết kiệm băng thông và lưu trữ.

Hạn chế:Yêu cầu giao thức tương tác phức tạp giữa các bên, làm tăng độ trễ và độ khó khi triển khai ở quy mô lớn.

Ứng dụng: Quản lý tài sản giá trị cao (ví lạnh), quản trị doanh nghiệp và các giao thức blockchain hiện đại.

1.2.2. Ký Gộp (Aggregate Signatures – AS)

Ký gộp là mô hình tập trung vào tối ưu hóa kích thước dữ liệu và chi phí xác minh khi có nhiều chữ ký độc lập.

Nguyên lý: Cho phép gộp nhiều chữ ký từ các người ký khác nhau (có thể trên các thông điệp khác nhau) thành một chữ ký tổng hợp duy nhất.

Quy trình: Một thực thể trung gian (Aggregator) thu thập các chữ ký đơn lẻ và kết hợp chúng bằng các cấu trúc toán học như đường cong Elliptic hoặc lưới.

Ưu điểm: Giảm chi phí xác minh từ O(n) xuống O(1) hoặc O(log n). Tiết kiệm băng thông và bộ nhớ lưu trữ.

Hạn chế (ngầm hiểu): Không bảo vệ khóa bí mật tập trung; mỗi người vẫn giữ khóa riêng.

Ứng dụng: Blockchain (ZK-rollups), nhật ký hệ thống và các mạng IoT quy mô lớn.

1.2.3. Ký Độc lập (Independent / Multi-Signature)

Đây là mô hình đơn giản nhất, trong đó mỗi bên ký độc lập bằng cặp khóa riêng.

Đặc điểm: Mỗi bên P_isở hữu cặp khóa (pk_i, sk_i)và tạo chữ ký riêng $\sigma_i$trên cùng một thông điệp.

Phân loại:

- Ký song song: Các chữ ký được tạo độc lập và song song. Kích thước dữ liệu và chi phí xác minh tăng tuyến tính theo số lượng người ký.
- Ký tuần tự: Người sau ký lên kết quả của người trước, tạo thành chuỗi phê duyệt. Phù hợp với quy trình hành chính nhưng có độ trễ cao.

1.3.Mật mã hậu lượng tử (PQC) và CRYSTALS-Dilithium

1.3.1. Nguy cơ từ máy tính lượng tử

Sự phát triển của máy tính lượng tử đặt ra mối đe dọa nghiêm trọng đối với các hệ mật mã khóa công khai truyền thống như RSA và ECC.

Khác với máy tính cổ điển sử dụng bit nhị phân, máy tính lượng tử hoạt động dựa trên qubit, cho phép khai thác các hiện tượng vật lý như chồng chập (superposition) và rối lượng tử (entanglement). Nhờ đó, máy tính lượng tử có khả năng thực hiện tính toán song song trên không gian trạng thái cực lớn, vượt xa năng lực của máy tính cổ điển.

Mối đe dọa cụ thể đến từ thuật toán Shor, được đề xuất năm 1994, cho phép giải các bài toán phân tích số nguyên lớn và logarit rời rạc trong thời gian đa thức bằng biến đổi Fourier lượng tử (QFT). Điều này đồng nghĩa với việc các hệ mật mã dựa trên độ khó của các bài toán này (RSA, DSA, ECDSA, ECC) có thể bị phá vỡ trong thời gian ngắn khi máy tính lượng tử đủ mạnh trở nên khả thi.

1.3.2. Mật mã hậu lượng tử (Post-Quantum Cryptography – PQC) và chuẩn hóa NIST

Để đối phó với nguy cơ trên, mật mã hậu lượng tử (PQC) được phát triển dựa trên các bài toán toán học được cho là khó giải ngay cả với máy tính lượng tử.

Các họ thuật toán PQC tiêu biểu bao gồm:

- Mật mã dựa trên mạng (Lattice-based)
- Mật mã dựa trên mã sửa sai (Code-based)
- Mật mã dựa trên hàm băm (Hash-based)
- Mật mã đa biến và đường cong đẳng cấu (Isogeny-based)

Từ năm 2016 đến 2022, Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) đã tổ chức quá trình chuẩn hóa PQC quy mô lớn. Kết quả, ba thuật toán chữ ký số được lựa chọn vào nhóm chuẩn hóa cuối cùng gồm:

- CRYSTALS-Dilithium (FIPS 204): Dựa trên mạng, hiệu suất cao, cân bằng tốt giữa tốc độ và kích thước.
- Falcon: Kích thước chữ ký nhỏ nhưng yêu cầu triển khai số học phức tạp, khó hiện thực an toàn.
- SPHINCS+: Dựa trên hàm băm, mức độ an toàn cao nhưng tốc độ chậm và kích thước chữ ký lớn.

1.3.3. Thuật toán CRYSTALS-Dilithium (FIPS 204)

CRYSTALS-Dilithium là thuật toán chữ ký hậu lượng tử được chọn làm chuẩn chính thức (Primary Standard) của NIST và là nền tảng kỹ thuật của đề tài.

Cơ sở toán học: Dilithium hoạt động trên mạng mô-đun (Module Lattices) với cấu trúc vành đa thức R_q, và dựa trên hai bài toán khó cốt lõi:

+ M-LWE (Module Learning With Errors): Đảm bảo tính bí mật của khóa, ngăn chặn việc suy ngược khóa bí mật từ khóa công khai.
+ M-SIS (Module Short Integer Solution): Đảm bảo tính toàn vẹn và khả năng chống giả mạo chữ ký.

Kỹ thuật tối ưu và bảo mật

+ Biến đổi NTT (Number Theoretic Transform): Giảm độ phức tạp nhân đa thức từ $O(n^2)$xuống $O(n\log n)$, cho phép thực thi hiệu quả trên phần cứng hiện đại.
+ Rejection Sampling: Đảm bảo chữ ký không rò rỉ thông tin về khóa bí mật, đóng vai trò tương tự một cơ chế bảo vệ dạng *zero-knowledge*.
+ Nén dữ liệu: Áp dụng các kỹ thuật như *Power2Round* và *MakeHint/UseHint* để giảm kích thước khóa và chữ ký mà vẫn đảm bảo khả năng xác minh chính xác.

1.4.Khảo sát và phân tích các nghiên cứu tiêu biểu

Việc triển khai các giao thức ký đa bên trên nền tảng mật mã lưới (Lattice-based) gặp phải thách thức lớn hơn nhiều so với RSA hay ECDSA do đặc thù của kỹ thuật "Lấy mẫu loại bỏ" (Rejection Sampling) và sự phức tạp của việc quản lý nhiễu. Dưới đây là phân tích các công trình nền tảng và cập nhật nhất liên quan đến vấn đề này.

1.4.1. Nghiên cứu về ký ngưỡng từ mô hình lý thuyết Cozzo & Smart (2019) đến đánh giá thực nghiệm của Roux (2022)

Hướng tiếp cận này dựa trên lý thuyết Tính toán đa bên an toàn (Secure Multi-Party Computation – MPC), với mục tiêu hiện thực hóa thuật toán chữ ký Dilithium trong môi trường phân tán mà không để lộ khóa bí mật.

Cơ sở lý thuyết: Cozzo và Smart đề xuất một mô hình lai ghép, trong đó các phép toán tuyến tính được xử lý bằng mạch số học, còn các phép toán phi tuyến được

hiện thực thông qua Garbled Circuits. Cách tiếp cận này cho phép mô phỏng đầy đủ thuật toán Dilithium trong khuôn khổ MPC tổng quát.

Kết quả thực nghiệm: Dominique Roux (2022) đã triển khai mô hình này và chỉ ra rằng hiệu năng thực tế rất thấp. Thời gian sinh một chữ ký lên tới khoảng 87 giây trong mô hình an toàn thụ động và 41 phút trong mô hình an toàn chủ động.

Hạn chế: Mô hình yêu cầu tài nguyên phần cứng cực lớn (khoảng 14GB RAM chỉ để biên dịch), độ trễ cao và hoàn toàn không phù hợp cho các ứng dụng thực tế, đặc biệt là các hệ thống nhúng hay IoT.

1.4.2. Nghiên cứu về đa chữ ký hậu lượng tử của Hamidreza Rahmati và Farhad Rahmati

Hướng tiếp cận này tập trung giải quyết bài toán độ trễ mạng và chi phí lưu trữ on-chain trong các hệ thống blockchain.

Cơ chế: Lược đồ Razhi-ms sử dụng kỹ thuật mã hóa mầm (seed encryption) để rút gọn quy trình ký xuống còn một vòng giao tiếp duy nhất, thay vì nhiều vòng như các giao thức truyền thống.

Ưu điểm: Kích thước chữ ký rất nhỏ (khoảng 2.2 KB), gần tương đương chữ ký Dilithium đơn lẻ, đặc biệt phù hợp cho lưu trữ trực tiếp trên blockchain.

Hạn chế: Không tuân thủ chuẩn: Sử dụng tham số mô-đun $q$khác với FIPS 204, gây khó khăn trong việc tận dụng các thư viện và phần cứng đã được tối ưu.

Thiếu linh hoạt: Chỉ hỗ trợ mô hình n-of-n, không đáp ứng được yêu cầu ngưỡng tổng quát t-of-n.

Chi phí tính toán cục bộ cao: Mỗi người ký phải mã hóa dữ liệu cho tất cả các thành viên khác, khiến chi phí tăng nhanh khi số lượng người tham gia lớn.

1.4.3. Nghiên cứu về ký ngưỡng trên thiết bị IOT: Davydov & Bezzateev (2023)

Hướng tiếp cận này nhắm tới các môi trường có tài nguyên hạn chế, như thiết bị IoT và wearables.

Cơ chế: Kết hợp mật mã dựa trên mạng với Shamir Secret Sharing và kỹ thuật Fiat–Shamir with Aborts để xây dựng giao thức ký ngưỡng hậu lượng tử.

Ưu điểm:

- Hiệu năng cao: Thời gian thực thi toàn bộ quy trình dưới 40 ms, phù hợp cho ứng dụng thời gian thực.
- Tuân thủ chuẩn: Sử dụng đầy đủ bộ tham số của FIPS 204 (Dilithium).
- Tính linh hoạt: Hỗ trợ trực tiếp mô hình ngưỡng t-of-n.

Nhược điểm: Kích thước chữ ký và lượng dữ liệu truyền tải tương đối lớn (khoảng 11.7 KB), gây áp lực lên băng thông mạng.

1.4.4. Tổng hợp so sánh và xác định hướng triển khai

Từ các phân tích trên (tổng hợp trong Bảng 1.2), đề án lựa chọn mô hình ký ngưỡng dựa trên nghiên cứu của Leevik et al. làm hướng tiếp cận chính.

Lý do lựa chọn:

- Hỗ trợ mô hình tổng quát $\boldsymbol{t}$-of-$\boldsymbol{n}$, bao trùm cả trường hợp $\boldsymbol{n}$-of-$\boldsymbol{n}$.
- Tuân thủ đầy đủ chuẩn FIPS 204, cho phép tận dụng các nguyên thủy mật mã đã được chuẩn hóa và kiểm chứng.
- Hiệu năng vượt trội (thời gian tính bằng mili giây), phù hợp cho triển khai thực tế, vượt xa các mô hình MPC tổng quát có độ trễ tính bằng giây hoặc phút.

Giải pháp cải tiến của đề án: Để khắc phục nhược điểm về kích thước chữ ký của mô hình Leevik, đề án đề xuất tích hợp kỹ thuật nén dữ liệu (bit-packing) theo

chuẩn FIPS 204 nhằm giảm dung lượng lưu trữ và băng thông truyền tải. Đồng thời, đề án triển khai mô hình ký độc lập như một phương án đối chứng để so sánh hiệu năng và chi phí với mô hình ký ngưỡng.

Chương 2. PHƯƠNG PHÁP NGHIÊN CỨU VÀ THIẾT KẾ MÔ HÌNH THỬ NGHIỆM

2.1.Mục tiêu và yêu cầu của thử nghiệm

Để giải quyết các khoảng trống nghiên cứu đã xác định ở Chương 1, đặc biệt là sự thiếu hụt các đánh giá thực nghiệm toàn diện về hiệu năng của Dilithium trong môi trường đa bên, quá trình thử nghiệm cần đạt được các mục tiêu và yêu cầu cụ thể sau.

2.1.1. Mục tiêu: Đo lường các chỉ số hiệu năng.

Mục tiêu cốt lõi là đo đạc và phân tích số liệu thực tế để kiểm chứng các nhận định lý thuyết, tập trung vào 3 khía cạnh chính:

- Chi phí tính toán (Computational Cost):
  - + Đo thời gian thực thi trung bình cho các pha: Sinh khóa (KeyGen), Ký (Sign) và Xác minh (Verify).
  - + So sánh sự chênh lệch thời gian giữa mô hình đơn lẻ và mô hình đa bên để xác định "chi phí cộng thêm" (overhead) của các thuật toán chia sẻ bí mật.
- Chi phí truyền thông (Communication Cost):
  - + Đây là mục tiêu quan trọng nhất để kiểm chứng nhược điểm về băng thông của mật mã lưới.
  - + Đo tổng dung lượng dữ liệu (KB) cần truyền tải để hoàn tất một phiên ký và kiểm tra hiệu quả của kỹ thuật nén dữ liệu (Bit-packing).
  - + Đếm số vòng tương tác và số vòng lặp phát sinh do cơ chế *Rejection Sampling* phân tán.
- Khả năng mở rộng (Scalability): phân tích xu hướng biến thiên của hiệu năng khi số lượng người tham gia để tìm ra giới hạn chịu đựng của hệ thống.

2.1.2. Yêu cầu: Đảm bảo tính chính xác, khách quan, có thể lặp lại.

- Tính chính xác và độ tin cậy: Các phép đo được thực hiện với đơn vị miligiây (ms). Kết quả được lấy trung bình trên nhiều lần chạy (100–1.000 lần) nhằm giảm nhiễu ngẫu nhiên và ảnh hưởng của cơ chế *Rejection Sampling*. Toàn bộ chữ ký sinh ra phải được xác minh hợp lệ bằng thuật toán `Verify` theo chuẩn.
- Tính khách quan và công bằng: Tất cả các mô hình được đánh giá trên cùng cấu hình phần cứng và hệ điều hành. Các phép toán mật mã nền tảng sử dụng chung thư viện chuẩn (liboqs hoặc PQClean), đảm bảo so sánh tập trung vào bản chất thuật toán thay vì mức độ tối ưu của mã nguồn.
- Khả năng lặp lại: Bộ tham số thử nghiệm tuân thủ chuẩn NIST (Dilithium 2, 3, 5) được công bố rõ ràng. Mã nguồn và kịch bản đo hiệu năng được mô tả chi tiết nhằm đảm bảo các nghiên cứu sau có thể tái lập kết quả.

2.2.Bộ tiêu chí đánh giá hiệu năng

Để đảm bảo tính khách quan và khả năng so sánh giữa các mô hình (Ký ngưỡng, Ký gộp, Ký độc lập), đề tài sử dụng bộ tiêu chí gồm 4 nhóm chỉ số chính:

2.2.1. Hiệu năng Tính toán (Computational Efficiency)

- Thời gian sinh khóa (KeyGen):
    + *Ký ngưỡng:* Đo tổng thời gian thực hiện giao thức sinh khóa phân tán (DKG) cho đến khi mỗi bên nhận được mảnh khóa bí mật và khóa công khai chung.
    + *Ký độc lập:* Đo thời gian sinh một cặp khóa Dilithium chuẩn.
- Thời gian ký (Signing):
    + *Ký ngưỡng:* Đo tổng thời gian từ khi nhận thông điệp đến khi tạo ra chữ ký hợp lệ, bao gồm cả tính toán cục bộ và thời gian đồng bộ giữa các bên.

+ *Ký độc lập:* Thời gian trung bình để tạo một chữ ký đơn lẻ.

– Thời gian xác minh: Mục tiêu là chứng minh lợi thế xác minh của chữ ký ngưỡng thông qua xác minh gộp

2.2.2. Hiệu năng Truyền thông

Đây là nhóm chỉ số quan trọng đối với đề tài, vì kích thước dữ liệu trao đổi lớn, dễ gây nghẽn mạng.

– Dung lượng dữ liệu trao đổi:
  + Định nghĩa: Tổng kích thước (tính bằng KB) của tất cả các gói tin (Commitments, Shares, Partial Signatures) được gửi đi giữa các bên để hoàn thành một chữ ký.
  + *Tham chiếu:* Nghiên cứu của Leevik (2023) cho thấy chỉ số này lên tới ~15KB/user, cần đo đạc lại.

2.2.3. Hiệu quả Lưu trữ (Storage Efficiency)

– Kích thước Chữ ký (Signature Size):
  + Ký ngưỡng: Kích thước chữ ký cuối cùng ~11.5 KB theo bài báo công bố.
  + Ký độc lập: Tổng kích thước của N chữ ký riêng biệt.
– Kích thước Khóa công khai (pk): So sánh kích thước của một Khóa công khai chung (PK_{group}) so với việc phải lưu trữ danh sách N khóa công khai rời rạc $(PK_1, PK_2, \dots, PK_N)$.

2.2.4. Độ ổn định và Mở rộng (Scalability & Stability)

– Số vòng lặp Rejection Sampling (Rejection Rounds):
  + Định nghĩa: Số vòng lặp trung bình, nếu một bên (signer) tạo ra chữ ký vi phạm biên độ an toàn, toàn bộ giao thức phải khởi động lại (Restart). Bài nghiên cứu của Leevik ghi nhận tỷ lệ chấp nhận khoảng 20-50% (tương đương cần 2-5 lần thử để thành công), số vòng lặp càng cao

tương đương với việc bắt buộc user phải tương tác với lược đồ ký nhiều lần để được chấp nhận. Chỉ số này càng thấp thì hệ thống càng ổn định.

+ *Mục tiêu:* Kiểm chứng xem mô hình triển khai có đạt được con số tối ưu được công bố là 2-5 vòng lặp hay không? Đây là thước đo quan trọng về độ ổn định của hệ thống phân tán, khác biệt hoàn toàn so với ký đơn (nơi việc lặp lại chỉ diễn ra cục bộ).

– Khả năng mở rộng (Scalability Factor): Phân tích xu hướng tăng của thời gian ký và dung lượng dữ liệu khi số lượng người tham gia tham gia (N) tăng dần (ví dụ: thử nghiệm với $N = 3, 5, 10, 20$). Mục tiêu là xác định giới hạn chịu đựng của hệ thống.

2.3.Thuyết minh mô hình ký ngưỡng (Threshold)

2.3.1. Phân tích giao thức.

Đề án xây dựng giao thức ký ngưỡng dựa trên sự kết hợp giữa mật mã lưới (M-LWE/M-SIS) và lược đồ chia sẻ bí mật Shamir, tuân thủ chặt chẽ chuẩn FIPS 204 (ML-DSA/Dilithium).

– Pha thiết lập (Setup)

+ Áp dụng mô hình Trusted Dealer trong giai đoạn khởi tạo nhằm đơn giản hóa thiết kế. Dealer sinh khóa chủ, phân phối các mảnh khóa và tiêu hủy khóa chủ ngay sau đó.
+ Áp dụng cơ chế bí mật kép cho mỗi người ký P_i:
+ Small Secret (s_i): Được giữ từ lúc sinh khóa, dùng để kiểm tra điều kiện an toàn cục bộ.
+ Large Share (x_i): Được tạo từ phân rã Shamir, là thành phần chính tham gia tính toán chữ ký.

– Pha ký số phân tán

+ Giao thức gồm 2 vòng tương tác: (i) trao đổi cam kết để sinh thử thách chung,(ii) gửi phần chữ ký cục bộ.
+ Tích hợp Rejection Sampling phân tán: mỗi bên tự kiểm tra biên độ an toàn trước khi gửi dữ liệu. Nếu vi phạm, toàn bộ phiên ký bị hủy và khởi động lại, đảm bảo không rò rỉ thông tin khóa bí mật.

– Tuân thủ chuẩn FIPS 204: Sử dụng đầy đủ tham số chuẩn (Level 2 hoặc 3), với $q = 8{,}380{,}417, N = 256$. Tận dụng các nguyên thủy chuẩn như NTT để tăng tốc nhân đa thức và ExpandA (tái tạo ma trận từ seed) nhằm giảm chi phí truyền thông.

2.3.2. Lưu đồ thuật toán (Sinh khóa, Ký, Xác minh).

2.3.2.1. Lưu đồ Sinh khóa phân tán (Distributed Key Generation – DKG)

Quy trình sinh khóa phân tán nhằm đảm bảo rằng không tồn tại bất kỳ thực thể đơn lẻ nào nắm giữ toàn bộ khóa bí mật S. Mỗi bên chỉ giữ một phần khóa (key share), và chỉ khi có đủ ngưỡng $t$bên hợp tác thì mới có thể thực hiện ký hợp lệ.

– Bước 1: Khởi tạo: Các bên tham gia $P_1, \dots, P_n$ thống nhất bộ tham số chung của hệ mật mã lưới (q, N, k, l)và seed công khai ρ. Từ ρ, tất cả các bên có thể tái tạo nhất quán ma trận công khai $A \in R_q^{k \times l}$ bằng cách sử dụng hàm expand_a() trong thư viện chuẩn FIPS 204. Mỗi bên P_i độc lập tạo các vector bí mật s_i từ phân phối Gaussian rời rạc, và vector nhiễu e_i, theo phân phối xác định trước. s_i được P_i giữ bí mật tuyệt đối.
– Bước 2: Tính khóa công khai phần (Partial Public Key): Mỗi bên tính khóa công khai cục bộ:

$$t_i = A \cdot s_i + e_i (\mathrm{mod} q) \quad (2.1)$$

– Bước 3: Chia sẻ bí mật (Shamir Secret Sharing):

+ Để phân tán khóa bí mật, mỗi bên P_i áp dụng lược đồ chia sẻ bí mật Shamir lên s_i, tạo ra n mảnh chia sẻ bằng cách xây dựng một đa thức

ngẫu nhiên $f(x) = s_1 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$, trên một trường hữu hạn phù hợp, sao cho $f(0) = s_1, sau$ đó gửi mảnh chia sẻ $f_i(\mathrm{uid}_i)$ cho các bên khác. Bên P_i tổng hợp tất cả các mảnh nhận được để tạo Large Share:$x_i = \sum_{j=1}^{n} f_j(\mathrm{uid}_i)$. Trong đó uid_ilà định danh duy nhất của P_i.

- Bước 4: Tổng hợp khóa:
  + Khóa công khai chung:

$$A, T = \sum_{i=1}^{n} t_i.$$

  + Khóa bí mật phần của bên P_i: $sk_i(x_i,\ s_i)$.

Cuối cùng hệ thống thu được khóa công khai chung $pk = T$ và tập các khóa bí mật phần $\{sk_i\}$. Không bên nào có thể suy ra khóa bí mật toàn cục.

2.3.2.2. Lưu đồ Ký ngưỡng (Threshold Signing)

Ký ngưỡng là giai đoạn phức tạp của hệ thống, yêu cầu tối thiểu t bên tham gia và bao gồm 4 vòng tương tác, kết hợp cơ chế Fiat–Shamir with Aborts (Rejection Sampling) để đảm bảo an toàn.

Đầu vào là thông điệp cần ký M và tập con gồm t người ký hợp lệ.

- Bước 1: Cam kết (Commitment)
  + Mỗi bên P_i sẽ sinh vector nhiễu ngẫu nhiên y_i, r_i và tính: $w_i = A \cdot y_i$.
  + Tạo cam kết: $com_i = \mathrm{Commit}(w_i, r_i)$, và gửi com_i cho các bên còn lại (hoặc cho bên điều phối).
- Bước 2: Sinh thử thách (Challenge)
  + Sau khi nhận đủ cam kết, tổng hợp: $com = \sum_{i=1}^{t} com_i$.

+ Sinh thử thách toàn cục: $c = H_0(com \parallel M \parallel pk)$,trong đó c là một đa thức được lấy mẫu theo hàm SampleInBall với trọng số Hamming nhỏ.

– Bước 3: Phản hồi và kiểm tra cục bộ (Response)

+ Người ký P_isử dụng s_i để kiểm tra biên chuẩn: $z_i' = y_i + c \cdot s_i$, chỉ khi thỏa mãn:$\| z_i' \| < \beta$.

+ Sau khi vượt qua bước kiểm tra, người ký sử dụng bí mật lớn x_iđể tính thành phần chữ ký: $z_i = y_i + c \cdot x_i$ Giá trị z_i có độ lớn rất lớn, không thực hiện kiểm tra biên, và được gửi trực tiếp tới nút tổng hợp. Các bên nhận sẽ thực hiện kiểm tra bằng cách tính lại giá trị băm: $H(\mathrm{z_i} \parallel r_\mathrm{i}) = ? h_\mathrm{i}$ nhằm xác thực tính toàn vẹn của dữ liệu nhận được.

– Bước 4: Tổng hợp chữ ký (Aggregation)

+ Tại phần điều phối, khi nhận đủ t chữ ký thành phần z_j cần tổng hợp lại:

$$z = \sum_{j=1}^{t} \lambda_i z_j.$$

Và cộng dồn các r cục bộ để tạo ra chìa khóa mở cam kết tổng:

$$r = \sum_{j=1} r_j$$

+ Rejection Sampling toàn cục sẽ kiểm tra: $\| z \|_\infty < t \cdot \mathrm{Bound}$. Nếu vi phạm sẽ Restart toàn bộ quy trình.

+ Nén chữ ký: Dùng thuật toán Bit-Packing để nén vector z (vốn là các số nguyên lớn) thành chuỗi bytes gọn nhẹ z_{packed}.

$$z_{\mathrm{packed}} = \mathrm{BitPack}(z).$$

+ Đầu ra: Chữ ký ngưỡng cuối cùng:

$$\sigma = (z_{packed}, c, com, r).$$

2.3.2.3. Lưu đồ Xác minh chữ ký (Verification)

Quy trình xác minh tuân thủ chuẩn FIPS 204 (Dilithium) và không phân biệt chữ ký được tạo bởi một người hay bởi nhiều người theo mô hình ngưỡng.

Giải nén: Từ chữ ký $\sigma = (z_{packed}, c, com, r)$và khóa công khai T, giải nén z_{packed} để thu được vector z. Kiểm tra biên, nếu: $\| z \| \geq t \cdot$ Bound, thì chữ ký không hợp lệ. Tái tạo tham số công khai bằng cách sử dụng seed ρ để dựng lại ma trận A.

Tính toán giá trị kiểm tra:

$$w = A \cdot z - c \cdot T.$$

Kiểm tra w có đúng là giá trị được cam kết trong *com* hay không qua hàm *commit_opening*(w, r, com) mục đích là tái tạo *com_new* và so sánh với *com*, nếu khớp thì tiếp tục với hàm băm:

$$c' = SampleInBall(H(M \parallel w \,||\, pk)).$$

So sánh:

+ Nếu $c' = c$, chúng ta có chữ ký hợp lệ (Valid).
+ Ngược lại thì không hợp lệ (Invalid).

2.3.3. Cấu trúc dữ liệu.

2.4.Thuyết minh mô hình ký độc lập

Mô hình này được thiết kế như một nhóm đối chứng. Thay vì áp dụng các kỹ thuật chia sẻ bí mật hay gộp chữ ký phức tạp, mô hình thực hiện ký tuần tự truyền thống, nơi chữ ký của mỗi cá nhân được tạo và lưu trữ độc lập.

2.4.1. Phân tích giao thức.

2.4.1.1. Giai đoạn Khởi tạo (Setup)

Không tồn tại thực thể trung tâm (Dealer). Mỗi người ký S_i độc lập sinh cặp khóa riêng của mình: (pk_i, sk_i) theo chuẩn thuật toán CRYSTALS-Dilithium. Các khóa công khai pk_i được công bố để phục vụ cho quá trình xác minh sau này.

2.4.1.2. Giai đoạn Ký (Sining)

+ Thông điệp hoặc tài liệu cần ký Mđược chuyển tuần tự qua danh sách người ký đã định trước:

$$L = S_1, S_2, \dots, S_N.$$

+ Người ký đầu tiên S_1sử dụng khóa bí mật sk_1để tạo chữ ký $\sigma_1$trên M. Người ký thứ $i(i > 1)$ nhận gói tin: $(M, \sigma_1, \dots, \sigma_{i-1})$,sau đó tạo chữ ký của riêng mình: $\sigma_i = \text{Sign}(sk_i, M)$,và chuyển tiếp gói tin: $(M, \sigma_1, \dots, \sigma_i)$ cho người ký tiếp theo.
+ Sau khi hoàn tất vòng ký, kết quả thu được là tập hợp chữ ký riêng biệt:

$$\Sigma = \sigma_1, \sigma_2, \dots, \sigma_N.$$

2.4.1.3. Giai đoạn Xác minh (Verification)

Quá trình xác minh được thực hiện một cách tuần tự:

– Với mỗi chữ ký $\sigma_i \in \Sigma$, hệ thống sử dụng khóa công khai tương ứng pk_i để kiểm tra tính hợp lệ.
– Văn bản M chỉ được chấp nhận nếu toàn bộ N chữ ký đều hợp lệ.

2.4.1.4. Đặc điểm kỹ thuật

Ưu điểm:

+ Cấu trúc đơn giản, dễ triển khai trong thực tế.
+ Không yêu cầu sửa đổi thuật toán Dilithium gốc.

+ Không cần cơ chế chia sẻ khóa hay kênh truyền bảo mật giữa các người ký.

Nhược điểm:

+ Kích thước dữ liệu chữ ký tăng tuyến tính theo số lượng người ký: $|\Sigma| = \mathcal{O}(N)$.
+ Thời gian xác minh cũng tăng tuyến tính theo N, gây tốn tài nguyên tính toán và lưu trữ. Không phù hợp với các hệ thống Blockchain hoặc môi trường on-chain, nơi chi phí lưu trữ và xác minh là yếu tố quan trọng, đặc biệt khi số lượng người ký lớn.

Môi trường và công cụ thử nghiệm

Chương 3.THỰC NGHIỆM, PHÂN TÍCH KẾT QUẢ VÀ KẾT LUẬN

3.1.Thiết kế thực nghiệm

3.1.1. Đối tượng và Kịch bản

Hệ thống thử nghiệm được triển khai để đánh giá hiệu năng của ba chiến lược ký số trên nền tảng CRYSTALS-Dilithium:

- Ký Độc lập (Independent): N chữ ký rời rạc.
- Ký Toàn phần ($t = n$): Yêu cầu 100% sự đồng thuận, tương đương với lược đồ ký đa của Hamidreza Rahmati và Farhad Rahmati.
- Ký Ngưỡng($t \approx 2/3n$): Yêu cầu đa số đồng thuận, cho phép chịu lỗi.

3.1.2. Môi trường đo lường

- Phần cứng: CPU Intel Xeon E5-2697 v4, 62GB RAM.
- Dữ liệu đo: Thời gian xử lý (CPU time), Dung lượng lưu trữ (Disk usage), và Lưu lượng mạng (Network I/O).

– Quy mô thử nghiệm: $N \in \{3, 5, 10, 20\}$ người tham gia.

3.2.Phân tích kết quả thực nghiệm

Thực nghiệm được tiến hành trên mô hình chữ ký ngưỡng Gaussian Threshold 3-of-5, gồm 5 người tham gia và yêu cầu tối thiểu 3 người ký để tạo chữ ký hợp lệ. Hệ thống sử dụng tham số phân phối Gaussian với σ = 261 và được đánh giá trên ba cấp độ an toàn của Dilithium (Level 2, 3, 5). Mỗi kịch bản được chạy 100 lần và lấy giá trị trung bình nhằm đảm bảo độ tin cậy thống kê.

3.2.1. Kích thước chữ ký và hiệu quả lưu trữ

Kết quả cho thấy chữ ký ngưỡng có kích thước lớn hơn chữ ký Dilithium đơn lẻ, nhưng không phụ thuộc vào số lượng người tham gia, duy trì đặc tính O(1).

Bảng 1.1: Kích thước chữ ký gộp

Cấp độ	Kích thước chữ ký	So với Dilithium chuẩn (~2.4 KB)
Level 2	9.03 KB	~3.7 lần
Level 3	11.28 KB	~3.5 lần
Level 5	14.28 KB	~3.1 lần

Phân tích: Sự gia tăng kích thước chủ yếu đến từ các thành phần đặc thù của ký ngưỡng gồm vector ngẫu nhiên *r* và cam kết *com*, vốn là yêu cầu bắt buộc trong giao thức Leevik et al. để đảm bảo tính an toàn.Mặc dù lớn hơn chữ ký đơn, chữ ký ngưỡng vẫn nhỏ hơn đáng kể so với việc lưu trữ nhiều chữ ký độc lập, và đặc biệt không tăng kích thước khi mở rộng số người tham gia. So với mô hình Ký độc lập (kích thước tăng tuyến tính), chữ ký ngưỡng có kích thước cố định. Với kích thước trung bình 2.4 KB/chữ ký đơn, chỉ cần nhóm ký có từ 4 người trở lên (KB), mô hình ký ngưỡng đã bắt đầu tiết kiệm dung lượng lưu trữ hơn. Đây là lợi thế lớn cho các ứng dụng Blockchain nơi phí lưu trữ (gas fee) rất đắt đỏ.

3.2.2. Hiệu năng tính toán

Bảng 3.2: Tổng quát thời gian giữa các quá trình

Cấp độ	KeyGen (DKG)	Signing	Verification
Level 2	0.118 s	0.070 s	0.006 s
Level 3	0.144 s	0.110 s	0.009 s
Level 5	0.207 s	0.158 s	0.016 s

Bảng 3.3: Phân rã thời gian thực thi giai đoạn Ký

Cấp độ An toàn	Thời gian Ký cục bộ ()	Thời gian Gộp ()	Tổng độ trễ ()	Thành phần phi tính toán (Network/Overhead)
Level 2	23 ms	2 ms	70 ms	~45 ms (64%)
Level 3	37 ms	2 ms	110 ms	~71 ms (64%)
Level 5	53 ms	3 ms	158 ms	~102 ms (65%)

Kết quả:

+ Ký: Thời gian tạo chữ ký dao động từ 70 ms đến 158 ms, nhanh hơn đáng kể so với các mô hình MPC truyền thống.
+ Xác minh: Thời gian xác minh rất thấp (6–16 ms), gần tương đương xác minh chữ ký đơn, giúp giảm tải cho bên xác thực.
+ DKG: Quá trình sinh khóa phân tán chỉ mất dưới 0.21 s, cho phép khởi tạo hệ thống gần như tức thời.

Phân tích:

+ Sự gia tăng đột biến trong mô hình Ký ngưỡng xuất phát từ cơ chế đồng bộ hóa Rejection Sampling, nếu một bên P_i tính toán ra vector không thỏa mãn điều kiện an toàn, quy trình phải khởi động lại (restart). Với n bên, xác suất để cả n bên cùng thành công trong một lần thử giảm mạnh theo hàm mũ ($P_{total} \approx p^n$). Do đó, số vòng lặp lại tăng lên, kéo theo độ trễ mạng tích lũy.
+ Ngược lại, ở mô hình Ký độc lập, các bên thực hiện Rejection Sampling cục bộ và độc lập. Bên P_1 làm lại không ảnh hưởng đến tiến độ của bên

P_2. Do đó, thời gian tổng chỉ phụ thuộc vào bên chậm nhất, không bị cộng dồn.

3.2.3. Phân tích cơ chế "Bí mật kép" (Dual Secrets)

Bảng 3.4: Trung bình các lần lặp từ chối

Tham số	Giá trị
Tỷ lệ chênh lệch x_i/s_i	~1.7×10^6
Số lần thử trung bình	5.5
Tỷ lệ chấp nhận	54.25%

Phân tích: Mảnh khóa Shamir $x_i$có giá trị rất lớn (~77 triệu), vượt xa biên an toàn chuẩn $B_{BOUND} \approx 14{,}173$. Nếu kiểm tra điều kiện an toàn trực tiếp trên x_i, chữ ký sẽ luôn bị từ chối. Việc tách riêng bí mật nhỏ s_iđể kiểm tra biên cho phép hệ thống vượt qua bước rejection sampling với xác suất thành công trên 50%, xác nhận tính đúng đắn và ổn định của cơ chế Dual Secrets.

3.2.4. Phân tích lưu lượng mạng

Bảng 3.5: Lưu lượng mạng

Cấp độ	Lưu lượng/User	Tổng lưu lượng
Level 2	9.03 KB	27.09 KB
Level 3	11.28 KB	33.84 KB
Level 5	14.28 KB	42.84 KB

Phân tích: Do phải truyền tải các tham số trung gian kích thước lớn của mật mã lưới (ma trận , vector , các cam kết , mảnh chia sẻ). Để tạo ra một chữ ký ngưỡng nhỏ gọn, hệ thống cần trao đổi lượng dữ liệu lớn hơn kích thước chữ ký cuối cùng, bao gồm các cam kết và chữ ký thành phần. Mức tiêu thụ băng thông này phù hợp với mạng Internet/LAN, nhưng cần cân nhắc tối ưu khi triển khai trên các hệ thống IoT băng thông thấp.

3.3.Thảo luận

Mô hình đề xuất đã giảm kích thước xuống còn 9.03 KB nhờ áp dụng kỹ thuật Bit-packing (nén các hệ số đa thức 32-bit xuống ~17-20 bit) theo chuẩn FIPS 204, giúp tiết kiệm băng thông và dung lượng lưu trữ đáng kể. (Theo nghiên cứu của

Leevik et al. là ~11.7 KB). Mặc dù chữ ký ngưỡng lớn hơn một chữ ký đơn lẻ (2.4 KB), nhưng nó thể hiện ưu thế vượt trội về lưu trữ khi số lượng người ký tăng lên. Với mô hình ký độc lập, dung lượng lưu trữ tăng tuyến tính; chỉ cần nhóm ký vượt quá 4 người (4*2.4KB), mô hình ký ngưỡng đã bắt đầu tiết kiệm không gian lưu trữ hơn,. Điều này đặc biệt có ý nghĩa đối với các ứng dụng Blockchain, nơi chi phí lưu trữ on-chain là cực kỳ đắt đỏ.

Thời gian để tạo ra một chữ ký ngưỡng khá lớn (70ms - 158ms) và chịu thêm ảnh hưởng bởi độ trễ mạng. Điều này khẳng định rằng điểm nghẽn của mật mã lưới phân tán không nằm ở tính toán CPU (vốn rất nhanh nhờ NTT) mà nằm ở sự phức tạp của giao thức tương tác (2 vòng) và đồng bộ hóa trạng thái. Đổi lại, bên xác thực chỉ cần tốn 6ms để kiểm tra một chữ ký ngưỡng duy nhất, thay vì phải tốn thời gian để kiểm tra từng chữ ký lẻ. Đây là lợi thế trong các hệ thống IoT hoặc xử lý giao dịch tần suất cao, việc chuyển gánh nặng tính toán cho bên ký là hợp lý.

Khả năng mở rộng (Scalability Assessment): Từ kết quả thực nghiệm, có thể phân loại khả năng ứng dụng của mô hình theo quy mô nhóm:

- Nhóm nhỏ (n=5): Hoạt động tối ưu. Thời gian tổng < 0.3s, băng thông thấp, tỷ lệ thành công cao. Phù hợp cho ví đa chữ ký hoặc phê duyệt văn bản cấp cao.
- Nhóm trung bình (n=10): Chấp nhận được. Thời gian < 1s, nhưng cần đường truyền mạng tốt để xử lý ~400KB dữ liệu. Phù hợp cho cơ chế đồng thuận nhóm nhỏ.
- Nhóm lớn (n=20): Gặp nút thắt cổ chai. Thời gian sinh khóa > 3s và tỷ lệ thành công vòng đầu < 1% đòi hỏi cơ chế thử lại phức tạp. Không khuyến nghị sử dụng trực tiếp mô hình này mà nên chuyển sang mô hình phân cấp hoặc chọn đại diện nhóm.

KẾT LUẬN

1. Tổng kết các kết quả đạt được

Đề án *"Nghiên cứu và đánh giá các mô hình ký số đa bên hậu lượng tử trên nền thuật toán CRYSTALS-Dilithium"* đã hoàn thành các mục tiêu đề ra:

- Về mặt lý thuyết: Hệ thống hóa thành công cơ sở lý thuyết về PQC và chữ ký ngưỡng, làm rõ các thách thức kỹ thuật của mật mã lưới trong môi trường phân tán.
- Về mặt kỹ thuật: Thiết kế và cài đặt hoàn thiện hệ thống Ký ngưỡng với khả năng tùy biến cao (t-of-n). Hệ thống đã giải quyết thành công các vấn đề khó như Rejection Sampling phân tán và đồng bộ hóa trạng thái ngẫu nhiên.
- Về mặt hiệu năng: Đạt được các chỉ số hiệu năng ấn tượng:
- Tốc độ: Ký ~23ms, Xác minh ~6ms.
- Kích thước: Chữ ký nhỏ gọn cố định ~11KB.
- Độ ổn định: Hoạt động tin cậy trong các bài kiểm tra tải cao.

2. Hạn chế của đề tài

Bên cạnh những thành quả đạt được, đề án vẫn còn tồn tại một số hạn chế cần khắc phục trong các nghiên cứu tiếp theo:

- Chi phí băng thông: Để đổi lấy sự tối ưu về lưu trữ, mô hình ký ngưỡng tiêu tốn lượng băng thông nội bộ khá lớn. Điều này có thể gây trở ngại khi triển khai trên các mạng diện rộng có độ trễ cao hoặc băng thông thấp.
- Nền tảng triển khai: Mã nguồn hiện tại được viết bằng Python để phục vụ mục đích kiểm thử ý tưởng. Mặc dù đã tối ưu hóa, nhưng hiệu năng chưa thể so sánh với các ngôn ngữ cấp thấp (như C/C++ hoặc Rust) trên các thiết bị phần cứng hạn chế tài nguyên.
- Môi trường thử nghiệm: Các kịch bản kiểm thử chủ yếu được thực hiện trong môi trường mạng giả lập lý tưởng, chưa đánh giá hết được các tác động của packet loss hay timeout trong môi trường mạng thực tế không ổn định.

3. Hướng phát triển trong tương lai

Dựa trên nền tảng vững chắc đã xây dựng, các hướng phát triển tiếp theo bao gồm:

- Tối ưu hóa giao thức truyền thông: Nghiên cứu áp dụng các kỹ thuật nén dữ liệu tiên tiến hoặc cải tiến giao thức để giảm số vòng tương tác và kích thước gói tin trao đổi, nhằm giảm thiểu chi phí băng thông.
- Triển khai trên thiết bị nhúng: Chuyển đổi mã nguồn sang ngôn ngữ Rust hoặc C để tích hợp vào các vi điều khiển, Smartcards hoặc thiết bị IoT, hướng tới các ứng dụng thực tế như ví phần cứng.
- Tích hợp vào Blockchain: Ứng dụng mô hình Ký ngưỡng linh hoạt ($t < n$) vào các nền tảng Blockchain (như Hyperledger Fabric hoặc Ethereum Layer 2) để giải quyết bài toán mở rộng quy mô và tiết kiệm phí lưu trữ (Gas cost).
- Nâng cao khả năng bảo mật: Nghiên cứu các biện pháp chống tấn công kênh kề đối với các thao tác lấy mẫu ngẫu nhiên trong môi trường phân tán.