ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

ĐÀO MẠNH HIỆP

NGHIÊN CỨU THIẾT KẾ BẢO MẬT THẺ RFID SỬ DỤNG MÃ HÓA ĐƯỜNG CONG ELLIPTIC

(Secure Lightweight RFID tag with Elliptic Curve Cryptography)

Ngành đào tạo: Kỹ thuật Điện tử
Mã số: 9520203

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT ĐIỆN TỬ

HÀ NỘI – 2025

Công trình được hoàn thành tại: Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội

Người hướng dẫn khoa học:

1. GS. TS Trần Xuân Tú
2. GS. TS Vincent Beroulle

Phản biện:.....

.....

Phản biện:.....

.....

Phản biện:.....

.....

Luận án sẽ được bảo vệ trước Hội đồng cấp Đại học Quốc gia chấm luận án tiến sĩ họp tại .....

vào hồi….. giờ…..ngày…..tháng…..năm……

Có thể tìm hiểu luận án tại:

- Thư viện Quốc gia Việt Nam
- Trung tâm Thông tin - Thư viện, Đại học Quốc gia Hà Nội

Lời mở đầu

Công nghệ nhận dạng tần số vô tuyến (RFID) đã tạo ra bước đột phá trong lĩnh vực xác thực không dây với nhiều ứng dụng từ quân sự đến thiết bị dân dụng. Trong hệ thống RFID tổng quát, tồn tại hai thành phần chính: thẻ và đầu đọc để xác thực. Tùy thuộc vào ứng dụng cụ thể, thẻ có thể sử dụng nguồn nuôi bên trong (thẻ RFID chủ động) hoặc thu năng lượng từ môi trường (thẻ RFID thụ động). Việc loại bỏ pin giúp thiết bị trở nên nhỏ gọn và tiết kiệm chi phí hơn. Do đó, thẻ RFID thụ động đóng vai trò quan trọng trong các ứng dụng cầm tay như hộ chiếu điện tử, thẻ dân sinh và thẻ thanh toán không tiếp xúc.

Mặc dù có vai trò quan trọng trong nhiều ứng dụng, đặc biệt là thiết bị xác thực bảo mật, thẻ RFID thụ động phải đối mặt với nhiều lỗ hổng bao gồm tấn công không dây và phần cứng. Để giảm thiểu các mối đe dọa này, việc tích hợp các cơ chế mật mã như Mật mã đường cong elliptic (ECC) vào thẻ RFID thụ động là yếu tố then chốt để bảo vệ dữ liệu. Tuy nhiên, triển khai ECC trên thẻ RFID thụ động đặt ra những thách thức đáng kể như sau:

1. **Hạn chế về tài nguyên vật lý:** Thẻ RFID thụ động chịu ràng buộc nghiêm ngặt về tiêu thụ năng lượng, diện tích và độ trễ. Do thiết bị thu thập năng lượng thông qua anten chỉnh lưu (rectenna), công suất hoạt động của thẻ bị giới hạn bởi hiệu suất chuyển đổi năng lượng. Ngoài ra, thời gian giao tiếp giữa thẻ và đầu đọc rất ngắn (theo tiêu chuẩn ISO/IEC-14443, dưới 20 ms), làm hạn chế nghiêm trọng nguồn năng lượng khả dụng. Đồng thời, việc thu nhỏ kích thước vật lý của thiết kế là yêu cầu cấp thiết để giảm chi phí sản xuất.

2. **Yêu cầu bảo mật:** Các biện pháp bảo vệ thẻ RFID thụ động trước tấn công không dây và tấn công phần cứng làm tăng độ phức tạp xử lý. Ở tầng giao thức, các biện pháp phòng thủ cho giao thức xác thực dựa trên ECC thường yêu cầu thêm các cơ chế bảo mật như bộ tạo số ngẫu nhiên, hàm băm và các phép toán nhân vô hướng. Hệ quả là chi phí triển khai hệ thống tăng đáng kể. Tại tầng thực thi phần cứng, các kỹ thuật che giấu hoặc

ngụy trang được thiết kế để chống lại tấn công kênh bên. Những kỹ thuật này đòi hỏi thêm tính toán trong quá trình xử lý để hạn chế rò rỉ thông tin. Do đó, chi phí thực thi phần cứng của hệ thống cũng gia tăng đáng kể.

Ngoài ra, quá trình triển khai giao thức xác thực dựa trên ECC trải dài qua nhiều tầng thiết kế (từ giao thức đến cơ chế bảo mật) với hàng loạt lựa chọn về sơ đồ truyền thông, thuật toán và kiến trúc. Điều này khiến không gian thiết kế của hệ thống xác thực sử dụng thuật toán mã hóa đường cong ECC trở nên cực kỳ phức tạp, làm tăng thời gian sản xuất và chi phí phát triển sản phẩm.

Để giải quyết các vấn đề trên, luận án này đề xuất một thiết kế phần cứng hiệu quả và phương pháp luận thiết kế mới. Các đóng góp chính bao gồm:

1. Đề xuất thiết kế mật mã đường cong elliptic chi phí thấp (BEC) cho thẻ RFID thụ động bằng phương pháp tiếp cận Top-down truyền thống.

2. Giới thiệu phương pháp luận đánh giá sớm EEMitM (Early Evaluation Meet-in-the-Middle) giúp đánh giá sớm các thiết kế tối ưu đa mục tiêu trong không gian thiết kế rộng. Ngoài ra, cơ chế ước lượng và đánh giá sớm khả năng rò rỉ kênh bên, cho phép dự đoán chi phí phần cứng và mức độ bảo mật từ giai đoạn đầu mà không cần triển khai vật lý toàn bộ hệ thống phần cứng cũng được đề xuất để giảm thời gian thiết kế sản xuất sản phẩm.

Chương 1

Hệ thống RFID và Các Vấn đề An ninh

Chương này trình bày các khái niệm tổng quan về hệ thống RFID và những thách thức của nó. Mục tiêu chính của nghiên cứu là triển khai thẻ RFID sử dụng thuật toán mã hóa đường cong elliptic (ECC) trong phần cứng. Các giải pháp hiện có cho thẻ RFID xác thực dựa trên ECC cũng được xem xét. Thông qua việc đánh giá các giải pháp này trong tài liệu nghiên cứu, chương này chỉ ra khoảng trống trong việc triển khai phần cứng cho các thẻ RFID thụ động dựa trên ECC. Bên cạnh đó, việc tìm kiếm một thiết kế phần cứng tối ưu cho thẻ RFID thụ động dựa trên ECC cân bằng giữa chi phí triển khai và mức độ bảo mật là hết sức cần thiết.

1.1 Khái niệm Tổng quan về Hệ thống RFID Thụ động An toàn

1.1.1 Hệ thống Xác thực bằng Tần số Vô tuyến

Một khái niệm có hệ thống về các hệ thống xác thực bằng tần số vô tuyến an toàn được trình bày trong phần này. Các thành phần chính của hệ thống xác thực bằng tần số vô tuyến cũng được trình bày trong Hình 1.1 trước khi minh họa quy trình xác thực giữa thẻ và đầu đọc.

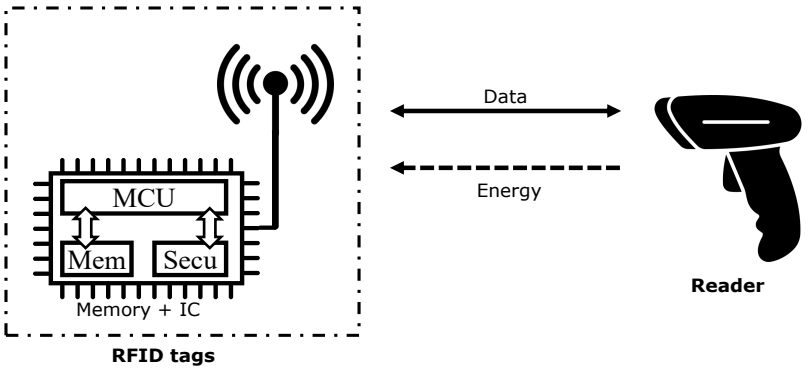
1.1.2 Thẻ Nhận dạng bằng Tần số Vô tuyến

Phần này đưa ra phân loại của hệ thống nhận dạng bằng tần số vô tuyến dựa trên cấu trúc của thẻ. Các lợi ích và hạn chế của từng loại thẻ RFID cũng được chỉ ra để làm nổi bật ưu điểm của thẻ RFID thụ động trong việc triển khai các ứng dụng hạn chế tài nguyên, chẳng hạn như quản lý hàng hóa bán lẻ hoặc thẻ thanh toán không tiếp xúc. Nhờ vào những lợi thế này, thị trường RFID toàn cầu được kỳ vọng sẽ phát triển nhanh chóng trong những thập kỷ tới.

1.2 Các Thách thức của Thẻ RFID Thụ động

1.2.1 Hạn chế về Chi phí Triển khai Phần cứng

Mặc dù hệ thống RFID đã phát triển đáng kể nhờ những lợi ích của nó, nhưng vẫn tồn tại một số nhược điểm. Phần này cung cấp cái nhìn



Hình 1.1: Hệ thống Xác thực Tổng quát bằng Tần số Vô tuyến

tổng quan ngắn gọn về thẻ RFID thụ động dưới góc độ chi phí triển khai, chẳng hạn như độ trễ và mức tiêu thụ điện năng.

1.2.2 Thách thức An ninh đối với Thẻ RFID Thụ động

Do thẻ RFID thụ động giao tiếp thông qua kênh không dây, chúng cũng phải đối mặt với nhiều mối đe dọa bảo mật khác nhau. Phần này giới thiệu các thách thức bảo mật đối với thẻ RFID thụ động dưới góc độ tấn công không dây và tấn công phần cứng. Nhìn chung, các mối đe dọa này khai thác các điểm yếu trong thuật toán xác thực hoặc cơ chế mã hóa để phá vỡ các đặc tính an ninh.

1.3 Các giải pháp bảo mật cho Thẻ RFID Thụ động

1.3.1 Giao thức Xác thực và Nhận dạng

Để bảo vệ dữ liệu người dùng, một số biện pháp đối phó cho thẻ RFID thụ động được triển khai ở các mức khác nhau trong hệ thống, từ các giao thức xác thực đến các nguyên thủy phần cứng bảo mật (Cryptography Primitives). Phần này giới thiệu ngắn gọn việc sử dụng các giao thức xác thực trong các ứng dụng RFID thụ động. Ngoài ra, các đặc điểm và chi phí triển khai của giao thức xác thực cũng được đề cập.

1.3.2 Các Cơ chế Mã hóa

Ở một mức độ khác trong triển khai biện pháp đối phó, các cơ chế mã hóa được sử dụng để mã hóa dữ liệu bằng khóa bí mật. Quá trình

này đảm bảo đặc tính toàn vẹn của hệ thống. Trong số các cơ chế mã hóa, mã hóa bất đối xứng như mã hóa đường cong elliptic (ECC) được đề xuất thay thế các phương pháp đối xứng nhờ lợi ích từ Bài toán Logarit Rời rạc.

Mặc dù ECC mang lại lợi thế về hiệu suất tính toán và hiệu quả năng lượng so với các thuật toán bất đối xứng khác trong triển khai phần cứng, nhưng vẫn gặp khó khăn trong việc đáp ứng các ràng buộc về chi phí và năng lượng của thiết bị, đặc biệt là các thẻ RFID thụ động. Tuy nhiên, việc tìm kiếm thiết kế phần cứng tối ưu cho thẻ RFID thụ động dựa trên ECC là một thách thức cho các nhà nghiên cứu nhằm cân bằng giữa mức độ bảo mật và chi phí triển khai.

Kết luận

Chương luận án này trình bày cái nhìn tổng quan về hệ thống RFID và những thách thức quan trọng của nó. Mục tiêu chính của nghiên cứu là triển khai giao thức xác thực dựa trên ECC trong phần cứng, nhằm cân bằng giữa các ràng buộc vật lý và yêu cầu về mức độ bảo mật.

Do không gian thiết kế của giao thức xác thực dựa trên ECC là cực kỳ lớn, việc tìm ra kiến trúc tối ưu để cân bằng giữa bảo mật và các ràng buộc vật lý là một thách thức đối với các nhà thiết kế. Các phương pháp thiết kế truyền thống chỉ cho phép đánh giá mức độ bảo mật sau giai đoạn thiết kế hoặc sau giai đoạn chế tạo. Hạn chế này thường đòi hỏi phải thực hiện tốn kém và mất nhiều thời gian để tìm được thiết kế tối ưu.

Để giải quyết hạn chế của các phương pháp thiết kế truyền thống, luận án này đề xuất một phương pháp luận thiết kế mới tích hợp đánh giá chi phí triển khai và tính bảo mật ngay từ những giai đoạn đầu trong chu trình phát triển hệ thống RFID thụ động dựa trên ECC.

Chương 2

Phương pháp thiết kế cho các thẻ RFID an toàn

Chương này trình bày tổng quan về các phương pháp thiết kế hiện có trong việc triển khai phần cứng an toàn, cùng với các phương pháp mới nổi dựa trên trí tuệ nhân tạo.

2.1 Cơ sở và Động lực nghiên cứu

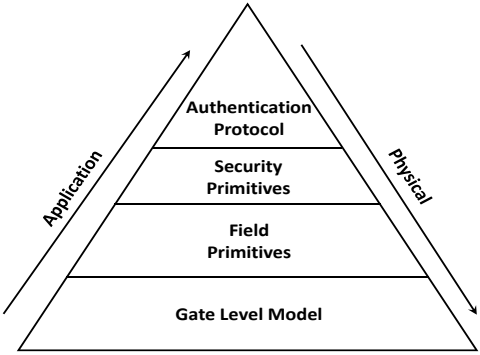
2.1.1 Định nghĩa về phương pháp thiết kế

Phần này trước tiên đưa ra định nghĩa về Phân tầng Hệ thống Điện tử (Electrical System Level - ESL), dùng để mô hình hóa và phân tích các hệ thống phức tạp dựa trên chức năng và kiến trúc của chúng. ESL của hệ thống RFID bao gồm bốn tầng, được minh họa trong Hình 2.1. ESL khởi tạo quá trình tìm kiếm trong Không gian Thiết kế (Design Space Exploration - DSE) nhằm xác định và đánh giá các phương án thiết kế khác nhau để tối ưu hóa hệ thống phần cứng. Thông qua việc áp dụng các phương pháp thiết kế, các nhà thiết kế nhận được một số lợi ích chính như sau:

- **Tạo mẫu nhanh**
- **Tối ưu hóa**
- **Tích hợp hệ thống**

2.1.2 Động lực nghiên cứu

Thông qua phân tích các phương pháp thiết kế phần cứng truyền thống và quy trình thiết kế bảo mật, luận án nhận thấy được các ràng buộc thiết kế trong hệ thống thẻ thụ động RFID sử dụng mã hóa đường cong ECC với đa mục tiêu làm tăng thời gian hoàn thiện sản phẩm. Cụ thể, khi không gian thiết kế mở rộng, hay nói cách khác DSE trở nên phức tạp hơn, số lần thử - sai trong thiết kế tăng lên đáng kể, kéo theo đó là chi phí và thời gian đưa sản phẩm ra thị trường cũng tăng theo.



Hình 2.1: Phân tầng các cấp độ triển khai trong thiết bị xác thực sử dụng ECC.

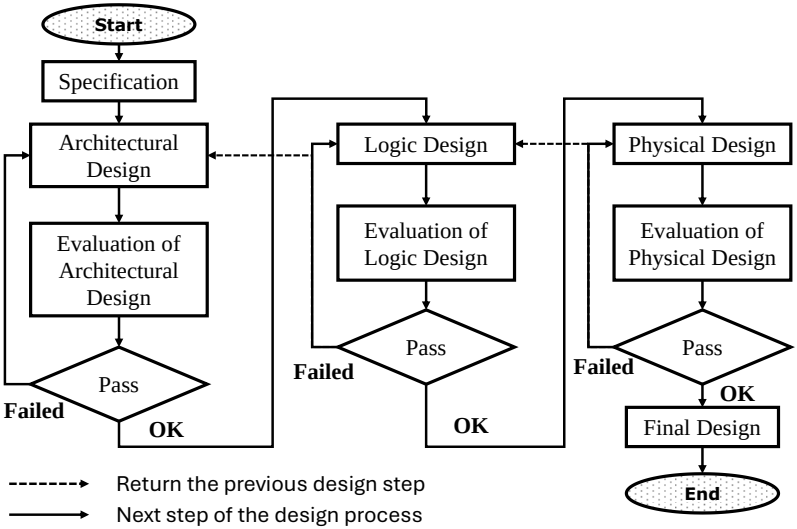
Nhận thấy khoảng trống này, luận án đề xuất một phương pháp thiết kế mới tích hợp cả đánh giá bảo mật và ước tính chi phí triển khai vào vòng lặp DSE nhằm rút ngắn thời gian nghiên cứu, phát triển, và hoàn thiện sản phẩm. Để chứng minh hiệu quả của phương pháp được đề xuất, chương này trước hết trình bày phân tích chi tiết các phương pháp thiết kế phần cứng truyền thống và tổng quan các phương pháp mới sử dụng trí tuệ nhân tạo.

2.2 Phương pháp thiết kế truyền thống cho triển khai phần cứng

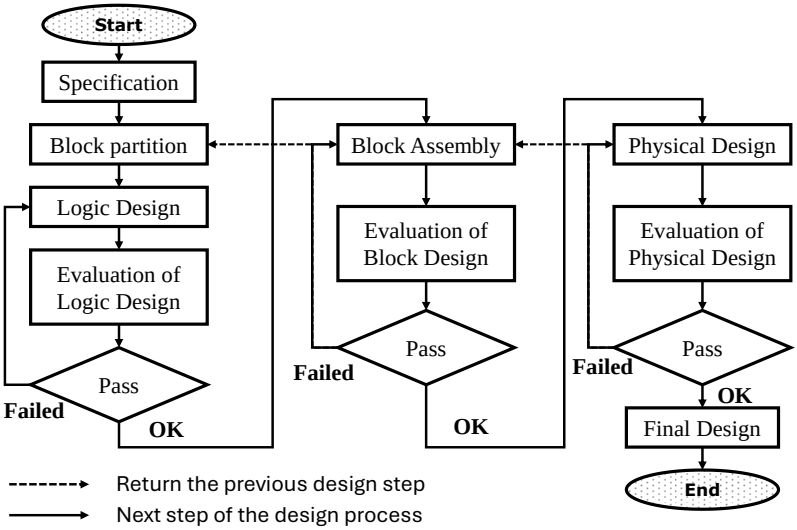
2.2.1 Quy trình thiết kế từ trên xuống (Top-down)

Trong thiết kế mạch số, đặc biệt là các ứng dụng mật mã như ECC, phương pháp thiết kế từ trên xuống là cách tiếp cận phổ biến và được áp dụng rộng rãi, như minh họa trong Hình 2.2.

Phần này trình bày những ưu và nhược điểm khi áp dụng phương pháp này trong thực tiễn. Hạn chế chính của phương pháp thiết kế từ trên xuống là độ chi tiết của kiến trúc các khối con chưa đủ ở giai đoạn đầu, khiến việc kiểm tra các ràng buộc quan trọng bị trì hoãn đến các giai đoạn sau. Ngoài ra, việc bổ sung các biện pháp đối phó vào cuối quy trình làm tăng chi phí triển khai. Trong một số trường hợp, việc thiết kế lại để đáp ứng yêu cầu bảo mật kéo dài thời gian hoàn thiện sản phẩm. Do đó, cần có sự đánh đổi hợp lý giữa bảo mật, chi phí và thời gian ra sản phẩm.



Hình 2.2: Phương pháp thiết kế theo hướng từ trên xuống trong thiết kế phần cứng.



Hình 2.4: Phương pháp thiết kế từ dưới lên trong thiết kế phần cứng.

2.2.2 Quy trình thiết kế từ dưới lên (Bottom-up)

Một phương pháp phổ biến khác là thiết kế theo hướng từ dưới lên, cho phép đánh giá cục bộ dễ dàng hơn, như thể hiện trong Hình 2.4.

Phần này cũng phân tích ưu và nhược điểm của phương pháp thiết kế từ dưới lên. Trước hết, việc tối ưu hóa từng khối nhỏ độc lập có thể dẫn đến tối ưu không đồng đều giữa các khối, phân tán các khối và làm lãng phí diện tích silicon. Thứ hai, sự phụ thuộc vào mô hình trừu tượng trong giai đoạn kết hợp có thể dẫn đến sai số, làm ảnh hưởng đến dự đoán ở cấp hệ thống. Thêm vào đó, việc mô phỏng toàn diện ở giai đoạn cuối trở nên không khả thi với các hệ thống phức tạp, như hệ thống xác thực sử dụng mật mã ECC.

2.2.3 Các phương pháp thiết kế mới dựa trên trí tuệ nhân tạo

Ứng dụng thành quả của lĩnh vực trí tuệ nhân tạo, các mô hình AI tạo sinh (generative AI) đóng vai trò then chốt trong việc hỗ trợ nhà thiết kế tối ưu hóa hệ thống phần cứng. Một số phương pháp thiết kế dựa trên AI được xem xét trong phần này, kèm theo những lợi ích và hạn chế của chúng.

2.3 Phương pháp thiết kế cho phần cứng bảo mật

Trong các ứng dụng cụ thể của thiết kế phần cứng, các bước bổ sung được tích hợp vào quy trình thiết kế, cho phép các nhà thiết kế đánh giá và điều chỉnh hệ thống sao cho phù hợp với các ràng buộc đặt ra. Phần này trình bày tổng quan về quy trình đánh giá bảo mật bổ sung trong thiết kế hệ thống xác thực sử dụng ECC, được xây dựng theo hướng thiết kế từ trên xuống.

2.3.1 Đánh giá bảo mật bổ sung trong phương pháp thiết kế

Đối với thiết kế phần cứng bảo mật, các nhà thiết kế sẽ tiến hành đánh giá các lỗ hổng bảo mật vào cuối quy trình thiết kế theo hướng từ trên xuống. Cách tiếp cận đầu tiên là sau khi sản xuất phần cứng, thực hiện các thử nghiệm để đo mức độ bảo mật của hệ thống. Ưu điểm lớn của phương pháp này là độ chính xác cao, nhưng nhược điểm chính là quy trình phức tạp, đòi hỏi hiệu chỉnh tín hiệu chính xác và đồng bộ hóa. Việc đạt được kết quả đáng tin cậy cần tài nguyên tính toán lớn

và chuyên môn sâu. Nếu đánh giá bảo mật thất bại, nhà thiết kế phải quay lại giai đoạn đầu, thiết kế lại hệ thống với các biện pháp bảo mật thay thế, gây ra hao tổn đáng kể chi phí và thời gian sản xuất.

Cách tiếp cận thứ hai là đánh giá bảo mật sau tổng hợp (post-synthesis). Mặc dù phương pháp này giúp giảm sự phụ thuộc vào các thử nghiệm hậu sản xuất tốn kém, nó vẫn gặp một số vấn đề. Đầu tiên là hạn chế của mô phỏng: các yếu tố như sai lệch quy trình, các giá trị điện ký sinh và nhiễu môi trường đều bị trừu tượng hóa, dẫn đến sự khác biệt giữa kết quả mô phỏng và thực tế. Ngoài ra, các vết công suất thu được nhờ quá trình mô phỏng hoạt động ở mức cổng (gate-level) gây ra vấn đề lưu trữ và thời gian xử lý. Do đó, đòi hỏi hệ thống đánh giá cần có bộ nhớ lớn và khả năng xử lý mạnh.

2.3.2 Đánh giá bảo mật cho thẻ RFID an toàn

Phần này nhấn mạnh các cách tiếp cận khác nhau để đánh giá bảo mật ở cả cấp độ giao thức và phần cứng. Ở cấp giao thức, việc đánh giá tập trung vào khả năng chống truy cập trái phép và khả năng chống lại các mối đe dọa qua sóng vô tuyến, đồng thời đảm bảo hiệu suất tối ưu của hệ thống. Ở cấp phần cứng, khả năng bị tấn công kênh kề (side-channel attacks – SCA) như phân tích công suất hoặc bức xạ điện từ được định lượng thông qua các công cụ như Test Vector Leakage Assessment hoặc Power Analysis.

Kết luận

Chương này của luận án đã tổng quan các phương pháp thiết kế hiện có trong triển khai phần cứng, trước khi trình bày kỹ thuật quy trình thiết kế trong các thẻ RFID an toàn. Các phương pháp luận thiết kế hiện tại được phân tích nhằm làm nổi bật cả ưu và nhược điểm. Nhìn chung, phần lớn các phương pháp đều gặp vấn đề về thời gian nghiên cứu, phát triển và hoàn thiện sản phẩm, ảnh hưởng lớn đến chi phí sản xuất. Ngoài ra, việc đưa các biện pháp bảo mật vào các giai đoạn cuối của thiết kế có nguy cơ dẫn đến các thỏa hiệp không tối ưu, hoặc phải thiết kế lại với chi phí cao hơn.

Những tiến bộ gần đây trong Khám phá Không gian Thiết kế tự động dựa trên AI (AI-based Automatic DSE) mang lại triển vọng giải quyết vấn đề này. Tuy nhiên, hầu hết vẫn xem bảo mật là một ràng buộc tĩnh thay vì là một tham số động cần được tối ưu đồng thời trong

quá trình thiết kế. Bằng cách phân tích những phương pháp hiện tại, chương này chỉ ra khoảng trống, nhấn mạnh nhu cầu thay đổi cách tiếp cận: tích hợp tối ưu hóa bảo mật cùng với chi phí thiết kế trong cùng một khuôn khổ DSE. Luận án này giải quyết hạn chế đó bằng cách đề xuất một phương pháp luận thiết kế mới tích hợp các ước lượng, đánh giá bảo mật theo thời gian thực và ước lượng chi phí triển khai trực tiếp vào vòng lặp DSE, sẽ được trình bày chi tiết hơn trong Chương 4.

Chương 3

Triển khai phần cứng cho Mật mã đường cong elliptic

Việc thiết kế một phần cứng cân bằng, thỏa hiệp giữa chi phí triển khai và mức độ an toàn trước các cuộc tấn công không dây và tấn công phần cứng, là một thách thức lớn đối với các nhà thiết kế khi triển khai bằng cách áp dụng các phương pháp thiết kế đã trình bày trong Chương 1. Trong chương này, chúng tôi đề xuất một phần cứng chi phí thấp, tiêu thụ điện năng thấp thực thi Mật mã đường cong elliptic (ECC) bằng cách sử dụng phương pháp thiết kế từ trên xuống.

3.1 Các công trình liên quan

3.1.1 Tối ưu hóa chi phí triển khai cho ECC

Phần này của luận án trình bày tổng quan các phương pháp hiện đại nhằm tối ưu hóa chi phí triển khai của ECC. Các phương pháp được xem xét bao gồm lựa chọn các đường cong nhẹ, sử dụng trường nhị phân $GF(2^m)$, ánh xạ tọa độ, và lựa chọn các toán tử trường dựa trên cơ sở Gaussian hoặc cơ sở đa thức. Các phương pháp này được đưa ra nhằm làm nổi bật cả ưu điểm và hạn chế, từ đó chỉ ra khoảng trống nghiên cứu còn tồn tại.

3.1.2 Cải thiện khả năng chống tấn công kênh kề (SCA) trong ECC

Trong ECC, phép nhân điểm bao gồm việc lặp đi lặp lại phép cộng điểm theo sau bởi phép nhân đôi điểm hoặc chỉ thực thi phép nhân đôi điểm, tùy thuộc vào giá trị bit tương ứng của khóa mật mã. Do đó, khi triển khai ECC trên phần cứng, hệ thống có nguy cơ bị tấn công kênh kề (SCA). Để giảm thiểu các lỗ hổng này, nhiều biện pháp đã được đề xuất trong tài liệu, từ việc lựa chọn đường cong đầy đủ hay các kỹ thuật che giấu và sử dụng mặt nạ cho thuật toán nhân điểm. Các phương pháp tiếp cận này cũng được xem xét trong chương này để nhấn mạnh đến hạn chế là làm gia tăng đáng kể chi phí triển khai. Do đó, mục này của luận án chỉ ra một cách khái quát khoảng trống trong nghiên cứu

liên quan đến triển khai các hệ thống xác thực sử dụng thuật toán mã hóa ECC trên phần cứng cho các thẻ RFID thụ động – vốn yêu cầu sự cân bằng giữa chi phí triển khai phần cứng và mức độ bảo mật.

3.2 Thuật toán đề xuất sử dụng Đường cong Edwards Nhị phân

Nhằm giải quyết khoảng trống đã nêu, phần này của luận án trình bày thuật toán đề xuất cho Đường cong Edwards Nhị phân (BEC).

3.2.1 Tọa độ xạ ảnh ω trong BEC

Nhằm mục tiêu tối ưu hóa chi phí triển khai của BEC, phần này trình bày giải pháp chuỗi cộng sai phân (Differential Addition Chain). Phương pháp này được phân tích để làm rõ độ phức tạp trong việc thực thi quá trình truy xuất các giá trị tọa độ Affine (x_Q, y_Q) từ các tọa độ sai phân ω. Do đó, nhấn mạnh tới nhược điểm về việc tiêu tốn đáng kể chi phí triển khai. Từ đó, thúc đẩy đề xuất đầu tiên trong chương này là chuyển toàn bộ quy trình truy xuất các giá trị tọa độ Affine từ tọa độ sai phân sang xử lý tại máy chủ hoặc đầu đọc nhằm giảm chi phí triển khai cho thẻ RFID thụ động.

3.2.2 Các toán tử điểm đề xuất sử dụng tọa độ xạ ảnh ω trong BEC

Để giảm thiểu chi phí thực thi hơn nữa, đề xuất thứ hai là thay thế các toán tử thông thường bằng công thức phương trình (3.1).

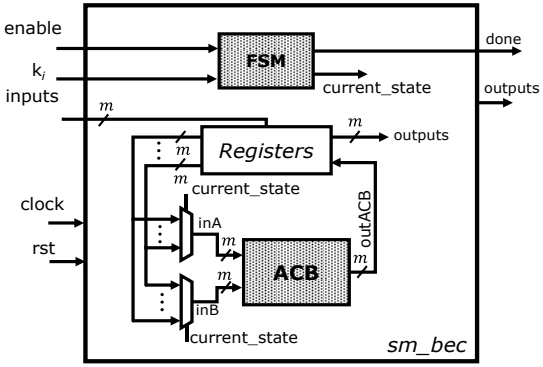
$$\begin{aligned} \frac{W_3}{Z_3} &= \frac{C + \frac{1}{\omega_0} \cdot C}{(Z_1 Z_2)^2 + \frac{1}{\omega_0} \cdot C} \\ \frac{W_4}{Z_4} &= \frac{A}{d \cdot (Z_1 \cdot Z_1)^2 + A} \end{aligned} \tag{3.1}$$

Đề xuất này giúp giảm thiểu số lượng các thanh ghi, từ đó, giảm đáng kể công suất tiêu thụ động trên các phần tử nhớ.

3.3 Kiến trúc phần cứng đề xuất cho Đường cong Edwards Nhị phân

3.3.1 Kiến trúc hệ thống BEC đề xuất

Mục này trình bày đề xuất thứ ba trong chương bằng một kiến trúc hệ thống của BEC chi phí thấp, tiêu thụ năng lượng thấp như minh họa trong Hình 3.2. Mô tả chi tiết về đề xuất thứ ba này sẽ làm rõ Khối



Hình 3.2: Kiến trúc đề xuất chi phí thấp, công suất thấp của Đường cong Edwards Nhị phân sử dụng xử lý nối tiếp bit.

tính toán số học được đề xuất.

3.3.2 Khối tính toán số học đề xuất

Một khối tích hợp tính toán số học (ACB) được đề xuất để xử lý phép nhân trường và phép bình phương trường ngay lập tức, như minh họa trong Hình 3.5, thực thi phép toán điểm trong đề xuất thứ hai nhằm giảm thiểu số lượng thanh ghi. Mô tả chi tiết về khối ACB đề xuất sẽ được trình bày trong phần này.

3.4 Kết quả triển khai phần cứng

3.4.1 Thiết lập thí nghiệm

Phần này trình bày việc triển khai thiết kế kiến trúc BEC đề xuất. Chi phí triển khai và các đặc tính bảo mật của thiết kế BEC cũng sẽ được trình bày và thảo luận nhằm minh họa điều kiện thử nghiệm.

3.4.2 Kết quả triển khai phần cứng

Các thử nghiệm được thực hiện bằng các công cụ Thiết kế Tự động Hóa Điện tử (EDA) của Synopsys như Design Compiler và Prime-Time với công nghệ CMOS 65nm từ TSMC. Tần số hoạt động từ $10MHz$ đến $0.4MHz$ cho thấy mức tiêu thụ năng lượng tương ứng là $4.66\mu W$@$0.4MHz$. Hiệu suất cao nhất của đề xuất cũng đáp ứng tốt yêu cầu của thẻ RFID thụ động với độ trễ $19.05ms$@$10MHz$.

3.4.3 Đánh giá bảo mật

Về đánh giá bảo mật, việc triển khai phần cứng được kiểm định bằng bài kiểm tra TVLA. Tuy nhiên, rò rỉ tối đa được đo là 3.36, nhỏ hơn ngưỡng tiêu chuẩn 4.5. Do đó, thiết kế đề xuất được xem là an toàn trước các cuộc tấn công kênh kề.

Kết luận

Phần này của luận án đề xuất kiến trúc chi phí thấp, tiêu thụ điện năng thấp với thuật toán nhân điểm BEC đã được điều chỉnh. Những đóng góp chính của chương này bao gồm:

- **Loại bỏ bước truy xuất tọa độ affine**.
- **Đề xuất các toán tử trường**.
- **Đề xuất kiến trúc BEC cùng với khối tính toán số học (ACB)**.

Theo kết quả tổng hợp sử dụng thư viện công nghệ CMOS 65nm của TSMC, kiến trúc BEC đề xuất cung cấp một thiết kế chi phí thấp, tiêu thụ điện năng thấp và có tính bảo mật cao trước các mối đe dọa SCA. Tuy nhiên, việc áp dụng phương pháp thiết kế từ trên xuống truyền thống khiến thời gian hoàn thiện sản phẩm bị kéo dài do việc chọn thiết kế bị lặp đi lặp lại. Bên cạnh đó, việc bổ sung muộn các biện pháp bảo mật khiến các người thiết kế không thể cân nhắc đồng thời cả yếu tố bảo mật và chi phí triển khai ngay từ giai đoạn đầu của quá trình thiết kế.

Chương 4

Phương pháp thiết kế đánh giá sớm được đề xuất

4.1 Giới thiệu

Mục này đề cập đến thách thức về thời gian nghiên cứu, phát triển, và hoàn thiện sản phẩm trong quy trình thiết kế VLSI, đặc biệt là đối với phần cứng bảo mật. Đối với các phương pháp thiết kế truyền thống, việc xem nhẹ các yếu tố bảo mật, dẫn đến khó khăn trong việc cân bằng giữa yêu cầu bảo mật và chi phí triển khai. Do đó, chương này đề xuất một phương pháp luận thiết kế mới nhằm giải quyết vấn đề này.

4.2 Phương pháp thiết kế đánh giá sớm được đề xuất

4.2.1 Quy trình thiết kế đánh giá sớm Meet-in-the-Middle (EEMitM

Quy trình thiết kế đề xuất Early Evaluation Meet-in-the-Middle (EEMitM) được đề xuất trong mục này nhằm giải quyết các bài toán nghiên cứu đã đề ra như được mô tả trong Hình 4.1. Phần này trình bày tổng quan về phương pháp luận thiết kế được đề xuất.

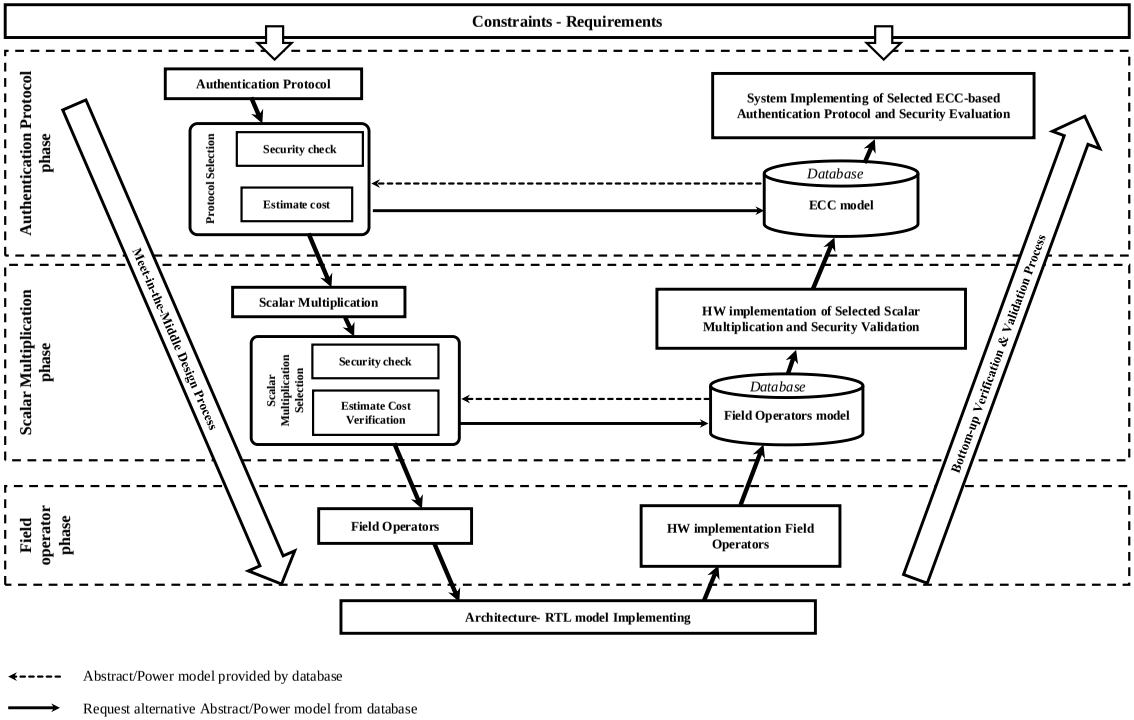
4.2.2 Quy trình xác minh và kiểm định từ dưới lên

Phần này của luận án mô tả Quy trình xác minh và kiểm định từ dưới lên (B2VP) được đề xuất nhằm xác thực việc triển khai phần cứng của các toán tử trường và các cơ chế bảo mật nền tảng.

4.3 Phương pháp sinh dấu vết tiêu thụ năng lượng giả định được đề xuất

4.3.1 Phân tích tiêu thụ năng lượng

Trong đề xuất thứ ba của chương này, một phương pháp ước lượng và đánh giá bảo mật mới, sử dụng khung thiết kế EEMitM, được giới thiệu trong phần này để đánh giá mức rò rỉ của hệ thống. Một phân tích lý thuyết về tiêu thụ năng lượng hệ thống được trình bày để làm rõ cơ chế ước lượng được đề xuất.



Hình 4.1: Phương pháp thiết kế đánh giá sớm được đề xuất.

4.3.2 Mô hình tiêu thụ năng lượng có hệ thống

Phần này trình bày phương pháp tiếp cận nhằm ước lượng dấu vết tiêu thụ năng lượng giả định cho các nguyên thủy mã hóa mà không cần tiến hành đo lường vật lý phức tạp. Hai phương pháp được đề xuất như sau:

- **Tạo thành dựa trên các dấu vết con của từng khối chức năng thành phần**.
- **Tạo thành như một hàm của hoạt động chuyển mạch (switching activity)**.

4.4 Kết quả đánh giá

4.4.1 Thiết lập thực nghiệm

Để đánh giá độ chính xác và hiệu quả của phương pháp thiết kế EEMitM được đề xuất, nhiều thí nghiệm đã được thực hiện nhằm định lượng các chỉ số chi phí triển khai, mức độ bảo mật và hiệu suất thời gian đưa vào sản xuất của cả phương pháp được đề xuất và phương pháp thiết kế truyền thống. Các thiết lập về điều kiện thực nghiệm bao gồm việc áp dụng cả hai phương pháp cho việc thiết kế các giao thức xác thực dựa trên ECC dưới các ràng buộc giống nhau, như minh họa trong Hình 4.14.

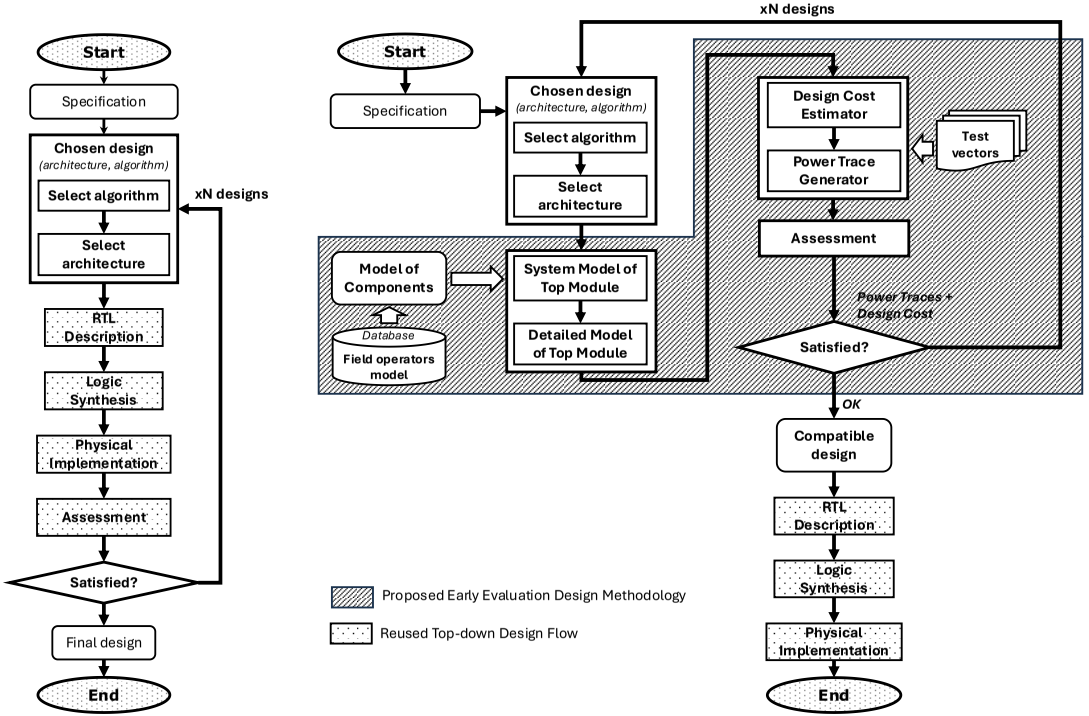
4.4.2 Kết quả thực nghiệm cho giai đoạn thiết kế và đánh giá giao thức

Mục này trình bày về việc đánh giá phần cứng ECC chi phí và năng lượng thấp cho các giao thức xác thực. Thông qua kết quả đánh giá, các giải pháp hiện tại không đáp ứng được yêu cầu về độ trễ đối với thẻ RFID thụ động. Bên cạnh đó, kết quả cũng chỉ ra ràng buộc về mặt phần cứng đối với giai đoạn thiết kế cơ chế bảo mật kế tiếp.

4.4.3 Kết quả thực nghiệm cho thiết kế và đánh giá cơ chế bảo mật

Sau khi hoàn thành giai đoạn thiết kế giao thức, giai đoạn thiết kế cơ chế bảo mật được tiến hành để tiếp tục tối ưu hóa trong phạm vi tài nguyên đã xác định. Kết quả đánh giá cho thấy kiến trúc sử dụng hai phần tử xử lý (PEs) mang lại điểm số $APT2$ cao hơn, cho thấy sự cân

bằng tối ưu hơn giữa chi phí và hiệu năng, mặc dù có sự gia tăng sử dụng tài nguyên.



(a) Các luồng thiết kế từ trên (b) Phương pháp đề xuất cho thiết kế đánh giá sớm cho việc triển khai xuống thông thường để triển phần cứng.
khai phần cứng.

Hình 4.14: Phương pháp đánh giá hiệu quả thực hiện phương pháp đề xuất so sánh với các luồng thiết kế thông thường.

Về độ chính xác của cơ chế ước lượng, phương pháp được đề xuất cho kết quả khớp hoàn toàn với kết quả của công cụ EDA sử dụng phương pháp thiết kế truyền thống, với tỉ lệ giống nhau là 1.75 và sai số nhỏ: 1.2% đối với kiến trúc đơn và 1.1% đối với kiến trúc kép. Nhìn chung, kết quả ước lượng có mối tương quan mạnh với kết quả của công cụ EDA, đặc biệt đối với các chỉ số diện tích và độ trễ, khẳng định hiệu quả của phương pháp ước lượng được đề xuất. Bên cạnh đó, các đo lường về mặt thời gian thiết kế giữa phương pháp truyền thống và phương pháp đề xuất cho thấy một sự cải thiện đáng kể. Bằng cách sử dụng phương pháp luận thiết kế đề xuất, thời gian thiết kế giảm tới 480 lần so với sử dụng phương pháp truyền thống. Cụ thể, lợi ích về mặt thời gian đem lại trong điều kiện giả định được rút ngắn từ 66 ngày xuống còn 3 giờ thiết kế. Lợi ích này đem lại nhiều tiềm năng để rút ngắn quá trình nghiên cứu và phát triển sản phẩm, từ đó, giảm giá thành sản phẩm.

Kết luận

Bằng cách sử dụng phương pháp thiết kế sáng tạo được đề xuất, quá trình ước lượng và đánh giá được thực hiện trong phần mềm với cơ sở dữ liệu đã xác định trong khoảng thời gian $T_{SW} << T_{HW}$. Sau khi hoàn tất đánh giá, thiết kế tối ưu sẽ được triển khai trên phần cứng trong khoảng thời gian T_{HW}. Tổng thời gian đưa vào sản phẩm khi sử dụng phương pháp EEMitM được tính là $N \cdot T_{SW} + T_{HW}$.

Về độ chính xác của ước lượng, đề xuất đạt độ sai số rất nhỏ: chỉ 1.2% đối với độ trễ. Trong trường hợp xấu nhất của ước lượng công suất tiêu thụ, sai số vẫn ở mức chấp nhận được là 22.6%.

Kết luận và Hướng phát triển tương lai

Với ưu điểm nổi bật về chi phí thấp và công suất tiêu thụ thấp, các thẻ RFID thụ động dựa trên ECC đã trở thành một phần không thể thiếu trong cuộc sống, từ ứng dụng dân sự đến quân sự, có ảnh hưởng đáng kể đến đời sống hằng ngày của con người. Tuy nhiên, những nỗ lực gần đây vẫn còn tồn tại các hạn chế sau:

- Các cách tiếp cận truyền thống thường xem bảo mật như một yếu tố phụ, được thêm vào ở giai đoạn thiết kế cuối cùng thay vì cân nhắc ngay từ đầu. Điều này dẫn đến khả năng tạo ra các giải pháp ECC không an toàn và tốn kém.

- Do không gian thiết kế rất lớn, phương pháp thiết kế truyền thống dựa trên thử-sai để tìm ra thiết kế tối ưu, dẫn đến chi phí thời gian đưa vào sản phẩm rất cao.

Nhằm khắc phục những điểm yếu nêu trên, mục tiêu cuối cùng của nghiên cứu này là đề xuất một thiết kế hệ thống xác thực ECC hoàn chỉnh chi phí thấp và công suất thấp. Bên cạnh đó, nhằm giải quyết các tồn tại của các phương pháp luận thiết kế truyền thống, nghiên cứu cũng đề xuất một phương pháp thiết kế mới cho phép người dùng ước lượng, đánh giá và lựa chọn nhanh chóng các cấu hình hệ thống tốt nhất cho việc triển khai phần cứng. Kết quả là giúp tiết kiệm đáng kể thời gian đưa vào sản phẩm. Các đóng góp chính của nghiên cứu được tóm tắt như sau:

1. Một kiến trúc phần cứng BEC tiết kiệm chi phí và tiêu thụ điện năng thấp với quy mô 21,68 $kGates$ logic đã được đề xuất và tổng hợp bằng công nghệ CMOS TSMC 65nm, theo phương pháp thiết kế Top-down truyền thống. Cấu trúc phần cứng đề xuất tiêu thụ công suất $126\mu W$ tại $10MHz$, được ước tính bằng công cụ Synopsys PrimeTime. Kết quả triển khai phần cứng cho thấy hệ thống đề xuất của chúng tôi hiệu quả về mặt chi phí triển khai và tiêu thụ năng lượng khi so sánh với các công trình khác. Bên cạnh đó, đánh giá TVLA chứng minh rằng đề xuất có khả năng

chống lại các lỗ hổng kênh bên. Những kết quả này đã được công bố trong [C1].

2. Để giải quyết vấn đề thời gian đưa sản phẩm ra thị trường, chúng tôi đã đề xuất phương pháp thiết kế Early Evaluation MitM. Bằng cách sử dụng cơ sở dữ liệu của các nguyên thủ bảo mật tham chiếu, các nhà thiết kế có thể mô hình hóa hệ thống được chọn mà không cần tạo nguyên mẫu. Khung làm việc được đề xuất cho phép mô hình hóa nhanh chóng trong môi trường phần mềm, từ đó giảm đáng kể thời gian đưa sản phẩm ra thị trường. Các thí nghiệm cho thấy, khi áp dụng đề xuất này, thời gian phát triển sản phẩm giảm 480 lần so với quy trình thiết kế truyền thống. Về độ chính xác trong việc ước lượng chi phí triển khai, các thí nghiệm cho thấy sai số về độ trễ chỉ 1,2%. Trong trường hợp ước lượng tiêu thụ điện năng kém nhất, độ chính xác vẫn duy trì ở mức sai số chấp nhận được là 22,6%. Những nội dung này đã được công bố trong [C2, C3, P1] và được trình bày một phần trong [J1].

Mặc dù nghiên cứu này đã giải quyết được một số thách thức then chốt trong việc khám phá không gian thiết kế cho các giao thức xác thực dựa trên ECC dành cho thẻ RFID thụ động, vẫn còn nhiều hướng nghiên cứu mở có thể tiếp tục phát triển. Để nâng cao lĩnh vực này, các hướng nghiên cứu tiếp theo sau được đề xuất:

1. **Đánh giá tính bảo mật của phần cứng đề xuất BEC trước kỹ thuật tấn công phần cứng như CPA hoặc DPA**.

2. **Phát triển các công cụ EDA thương mại tích hợp phương pháp thiết kế EEMitM được đề xuất**.

3. **Mở rộng cơ sở dữ liệu ứng dụng đặc thù (Application-Specific Database)**.

Danh sách công trình, công bố

Danh sách công trình, công bố liên quan tới luận án

C1 **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, Xuan-Tu Tran, and Duy-Hieu Bui. "Low-cost Low-Power Implementation of Binary Edwards Curve for Secure Passive RFID Tags."In 2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), pp. 494-500. IEEE, 2023.

C2 **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, and Xuan-Tu Tran. "How to Develop ECC-Based Low-Cost RFID Tags Robust Against Side-Channel Attacks."In International Conference on Industrial Networks and Intelligent Systems, pp. 433-447. Cham: Springer International Publishing, 2021.

C3 **Manh-Hiep Dao**, Vincent Beroulle, Yann Kieffer, and Xuan-Tu Tran (2023). Secure-by-Design methodology using Meet-in-the-Middle design flow for hardware implementations of ECC-based passive RFID tags. In ICWMC 2023, The Nineteenth International Conference on Wireless and Mobile Communications. IARIA (pp. 14-19).

J1 Souhir Gabsi, Vincent Beroulle, Yann Kieffer, **Manh-Hiep Dao**, Yassin Kortli, and Belgacem Hamdi. "Survey: Vulnerability analysis of low-cost ECC-based RFID protocols against wireless and side-channel attacks."Sensors 21, no. 17 (2021): 5824. (**SCIE, Q2**).

P1 **Đào Mạnh Hiệp**(2023), "Quy trình thiết kế phần cứng bảo mật cân bằng giữa chi phí thực thi và mức độ bảo mật" (VN Patent No. 1-2023-06893) (*Accepted*)

Danh sách công trình, công bố trong thời gian thực hiện luận án

J2 **Manh-Hiep Dao**, Koichiro Ishibashi, The-Anh Nguyen, Duy-Hieu Bui, Hiroshi Hirayma, Tuan-Anh Tran, and Xuan-Tu Tran. "Low-cost, High Accuracy, and Long Communication Range Energy-

Harvesting Beat Sensor with LoRa and Ω-Antenna for Water-Level Monitoring."IEEE Sensors Journal (2025). (**SCIE, Q1**).