HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Hoàng Mạnh Thắng

NGHIÊN CỨU HỆ MẬT HẠNG NHẸ TRÊN VÀNH ĐA THỨC ỨNG DỤNG VÀO THIẾT BỊ CÓ TÀI NGUYÊN HẠN CHẾ

Chuyên ngành: Kỹ thuật điện tử

Mã số: 9.52.02.03

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT ĐIỆN TỬ

Hà Nội - 2023

Công trình được hoàn thành tại:

Học viện Công nghệ Bưu chính Viễn thông

Người hướng dẫn khoa học:

1. GS.TS. Nguyễn Bình

Phản biện 1:……

Phản biện 2:……

Phản biện 3……

Luận án được bảo vệ trước Hội đồng chấm luận cấp Học viện họp tại:

Học viện Công nghệ Bưu chính Viễn thông

Vào hồi giờ ngày tháng năm

Có thể tìm hiểu luận án tại:

Thư viện Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Mật mã hạng nhẹ đang trở thành một lĩnh vực quan trọng trong lĩnh vực bảo mật thông tin. Với sự phát triển nhanh chóng của IoT(Internet of Things) và các thiết bị di động, yêu cầu về bảo mật thông tin trên các thiết bị có tài nguyên hạn chế ngày càng tăng cao. Tuy nhiên, các thuật toán và giao thức mật mã truyền thống thường không phù hợp với các thiết bị nhỏ gọn và có tài nguyên hạn chế do yêu cầu tính toán cao và sử dụng tài nguyên lớn. Do đó, cần có sự nghiên cứu và phát triển các thuật toán và giao thức mật mã hạng nhẹ để đáp ứng yêu cầu này.

Vành đa thức cung cấp một cấu trúc toán học mạnh mẽ và linh hoạt, cho phép các phép toán nhân, cộng, trừ và chia trên các đa thức được thực hiện nhanh chóng. Điều này dẫn đến hiệu suất tính toán cao, có tiềm năng ứng dụng trên các thiết bị có tài nguyên hạn chế.

Nghiên cứu mật mã hạng nhẹ trên vành đa thức đã và đang được các nhà khoa học mật mã quan tâm.

Mục tiêu và phạm vi nghiên cứu

Mục tiêu chính của luận án là xây dựng được các hệ mật hạng nhẹ trên vành đa thức. Nghiên cứu tập trung vào các câu hỏi nghiên cứu sau:

- Câu hỏi 1: Làm rõ tiềm năng ứng dụng của vành đa thức trong xây dựng các hệ mật hạng nhẹ, hiện trạng và các định hướng nghiên cứu?
- Câu hỏi 2: Ứng dụng vành đa thức để xây dựng một hệ mật hạng nhẹ mới?
- Câu hỏi 3: Ứng dụng vành đa thức để cải tiến hệ mật thông thường thành hệ mật hạng nhẹ?

Phạm vi nghiên cứu bao gồm việc xem xét các phương pháp và công nghệ liên quan đến ứng dụng vành đa thức trong mật mã hạng nhẹ, đề xuất và phát triển các hệ mật mã hạng nhẹ mới, cũng như đánh giá về hiệu suất và tính bảo mật của chúng.

Ý nghĩa khoa học và thực tiễn của luận án

Về mặt khoa học, kết quả nghiên cứu của luận án góp phần khẳng định vai trò của vành đa thức trong mật mã, đã đóng góp thêm được hai hệ mật mới và gia tăng độ an toàn của một hệ mật trên vành đa thức, đã tổng quát hóa được phương pháp ứng dụng vành đa thức để cải tiến các hệ mật thông thường thành các hệ mật có tài nguyên hạn chế, cụ thể các đóng góp của luận án gồm:

- Về mặt phương pháp xây dựng hệ mật:
    - Bốn phương pháp sử dụng vành đa thức để thêm tính xác thực vào hệ mật khóa công khai.
    - Tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường hữu hạn $GF(p)$ và phương pháp cải tiến hệ mật trên trường số thành hệ mật trên vành đa thức.
- Về xây dựng các hệ mật mới:
    - CBC-QRHE, hệ mật mã lai ghép trên vành đa thức có khả năng chống lại tấn công bản rõ chọn trước CPA và có tiềm năng ứng dụng trong thiết bị có tài nguyên hạn chế.
    - OM-CA, hệ mật OMURA-MASSEY trên vành đa thức hai lớp kề Cyclic có khả năng xác thực.
    - OM-PI, hệ mật OMURA-MASSEY trên vành đa thức hai lũy đẳng nguyên thủy.

Về mặt thực tiễn, thông qua việc thử nghiệm cài đặt và đánh giá hệ mật trên thiết bị Arduino, kết quả đề tài đã đóng góp vào sự phát triển công nghệ trong lĩnh vực an ninh thông tin, mật mã học, IoT và hệ thống nhúng.

Bố cục của luận án

Luận án được trình bày trong 4 chương. ***Chương 1*** trình bày ngắn gọn các lý thuyết nền tảng toán học và vành đa thức cũng như các khái niệm, định nghĩa về mật mã hạng nhẹ, phân loại mật mã hạng nhẹ, phân tích, đánh giá các hệ mật mã hạng nhẹ phổ biến hiện nay, từ đó rút ra đặc điểm của mật mã hạng nhẹ. Đồng thời nghiên cứu, đánh giá một số mật mã hạng nhẹ điển hình trên vành đa thức, cũng như các phương pháp nghiên cứu, đánh giá các hệ mật này, từ đó phát biểu bài toán cần giải và phương pháp nghiên cứu để giải bài toán đặt ra. ***Chương 2*** tập trung trả lời câu hỏi nghiên cứu 2 về việc ứng dụng vành đa thức để cải tiến độ an toàn của hệ mật, kết quả đã xây dựng được hệ mật CBC-QRHE có khả năng chống lại tấn công bằng bản rõ chọn trước. Ngoài ra, chương này cũng đã hệ thống hóa các cải tiến từ một hệ mật mã nguyên thủy thành các hệ mật trên vành đa thức, chứng minh độ an toàn về mặt lý thuyết cũng như cài đặt và đánh giá trên thiết bị thực tế. ***Chương 3*** tập trung trả lời câu hỏi nghiên cứu 3 về việc ứng dụng vành đa thức để cải tiến hệ mật phổ biến trên vành số thành hệ mật mã hạng nhẹ, đặc biệt, đã chứng minh được tính chất tựa đẳng cấu giữa trường số và vành đa thức đặc biệt, từ đó mở ra hướng nghiên cứu, phát triển các hệ mật mới trên vành đa thức tương tự như trên trường số. Cuối cùng, ***Kết luận t***ổng hợp đánh giá các kết quả đạt được của luận án đồng thời xác định các hướng nghiên cứu tiếp theo.

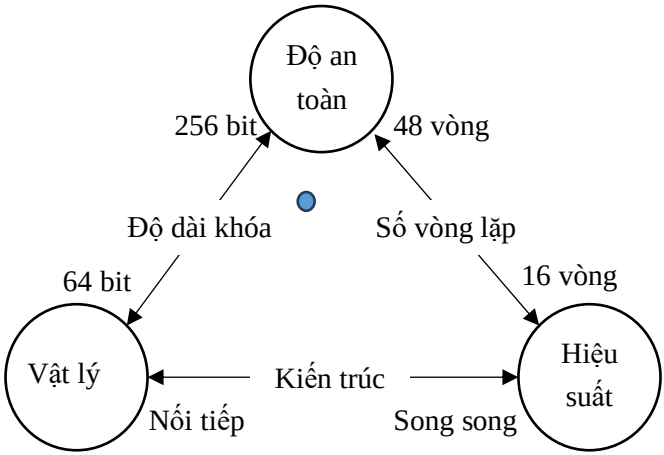
CHƯƠNG 1. LÝ THUYẾT NỀN TẢNG VỀ VÀNH ĐA THỨC VÀ MẬT MÃ HẠNG NHẸ

1.1 Khái niệm về mật mã hạng nhẹ

Theo tiêu chuẩn ISO/IEC 29192, mật mã hạng nhẹ là mật mã được dùng cho mục đích bảo mật, xác thực, nhận dạng và trao đổi khóa; phù hợp cài đặt cho những môi trường tài nguyên hạn chế. Trong ISO/IEC 29192, tính chất nhẹ được mô tả dựa trên nền tảng cài đặt, có thể được cài đặt đánh giá riêng trên phần mềm hoặc riêng trên phần cứng. Đối với riển khai phần cứng, diện tích chip và năng lượng tiêu thụ là những tiêu chí quan trọng để đánh giá tính nhẹ của hệ mật. Đối

với triển khai phần mềm thì kích thước mã nguồn, kích thước RAM lại là tiêu chí cho một hệ mật được coi là nhẹ.

Hầu hết các hệ mật mã hạng nhẹ hoạt động trên khối dữ liệu từ 64 tới 128 bít dữ liệu, với chiều dài khóa từ 64 bit đến 256 bit tùy theo yêu cầu về độ an toàn, số vòng lặp từ 16 vòng đến 48 vòng, độ phức tạp tính toán của các Hệ mật có nhiều vòng là $O(n^2)$, của các hệ mật chỉ có các phép toán dịch bit, XOR, AND, hoán vị là $O(n)$. Các tham số này được tổng hợp như trong Hình 1-1, thể hiện mối quan hệ ràng buộc giữa ba tham số là Độ an toàn, Hiệu suất và Vật lý (có thể thể đại diện bởi giá thành) như ba đỉnh của một tam giác. Mỗi hệ mật được được coi là hạng nhẹ khi tổng hợp các tham số là một chấm (ví dụ như chấm màu xanh) trong tam giác này.



Hình 1-1: Các tham số cơ bản của một hệ mật mã hạng nhẹ

1.2 Hệ mật trên vành đa thức và vấn đề còn tồn tại

1.2.1 Hệ mật mã khóa công khai NTRU

NTRU là hệ mật đầu tiên trên vành đa thức, NTRU được IEEE bắt đầu chuẩn hóa từ năm 2008 trong nhóm chuẩn P.1363.1. Hiện nay, NTRU được cộng đồng mật mã coi là một thay thế hợp lý cho các hệ mật dựa trên các bài toán phân tích số nguyên thành thừa số nguyên tố và các thuật toán logarit rời rạc trên các trường hữu hạn hoặc các

đường cong eliptic. Hệ mật này cũng được coi là khả thi nhất cho thế hệ mật mã khóa công có khả năng chống lại các tấn công bằng máy tính lượng tử. NTRU nhanh hơn các hệ mật RSA và ECC khá nhiều ở các mức độ an toàn tương đương.

Một trong những điểm hạn chế của NTRU là bản mã có dung lượng gấp $log_p q$ bản rõ. Trong chế độ an toàn cao của NTRU, với p = 3 và q = 128 , bản mã dài gấp khoảng 4 lần bản rõ.

Hệ mật NTRU là một minh chứng cho khả năng ứng dụng vành đa thức trong mật mã, tuy nhiên để ứng dụng trong thiết bị có tài nguyên hạn chế cần phải có nhiều nghiên cứu thêm nữa, đặc biệt là việc cài đặt và thử nghiệm trên thiết bị thực.

1.2.2 Hệ mật mã khóa công khai trên mã CYCLIC cục bộ

Hệ mật mã khóa công khai trên vành đa thức tại Việt Nam có thể kể đến là hệ mật Mc.Eliece trên vành đa thức, trong đó mã Goppa được thay thế bằng một mã cyclic cục bộ (64, 7, 32) kết hợp với một mã kiểm tra chẵn (8, 7, 2). Hệ mật mã này đã bước đầu khẳng định được hướng đi về việc ứng dụng mã Cyclic nói riêng, vành đa thức nói chung trong việc xây dựng các hệ mật mã, có tiềm năng trong việc tận dụng đặc tính tính toán nhanh, nhẹ của vành đa thức để xây dựng các hệ mật mã hạng nhẹ. Hệ mật Mc.Eliece trên vành đa thức vẫn giữ nguyên được độ án toàn như hệ mật Mc.Eliece với giả thiết bài toán giải hệ phương trình tuyến tính ngẫu nhiên là khó.

Tuy nhiên, nhược điểm của hệ mật này là độ phức tạp tính toán cao hơn hệ mật Mc.Eliece và cũng như Mc.Eliece, không khả thi trong triển khai thực tế vì khóa công khai quá lớn.

1.2.3 Hệ mật mã khóa công khai IPKE

Hệ mật mã khóa công khai IPKE sử dụng các phần tử khả nghịch trong vành đa thức chẵn tuyệt đối để làm cặp khóa, vành đa thức chẵn tuyệt đối. Uu điểm quan trọng của hệ mật IPKE là cả hai thuật toán mã hóa và giải mã đều sử dụng phép nhân đa thức modulo rất đơn giản tương tự như NTRU trong khi RSA phải sử dụng hàm mũ modulo với độ phức tạp $O(n^2)$.

IPKE có một số ưu điểm, tuy nhiên vẫn cần xem xét kỹ lưỡng hơn (đảm bảo cân bằng giữa không gian bản rõ và không gian khóa,

mở rộng không gian khóa, thử các loại tấn công khác,…) cho các ứng dụng thực tế đặc biệt là các ứng dụng đòi hỏi tốc độ tính toán cao với tài nguyên hạn chế.

1.3 Nhận xét

Mật mã hạng nhẹ đã và đang được quan tâm không những trên thế giới mà cả Việt Nam. Do đó, có thể nói nghiên cứu về hệ mật mã hạng nhẹ có ý nghĩa rất lớn không những trên thế giới mà cả ở Việt Nam.

Mật mã hạng nhẹ đã được chuẩn hóa bởi các tổ chức chuẩn hóa hàng đầu quốc tế, đồng nghĩa với việc nghiên cứu về mật mã hạng nhẹ đã có những kết quả rõ ràng; Tuy nhiên, các kết quả nghiên cứu về mật mã hạng nhẹ sử dụng vành đa thức vẫn còn rất khiêm tốn, trên thế giới mới có một hệ mật liên quan đến vành đa thức là NTRU và một số biến thể, tại Việt Nam chủ yếu là các công trình ứng dụng vành đa thức trong cải tiến các hệ mật của của GS.TS Nguyễn Bình và cộng sự, tuy nhiên chưa có công trình nào phát biểu hệ mật mã hạng nhẹ, cũng như tiến hành cài đặt và thử nghiệm đánh giá trên thiết bị có tài nguyên hạn chế.

Chương này đã tổng quát hóa từ các nghiên cứu đi trước về hướng xây dựng và phát triển các hệ mật mã hạng nhẹ đó là các thuật toán của các hệ mật mã hạng nhẹ muốn "nhẹ" thì các phép tính chủ yếu là các phép tính bit (bitwise) bao gồm XOR, AND, dịch bit, hoán vị bit.

Chương này cũng đã cung cấp nền tảng toán học về vành đa thức, các phép tính cơ bản trên vành đa thức cũng như các loại vành đa thức đặc biệt. có thể thấy rằng các phép tính trên vành đa thức hệ số nhị phân đều quy được về các phép tính bit. Đặc điểm này của vành đa thức một lần nữa khẳng định hướng nghiên cứu hệ mật trên vành đa thức là rất tiềm năng và có triển vọng.

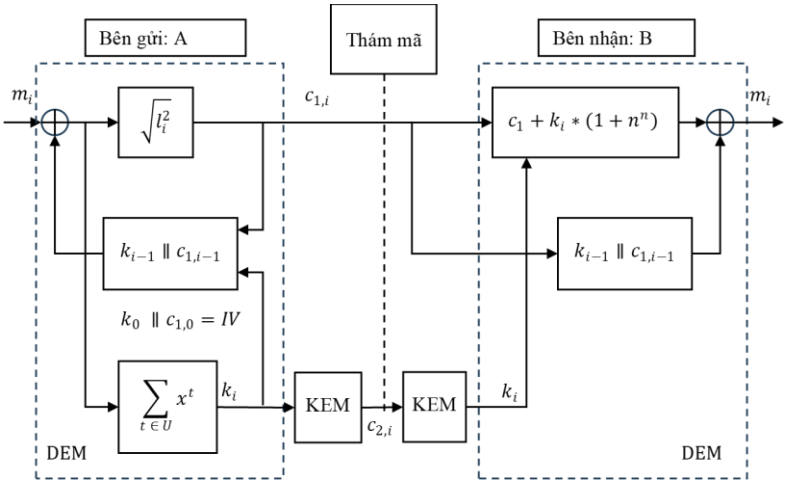
Theo hướng này, chương 2 và chương 3 nghiên cứu sâu hơn về cách sử dụng vành đa thức trong việc xây dựng hệ mật, cũng như ứng dụng các vành đa thức đặc biệt để cải tiến, xây dựng các hệ mật mới có khả năng phù hợp với thiết bị có tài nguyên hạn chế tương ứng trả lời câu hỏi nghiên cứu 2 và 3.

CHƯƠNG 2. HỆ MẬT CBC-QRHE TRÊN VÀNH ĐA THỨC CÓ KHẢ NĂNG CHỐNG TẤN CÔNG BẰNG BẢN RÕ CHỌN TRƯỚC (CPA)

2.1 Hệ mật lai ghép CBC-QRHE

Sơ đồ hoạt động của hệ mật QRHE ở chế độ CBC được mô tả trên Hình 2-1.

Trong mô hình này, $2n\ bit\ k_{i-1} \parallel c_{1,i-1}$ của phiên thứ $i-1$ sẽ được hồi tiếp và cộng modulo 2 với m_i để tạo thành bản rõ trung gian l_i trước khi tiến hành thủ tục mã hóa ở phiên thứ i. Đồng thời, ở phía giải mã, sau khi tìm được l_i từ $c_{1,i}$ và k_i, Bob phải sử dụng $2n\ bit\ k_{i-1} \parallel c_{1,i-1}$ để khôi phục m_i từ l_i.



Hình 2-1: Sơ đồ hoạt động của hệ mật CBC-QRHE

Để có thể hoạt động ở chế độ CBC, Alice và Bob cần thống nhất 2n bit vec-tơ khởi tạo (IV: $Initial\ Vector$):

$$IV = k_0 \parallel c_{1,0} \qquad (2.1)$$

trong đó || là ký hiệu ghép hai chuỗi bit trong đó k_0 và $c_{1,0}$ tương ứng với n bít cao và thấp của IV. Lưu ý rằng, giá trị IV cần được được giữ bí mật, A và B cần phải trao đổi IV trên kênh bí mật trước khi thực hiện thuật toán, ví dụ có thể sử dụng luôn khối KEM để trao đổi. Với mô hình này, các cặp bản mã $(C_{1,i}, C_{2,i})$ và $(C_{1,j}, C_{2,j})$ tại các phiên thứ i và j với của cùng một bản rõ m là không giống nhau và có thể hạn chế được các tấn công CPA.

2.1.1 Tạo khóa

Điểm thay đổi trong thủ tục tạo khóa của CBC-QRHE là sử dụng thêm một phép cộng để hồi tiếp giá trị $2n\ bit\ k_{i-1} \parallel c_{1,i-1}$ của phiên thứ $i-1$ vào bản rõ m_i thành bản rõ trung gian

$$l_i = m_i + k_{i-1} \parallel c_{1,i-1} \tag{2.2}$$

Tiếp đó A tính khóa

$$k_{ij} = l_{i(j+n)} \tag{2.3}$$

như trong QRHE

2.1.2 Mã hóa

Đầu tiên, A tính

$$c_{1,ij} = l_{ij} + l_{i(j+n)}\ mod\ 2 \tag{2.4}$$

như trong QRHE. Kích thước của bản mã $c_{1,i}$ vẫn không thay đổi và bằng n bit.

Tiếp đó A sử dụng thuật toán mã hóa của phần KEM để mã hóa khóa k_i thành từ mã $c_{2,i}$.

Cuối cùng, A gửi cặp bản mã $c_{1,i}$ và $c_{2,i}$ tới B.

2.1.3 Giải mã

Khi nhận được cặp bản mã $c_{1,i}$ và $c_{2,i}$, Bob sẽ:

2. Sử dụng thuật toán giải mã của phần KEM để tính khóa k_i từ $c_{2,i}$;
3. Sử dụng khóa k_i để tính l_i từ $c_{1,i}$ với

$$l_{ij} = \begin{cases} (C_{1,ij} + K_{ij}) \, mod \, 2 & với \quad 0 \le j \le (n-1) \\ K_{i(j-n)} & với \quad n \le j \le (2n-1) \end{cases} \tag{2.5}$$

4. Tiếp đó, Bob khôi phục

$$m_i = l_i + \, k_{i-1} \parallel c_{1,i-1} \tag{2.6}$$

2.1.4 Phân tích độ an toàn lý thuyết của CBC-QRHE

Trong QRHE, do thuật toán mã hóa không đổi và khóa bí mật được sinh từ bản rõ nên kẻ tấn công hoàn toàn có thể đoán chính xác một bản mã $c_{1,i}$ là của bản rõ nào trong hai bản rõ được chọn trước. Ngoài ra, phân bố của khóa bí mật k_i phụ thuộc hoàn toàn vào bản rõ và không thay đổi theo chỉ số phiên nên dựa vào phân bố bản mã kẻ tấn công còn đoán được phân bố của bản rõ từ đó có thể dò tìm trực tiếp bản rõ hoặc khóa bí mật.

Để đổi lại khả năng chống lại các tấn công CPA trong thủ tục mã hóa thêm một phép cộng

$$l_i = m_i + k_{i-1} \parallel c_{1,i-1} \tag{2.7}$$

và tương ứng ở phía giải mã là một phép cộng

$$m_i = l_i + \, k_{i-1} \parallel c_{1,i-1} \tag{2.8}$$

Tuy nhiên có thể thấy các phép tính này có độ phức tạp chỉ là $O(n)$ và không làm tăng tài nguyên thực thi so với trường hợp QRHE.

Bên cạnh đó, so với QRHE, sơ đồ CBC-QRHE cần phải lưu thêm $2n$ bit giá trị $k_{i-1} \parallel c_{1,i-1}$ để đảm bảo chế độ hoạt động CBC.

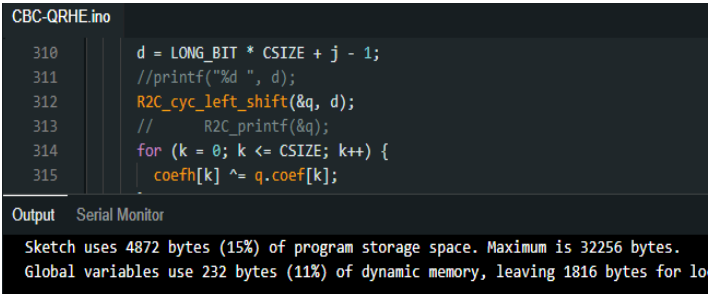
Đối với trường hợp CBC-QRHE, do phụ thuộc vào bản rõ của phiên i và giá trị *IV* nên nếu *IV* được chọn ngẫu nhiên phân bố đều thì khóa k_i cũng sẽ có phân bố đều. Trong thực tế, hai bên có thể cần phải sử dụng thêm một hệ mật khóa công khai để để trao đổi thống nhất IV.

Trong trường hợp này xác suất để kẻ tấn công đoán được bản mã là $c_{1,i}$ là của bản rõ nào trong hai bản rõ được chọn trước sẽ là xác suất đoán đúng khóa bí mật, có giá trị là $\frac{1}{n}$. Với n chọn đủ lớn, xác suất

này là không đáng kể và có thể coi CBC-QRHE an toàn với các tấn công CPA.

2.2 Thử nghiệm cài đặt CBC-QRHE trên thiết bị có tài nguyên hạn chế

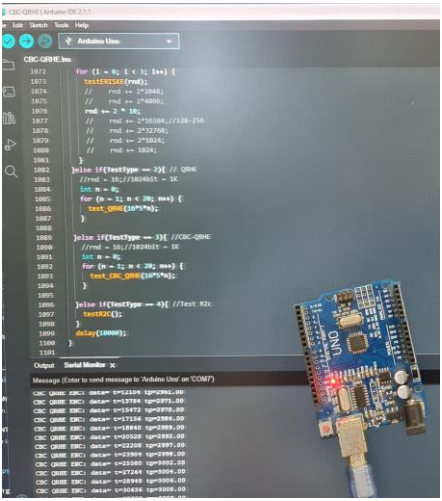
Hệ mật CBC-QRHE được thử nghiệm và đánh giá trên thiết bị Arduino UNO R3, thiết bị này có Vi điều khiển Atmeda328 họ 8 bit, RAM 2KB rất nhỏ, hiện nay được coi là thiết bị có tài nguyên hạn chế. Toàn bộ mã nguồn của QRHE và CBC-QRHE được đóng gói và cài đặt trên thiết bị chiếm không gian lưu chữ là 4872 byte như Hình 2-2.



Hình 2-2: Kích thước mã nguồn CBC-QRHE khi đóng gói

Để đánh giá hệ mật CBC-QRHE có khả năng phù hợp với thiết bị có tài nguyên hạn chế, tác giả đã chọn tham số của hệ mật là:

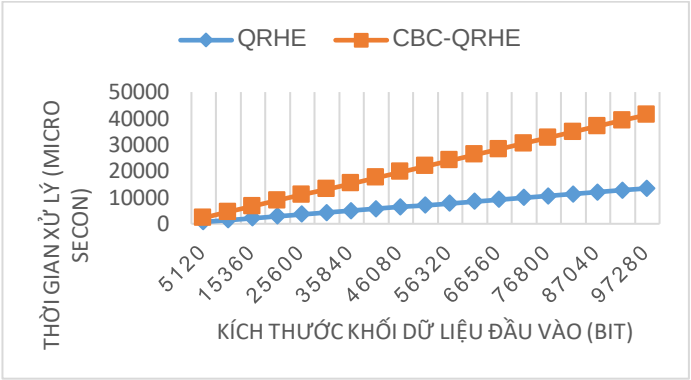
- Hệ mật hoạt động trên vành đa thức chẵn R_{2*32}, tức là mỗi một khối dữ liệu mà module mã hõa và giải mã phải xử lý là 64 bit, trong đó khóa được chọn là 32 bit.
- Các bản rõ đầu vào có kích thước tăng dần, bước nhảy là 5kb tăng dần trong mỗi lần thử.



Vi điều khiển	ATmega328 họ 8bit
Điện áp hoạt động	5V DC (chỉ được cấp qua cổng USB)
Tần số hoạt động	16 MHz
Dòng tiêu thụ	khoảng 30mA
Điện áp vào khuyên dùng	7-12V DC
Điện áp vào giới hạn	6-20V DC
Số chân Digital I/O	14 (6 chân hardware PWM)
Số chân Analog	6 (độ phân giải 10bit)
Dòng tối đa trên mỗi chân I/O	30 mA
Dòng ra tối đa (5V)	500 mA
Dòng ra tối đa (3.3V)	50 mA
Bộ nhớ flash	32 KB (ATmega328) với 0.5KB dùng bởi bootloader
SRAM	2 KB (ATmega328)
EEPROM	1 KB (ATmega328)

Hình 2-3: Thiết bị thử nghiệm cài đặt và đánh giá hệ mật CBC-QRHE

Kết quả thử nghiệm của module mã hóa được trình bày trong Hình 2-4, trong đó hiệu năng của hệ mật CBC-QRHE có kém hơn hiệu năng của hệ mật nguyên gốc QRHE, tuy nhiên, tốc độ tính toán vẫn chưa đến 100 ms.



Hình 2-4: So sánh tốc độ giữa QRHE và CBC-QRHE

Kết quả cho thấy tốc độ mã hóa và giải mã của hệ mật CBC-QRHE là khá khả quan trên thiết bị có tài nguyên hạn chế. Cụ thể, với kích thước đầu vào là $5Kb$, thời gian xử lý chưa đến $1ms$, với kích thước là $100Kb$, thời gian xử lý khoảng $45ms$.

2.3 Nhận xét, đánh giá hệ mật CBC-QRHE

CBC-QRHE cho thấy đã chống được tấn công bản rõ chọn trước CPA, đồng thời không làm tăng mức độ phức tạp của tính toán so với hệ mật gốc QRHE. CBC- không giảm nhiều về tốc độ tính toán và không tiêu tốn thêm đáng kể tài nguyên phần cứng. Tuy vậy, sơ đồ CBC-QRHE vẫn cần phải xem xét kỹ lưỡng hơn với một số tấn công khác và đặc biệt để chứng minh được độ an toàn ngữ nghĩa của hệ mật lai ghép này.

Hệ mật CBC-QRHE là một cải tiến tốt của hệ mật QRHE, đã được chứng minh về mặt lý thuyết là chống được tấn công bằng bản rõ chọn trước (CPA), đồng thời đã được cài đặt và thử nghiệm so sánh về mặt hiệu năng với một số hệ mật mã hạng nhẹ phổ biến khác, kết quả bước đầu cho thấy hệ mật CBC-QRHE có khả năng cài đặt được trên thiết bị có tài nguyên hạn chế.

Kết quả này cho thấy việc ứng dụng vành đa thức để cải tiến hệ mật là rất khả thi, mà việc cải tiến hệ mật QRHE chỉ ra một ví dụ, phương pháp này có thể áp dụng để cải tiến các hệ mật khác. Trong

tương lai, với kết quả bước đầu này, tác giả sẽ tiếp tục nghiên cứu áp dụng vào các hệ mật trên vành đa thức khác, đồng thời tiếp tục nghiên cứu chuyên sâu, cài đặt và thử nghiệm hệ mật CBC-QRHE vào các thiết bị có tài nguyên hạn chế hơn.

Kết quả chương này cũng thể hiện một trong các hướng nghiên cứu hiện nay về mật mã hạng nhẹ ứng dụng vành đa thức là "Ứng dụng vành đa thức để cải tiến hệ mật mã hạng nhẹ nhằm tăng độ tin cậy của hệ mật" cũng như một phần của hướng nghiên cứu "Tối ưu cài đặt hệ mật trên thiết bị". Chương tiếp theo sẽ trình bày hướng tiếp cận cuối cùng trong 3 hướng nghiên cứu là "Ứng dụng vành đa thức để cải tiến hệ mật thông thường thành hệ mật có tài nguyên hạn chế"

CHƯƠNG 3. HỆ MẬT OMURA-MASSEY TRÊN VÀNH ĐA THỨC

3.1 Hệ mật Omura-Massey trên vành đa thức hai lớp kề Cyclic có nhận thực (OM-CA) theo phương pháp nhân

a) Tạo khóa

Chọn $Z_2(\mathrm{x})\backslash(x^n+1)$ là vành đa thức với hai lớp kề Cyclic, các khóa được tạo như sau:

Khóa công khai:

1. A Chọn $ID(A)$ – đây là tham số nhận dạng của A, và $ID(A)$ được quảng bá tới bên thu (ở đây là B)
2. Tương tự phía bên thu, B chọn $ID(B)$ – đây là tham số nhận dạng B, tham số $ID(B)$ cũng được quảng bá tới bên phát là A

Khóa bí mật:

1. A lựa chọn cặp số ngẫu nhiên (m,n):

$$(mID(B),n) \equiv 1\ mod\ (2^{n-1}-1) \qquad (3.1)$$

2. B lựa chọn cặp số ngẫu nhiên (u,v) và tính:

$$(uID(A),v) \equiv 1\ mod\ (2^{n-1}-1) \qquad (3.2)$$

(Với vành đa thức có hai lớp kề Cyclic, có thể lựa chọn số nhận dạng như sau: $ID(A), ID(B) \in Z_2(\mathrm{x})\backslash(x^n + 1)$

b) Thủ tục trao đổi thông tin

A muốn gửi một bản tin tới B, có dạng:

$$M(x) \in Z_2(x)\backslash(x^n + 1) \qquad (3.3)$$

Bảng 3-1: Thủ tục trao đổi thông tin của hệ mật O-M trên vành đa thức

$A(mID(B), n) \leftrightarrow B(uID(A), v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [M(x)]^{mID(B)} \ mod\ (\mathrm{x^n} + 1)$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = \left[[M(x)]^{mID(B)}\right]^{uID(A)} \ mod\ (\mathrm{x^n} + 1)$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = \left[[M(x)]^{mID(B).uID(A)}\right]^n \ mod\ (\mathrm{x^n} + 1) \equiv [M(x)]^{uID(A)} \ mod\ (\mathrm{x^n} + 1)$
B giải mã C_B lấy M	B tính $\left[[M(x)]^{uID(A)}\right]^n \ mod\ (\mathrm{x^n} + 1) = M$

c) Ví dụ

Giả sử n = 5 ta có:

$$Z_2(\mathrm{x})\backslash(x^n + 1) = Z_2(\mathrm{x})\backslash(x^5 + 1) \text{ và } ID(A) = 4;\ ID(B) = 2;$$

Khóa bí mật của A(m,n) = (1,8): (mID(B),n) = (1.2,8) ≡ 1 mod 15

Khóa bí mật của B(u,v) = (1,4): (uID(A),v) = (1.4,4) ≡ 1 mod 15

A muốn gửi bản tin M = (034) tới B

3.2 Hệ mật OM-CA theo phương pháp cộng

a) Tạo khóa

Chọn $Z_2(\mathrm{x})\backslash(x^n+1)$ là vành đa thức với hai lớp kề Cyclic, các khóa được tạo như sau:

Khóa công khai:

1. A Chọn $ID(A)$ – đây là tham số nhận dạng của A, và $ID(A)$ được quảng bá tới bên thu (ở đây là B)
2. Tương tự phía bên thu, B chọn $ID(B)$ – đây là tham số nhận dạng B, tham số $ID(B)$ cũng được quảng bá tới bên phát là A

Khóa bí mật:

3. A chọn ngẫu nhiên cặp số (m,n): $(m+ID(B),n) \equiv 1\ mod\ (2^{N-1}-1)$
4. B chọn ngẫu nhiên cặp số (u,v): $(u+ID(A),v) \equiv 1\ mod\ (2^{N-1}-1)$

(Với vành đa thức có hai lớp kề Cyclic, có thể lựa chọn số nhận dạng như sau: $ID(A), ID(B) \in Z_2(\mathrm{x})\backslash(x^n+1)$)

b) Thủ tục trao đổi thông tin

A muốn gửi một bản tin sang B, được trình bày dạng:

$$M(x) \in Z_2(x)\backslash(x^n+1) \qquad (3.4)$$

Bảng 3-2: Thủ tục trao đổi thông tin của hệ mật O-M cải tiến với phép cộng

$A(mID(B),n) \leftrightarrow B(uID(A),v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [M(x)]^{m+ID(B)}\ mod\ (x^n+1)$

B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = \left[[M(x)]^{m+ID(B)}\right]^{u+ID(A)} mod\ (x^n + 1)$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = \left[[M(x)]^{(m+ID(B)).(u+ID(A))}\right]^n mod\ (x^n + 1) \equiv [M(x)]^{u+ID(A)} mod\ (x^n + 1)$
B giải mã C_B lấy M	B tính $\left[[M(x)]^{u+ID(A)}\right]^v mod\ (x^n + 1) = M$

3.3 Hệ mật OM-CA theo phương pháp lũy thừa

a) Tạo khóa

Chọn Z_2(x)\$(x^n + 1)$ là vành đa thức với hai lớp kề Cyclic, các khóa được tạo như sau:

Khóa công khai:

1. A Chọn ID(A) – đây là tham số nhận dạng của A, và ID(A) được quảng bá tới bên thu (ở đây là B)
2. Tương tự phía bên thu, B chọn ID(B) – đây là tham số nhận dạng B, tham số ID(B) cũng được quảng bá tới bên phát là A

Khóa bí mật:

1. A chọn cặp số ngẫu nhiên (m,n):

$$\left(m^{ID(B)}, n\right) \equiv 1\ mod\ (2^{N-1} - 1) \qquad (3.5)$$

2. B chọn cặp số ngẫu nghiên (u,v):

$$\left(u^{ID(A)}, v\right) \equiv 1\ mod\ (2^{N-1} - 1) \qquad (3.6)$$

(Với vành đa thức có hai lớp kề Cyclic, có thể lựa chọn số nhận dạng như sau: $ID(A), ID(B) \in Z_2(\mathrm{x})\backslash(x^n+1)$

b) Thủ tục trao đổi thông tin

A muốn gửi bản tin sang B, được trình bày dạng:

$$M(x) \in Z_2(x)\backslash(x^n+1) \qquad (3.7)$$

Bảng 3-3: Thủ tục trao đổi thông tin của hệ mật O-M cải tiến với phép lũy thừa

$A(mID(B), n) \leftrightarrow B(uID(A), v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [M(x)]^{m^{ID(B)}} \ mod\ (x^n+1)$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = \left[[M(x)]^{m^{ID(B)}}\right]^{u^{ID(A)}} \ mod\ (x^n+1)$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = \left[[M(x)]^{m^{ID(B)}u^{ID(A)}}\right]^{n} \ mod\ (x^n+1) \equiv [M(x)]^{u^{ID(A)}} \ mod\ (x^n+1)$
B giải mã C_B lấy M	B tính $\left[[M(x)]^{u^{ID(A)}}\right]^{v} \ mod\ (x^n+1) = M$

3.4 Hệ mật OM-CA theo phương pháp Logarit

a) Tạo khóa

Chọn $Z_2(\mathrm{x})\backslash(x^n+1)$ là vành đa thức với hai lớp kề Cyclic, các khóa được chọn như sau:

Khóa công khai:

1. A Chọn ID(A) – đây là tham số nhận dạng của A, và ID(A) được quảng bá tới bên thu (ở đây là B)

2. Tương tự phía bên thu, B chọn ID(B) – đây là tham số nhận dạng B, tham số ID(B) cũng được quảng bá tới bên phát là A

Khóa bí mật:

1. A chọn ngẫu nhiên cặp số (m,n):

$$\left(\left(ID(B)\right)^{m}, n\right) \equiv 1\ mod\ (2^{N-1} - 1) \qquad (3.8)$$

2. B chọn ngẫu nhiên cặp số (u,v):

$$\left(\left(ID(A)\right)^{u}, v\right) \equiv 1\ mod\ (2^{N-1} - 1) \qquad (3.9)$$

(Với vành đa thức có hai lớp kề Cyclic, có thể lựa chọn số nhận dạng như sau: $ID(A), ID(B) \in Z_2(x)\backslash(x^n + 1)$

b) Thủ tục trao đổi thông tin

A muốn gửi bản tin M tới B, được trình bày dạng:

$$M(x) \in Z_2(x)\backslash(x^n + 1) \qquad (3.10)$$

Bảng 3-4: Thủ tục trao đổi thông tin của hệ mật O-M cải tiến với phép logarit

$A(mID(B), n) \leftrightarrow B(uID(A), v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [M(x)]^{\left(ID(B)\right)^{m}}\ mod\ (x^n + 1)$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = \left[[M(x)]^{\left(ID(B)\right)^{m}}\right]^{\left(ID(A)\right)^{u}}\ mod\ (x^n + 1)$

A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = \left[[M(x)]^{(ID(B))^m.(ID(A))^u}\right]^n \ mod\ (x^n + 1)$ $\equiv [M(x)]^{(ID(A))^u} \ mod\ (x^n + 1)$
B giải mã C_B lấy M	B tính $\left[[M(x)]^{(ID(A))^u}\right]^v \ mod\ (x^n + 1) = M$

3.5 Hệ mật Omura-Massey trên vành đa thức hai lũy đẳng nguyên thủy (OM-PI)

Do tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường số nguyên $GF(p)$, nên các phần tử và phép tính nhân trên vành đa thức có thể thay thế được các số nguyên và phép tính nhân trong trường số $GF(p)$ của hệ mật O-M. Phần tiếp theo trình bày chi tiết việc thay thế này như là một cải tiến của hệ mật O-M trên vành đa thức.

Để tiện theo dõi, hệ mật O-M cải tiến được trình bày theo các bước của giao dịch như sau:

a) Tạo khóa

Trước tiên, hai bên A và B cần thống nhất đa thức hai lũy đẳng nguyên thủy cũng như nhóm nhân sẽ sử dụng, cụ thể là đa thức $g(x)$ và nhóm nhân $\mathcal{A}$ hay $\mathcal{B}$ như công thức (3.9) hay (3.10), ở đây chọn nhóm nhân $\mathcal{A}$ để trình bày chi tiết.

Khi chọn đa thứ bất khả quy $g(x)$ sẽ xác định được bậc cao nhất của đa thức là l.

Sau đó, A và B chọn cặp khóa bí mật như sau:

- Khóa bí mật của A: *(m, n):*

$$m.n \ \equiv \ 1 \ mod\ 2^l \ - 1 \qquad (3.11)$$

- Khóa bí mật của B: *(u, v):*

$$u.v \ \equiv \ 1 \ mod\ 2^l \ - 1 \qquad (3.12)$$

b) Thủ tục trao đổi thông tin

Bảng 3-5: Thủ tục trao đổi thông tin của hệ mật O-M trên vành đa thức có hai lũy đẳng nguyên thủy

$A(m,n) \leftrightarrow B(u,v)$ Bản tin A muốn gửi cho B được trình bày dạng: $M = k(x)$	
A mã hóa M thành C_A	A tính $C_A = k(x).m \bmod (1+x)g(x)$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = k(x).m.u \bmod (1+x)g(x)$
A giải mã C_{AB} thành C_B	A tính $C_B = k(x).m.u.n \bmod (1+x)g(x)$
B giải mã C_B lấy M	B tính $k(x).u.v \bmod (1+x)g(x) = k(x) = M$

c) Lưu ý

Hệ mật này vẫn giữa nguyên các đặc tính của hệ mật gốc là

- Để đảm bảo độ mật, cần phải thay khóa trong mỗi một phiên trao đổi thông tin.
- Chưa có tính xác thực các bên tham gia hệ mật.
- Hệ số mở rộng bản tin vẫn bằng 3.

Chi tiết thủ tục trao đổi bản tin, để tiện theo dõi, các đa thức được trình bày theo dạng rút gọn:

Bảng 3-6: Ví dụ về trao đổi bản tin của hệ mật O-M trên cành đa thức hai lũy đẳng nguyên thủy

$A\big((2),(023)\big) \leftrightarrow B\big((4),(123)\big)$ Bản tin A muốn gửi cho B được trình bày dạng: $M(x) = (134)$

A mã hóa M thành C_A	A tính $C_A = (134)(2)\ mod\ (0245) = (1)$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = (1)(4) mod\ (0245) = (024)$
A giải mã C_{AB} thành C_B	A tính $C_B = (024)(023)\ mod\ (0245) = (3)$
B giải mã C_B lấy M	B tính $(3)(123) mod\ (0245) = (134) = M$

3.6 Nhận xét

Có thể thấy, chương này có 3 kết quả có thể mở ra 2 hướng nghiên cứu tiếp theo về việc ứng dụng vành đa thức trong việc cải tiến xây dựng hệ mật mã nói chung, mật mã hạng nhẹ nói riêng.

Kết quả thứ nhất là là một giải pháp tăng cường độ an toàn của hệ mật O-M trên vành đa thức hai lớp kề Cyclic, với bốn phương pháp tương ứng với 4 phép toán trên vành. Với 4 phương pháp này, có thể ứng dụng để cải tiến, bổ sung tính xác thực vào các hệ mật tương tự trên vành đa thức.

Kết quả thứ hai là làm rõ tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường hữu hạn $GF(p)$. Với tính chất này, có thể mở ra hướng ứng dụng vành đa thức hai lũy đẳng nguyên thủy để cải tiến các hệ mật trên trường số thành hệ mật trên vành đa thức.

Kết quả thứ ba là hệ mật O-M trên vành đa thức hai lũy đẳng nguyên thủy, có độ phức tạp tính toán $O(n)$, có khả năng phù hợp với thiết bị có tài nguyên hạn chế, cũng như một trường hợp ứng dụng trong thực tế của Kết quả thứ hai.

Tuy kết quả chưa có cài đặt, đánh giá hiệu quả trên thiết bị có tài nguyên hạn chế, nhưng các kết quả đã gợi mở được các phương pháp cải tiến cả về mặt lý thuyết và thực tiễn trong việc xây dựng các hệ mật trên vành đa thức, cơ bản đã trả lời được câu hỏi nghiên cứu 3 của luận án.

KẾT LUẬN

Trên cơ sở các kết quả nghiên cứu về các hệ mật mã hạng nhẹ trên vành đa thức, tôi đã nhận thấy rằng các mục tiêu nghiên cứu đã được đạt được và những câu hỏi nghiên cứu đã được giải quyết. Công trình nghiên cứu này đã đóng góp quan trọng và đáng kể vào lĩnh vực mật mã hạng nhẹ trên vành đa thức và cung cấp một cơ sở vững chắc cho các nghiên cứu tiếp theo.

Các đóng góp nổi bật của luận án là:

(1) Xây dựng được hệ mật CBC-QRHE (Hệ mật lai ghép dựa trên thặng dư bậc hai và các phần tử liên hợp của vành đa thức chẵn có khả năng chống tấn công bằng bản rõ chọn trước). Với khả năng chống tấn công bằng bạn rõ chọn trước (CPA), hệ mật CBC-QRHE được coi là đã đảm bảo độ an toàn. Ngoài ra, về mặt lý thuyết, các thuật toán giải mã và mã hóa của hệ mật CBC-QRHE có độ phức tạp tính toán $O(n)$, và về mặt thực tế, các module của hệ mật đã được cài đặt trên thiết bị có tài nguyên hạn chế, và đã đã được đánh giá là hiệu quả hơn hệ mật nguyên gốc. Như vậy, hệ mật CBC-QRHE được coi là phù hợp với thiết bị có tài nguyên hạn chế. Toàn bộ thông tin về hệ mật CBC-QRHE đã được công bố trong công trình [C1].

(2) Xây dựng được hệ mật OM-CA (Hệ mật Omura-Massey trên vành đa thức có hai lớp kề Cyclic có nhận thực). Hệ mật OM-CA tuy chưa được thử nghiệm trên thiết bị thực, nhưng về mặt lý thuyết, thuật toán giải mã và mã hóa của hệ mật OM-CA có độ phức tạp tính toán $O(n)$, có thể coi là hệ mật mã có khả năng phù hợp với thiết bị có tài nguyên hạn chế. Ngoài ra, trong quá trình xây dựng hệ mật OM-CA, tác giả đã đề xuất bốn phương pháp bổ sung tính nhận thực vào các hệ mật trên vành đa thức. Toàn bộ thông tin về hệ mật OM-CA đã được công bố trong công trình [J1].

(3) Xây dựng được hệ mật OM-PI (Hệ mật Omura-Massey trên vành đa thức có hai lũy đẳng nguyên thủy). Hệ mật OM-PI cũng chưa được thử nghiệm trên thiết bị thực, tuy

nhiên, về mặt lý thuyết, hệ mật OM-PI có độ phức tạp tính toán là $O(n)$, tương tự như hệ mật OM-CA, OM-PI cũng được coi là phù hợp với thiết bị có tài nguyên hạn chế. Một trong những kết quả quan trọng khác khi xây dựng hệ mật OM-PI là đã làm rõ được tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy với trường hữu hạn $GF(p)$, đây là nền tảng toán học để xây dựng hệ mật OM-PI. Toàn bộ thông tin về hệ mật OM-PI đã được công bố trong công trình [J2].

Bên cạnh những kết quả đạt được, luận án vẫn còn tồn tại một số vấn đề chưa giải quyết được như chưa đưa hệ mật vào ứng dụng, chưa đánh giá trên các kịch bản sử dụng trong thực tế mà mới dừng lại ở mức độ trong phòng thí nghiệm. Chưa thử nghiệm trên các thiết bị có tài nguyên hạn chế dạng FPGA, ASIC.

Kiến nghị hướng phát triển tiếp theo:

(1) Tiếp tục mở rộng và hoàn thiện lý thuyết về ứng dụng vành đa thức trong mật mã nói chung, mật mã hạng nhẹ nói riêng. Đặc biệt các ứng dụng của vành đa thức hai lũy đẳng nguyên thủy trong cải tiến, xây dựng các hệ mật mã hạng nhẹ mới.

(2) Cài đặt và đánh giá hệ mật CBC-QRHE, OM-CA, OM-PI vào các thiết bị có tài nguyên thực tế, so sánh, đánh giá với các hệ mật mã hạng nhẹ khác.

(3) Đưa các hệ mật CBC-QRHE, OM-CA, OM-PI vào trong các ứng dụng thực tế, cả phần cứng và phần mềm trên thiết bị có tài nguyên hạn chế.

Cuối cùng, tôi hy vọng rằng công trình nghiên cứu này sẽ góp phần vào việc phát triển tri thức và ứng dụng thực tiễn trong lĩnh vực mật mã hạng nhẹ nói riêng, mật mã trên vành đa thức nói chung. Do điều kiện về thời gian và trình độ còn hạn chế, nên những vấn đề trình bày trong luận án không tránh khỏi những thiếu sót, tôi rất mong được sự góp ý của các nhà khoa học, đồng nghiệp và bạn bè để khắc phục và hoàn thiện các công trình nghiên cứu trong luận án, mang lại nhiều giá trị hơn cho cộng đồng vã xã hội.

DANH MỤC CÔNG TRÌNH CÔNG BỐ CỦA TÁC GIẢ

BÀI BÁO KHOA HỌC

J1. Hoang Manh Thang, Nguyen Binh, Cao Minh Thang (2018), "Omura-Massey cyptosystem with authentication over polynomial rings with two cyclotomic cosets", *Tạp chí khoa học công nghệ Thông tin và Truyền thông*, số 03 (CS.01), pages 17-20.

J2. Hoàng Mạnh Thắng, Nguyễn Trung Hiếu, Nguyễn Bình, Cao Minh Thắng, Hoàng Thị Thu (2023), "Hệ mật Omura-Massey trên vành đa thức hai lũy đẳng nguyên thủy", *Tạp chí khoa học công nghệ Thông tin và Truyền thông*, số 01 (CS.01).

HỘI NGHỊ KHOA HỌC

C1. Hoàng Mạnh Thắng, Cao Minh Thắng, Nguyễn Chí Thành, Bùi Hoàng Phương (2017), "Một giải pháp tăng cường khả năng chống tấn công bằng bản rõ chọn trước (CPA) cho hệ mật lai ghép QRHE", *Kỷ yếu hội thảo quốc gia REV-ECIT 2017*, (Issue 14.12.2017 - 15.12.2017 , ISSN 987-604-931253-3). Nhà xuất bản khoa học kỹ thuật, pages 79-83.