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

LUẬN ÁN TIẾN SĨ KỸ THUẬT ĐIỆN TỬ

Hà Nội - 2023

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

LUẬN ÁN TIẾN SĨ KỸ THUẬT ĐIỆN TỬ

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. GS.TS. Nguyễn Bình

Hà Nội - 2023

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu do tôi thực hiện. Các số liệu và kết quả trình bày trong luận án là trung thực và chưa được công bố ở bất kỳ tác giả nào hay ở bất kỳ công trình nào khác.

Hà Nội, tháng 2 năm 2023

Tác giả

Hoàng Mạnh Thắng

LỜI CẢM ƠN

Luận án Tiến sĩ kỹ thuật này được thực hiện tại Học viện Công nghệ Bưu chính Viễn thông, để hoàn thành công trình này tôi xin chân thành cảm ơn GS.TS. Nguyễn Bình, người thầy trực tiếp hướng dẫn tôi thực hiện luận án này.

Tôi xin chân thành cảm ơn Ban giám đốc, Khoa Quốc tế và Đào tạo sau đại học - Học viện Công nghệ Bưu chính Viễn thông, Viện Công nghệ Thông tin và Truyền thông CDIT, cũng như Ban lãnh đạo và các đồng nghiệp tại Ban Chiến lược sản phẩm VNPT-IT, nơi tôi đang công tác, đã tạo mọi điều kiện thuận lợi cho tôi trong suốt quá trình thực hiện luận án.

Cuối cùng tôi xin gửi lời cảm ơn gia đình đã động viên, chăm sóc và chia sẻ các khó khăn với tôi trong suốt quá trình thực hiện luận án.

Hà nội, tháng 2 năm 2023

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CẢM ƠN ii
MỤC LỤC iii
DANH MỤC CÁC TỪ VIẾT TẮT vi
DANH MỤC CÁC KÝ HIỆU x
DANH MỤC CÁC BẢNG xii
DANH MỤC CÁC HÌNH VẼ xiii
MỞ ĐẦU 1
CHƯƠNG 1. CƠ SỞ LÝ THUYẾT VỀ VÀNH ĐA THỨC VÀ MẬT MÃ HẠNG NHẸ 5
1.1 MỞ ĐẦU CHƯƠNG 5
1.2 CƠ SỞ TOÁN HỌC VỀ VÀNH ĐA THỨC VÀ ỨNG DỤNG TRONG MẬT MÃ 5
1.2.1 Vành 5
1.2.2 Trường hữu hạn 6
1.2.3 Vành đa thức 6
1.2.4 Vành đa thức hai lớp kề Cyclic 8
1.2.5 Lũy đẳng trong vành đa thức 8
1.3 MẬT MÃ HẠNG NHẸ 10
1.3.1 Khái niệm và phân loại mật mã hạng nhẹ 10
1.3.2 Đặc điểm thuật toán của một số hệ mật mã hạng nhẹ điển hình hiện nay 13
1.3.3 Một số hệ mật trên vành đa thức 22
1.4 PHƯƠNG PHÁP ĐÁNH GIÁ MỘT HỆ MẬT MÃ HẠNG NHẸ 27
1.4.1 Phương pháp tiếp cận nghiên cứu hệ mật mã hạng nhẹ 27

1.4.2 Phương pháp đánh giá hệ mật bằng các hình thức tấn công an toàn bảo mật 31
1.4.3 Các tham số cơ bản khi phân tích, đánh giá một hệ mật 33
1.5 KẾT LUẬN CHƯƠNG 37
CHƯƠNG 2. HỆ MẬT CBC-QRHE TRÊN VÀNH ĐA THỨC CÓ KHẢ NĂNG CHỐNG TẤN CÔNG BẰNG BẢN RÕ CHỌN TRƯỚC (CPA) 39
2.1 MỞ ĐẦU CHƯƠNG 39
2.2 CÁC CẢI TIẾN CỦA HỆ MẬT OTP TRÊN VÀNH ĐA THỨC 39
2.2.1 Hệ mật khóa bí mật OTP 39
2.2.2 Hệ mật khóa bí mật RISKE 40
2.2.3 Hệ mật lai ghép QRHE 43
2.3 HỆ MẬT LAI GHÉP CBC-QRHE 49
2.3.1 Giới thiệu về hệ mật CBC-QRHE 49
2.3.2 Sơ đồ hoạt động của hệ mật CBC-QRHE 50
2.3.3 Phân tích độ an toàn lý thuyết của CBC-QRHE 52
2.4 THỬ NGHIỆM CÀI ĐẶT CBC-QRHE TRÊN THIẾT BỊ CÓ TÀI NGUYÊN HẠN CHẾ 52
2.5 KẾT LUẬN CHƯƠNG 54
CHƯƠNG 3. HỆ MẬT OMURA-MASSEY TRÊN VÀNH ĐA THỨC 55
3.1 MỞ ĐẦU CHƯƠNG 55
3.2 GIỚI THIỆU VỀ HỆ MẬT OMURA-MASSEY 56
3.3 HỆ MẬT OM-CA TRÊN VÀNH ĐA THỨC HAI LỚP KỀ CYCLIC CÓ NHẬN THỰC 58
3.3.1 Giới thiệu 58
3.3.2 Hệ mật OM-CA trên vành đa thức hai lớp kề Cyclic có nhận thực 59
3.3.3 Nhận xét 66

3.4 HỆ MẬT OM-PI TRÊN VÀNH ĐA THỨC CÓ HAI LŨY ĐẲNG NGUYÊN THỦY 67
3.4.1 Giới thiệu 67
3.4.2 Vành đa thức có hai lũy đẳng nguyên thủy và tính chất tựa đẳng cấu với trường hữu hạn GF(p) 67
3.4.3 Hệ mật OM-PI trên vành đa thức có hai lũy đẳng nguyên thủy 71
3.4.4 Nhận xét 75
3.5 KẾT LUẬN CHƯƠNG 75
KẾT LUẬN 76
DANH MỤC CÔNG TRÌNH CÔNG BỐ CỦA TÁC GIẢ 78
TÀI LIỆU THAM KHẢO 79
Tiếng Việt 79
Tiếng Anh 81

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	*Đầy đủ tiếng Anh*	*Nghĩa tiếng Việt*
ACL	Access Control List	Danh sách điều khiển truy nhập
AES	Advanced Encryption Standard	Chuẩn mã hóa tiên tiến
ASIC	Application Specific Integrated Circuit	Mạch tích hợp dành riêng cho ứng dụng
CBC	Cipher Block Chaining	Chuỗi khối mật mã
CBC-QRHE	Cipher Block Chaining - Hybrid Encryption cheme based-on Quadratic Residue	Hệ mật mã lai ghép dựa trên các thặng dư bậc hai và phần tử liên hợp trên vành đa thức chẵn R_{2n} theo chế độ chuỗi khối
CCA	Chosen Ciphertext Attack	Tấn công bằng bản mã được chọn
CCA2	Adaptive Chosen Plaintext Attack	Tấn công bằng bản mã được chọn thích ứng
COA	Ciphertext Only Attack	Tấn công chỉ bằng bản mã
CPA	Chosen Plaintext Attack	Tấn công bằng bản rõ được chọn
DEM	Data Encapsulation Mechanism	Cơ chế đóng gói dữ liệu
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DTRU	Dual Truncated public-key cryptosystem	Hệ mật khóa công khai DTRU dựa trên hai vành đa

Từ viết tắt	*Đầy đủ tiếng Anh*	*Nghĩa tiếng Việt*
		thức hệ số nhị phân bậc hữu hạn
ECC	Elliptic Curve Cryptography	Mật mã đường cong elip
E-RISKE	Extended Random Invertible Secret-key Encryption scheme	Hệ mật khóa bí mật RISKE mở rộng trên vành R_{2C}
FPGA	Field Programmable Gate Arrays	Vi mạch dùng cấu trúc mảng phần tử logic có thể lập trình được
GE	Gate Equivalence	Cổng tương đương - một đơn vị đo lường cho phép xác định độ phức tạp độc lập về công nghệ sản xuất của các mạch kỹ thuật số
IEEE	Institute of Electrical and Electronics Engineers	Viện các kỹ sư điện và điện tử
IDS	Intrusion Detection Systems	Hệ thống phát hiện xâm nhập
IND	Indistinguishable	Không thể phân biệt
IND-CCA	Indistinguishable under Chosen Ciphertext Attack	Không thể phân biệt với các tấn công bằng bản rõ được chọn
IND-CPA	Indistinguishable under Chosen Plaintext Attack	Không thể phân biệt với các tấn công bằng bản rõ được chọn
IND-EAV	Indistinguishable under Eavesdropping Attack	Không thể phân biệt với các tấn công bằng bản rõ được chọn
IoT	Internet of Things	Internet của vạn vật

Từ viết tắt	*Đầy đủ tiếng Anh*	*Nghĩa tiếng Việt*
IPS	Intrusion Prevention System	Hệ thống ngăn ngừa truy nhập trái phép
ISO	International Organization for Standardization	Tổ chức Tiêu chuẩn hóa Quốc tế
ITU	International Telecommunication Union	Liên minh Viễn thông Quốc tế
KEM	Key Encapsulation Mechanism	Mô hình mật mã lai ghép mã hóa Khóa/Dữ liệu
KPA	Known Plaintext Attack	Tấn công bằng bản rõ đã biết
LCC	Local Cyclic Code	Mã xyclic cục bộ
MAC	Message Authentication Code	Mã xác thực thông báo
MITM	Man in the Middle	Tấn công kẻ đứng giữa
NAT	Network Address Translation	Biên dịch địa chỉ mạng
NIST	National Institute of Standards and Technology	Viện tiêu chuẩn và công nghệ quốc gia (Hoa Kỳ)
NSA	National Security Agency	Cơ quan an ninh quốc gia (Hoa Kỳ)
NTRU	N-th Truncated public-key cryptosystem	Hệ mật khóa công khai NTRU
OM-CA	Omura-Massey Cyptosystem with Authentication over polynomial rings with two cyclotomic cosets	Hệ mật Omura-Massey trên vành đa thức hai lớp kề Cyclic có xác thực
OM-PI	Omura-Massey cyptosystem built on Polynomial rings with two primitive Idempotents	Hệ mật Omura-Massey trên vành đa thức hai lũy đẳng nguyên thủy

Từ viết tắt	*Đầy đủ tiếng Anh*	*Nghĩa tiếng Việt*
OpenPGP	Open Pretty Good Privacy	Một chương trình mã hóa dữ liệu mở
OTP	One-Time-Pad	Hệ mật dùng khóa một lần
PKI	Public Key Infrastructure	Hạ tầng khoá công khai
QRHE	Hybrid Encryption scheme based-on Quadratic Residue	Hệ mật lai ghép QRHE dựa trên các thặng dư bậc hai trên vành đa thức R_{2n} theo mô hình KEM/DEM
RAM	Random Access Memory	Một loại bộ nhớ khả biến cho phép truy xuất đọc-ghi ngẫu nhiên đến bất kỳ vị trí nào trong bộ nhớ dựa theo địa chỉ bộ nhớ
RFID	Radio Frequency Identification	Hệ thống nhận dạng bằng tần số của sóng vô tuyến
RISKE	Random Invertible Secret-key Encryption	Hệ mật khóa bí mật dựa trên các phần tử khả nghịch ngẫu nhiên
SPN	Substitution-Permutation Network	Mạng Thay thế - Hoán vị
SVP	Shortest Vector Problem	Bài toán vectơ ngắn nhất

DANH MỤC CÁC KÝ HIỆU

Ký hiệu	Giải nghĩa
$\mathcal{A}, \mathcal{B}$	Nhóm nhân $\mathcal{A}, \mathcal{B}$
deg	Bậc của một đa thức
gcd	Ước chung lớn nhất
I_n	Tập các đa thức khả nghịch trong R_n
Π	Hệ mật
Π_{Sec}	Hệ mật khóa bí mật
Π_{Pub}	Hệ mật khóa công khai
Π_{Hy}	Hệ mật lai ghép
N_{2^k}	Tập các giá trị nguyên n là lũy thừa của 2
N_{2C}	Tập các giá trị nguyên n để R_n là vành có hai lớp kề cyclic
K_n	Tỉ lệ giữa số đa thức khả nghịch trên tổng số đa thức trong R_n
$R_{n,q}$	Vành đa thức bậc hữu hạn hệ số nguyên $Z_q[x]\backslash(x^n + 1)$
R_n	Vành đa thức bậc hữu hạn hệ số nhị phân $Z_2[x]\backslash(x^n + 1)$
R_{2n}	Vành đa thức bậc hữu hạn chẵn hệ số nhị phân $Z_2[x] \setminus (x^n + 1) \mid n = 2l, l \in Z^+$
R_{2^k}	Vành đa thức bậc hữu hạn chẵn tuyệt đối hệ số nhị phân $Z_2[x] \setminus (x^n + 1) \mid n = 2^k, k \in Z^+$
R_{2c}	Vành đa thức bậc hữu hạn hệ số nhị phân có hai lớp kề cyclic
ord	Cấp của một đa thức
$\equiv$	Phép "=" trong các phép tính Modulo

Ký hiệu	Giải nghĩa
$a \mid b$	a là ước của b
$\varphi(n)$	Số các số nguyên trong khoảng $[1, n]$ nguyên tố cùng nhau với n
Z_n	Các số nguyên module n
Z_n^*	Nhóm nhân các số nguyên module n
$\lvert Z_n^* \rvert$	Cấp của nhóm nhân Z_n^*

DANH MỤC CÁC BẢNG

Bảng 3-1: Hoạt động của hệ mật Omura-Massey 57
Bảng 3-2: Hoạt động của hệ mật Omura-Massey với p = 17 57
Bảng 3-3: Thủ tục của hệ mật O-M theo phương pháp nhân 59
Bảng 3-4: Ví dụ minh họa hệ mật O-M theo phương pháp nhân với n = 5 60
Bảng 3-5: Thủ tục của hệ mật O-M theo phương pháp cộng 61
Bảng 3-6: Ví dụ minh họa hệ mật O-M theo phương pháp cộng (n = 5) 62
Bảng 3-7: Thủ tục của hệ mật O-M theo phương pháp lũy thừa 63
Bảng 3-8: Ví dụ minh họa hệ mật O-M theo phương pháp lũy thừa (n = 5) 64
Bảng 3-9: Thủ tục của hệ mật O-M theo phương pháp logarit 65
Bảng 3-10: Ví dụ minh họa hệ mật O-M theo phương pháp logarit (n = 5) 66
Bảng 3-11: Bảng ánh xạ các phần tử giữa nhóm nhân $\mathcal{A}$ và trường $GF(p)$ 69
Bảng 3-12: Bảng ánh xạ các phần tử giữa nhóm nhân $\mathcal{B}$ và trường $GF(p)$ 70
Bảng 3-13: Bảng ánh xạ các tính chất giữa nhóm nhân và trường $GF(p)$ 71
Bảng 3-14: Thủ tục trao đổi thông tin của hệ mật O-M trên vành đa thức có hai lũy đẳng nguyên thủy 72
Bảng 3-15: Ví dụ về trao đổi thông tin của hệ mật O-M trên cành đa thức hai lũy đẳng nguyên thủy 74

DANH MỤC CÁC HÌNH VẼ

Hình 1-1: Nguyên lý thiết kế thuật toán mật mã hạng nhẹ.....10
Hình 1-2: Thống kế số lượng phát triển các hệ mật mã nhẹ 12
Hình 1-3: Các tham số cơ bản của một hệ mật mã hạng nhẹ 22
Hình 1-4: Frame work về an toàn thông tin cho hệ thống thông tin.....28
Hình 2-1: Mô hình mật mã lai ghép KEM/DEM.....44
Hình 2-2: Sơ đồ hoạt động của hệ mật QRHE 46
Hình 2-3: Sơ đồ hoạt động của hệ mật CBC-QRHE 50
Hình 2-4: Kích thước mã nguồn CBC-QRHE khi đóng gói 53
Hình 2-5: Thiết bị thử nghiệm cài đặt và đánh giá hệ mật CBC-QRHE 53
Hình 2-6: So sánh tốc độ mã hóa giữa QRHE và CBC-QRHE.....54
Hình 3-1: Hoạt động của hệ mật Omura-Massey 56

MỞ ĐẦU

Trong thời đại kỹ thuật số hiện nay, bảo mật thông tin trở thành một yếu tố cực kỳ quan trọng trong việc bảo vệ dữ liệu và đảm bảo tính riêng tư của cá nhân. Mật mã hạng nhẹ (lightweight cryptography) là một lĩnh vực nghiên cứu nổi lên nhằm đáp ứng nhu cầu bảo mật thông tin trên các thiết bị có tài nguyên hạn chế như các thiết bị di động, cảm biến IoT (Internet of Things) và các hệ thống nhúng. Nghiên cứu về mật mã hạng nhẹ tập trung vào việc phát triển các thuật toán và giao thức mật mã hiệu quả, đồng thời tối ưu hóa sử dụng tài nguyên như bộ nhớ, thời gian tính toán và năng lượng tiêu thụ.

Mật mã hạng nhẹ đang trở thành một lĩnh vực quan trọng trong việc bảo mật thông tin. Với sự phát triển nhanh chóng của 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, đặc biệt là 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. Công trình đầu tiên về mật mã trên vành đa thức kể đến là hệ mật NTRU [56] và các biến thể, tuy NTRU có hiệu năng tính toán tốt nhưng vẫn chưa thực sự phù hợp cho các hệ thống có tài nguyên tính toán hạn chế vì khóa và hệ số mở rộng bản tin vẫn khá lớn. Tại Việt Nam, đã có các công trình nổi bật như [6], [5], [7], [8] .. tuy nhiên chủ yếu là cải tiến thuận toán của các hệ mật mã trên trường số thành các hệ mật mã trên vành đa thức. Đối với mật mã hạng nhẹ, đã có các công trình [8], [9], [12], [13], [14], [16] mở ra hướng nghiên cứu, triển khai trên các thiết bị có tài nguyên hạn chế, nhưng mới được chứng minh về mặt lý thuyết về độ an toàn và tốc độ tính toán là có khả năng phù hợp với hệ thống IoT.

Do vậy, nghiên cứu sinh đã lựa chọn đề tài của luận án: ***"Nghiên cứu hệ mật hạng nhẹ trên vành đa thức ứng dụng vào thiết bị có tài nguyên hạn chế":***

Mục tiêu: mục tiêu chính của luận án là xây dựng được các hệ mật mã hạng nhẹ trên vành đa thức. Nghiên cứu tập trung vào việc trả lời các câu hỏi 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?

Đối tượng nghiên cứu: vành đa thức, hệ mật mã hạng nhẹ trên vành đa thức.

Phạm vi nghiên cứu: Nghiên cứu này tập trung phát triển và đánh giá các hệ mật mã hạng nhẹ trên vành đa thức. 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.

Phương pháp nghiên cứu: phương pháp chính được sử dụng trong luận án là nghiên cứu lý thuyết kết hợp với thực nghiệm, so sánh định tính, định lượng và phân tích, đánh giá kết quả.

Công cụ nghiên cứu: là các công cụ toán học và một số thiết bị có tài nguyên hạn chế.

Các đóng góp của luận án:

- CBC-QRHE, hệ mật mã lai ghép ứng dụng thặng dư bậc hai và các phần tử liên hợp trên vành đa thức chẵn có khả năng chống tấn công bản rõ chọn trước (CPA) [C1].
- OM-CA, hệ mật khóa công khai Omura-Massey trên vành đa thức hai lớp kề Cyclic có nhận thực [J1].
- OM-PI, hệ mật khóa công khai Omura-Massey trên vành đa thức hai lũy đẳng nguyên thủy [J2].

Về 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, đóng góp thêm được hai hệ mật mới và gia tăng độ an toàn của một hệ mật trên vành đa thức, 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.

- 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. Đồng thời, những kiến thức, kỹ năng của quá trình thực hiện luận án đã gián tiếp giúp tác giả góp phần thực hiện thành công hai đề tài cấp nhà nước [10], [11].

Nội dung của luận án được trình bày theo cấu trúc sau:

1) ***"Chương 1: Cơ sở lý thuyết về vành đa thức và mật mã hạng nhẹ":*** NCS đã 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 NCS đã rút ra được đặc điểm của mật mã hạng nhẹ. Tiếp theo, NCS đã 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.
2) ***"Chương 2: Hệ mật CBC-QRHE trên vành đa thức có khả năng chống lại tấn công bằng bản rõ chọn trước (CPA)":*** Tập trung trả lời câu hỏi 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. Hệ mật này đã được chứng minh là 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.
3) ***"Chương 3: Hệ mật Omura-Massey trên vành đa thức":*** Chương này tập trung trả lời câu hỏi 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.

4) ***"Kết luận":*** Tổng hợp đánh giá các kết quả đạt được của luận án đồng thời xác định các hướng nghiên cứu tiếp theo.

CHƯƠNG 1. CƠ SỞ LÝ THUYẾT VỀ VÀNH ĐA THỨC VÀ MẬT MÃ HẠNG NHẸ

1.1 MỞ ĐẦU CHƯƠNG

Chương này tập trung trình bày các nghiên cứu tổng quan, các khái niệm, định nghĩa cơ bản làm nền tảng cho các chương tiếp theo.

Bố cục chương được chia làm 4 mục chính. Trong đó, mục 1.2 trình bày các khái niệm cơ bản về vành đa thức được dùng để xây dựng các hệ mật mã trong các chương tiếp theo. Mục 1.3 trình bày khái niệm về mật mã hạng nhẹ, bức tranh tổng quan nghiên cứu về mật mã hạng nhẹ hiện nay trên thế giới và Việt Nam, những đặc điểm cơ bản của Mật mã hạng nhẹ phổ biến cũng như một số hệ mật mã điển hình trên vành đa thức, làm tiền đề cho việc chứng minh các hệ mật trên vành đa thức là mật mã hạng nhẹ ở các chương tiếp theo. Tiếp theo, mục 1.4 trình bày tổng quan về phương pháp tiếp cận để xây dựng hệ mật, các tiêu chí và phương pháp để đánh giá một hệ mật, làm nền tảng kiến thức để đánh giá các hệ mật trong chương 2 và 3. Cuối cùng, phần nhận xét chương sẽ tổng kết, đánh giá lại những vấn đề còn tồn tại, những nhận định mới, đồng thời dẫn dắt, giới thiệu các nội dung của các chương tiếp theo nhằm giải quyết vấn đề đã đặt ra và làm rõ các đề xuất mới.

1.2 CƠ SỞ TOÁN HỌC VỀ VÀNH ĐA THỨC VÀ ỨNG DỤNG TRONG MẬT MÃ

1.2.1 Vành

Định nghĩa 1-1: Vành ký hiệu là R (Ring) là một tập các phần tử trên đó xác định 2 phép toán 2 ngôi (phép cộng và phép nhân) và thỏa mãn các tiên đề R1 ÷ R4.

Phép toán cộng ký hiệu là $a + b$. Phép toán nhân ký hiệu là $a.b$ (a, b là 2 phần tử trong R).

Tiên đề R1:

Tập R là một nhóm Abel (tức là nhóm Abel theo phép cộng).

Tiên đề R2: (tính đóng kín)

Với 2 phần tử bất kỳ $a, b \in R$ đều xác định tích a.b là một phần tử của R.

Tiên đề R3: (luật kết hợp)

$$\forall\, a, b, c \in R \; ta \; có \; a.(b.c) = (a.b).c \qquad (1.1)$$

Tiên đề R4: (luật phân phối)

Đối với 3 phần tử a, b, c trong tập R ta có:

$$a.(b + c) = a.b + a.c \quad (1.2)$$

$$(b + c).a = b.a + c.a \quad (1.3)$$

Vành được gọi là vành giao hoán nếu $\forall a, b \in R$ luôn có $a.b = b.a$.

1.2.2 Trường hữu hạn

Định nghĩa 1-2: Trường ký hiệu là F (Fields) là một vành giao hoán có phần tử đơn vị với phép nhân. Trong vành này mỗi phần tử khác 0 đều có phần tử ngược đối với phép nhân.

Định nghĩa 1-3: Trường hữu hạn là một trường F có chứa hữu hạn số phần tử. Cấp của trường là cơ sở các phần tử trong F.

Định lý 1-1 (Sự tồn tại và tính duy nhất của các trường hữu hạn): Nếu F là một trường hữu hạn thì nó chứa p^m phần tử với p là một số nguyên tố nào đó và m là một số nguyên dương ($m \geq 1$). Với mỗi giá trị p^m tồn tại duy nhất một trường hữu hạn cấp p^m. Trường này ký hiệu $GF(p^m)$.

Hai trường được gọi là đẳng cấu nếu chúng giống nhau về mặt cấu trúc, mặc dù cách biểu diễn các phần tử có thể là khác nhau. Chú ý rằng nếu p là số nguyên tố thì Z_n là một trường và vì vậy mọi trường cấp p đều đẳng cấu với Z_p.

Trong trường hợp đặc biệt $p = 2$, trường được gọi là trường nhị phân. Khi đó $q = 2^m$ và $GF(2^m)$.

1.2.3 Vành đa thức

Định nghĩa 1-4: Cho F_p là một trường hữu hạn, một vành đa thức trên trường F_P được ký hiệu là $R_{n,p} = F_p[x] \setminus (x^n - 1)$ là tập hợp tất cả các đa thức của biến x với hệ số trong F_P. Hai phép toán là phép cộng và phép nhân đa thức theo modulo $(x^n - 1)$.

Trong trường hợp các hệ số của đa thức nằm trong vành số nguyên Z_q, vành sẽ được gọi là đa thức bậc hữu hạn hệ số nguyên, ký hiệu là $Z_q[x]\backslash(x^n - 1) \mid n \in Z^+$ hay dạng ngắn gọn là $R_{n,q}$.

Trong trường hợp $q = 2$ hay các hệ số của đa thức nằm trong vành Z_2, vành đa thức này sẽ được gọi là vành đa thức có bậc hữu hạn hệ số nhị phân, ký hiệu là $Z_2[x]\backslash(x^n - 1)|n \in Z^+$ hay dạng ngắn gọn là R_n.

Lưu ý rằng trong vành Z_2, $-1 = 1$ nên người ta thường viết $R_n = Z_2[x]) \setminus (x^n + 1)|n \in Z^+$.

Bậc của một đa thức f trong vành được ký hiệu là $\deg f$. Do bậc có bậc tối đa là $n - 1$, mọi đa thức trong vành đa thức có thể biểu diễn dưới dạng đầy đủ

$$f = \sum_{i=0}^{n-1} f_i x^i \mid f_i \in Z_q \tag{1.4}$$

hoặc dưới dạng véc-tơ

$$f = (f_0, f_1, \dots, f_{n-1}) \mid f_i \in Z_q \tag{1.5}$$

Để tiện theo dõi, một đa thức $f(x)$ thuộc vành sẽ được viết dạng rút gọn là f và sử dụng nhất quán trong luận án.

1.2.3.1 Phép cộng hai đa thức trong vành đa thức

Trong $R_{n,q}$, xét hai đa thức $a = \sum_{i=0}^{n-1} a_i x^i$và $b = \sum_{i=0}^{n-1} b_i x^i$, phép cộng hai đa thức được ký hiệu là '+' . Nếu đa thức c là tổng của a và b ta có

$$c = a + b = \sum_{i=0}^{n-1} c_i x^i \tag{1.6}$$

Trong đó và $c_i = a_i + b_i \mod q$. Lưu ý ở đây phép cộng các hệ số a_i và b_i được thực hiện trên vành Z_q. Có thể thấy

$$max(deg(c)) = max(\, deg(a)\,, deg(b)) \leq n - 1 \tag{1.7}$$

1.2.3.2 Phép nhân hai đa thức trong vành đa thức

Trong $R_{n,q}$, xét hai đa thức $a = \sum_{i=0}^{n-1} a_i x^i$và $b = \sum_{i=0}^{n-1} b_i x^i$, phép cộng hai đa thức được ký hiệu là '*' . Nếu đa thức c là tích của a và b ta có

$$c = a * b = \sum_{k=0}^{n-1} c_k x^k \tag{1.8}$$

trong đó

$$c_k = \sum_{i+j=k \bmod q}^{n-1} a_i . b_j \quad (1.9)$$

1.2.3.3 Phép modulo một đa thức với một số nguyên p trong vành đa thức

Trong $R_{n,q}$, kết quả phép tính modulo một đa thức $a = \sum_{i=0}^{n-1} a_i x^i$ với một số nguyên p, ký hiệu là $a \bmod p$ là một đa thức

$$c = \sum_{i=0}^{n-1} c_i x^i \quad (1.10)$$

với $c_i = a_i \, mod \, p$.

1.2.4 Vành đa thức hai lớp kề Cyclic

Định nghĩa 1-5: Vành đa thức theo modulo $x^n + 1$ được gọi là vành đa thức có hai lớp kề cyclic nếu phân tích của xn+1 thành tích của các đa thức bất khả quy trên trường $GF(2)$ có dạng sau:

$$x^n + 1 = (x + 1) \sum_{i=0}^{n-1} x^i \quad (1.11)$$

Trong đó, $(x + 1)$ và $e_0(x) = \sum_{i=0}^{n-1} x^i$ là các đa thức bất khả quy.

Vành đa thức hai lớp kề Cyclic chỉ có hai chu trình:

$$C_0 = \{0\} \quad (1.12)$$

Và

$$C_1 = \{1,2,2^2, \dots, 2^{n-2}\} \mid 2^{n-1} \equiv 1 \, mod \, n \quad (1.13)$$

1.2.5 Lũy đẳng trong vành đa thức

Định nghĩa 1-6: Trong vành đa thức R_n, một đa thức e được gọi là lũy đẳng nếu $e^2 = e$.

Bổ đề 1-1: Trong vành đa thức R_n, xét đa thức $e_{0n} = \sum_{i=0}^{n-1} x^i$, với mọi đa thức $f \in R_n$ ta có $f * e_{0n} = (w(f) \, mod \, 2) . e_{0n}$.

Chứng minh: Giả sử f được biểu diễn là

$$f = \sum_{i=0}^{n-1} f_i x^i \tag{1.14}$$

ta có

$$f * x^0 = f_0 + f_1 x + \cdots + f_{n-2} x^{n-2} + f_{n-1} x^{n-1} \tag{1.15}$$

$$f * x^1 = f_{n-1} + f_0 x + \cdots + f_{n-3} x^{n-2} + f_{n-2} x^{n-1} \tag{1.16}$$

...

$$f * x^{n-1} = f_1 + f_2 x + \cdots + f_{n-1} x^{n-2} + f_0 x^{n-1} \tag{1.17}$$

Và

$$f * e_{0n} = \sum_{i=0}^{n-1} f * x^i = \sum_{i=0}^{n-1} \left(\sum_{i=0}^{n-1} f * x^i \right) mod\ 2 . x^i$$

$$= \left(\sum_{i=0}^{n-1} f_i \right) mod\ 2 . \sum_{i=0}^{n-1} x^i = (w(f) mod\ 2\ ) . e_{0n} \tag{1.18}$$

Bổ đề này có ý nghĩa rất quan trọng trong việc chứng minh các tính chất của lũy đẳng nuốt và qua đó xác định các phần tử khả nghịch mở rộng trong vành R_n.

Bổ đề 1-2: Trong các vành R_n với n lẻ , $e_{0n} = \sum_{i=0}^{n-1} x^i$ là một lũy đẳng.

Chứng minh: Ta có

$$e_{0n}^2 = e_{0n} * \left(1 + \sum_{i=1}^{n-1} x^i \right) = e_{0n} + e_{0n} * \sum_{i=1}^{n-1} x^i \tag{1.19}$$

$$e_{0n}^2 = e_{0n} * \left(1 + \sum_{i=1}^{n-1} x^i \right) = e_{0n} + e_{0n} * \sum_{i=1}^{n-1} x^i \tag{1.20}$$

Do n lẻ nên $w(\sum_{i=1}^{n-1} x^i)$ là chẵn theo đó, $e_{0n} * \sum_{i=1}^{n-1} x^i = 0$ hay

$$e_{0n}^2 = e_{0n} \tag{1.21}$$

Ví dụ trong vành R_5, $e_{05} = 1 + x + x^2 + x^3 + x^4$.

Định nghĩa 1-7: Trong các vành R_n một lũy đẳng e được gọi lũy đẳng nuốt (Swallowing Idempotent) nếu :

$$f * e = (w(f)\ mod\ 2).e \big| \forall f \in R_{n,2}) \qquad (1.22)$$

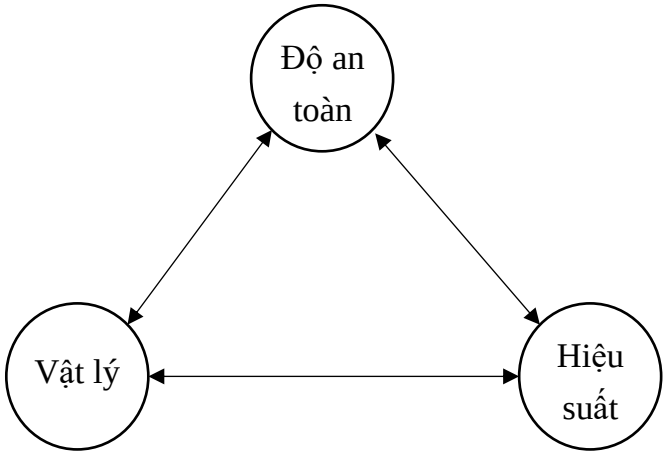
Rõ ràng trong mọi vành R_n với n lẻ , $e_{0n} = \sum_{i=0}^{n-1} x^i$ là lũy đẳng nuốt. Đây là đa thức chứa toàn bộ các đơn thức trong vành.

1.3 MẬT MÃ HẠNG NHẸ

1.3.1 Khái niệm và phân loại mật mã hạng nhẹ

Theo tiêu chuẩn ISO/IEC 29192[52], 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.

Tổng kết từ các bài báo quốc tế cũng như các bài báo trong nước về mật mã hạng nhẹ [5], [6], [7], có thể phát biểu ngắn gọn, mật mã nhẹ là hệ mật có tính thỏa hiệp, cân đối giữa ba tiêu chí về độ an toàn, hiệu suất và các tham số vật lý (RAM, CPU, Nguồn …).



Hình 1-1: Nguyên lý thiết kế thuật toán mật mã hạng nhẹ

Có nhiều cách phân loại mật mã hạng nhẹ, để thuận tiện cho quá trình nghiên cứu, như trong [17] đã phân loại theo theo cấu trúc thuật toán, kèm theo là danh sách các hệ mật điển hình theo từng loại như trình bày trong Bảng 1-1.

Bảng 1-1: Phân loại mật mã hạng nhẹ theo cấu trúc thuật toán

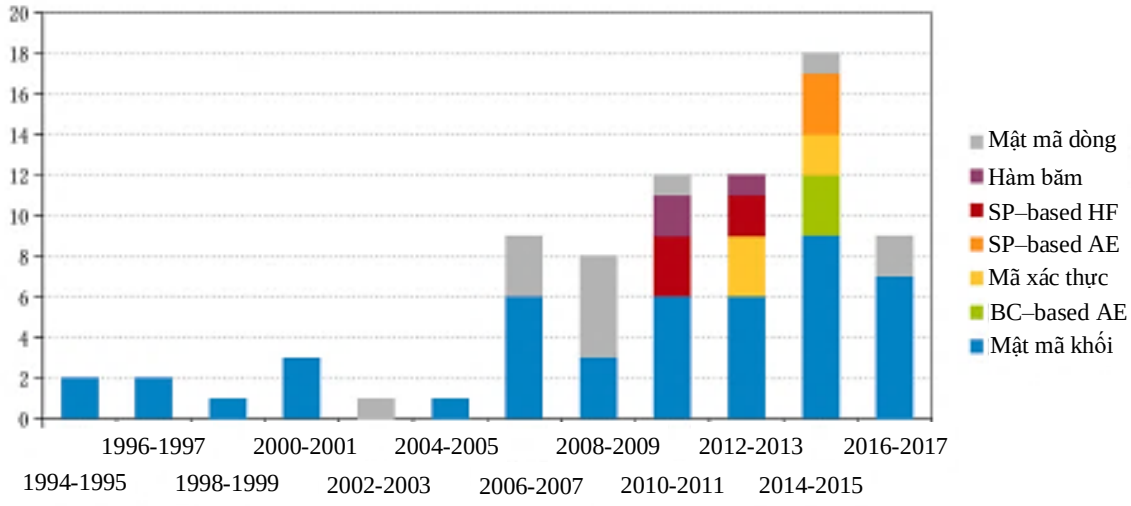
STT	***Cấu trúc thuật toán***	***Các hệ mật điển hình***
1	Mạng thay thế - hoán vị (SPN)	AES, Present, GIFT, SKINNY, Rectangle, Midori, mCrypton, Noekeon, Iceberg, Puffin-2, Prince, Pride, Print, Klein, Led, Picaro, Zorro, I-Present, EPCBC
2	Mạng Feistel (FN)	DESL/DESXL, TEA/XTEA/XXTEA, Camellia, Simon, SEA, KASUMI, MIBS, LBlock, ITUbee, FeW, GOST, Robin, Fantomas
3	Mạng Feistel tổng quát (GFN)	CLEFIA, Piccolo, Twis, Twine, HISEC
4	Add-Rotate-XOR (ARX)	SPECK, IDEA, HIGHT, BEST-1, LEA
5	Thanh ghi dịch chuyển phản hồi không tuyến tính (NLFSR)	KeeLoq, KATAN/KTANTAN, Halka
6	Hỗn hợp (Hybrid)	Hummingbird, Hummingbird-2, Present-GRP

Trong các hệ mật trên, chỉ có một số hệ mật dược chuẩn hóa bởi tổ chức uy tín trên thế giới. Cụ thể, theo tổ chức tiêu chuẩn quốc tế *ISO* và ủy ban kỹ thuật điện quốc tế *IEC*, đơn vị ban hành và duy trì các tiêu chuẩn về thông tin và công nghệ truyền thông, hiện nay đã công bố hai tiêu chuẩn cho mật mã hạng nhẹ là:

- Tiêu chuẩn *ISO/IEC 29167*: công nghệ thông tin-kỹ thuật nhận diện và thu thập dữ liệu tự động, trong phần *10, 11* và *13*. Với mật mã đối xứng nên được sử dụng trong giao tiếp không gian và thẻ *RFID*. Các phần này được mô tả cụ thể trong *AES-128, PRESENT-80* và *Grain-128A*.

- Tiêu chuẩn *ISO/IEC 29192* với một loạt các tiêu chuẩn về mã khối như *PRESENT, CLEFIA*, mã dòng như *Trivium, Enocoro* hay hàm băm *PHOTON, Spongent, Lesamnta-LW*. Một vài tiêu chuẩn được đề cập trong *ISO/IEC 29192* là:
    - Sự an toàn của cơ chế mã hóa, bảo mật 80 bits được coi là độ an ninh tối thiểu cho một hệ mật mã nhẹ. Tuy nhiên, tiêu chuẩn áp dụng có thể lên tới *112* bits cho các hệ thống yêu cầu bảo mật trong thời gian dài.
    - Yêu cầu khi triển khai phần cứng, chẳng hạn: vùng chip được sử dụng cho cơ chế mã hóa, sự tiêu thụ năng lượng.
    - Yêu cầu khi triển khai phần mềm, đặc biệt là về kích thước mã (code size), kích thước *RAM*.
    - Sự trưởng thành của cơ chế mã hóa
    - Tổng quát các thuộc tính nhẹ được yêu cầu cho một hệ mật.

Một góc nhìn khác về sự phát triển mật mã, tương tự như mật mã truyền thống, mật mã hạng nhẹ cũng được chia thành 3 loại là mật mã khóa công khai, mật mã khóa bí mật, hàm băm. Trong mật mã khóa bí mật có mật mã dòng, mật mã khối … Theo thống kê như Hình 1-2 cho thấy sự quan tâm của động đồng về mật mã, theo hướng tiếp cận này, có thể nhận thấy mật mã khối hạnh nhẹ được quan tâm nhiều nhất, cũng phản ánh thực tế là mật mã khối hạng nhẹ có vai trò quan trọng nhất trong các ứng dụng về mật mã.



Hình 1-2: Thống kế số lượng phát triển các hệ mật mã hạng nhẹ

1.3.2 Đặc điểm thuật toán của một số hệ mật mã hạng nhẹ điển hình hiện nay

Trong Bảng 1-1 có 6 loại cấu trúc thuật toán và 48 hệ mật. Tuy nhiên, để phục vụ đánh giá mức độ tính toán nhẹ cũng như tính nhẹ trong cài đặt, trong Bảng 1-2 đánh giá một số hệ mật mã hạng nhẹ điển hình, từ đó rút ra được các tính chất của một hệ mật mã hạng nhẹ.

Bảng 1-2: Bảng phân tích đặc điểm thuật toán của hệ mật mã hạng nhẹ

STT	***Cấu trúc thuật toán***	***Các hệ mật điển hình***	***Đặc điểm thuật toán***
1	Mạng thay thế - hoán vị (SPN)	AES	Hệ mật mã khóa bí mật AES có thể cói là hệ mật mã linh hoạt nhất hiện nay, có thể triển khai trên nhiều loại phần cứng khác nhau với các khối bit đưa vào xử lý khác nhau, hiện nay ứng dụng cho mật mã hạng nhẹ có các phiên bản là AES-128/192/265 tương ứng với mỗi khối bit đưa vào xử lyà là 128/192/256 bit, để đảm bảo độ mật, số lượng vòng lặp tương ứng là 10/12/14 vòng lặp. Mỗi vòng lặp của AES bao gồm các phép toán XOR, thay thế byte (SubBytes), dịch bit (ShiftRows), và trộn cột (MixColumns). Phiên bản được sử dụng phổ biến nhất cho mật mã hạng nhẹ của AES là AES-128, mỗi vòng lặp có khoảng 40 phép toán trên 128 bit dữ liệu. Như vậy, số lượng phép toán khoảng ***400*** phép toán, được coi là rất nhanh và hiệu quả.
		PRESENT	Hệ mật mã khóa bí mật PRESENT được coi là hệ mật siêu nhẹ, chỉ sử dụng các phép toán đơn giản như XOR, AND, OR và dịch bit. Thuật toán của hệ mật PRESENT bao gồm 16 phép toán XOR, 16 phép toán AND và 48 phép toán OR trên mỗi vòng lặp, tổng cộng là 80 phép

STT	***Cấu trúc thuật toán***	***Các hệ mật điển hình***	***Đặc điểm thuật toán***
			toán trên 64 bit dữ liệu. Như vậy, với tổng cộng 31 vòng lặp, tổng số phép toán trong quá trình mã hóa là ***2480*** phép toán.
		GIFT	Hệ mật mã khóa bí mật GIFT (Galois/Counter Mode Integer/Fast Transform) hoạt động theo các khối 64 bit dữ liệu, ký hiệu là GIFT-64. GIT-64 sử dụng 28 vòng lặp, trong đó mỗi vòng lặp bao gồm các phép toán XOR, thay thế byte (SubBytes), hoán vị hàng (ShiftRows) và hoán vị cột (MixColumns). Mỗi vòng lặp của GIFT-64 bao gồm khoảng 33 phép toán trên 64 bit dữ liệu. Tổng cộng phép toán của GIFT-64 khoảng ***924*** phép toán.
		SKINNY	Hệ mật mã khóa bí mật SKINNY hoạt động theo các khối dữ liệu 128 bit. Phiên bản SKINNY-128/128 sử dụng 40 vòng lặp, trong đó mỗi vòng lặp bao gồm các phép toán XOR, thay thế byte (SubBytes), hoán vị hàng (ShiftRows), hoán vị cột (MixColumns) và phép toán hoán vị phiên (AddRoundConstant). Mỗi vòng lặp của SKINNY-128/128 bao gồm khoảng 64 phép toán trên 128 bit dữ liệu. Tổng số khoảng ***2560*** phép toán trên một khối dữ liệu.
		Rectangle	Hệ mật mã khóa bí mật Rectangle hoạt động trên khối dữ liệu 64 bit. Phiên bản Rectangle-64 sử dụng 17 vòng lặp, trong đó mỗi vòng lặp bao gồm các phép toán XOR, thay thế byte (SubBytes), hoán vị hàng (ShiftRows), và trộn

STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
			cột (MixColumns). Mỗi vòng lặp của Rectangle-64 bao gồm khoảng 16 phép toán trên 64 bit dữ liệu. Tổng số phép tính trên một khối dữ liệu là ***272*** phép toán.
		Midori	Hệ mật mã khóa bí mật Midori hoạt động trên khối dữ liệu 64 bit, ký hiệu Midori-64, hệ mật này sử dụng 20 vòng lặp, trong đó mỗi vòng lặp bao gồm các phép toán XOR, thay thế byte (SubBytes), hoán vị hàng (ShiftRows), hoán vị cột (MixColumns) và phép toán hoán vị phiên (AddRoundConstant). Mỗi vòng lặp của Midori-64 bao gồm khoảng 15 phép toán trên 64 bit dữ liệu. Tổng cộng khoảng ***300*** phép toán trên một khối 64 bit dữ liệu.
		Noekeon	Hệ mật khóa bí mật Noekeon hoạt động trên khối dữ liệu 128 bit. Noekeon sử dụng 4 vòng lặp, trong đó mỗi vòng lặp bao gồm các phép toán XOR, thay thế byte (SubBytes), hoán vị hàng (ShiftRows), hoán vị cột (MixColumns) và phép toán hoán vị phiên (AddRoundKey). Mỗi vòng lặp của Noekeon bao gồm khoảng 32 phép toán trên 128 bit dữ liệu. Tổng số phép toán là ***128*** phép toán.
		$PRINT_{CIPHER}$	Hệ mật $PRINT_{CIPHER}$ mã hóa dữ liệu theo khối có kích thước 64 bit. PRINTcipher sử dụng một số lượng vòng lặp lặp lại để thực hiện phép toán trên dữ liệu. Số lượng vòng lặp trong PRINTcipher có thể được điều chỉnh để cân bằng giữa hiệu suất và độ an toàn. $PRINT_{CIPHER}$

STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
			48 sử dụng 48 bits khóa bí mật và cộng thêm 32 bits được sinh ra từ thuật toán mã hóa sử dụng 16 S-box 3 bits.
		Klein	Hệ mật KLEIN mã hóa dữ liệu theo khối có kích thước 64 bit hoặc 128 bit. Phiên bản KLEIN-64 sử dụng khối 64 bit và phiên bản KLEIN-128 sử dụng khối 128 bit. Số lượng vòng lặp trong KLEIN có thể được điều chỉnh để cân bằng giữa hiệu suất và độ an toàn.
		PICARO	Hệ mật PICARO hoạt động trên khối dữ liệu 128 bit. Số lượng vòng lặp trong PICARO thường được đặt là 10 vòng lặp.
		I-Present	Hệ mật I-Present hoạt động trên khối dữ liệu 64 bit. Số lượng vòng lặp trong I-Present thường được đặt là 32 hoặc 48 vòng lặp.
		EPCBC	Hệ mật mã khóa bí mật EPCBC là một hệ mật mã hạng nhẹ được thiết kế phù hợp với thiết bị EPC (Electronic Product Code). EPCBC hoạt động trên khối dữ liệu 48 và 96 bit, và khóa 96 bit.
2	Mạng Feistel (FN)	DESL/DESXL	DESL (Data Encryption Standard with LFSR-based Whitening) và DESXL (Data Encryption Standard with XORing and LFSR-based Whitening) là các phiên bản mở rộng của thuật toán mã hóa DES (Data Encryption Standard). DESL và DESXL hoạt động trên khối dữ liệu 64 bit. DESL và DESXL sử dụng 16 vòng lặp DES lặp lại một S-box (6*4 bits) 8 lần.

STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
		TEA/XTEA /XXTEA	TEA (Tiny Encryption Algorithm), XTEA (Extended Tiny Encryption Algorithm) và XXTEA (Corrected Block TEA) hoạt động trên khối dữ liệu 64 bit, các phép toán dùng trong hệ mật là dịch bit và XOR. TEA có 32 vòng lặp, XTEA có 64 vòng lặp và XXTEA sử dụng số vòng lặp biến đổi (tùy thuộc vào kích thước khối dữ liệu).
		Camellia	Hệ mật mã khóa bí mật Camellia hoạt động trên khối dữ liệu 128 bit. Camellia hỗ trợ các kích thước khóa từ 128 bit đến 256 bit. Số lượng vòng lặp trong Camellia phụ thuộc vào kích thước khóa và được thiết kế để đảm bảo độ bảo mật và hiệu suất tối ưu. Đối với các khóa có độ dài 128 bit, Camellia sử dụng 18 vòng lặp. Với khóa 192 bit và 256 bit, Camellia sử dụng 24 vòng lặp.
		SIMON	SIMON hoạt động trên khối dữ liệu có kích thước cố định là 64 bit. SIMON hỗ trợ các kích thước khóa từ 64 bit đến 128 bit. Số lượng vòng lặp trong SIMON phụ thuộc vào kích thước khóa. Tương ứng với kích thước khóa 64/96/129bit, số lượng vòng lặp của SIMON sử dụng 32/36/42 vòng lặp.
		KASUMI	Hệ mật KASUMI thường được sử dụng trong các mạng di động GSM (Global System for Mobile Communications) và công nghệ GPRS (General Packet Radio Service). KASUMI hoạt động trên khối dữ liệu 64 bit. KASUMI sử

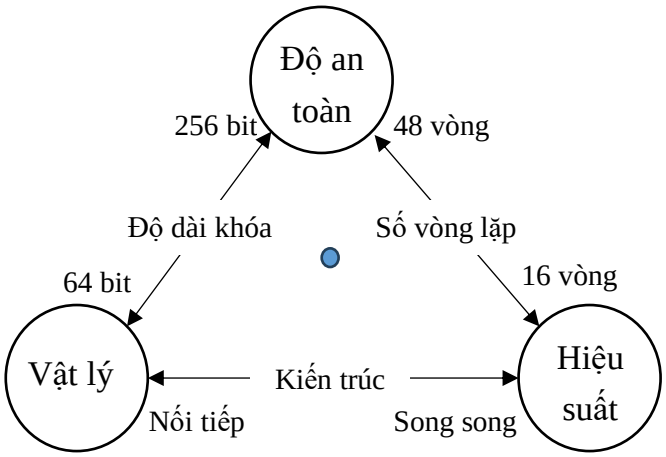
STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
			dụng khóa có kích thước 128 bit. Số lượng vòng lặp trong KASUMI là 8. Mỗi vòng lặp trong KASUMI bao gồm các phép thay thế, hoán vị và phép XOR để thực hiện phép toán mã hóa/giải mã.
		LBlock	Hệ mật LBlock hoạt động trên khối dữ liệu có kích thước cố định là 64 bit. Lblock có hai phiên bản là LBlock cơ bản có kích thước khóa 80 bit và phiên bản mở rộng với kích thước khóa 128 bit. LBlock sử dụng 32 vòng lặp cho khóa 80 bit và 48 vòng lặp cho khóa 128 bit. Mỗi vòng lặp trong LBlock bao gồm các phép thay thế, hoán vị và phép XOR để thực hiện phép toán mã hóa/giải mã.
		GOST	GOST (Government Standard) hoạt động trên các khối dữ liệu 64 bit và khóa 256 bit. GOST sử dụng 32 vòng lặp để thực hiện quá trình mã hóa/giải mã. Mỗi vòng lặp trong GOST bao gồm các phép thay thế, hoán vị và phép XOR để thực hiện phép toán mã hóa/giải mã.
3	Mạng Feistel tổng quát (GFN)	CLEFIA	CLEFIA hoạt động trên các khối dữ liệu 128 bit. CLEFIA hỗ trợ khóa có kích thước 128, 192 và 256 bit. CLEFIA sử dụng 18 vòng lặp (hoặc 24 vòng lặp tùy thuộc vào kích thước khóa) để thực hiện quá trình mã hóa/giải mã. Mỗi vòng lặp trong CLEFIA bao gồm các phép thay thế, hoán vị và phép XOR để thực hiện phép toán mã hóa/giải mã.

STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
		Piccolo	Piccolo hoạt động trên các khối dữ liệu 64 bit. Piccolo hỗ trợ khóa có kích thước 80, 128 và 192 bit. Piccolo sử dụng 31 vòng lặp để thực hiện quá trình mã hóa/giải mã. Mỗi vòng lặp trong Piccolo bao gồm các phép toán như hoán vị, thay thế và phép XOR để thực hiện phép toán mã hóa/giải mã.
		Twine	Twine hoạt động trên các khối dữ liệu 128 bit. Twine hỗ trợ khóa có kích thước 80, 128 và 192 bit. Twine sử dụng một số vòng lặp (thường là 32 hoặc 36 vòng lặp) để thực hiện quá trình mã hóa/giải mã. Mỗi vòng lặp trong Twine bao gồm các phép toán như hoán vị, thay thế và phép XOR để thực hiện phép toán mã hóa/giải mã.
4	Add-Rotate-XOR (ARX)	SPECK	SPECK hoạt động trên các khối dữ liệu có kích thước 64 bit và khóa có kích thước 64, 96 và 128 bit. SPECK sử dụng một số lượng vòng lặp cố định để thực hiện quá trình mã hóa/giải mã. Số lượng vòng lặp được lựa chọn sao cho cân đối giữa hiệu suất và độ bảo mật.
		IDEA	Hệ mật IDEA (International Data Encryption Algorithm) hoạt động trên các khối dữ liệu 64 bit và khóa có kích thước 128 bit. IDEA sử dụng 8 vòng lặp để thực hiện quá trình mã hóa/giải mã. Mỗi vòng lặp trong IDEA bao gồm các phép toán như hoán vị, thay thế và phép XOR để thực hiện phép toán mã hóa/giải mã.

STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
		HIGHT	Hệ mật HIGHT hoạt động trên các khối dữ liệu có kích thước 64 bit và khóa 128 bit. HIGHT sử dụng 32 vòng lặp. Các phép toán là XOR, mod, dịch bits. để thực hiện quá trình mã hóa/giải mã.
		LEA	LEA (Lightweight Encryption Algorithm) hoạt động trên các khối dữ liệu 128 bit, và khóa 128, 192 hoặc 256 bit. LEA sử dụng một số lượng vòng lặp tùy thuộc vào kích thước khóa được sử dụng. Ví dụ: Với khóa 128 bit, LEA sử dụng 24 vòng lặp, với khóa 192 bit sử dụng 28 vòng lặp, và với khóa 256 bit sử dụng 32 vòng lặp.
5	Thanh ghi dịch chuyển phản hồi không tuyến tính (NLFSR)	KeeLoq	KeeLoq hoạt động trên các khối dữ liệu 32 bit, và khóa 64 bit. KeeLoq sử dụng 528 vòng lặp để thực hiện quá trình mã hóa/giải mã. Mỗi vòng lặp trong KeeLoq bao gồm các phép toán hoán vị, thay thế và XOR. Đặc điểm thuật toán của KeeLoq là cấu trúc mạng đặc biệt gọi là "Time-Memory Trade-Off (TMTO)" để thực hiện quá trình mã hóa/giải mã. Quá trình này bao gồm các bước hoán vị, thay thế và XOR để thực hiện các phép toán logic trên các khối dữ liệu.
		KATAN/ KTANTAN	KATAN và KTANTAN hoạt động trên các khối dữ liệu 64 bit.và khóa 64, 80 hoặc 128 bit. KATAN sử dụng 254 vòng lặp, trong khi KTANTAN sử dụng 254 hoặc 1022 vòng lặp. Mỗi vòng lặp trong KATAN/KTANTAN bao gồm các phép toán thay thế và XOR. Kiến trúc

STT	*Cấu trúc thuật toán*	*Các hệ mật điển hình*	*Đặc điểm thuật toán*
			của KATAN, KATANTAN rất đơn giản; bản rõ được lưu bởi 2 thanh ghi. Trong mỗi vòng, một số bit được lấy ra và đưa vào hàm phi tuyến Boolean, và LFRS 8 bits để mã hóa.
6	Hỗn hợp (Hybrid)	Hummingbird	Hummingbird hoạt động trên các khối dữ liệu 64 bit, và khóa có kích thước 128, 192 hoặc 256 bit. Hummingbird sử dụng một số lượng vòng lặp tùy chọn, từ 3 đến 7 vòng lặp. Mỗi vòng lặp trong Hummingbird bao gồm các phép toán thay thế, hoán vị và phép XOR.
		Hummingbird-2	Hummingbird-2 là một phiên bản cải tiến của hệ mật mã Hummingbird, vẫn hoạt động trên các khối dữ liệu có kích thước 64 bit, nhưng khóa chỉ có 128 bit. Hummingbird-2 sử dụng 4 vòng lặp. Mỗi vòng lặp trong Hummingbird-2 bao gồm các phép toán thay thế, hoán vị và phép XOR.

Bảng 1-2 cho thấy 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, như vậy theo [1.4.3.1], 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 1-3, 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 thấp hay cao) 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 1-3: Các tham số cơ bản của một hệ mật mã hạng nhẹ

1.3.3 Một số hệ mật trên vành đa thức

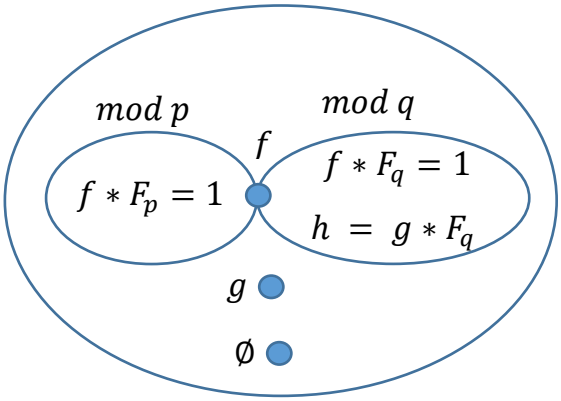
Như trong Bảng 1-1, nhằm cung cấp hiệu suất cao và tiêu thụ năng lượng thấp trên các thiết bị có tài nguyên hạn chế, các hệ mật đều được thiết kế dựa trên các phép tính đơn giản trên trường hữu hạn $GF(2)$. Xem xét tiêu chí độ phức tạp tính toán, các phép toán trên vành đa thức chủ yếu được thực hiện trên trường hữu hạn $GF(2)$, do vậy, bước đầu có thể nhận thấy vành đa thức là hướng đi đúng hướng để xây dựng các hệ mật mã hạng nhẹ. Dưới đây là một số hệ mật mã trên vành đa thức điển hình, tuy chưa phù hợp với thiết bị có tài nguyên hạn chế, nhưng có thể coi là những viên gạch đầu tiên trong việc xây dựng các hệ mật mã hạng nhẹ trên vành đa thức.

1.3.3.1 Hệ mật mã NTRU

Có thể nói, hệ mật trên vành đa thức đầu tiên là hệ mật NTRU [56], công bố nằm 1995. NTRU, phát minh bởi Hoffstein, Pipher và Silverman, lần đầu tiên được giới thiệu tại Crypto'96. Mặc dù về hình thức NTRU hoạt động trên các vành đa thức bậc hữu hạn hệ số nguyên dương $\frac{Z_q[x]}{x^n+1}$, tuy nhiên độ mật của NTRU lại được chứng minh có liên quan đến bài toán khó trên dàn Euclidean [29]. Tại hội thảo ANTS'98, các tác giả của NTRU đã đưa ra phiên bản cải tiến trong đó đã đánh giá kỹ lưỡng về độ mật của NTRU đối với các tấn công dựa trên dàn [56]. NTRU được IEEE bắt đầu chuẩn hóa từ năm 2008 [56] 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 [83].

Bảng 1-3: Thủ tục trao đổi bản tin của hệ mật khóa công khai NTRU

<table>
<tr><td colspan="2">A và B muốn trao đổi thông tin với nhau, A và B thống nhất các tham số của vành đa thức bậc hữu hạn hệ số nguyên dương p và q:
$$R_{n,p} = \frac{Z_p(x)}{x^n+1} \mid n,p \in N^*$$
$$R_{n,q} = \frac{Z_q(x)}{x^n+1} \mid n,q \in N^*$$
Trong đó, p và q là hai số nguyên, với
$$q \gg p \text{ và } \gcd(p,q) = 1$$</td></tr>
<tr><td>Có thể mô hình hóa hệ mật NTRU bằng các nhóm nhân mod p và q, cũng như các đa thức ngẫu nhiên trên vành $x^n + 1$ như sau</td><td> 
</td></tr>
<tr><td>Các thông số về khóa bí mật và khóa công khai</td><td>- Khóa bí mật B: f, F_p
- Khóa công khai của B: h</td></tr>
<tr><td>A mã hóa bản tin m thành bản mã C rồi gửi sang B</td><td>$$C = p\emptyset * h + m(mod\ q)$$</td></tr>
</table>

B giải mã mã bản tin C bằng khóa bí mật F_p để lấy bản rõ m như sau	B tính bản tin M: $$M = f * C(mod\ q)$$ Sau đó dùng khóa bí mật để lấy bản tin m như sau: $$(F_p * M) mod\ p =$$ $$(F_p *\ f * C(mod\ q)) mod\ p =$$ $$(F_p *\ f * (p\emptyset * h + m)(mod\ q)) mod\ p =$$ $$(F_p * f * p\emptyset * h + F_p * f * m)(mod\ p) =$$ $$(F_p * f * p\emptyset * g * F_q + F_p * f * m)(mod\ p) = m$$

Sau gần 20 năm kể từ khi ra đời, NTRU đã thu hút rất nhiều sự quan tâm của cộng đồng mật mã với nhiều kiểu tấn công và song song là các bản hiệu chỉnh cũng như các biến thể. Ngoài ra, một số biến thể của NTRU cũng đã được đề xuất. Đầu tiên là sơ đồ NTRU sử dụng đa thức không khả nghịch làm khóa thay và kéo theo hai khóa công khai thay vì một như trong NTRU [56]. Một biến thể khác của NTRU được đề xuất năm 2002 có tên là CTRU [46] trong đó các hệ số nguyên của các đa thức trong NTRU được thay bằng các đa thức trên các vành để tránh các loại tấn công lattice-based như đối với NTRU. MaTRU [66], một hệ mật tương tự NTRU nhưng hoạt động trên các vành các ma trận vuông $k - by - k$ có phần tử là các đa thức trên vành $R_n = \frac{Z[x]}{x^n+1}$ với $nk^2 = N$, được giới thiệu năm 2005 với một số cải thiện về tốc độ tính toán so với NTRU. Năm 2010, trong [67], đại số octonions được khai thác để xây dựng một biến thể của NTRU có tên là OTRU. Do NTRU là một hệ mật dựa trên dàn, năm 2012, bài toán tìm vector gần nhất (CVP: Closet Vector Problem) đã được sử dụng trong [96] để đề xất một biến thể tổng quát hóa của NTRU. Gần đây, trong [59], vành số nguyên Z trong NTRU được thay thế bởi vành các số nguyên Eisenstein để xây dựng hệ mật ETRU có tốc độ tính toán nhanh với khóa nhỏ hơn ở các mức độ mật tương đương so với NTRU.

So với các hệ mật thông dụng như RSA, ECC, NTRU có một số ưu điểm:

- Có sự khác biệt với bài toán cơ sở hoàn toàn khác, có liên quan đến bài toán SVP trên dàn, một bài toán NP-hard chưa có thuật giải trong thời gian đa thức, kể cả đối với các máy tính lượng tử;
- Thuật toán mã hóa và giải mã đơn giản kéo theo tốc độ tính toán rất nhanh, được coi là nhanh nhất trên thị trường hiện nay;

- Sử dụng khóa ngắn nhất so với các hệ mật khóa công khai hiện có hơn ở các độ mật tương đương;
- Tốn ít tài nguyên tính toán nên được nghiên cứu ứng dụng cho các hệ thống nhúng có tài nguyên hạn chế [RFID, cảm biến, thiết bị y tế];

Tuy nhiên, NTRU cũng có những hạn chế,:

- Bản thân các tác giả không đưa ra được bài toán khó nền tảng của NTRU. Việc chứng minh độ khó của NTRU lại do một số tác giả khác đưa ra sau 16 năm kể từ ngày hệ mật này được công bố;
- Có thể bị tấn công trên dàn, mặc dù điều này rất khó khăn khi số chiều của dàn (bậc của đa thức lớn);
- Bị tấn công khi phát lại liên tiếp bản mã của cùng một bản rõ;
- Bị tấn bản rõ được chọn;
- Kích thước khóa công khai lớn;
- Hệ số mở rộng bản tin lớn.

Vậy NTRU, vì thủ tục mã sử dụng một phép cộng và một phép nhân đa thức modulo đơn giản trong khi thủ tục giải mã cũng chỉ sử dụng hai phép nhân đa thức modulo của hai đa thức có hệ số nhỏ nên điểm mạnh nhất của NTRU là tốc độ tính toán. Theo [56], NTRU nhanh hơn các hệ mật RSA và ECC khá nhiều ở các mức độ an toàn tương đương. Hơn nữa, tốc độ của NTRU có thể được nâng cao bằng cách chọn các vành và các phép biến đổi tuyến tính hiệu quả hơn như trong [46].

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 [56], với $p = 3$ và $q = 128$, bản mã dài gấp khoảng 4 lần bản rõ.

Trong biến thể của NTRU, đáng chú ý nhất là hai hệ mật CTRU và hệ mật pNE [86]. Khác với NTRU, pNE hoạt động dựa trên vành đa thức chẵn tuyệt đối hệ số nguyên $Z_p\ [x]\ (x^n + 1)|n = 2^k$. Hệ mật này có ưu điểm là có độ an toàn ngữ nghĩa IND-CPA dựa trên độ khó của bài toán R-LWE. Tuy nhiên, hiệu năng của pNE tính toán thấp hơn NTRU và hệ số mở rộng bản tin khá lớn.

1.3.3.2 Hệ mật mã trên mã CYCLIC cục bộ

Hệ mật khóa công khai đầu tiên dựa vành đa thức $\frac{Z_2[x]}{x^n+1}$ do tác giả Phạm Việt Trung đưa ra năm 2005 trong công trình [16]. Hệ mật này thực chất là một biến thể của hệ mật Mc.Eliece, 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 Xyclic 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. Bài báo tuy dùng vành đa thức để cải tiến hệ mật Mc.Eliece nhưng 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.

1.3.3.3 Hệ mật mã IPKE

Hệ mật mã khóa công khai IPKE [14] sử dụng các phần tử khả nghịch trong vành đa thức chẵn tuyệt đối để làm cặp khóa, vành đa thức chẵn tuyệt đối được được trình bày như sau:

$$R_{2^k} = \frac{Z_2(x)}{x^{2^k}+1} \mid k \in N^* \qquad (1.23)$$

Bảng 1-4: Thủ tục trao đổi bản tin của hệ mật khóa công khai IPKE

<table>
<tr><td colspan="2">A và B muốn trao đổi thông tin với nhau, A và B thực hiện thủ tục tạo khóa như sau:
- A và B thống nhất một số nguyên dương $p < 2^{k-1}$, mỗi bản rõ sẽ có chiều dài là $(p-1)$ bit
- B chọn ngẫu nhiên hai đa thức khác 0 là $s_1, s_2 \in R_{2^{k-1}}$ sau đó tính $s = s_1 * x^{2^{k-1}} + s_2$. Từ s, chọn ra một khóa bí mật của B.
- Từ khóa bí mật s, B tính ra khóa công khai h rồi gửi tới A: $h = s * (x^p + 1)$ hay $h * s \; mod \; (x^p + 1) = 1$</td></tr>
<tr><td>A mã hóa m thành C sau đó gửi sang B</td><td>A chia dữ liệu cần truyền thành các bản tin m có chiều dài $(p-1)$ bit, sau đó tính p bit như sau:
$M = (w(m)+1) mod\ 2.x^{n-1} + m$
Sau đó mã hóa bản tin M thành C như sau:
$C = \mathrm{M} * \mathrm{h}$</td></tr>
<tr><td>B nhận được C và giải mã để lấy bản tin m</td><td>B giải mã C để lấy M:
$\mathrm{C} * s = M * h * s = M$</td></tr>
</table>

	Sau đó, khôi phục m từ M: $m = M_{n-1}.x^{n-1} + M$

Nhận xét:

- Một nhược điểm của hệ mật IPKE là hệ số mở rộng bản tin là $2^k/p$. Do phải chọn $p < 2^{k-1}$ nên hệ số này luôn lớn hơn 2 hay bản mã dài gấp hơn hai lần bản rõ. Do đó, mặc dù k càng lớn thì khả năng bảo mật của hệ mật càng cao, ta cần phải chọn k phù hợp để đảm bảo hiệu quả mã hóa.
- Một ưu 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 $O(n^2)$.
- Ngoài ra, với cùng độ dài khóa công khai, IPKE chỉ cần sử dụng n bit khóa bí mật s trong khi NTRU sử dụng hai khóa f và F_p với tổng độ dài là $2n$ bit.

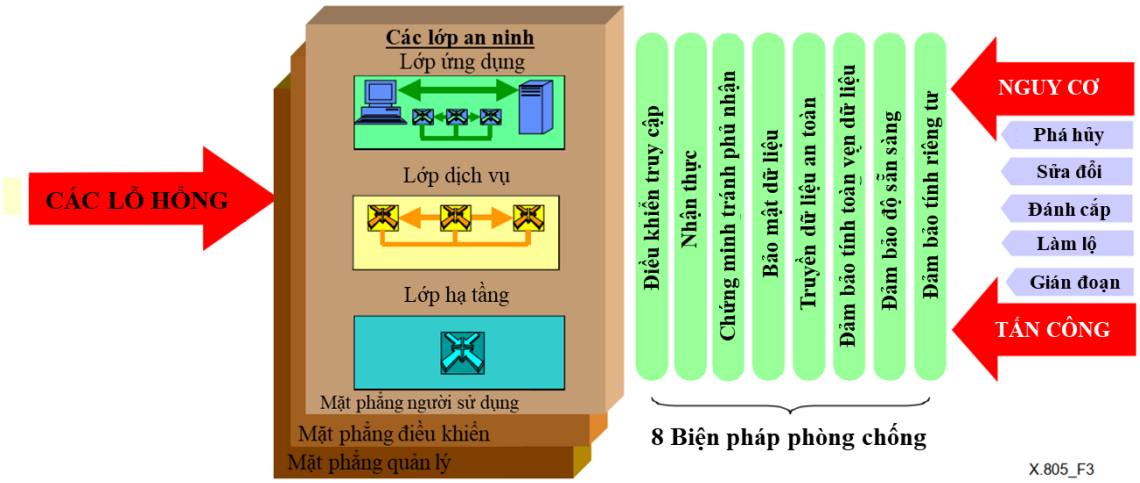
Như vậy, IPKE có một số ưu điểm, tuy nhiên vẫn cần xem xét kỹ lưỡng hơn (đảm bảo cân bằng giữa không gian bản rõ và không gian khóa, mở rộng không gian khóa, thử các loại tấn công khác,…) cho các ứng dụng thực tế đặc biệt là các ứng dụng đòi hỏi tốc độ tính toán cao với tài nguyên hạn chế.

1.4 PHƯƠNG PHÁP ĐÁNH GIÁ MỘT HỆ MẬT MÃ HẠNG NHẸ

1.4.1 Phương pháp tiếp cận nghiên cứu hệ mật mã hạng nhẹ

Về an toàn thông tin cho một hệ thống thông tin, trong nhiều cách tiếp cận hiện nay, cách tiếp cận của ITU-T được coi là toàn diện và có hệ thống nhất, gọi là Framework về An toàn thông tin từ đầu cuối đến đầu cuối của hệ thống thông tin, được trình bày trong khuyến nghị có mã X.805 [51]; tuy Framework này được công bố năm 2003, nhưng Framework này có tính tổng quát hóa cao, nên vẫn còn nguyên giá trị cho các hệ thống thông tin ngày nay.

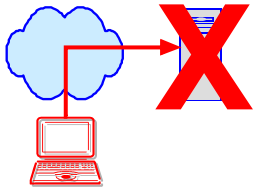
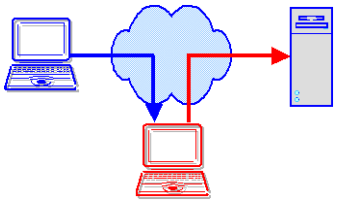
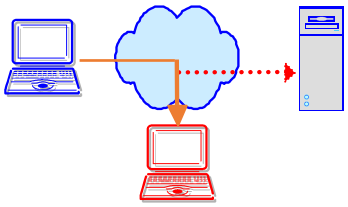
Để áp dụng Framework X.805, hệ thống thông tin được mô hình hóa thành 3 tầng và 3 mặt phẳng, đồng thời chỉ ra 5 nhóm nguy cơ và 8 giải pháp để phòng chống các nguy cơ đó.

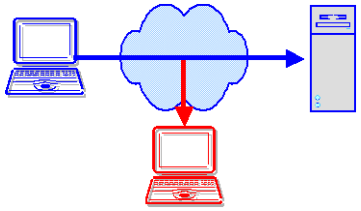


Hình 1-4: Frame work về an toàn thông tin cho hệ thống thông tin

ITU-T Rec. X.805 tổng quát hóa các nguy cơ về an toàn thông tin (Threats) thành 5 nhóm:

Bảng 1-5: Nhóm các nguy cơ an toàn bảo mật theo X.805

STT	Nhóm các nguy cơ	Minh họa
1	Phá huỷ thông tin hay các tài nguyên khác (Destruction)	
2	Sửa đổi thông tin (Corruption)	
3	Đánh cắp thông tin hay các tài nguyên khác (Removal)	

4	Làm lộ thông tin (Disclosure)	
5	Làm gián đoạn dịch vụ (Interuption)	

Với 5 nhóm nguy cơ này, X.805 cũng đã tổng quát hóa 8 biện pháp (Dimentions) để bảo vệ hệ thống trước 5 nhóm nguy cơ như sau:

1. Điều khiển truy nhập (Access Control): Phương pháp này nhằm hạn chế và điều khiển việc truy nhập vào các phần tử mạng, các dịch vụ và các ứng dụng. Một số cơ chế phổ biến để thực hiện biện pháp này đó là: Sử dụng mật khẩu, sử dụng danh sách điều khiển truy nhập (ACL), sử dụng Firewall.
2. Nhận thực người sử dụng (Authentication): Phương pháp này sử dụng nhận dạng người sử dụng để kiểm tra tính đúng đắn của người sử dụng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng khoá chia sẻ, sử dụng hạ tầng khoá công cộng – PKI, sử dụng chữ ký số, sử dụng chứng chỉ số.
3. Chứng minh tránh phủ nhận (NonRepudation): Phương pháp này nhằm ngăn chặn khả năng người sử dụng từ chối hành động mà họ đã thực hiện vào mạng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng cơ chế ghi lại sự kiện hệ thống, sử dụng chữ ký số.
4. Bảo mật dữ liệu (Confidentiality of Data): Phương pháp này nhằm đảm bảo tính bí mật cho dữ liệu của người sử dụng tránh không được biết bởi người không mong muốn. Cơ chế phổ biến để thực hiện biện pháp này đó là: mật mã.
5. Đảm bảo an toàn trong quá trình truyền dữ liệu (Communication): Phương pháp này nhằm đảm bảo dòng thông tin chỉ đi từ nguồn đến đích mong muốn, các điểm trung gian không mong muốn được biết thông tin không thể truy nhập vào dòng thông tin. Một số cơ chế

phổ biến để thực hiện biện pháp này đó là: sử dụng VPN thông qua MPLS hay một số giao thức như là L2TP,…

6. Đảm bảo tính toàn vẹn dữ liệu (Data Integrity): Phương pháp này nhằm đảm bảo rằng dữ liệu nhận được và được phục hồi là giống với dữ liệu đã được gửi đi từ nguồn. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng thuật toán băm MD5, sử dụng chữ ký số, hay phần mềm chống virus.
7. Đảm bảo tính khả dụng (Avaiability): Phương pháp này nhằm đảm bảo cho người sử dụng hợp lệ luôn có thể sử dụng các phần tử mạng, các dịch vụ và các ứng dụng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng hệ thống phát hiện/ngăn ngừa truy nhập trái phép (IDS/IPS), sử dụng cơ chế dự phòng, sử dụng BC/DR (Business Continuity/Disaster Recovery).
8. Đảm bảo tính riêng tư cho người sử dụng (Privacy): Phương pháp này nhằm đảm bảo tính riêng tư cho nhận dạng và việc sử dụng mạng của người sử dụng. Một số cơ chế phổ biến để thực hiện biện pháp này mà chúng ta thường thấy đó là: sử dụng NAT, sử dụng mật mã, tuy nhiên, độ phức tạp của các kết nối, sự gia tăng dữ liệu lại gây ra nguy cơ về sự gia tăng lỗ hổng cho các cuộc tấn công mạng. Đảm bảo ATTT là yếu tố quan trọng để đảm bảo kết nối liên tục và an toàn dữ liệu. Phân nhóm ATTT có thể được thiết lập thông qua việc áp dụng các quy chuẩn, tiêu chuẩn về ATTT, áp dụng các biện pháp xác thực giữa các bên tham gia vào quá trình giao dịch trao đổi thông tin,...

Trong 8 biện pháp phòng chống nêu trên, biện pháp [4], [5], [6], [8] có thể thực hiện được với một hệ mật thông thường; biện pháp [1], [7] có thể giải quyết bằng các công vụ về an toàn bảo mật phổ biến hiện nay như hệ thống nhận thực, cấp quyền, hệ thống firewall; biện pháp [2] hiện nay cũng đã có những giải pháp, tuy nhiên rất cồng kềnh và tốn nhiều chi phí (Như chữ ký số, hệ thống quản lý mã khóa công khai PKI …). Đây cũng là lý do mà tác giả đã đề xuất giải pháp cải tiến hệ mật OMURA-MASSEY bằng cách thêm tính năng nhận thực vào hệ mật như trong công trình [J1].

1.4.2 Phương pháp đánh giá hệ mật bằng các hình thức tấn công an toàn bảo mật

Tương tự như các hệ mật truyền thống, các mô hình phân tích mã bằng hình thức tấn công an toàn bảo mật trong mật mã hạng nhẹ chia làm 9 loại [55] như sau:

1. Tấn công chỉ bằng bản mã (COA: Ciphertext Only Attack): Trong loại tấn công này, thám mã chỉ được truy cập tới các bản mã mà không thể truy cập đến các bản rõ. Đây là loại tấn công mật mã yếu nhất và trên thực tế, loại tấn công này ít được xem xét vì không thể đảm bảo $\mathcal{A}$ không có thông tin gì về không gian bản rõ.
2. Tấn công bằng bản rõ đã biết (KPA: Known Plaintext Attack): Trong loại tấn công này, thám mã được truy cập đến một danh sách giới hạn các cặp bản rõ và bản mã tương ứng. Trên thực tế, tấn công này khó triển khai hơn COA.
3. Tấn công brute-force hay tấn công vét cạn: Trong tấn công này, các khóa trong không gian khóa sẽ được thử cho đến khi tìm ra khóa chính xác của hệ mật. Loại tấn công này cũng có thể áp dụng cho để tìm các bản rõ mà không cần khóa. Loại tấn công này thực chất là một lớp con của các tấn COA và KPA.
4. Tấn công bằng bản rõ được chọn (CPA: Chosen-Plaintext Attack): Trong loại tấn công này, thám mã có thể lựa chọn trước một số bản rõ để mã hóa và có thể truy cập đến các bản mã tương ứng. Điều này cho phép thám mã có đầy đủ thông tin về không gian bản rõ và có thể cho phép họ khai thác các lỗ hổng có thể xảy ra với một số bản rõ nhất định. Đối với các hệ mật khóa công khai thì khả năng chống lại loại tấn công này là bắt buộc.
5. Tấn công nghe lén (EAV: Eaveasdropping Attack): Tương tự như tấn công như CPA. Tuy nhiên, thám mã chỉ được chọn bản rõ để mã hóa một lần chứ không được truy cập không giới hạn đến bộ mã hóa.
6. Tấn công bằng bản rõ được chọn thích ứng: (CPA2: Adaptive chosen-plaintext attack): Trong loại tấn công này, thám mã có thể lựa chọn một chuỗi các bản rõ để mã hóa và có thể truy cập đến bản mã tương ứng. Tại mỗi bước, thám mã sẽ có cơ hội phân tích kết quả trước đó trước khi chọn bản rõ tiếp theo. Điều này cho phép thám mã có nhiều thông tin hơn khi lựa chọn các bản rõ hơn là chọn tất cả các bản rõ trước khi tấn công như trong thủ tục CPA.

7. Tấn công bằng bản mã được chọn (CCA: Chosen-ciphertext attack CCA): Trong loại tấn công này, thám mã có thể lựa chọn tùy ý các bản mã và được truy cập tới bản bản rõ là kết quả giải mã. Trên thực tế, điều kiện này đòi hỏi thám mã phải có quyền truy cập kênh truyền thông và phía nhận.
8. Tấn công bằng bản mã được chọn thích ứng (CCA2: Adaptive chosen-ciphertext attack CCA2): Trong loại tấn công này, thám mã có thể chọn một chuỗi các bản mã và được truy cập tới các bản rõ là kết quả giải mã. Tại mỗi bước, thám mã sẽ có cơ hội phân tích kết quả giải mã trước đó trước khi lựa chọn bản mã tiếp theo.
9. Tấn công phân biệt (distinguishing attack): là một loại tấn công trong đó thám mã chọn trước hai mẫu (có thể là hai bản rõ hoặc hai bản mã) và sử dụng một thủ tục tấn công nào đó (ví dụ EAV, CPA, CCA,…) để lấy kết quả trả về và tìm cách đoán xem kết quả đó là ứng với mẫu nào trong hai mẫu được chọn. Với loại tấn công này, rõ ràng xác suất để thám mã đoán đúng tối thiểu là $\frac{1}{2}$, đây là xác suất có được khi $\mathcal{A}$ đoán ngẫu nhiên một cách tầm thường.

1.4.2.1 Thủ tục tấn công phân biệt bằng cách nghe lén

Định nghĩa 1-8: Thủ tục tấn công phân biệt bằng nghe lén đối với một hệ mật khóa bí mật, ký hiệu là $"Sec"\ "K"^{eav}_{\mathcal{A},\Pi}(n)$, được mô tả như sau:

1. Thám mã A chọn một cặp bản rõ m_0, m_1 có cùng độ dài (có thể khác n) và đưa vào thủ tục mã mã hóa.
2. Một khóa bí mật $k \in \mathcal{K}$ có độ dài n ngẫu nhiên trong không gian khóa và một bit ngẫu nhiên $b \in \{"0,1"\}$ được lựa chọn để mã hóa $m\_b \mid b \in \{0,1\}$ và trả lại cho A bản mã $c = \mathcal{E}_k(m_b)$. c được gọi là bản mã thách thức.
3. Sau khi nhận được c, $\mathcal{A}$ thực hiện đoán bit b bằng một giá trị b'.

Đầu ra của tấn công là 1 nếu $b = b'$ và 0 trong trường hợp ngược lại. Nếu $"Sec"\ "K"^{eav}_{\mathcal{A},\Pi}(n) = 1$ ta nói rằng A đã thành công. Một hệ mật khóa bí mật có khả năng chống lại tấn công này sẽ được gọi là có độ an toàn IND-EAV.

1.4.2.2 Thủ tục tấn công phân biệt bằng bản rõ được chọn

Định nghĩa 1-9: Thủ tục tấn công phân biệt bằng bản rõ được chọn đối với một hệ mật khóa bí mật, ký hiệu là $"Sec"\ "K"^{cpa}_{\mathcal{A},\Pi}(n)$, được mô tả như sau:

1. Thám mã A chọn một cặp bản rõ m_0, m_1 có cùng độ dài (có thể khác n) và đưa vào thủ tục mã mã hóa.
2. Một khóa bí mật $k \in \mathcal{K}$ có độ dài n ngẫu nhiên trong không gian khóa và một bit ngẫu nhiên $b \in \{"0,1"\}$ được chọn để mã hóa $m_b \,|b \in \{0,1\}$ và trả lại cho A bản mã $c = \mathcal{E}_k(m_b)$. c được gọi là bản mã thách thức.
3. A vẫn tiếp tục được truy cập không giới hạn tới thủ tục mã hóa $\mathcal{E}$.
4. Sau khi nhận được c, A thực hiện đoán bit b bằng một giá trị b'.

Đầu ra của tấn công là 1 nếu $b = b'$ và 0 trong trường hợp ngược lại. Nếu $"Sec" "K"_{\mathcal{A},\Pi}^{cpa}(n) = 1$ ta nói rằng A đã thành công. Một hệ mật khóa bí mật có khả năng chống lại tấn công này sẽ được gọi là có độ an toàn IND-CPA.

1.4.3 Các tham số cơ bản khi phân tích, đánh giá một hệ mật

1.4.3.1 Độ phức tạp tính toán

Độ phức tạp tính toán (hay độ phức tạp thuật toán) là giá trị để ước lượng tài nguyên khi thực thi một thuật toán về mặt lý thuyết. Thực tế, để đánh giá một thuật toán có hiệu quả hay không, các nhà khoa học thường đánh giá hai yếu tố là thời gian thực hiện thuật toán (còn gọi là độ phức tạp thuật toán) và dung lượng bộ nhớ cần thiết để lưu trữ dữ liệu. Tuy nhiên, khoa học mật mã, khái niệm độ phức tạp tính toán thường là thời gian thực hiện thuật toán.

Thật vậy, gọi A là một thuật toán, m là dữ liệu đầu vào của module phần mềm thuật toán, thuật toán A tính trên dữ liệu vào e phải trả một chi phí về thời gian và bộ nhớ nhất định, ký hiệu như sau:

- Chi phí về thời gian: $t_A(m)$ là thời gian để hoàn thành thuật toán trên khối dữ liệu m.
- Chi phí về bộ nhớ: $l_A(m)$ là bộ nhơ để hoàn thành thuật toán trên khối dữ liệu m.

Độ phức tạp tính toán về thời gian và Bộ nhớ chính là chi phí về thời gian và bộ nhớ trong trường hợp xấu nhất (trường hợp tiêu tốn nhiều tài nguyên nhất):

- $T_A(n) = \max\{t_A(m), với\ |m| \leq n\}$, n là kích thước khối dữ liệu đầu vào của thuật toán.
- $L_A(n) = \max\{l_A(m), với\ |m| \leq n\}$, n là kích thước khối dữ liệu đầu vào của thuật toán.

Trong thực tế, với các khối dữ liệu n đầu vào thay đổi, thời gian tính toán cũng thay đổi theo, tùy thuộc vào bản chất của thuật toán là tuyến tính hay phi tuyến mà chi phí thời gian thay đổi theo, nên để biểu diễn độ thức tạp tính toán về mặt thời gian, thường dùng khái niệm là Độ phức tạp tiệm cận.

Độ phức tạp $T_A(n)$ được gọi là tiệm cận tới hàm $f(n)$, ký hiệu và $O(f(n))$ nếu tồn tại các số n_0, c mà $T_A(n) \leq c.f(n), \forall\, n \geq n_0$.

Như vậy, với hàm $f(n)$ là đa thức thì độ phức tạp $T_A(n)$ được gọi là độ phức tạp đa thức.

Để thuận tiện tính độ phức tạp tính toán các hệ mật, dưới đây là một số quy tắc để xác định độ phức tạp tính toán:

- Các lệnh đơn (lệnh khai báo, gán, nhập xuất dữ liệu, phép toán số học,...), thời gian thực hiện là $O(1)$.
- Các khối lệnh: Giả sử một khối lệnh gồm các câu lệnh $S_1, S_2, \dots, S_m$ có thời gian thực hiện lần lượt là $O(f_1(n)), O(f_2(n), \dots, O(f_m(n))$ thì thời gian thực hiện của cả khối lệnh là: $O(max(f_1(n), f_2(n), \dots, f_m(n)))$.
- Câu lệnh rẽ nhánh: Giả sử thuật toán có câu lệnh có hai nhánh, thời gian thực hiện của câu lệnh nhánh 1 và câu lệnh nhánh 2 lần lượt là $O(f_1(n))$ và $O(f_2(n))$ thì thời gian thực hiện lệnh rẽ nhánh là: $O(max(f_1(n), f_2(n)))$.
- Câu lệnh lặp: Giả sử thời gian thực hiện phần thân của lệnh lặp là $O(f(n))$ và số lần lặp tối đa của vòng lặp là $g(n)$ thì thời gian thực hiện của cả vòng lặp là $O(f(n).g(n))$.
- Sau khi đánh giá được thời gian thực hiện của tất cả các câu lệnh trong chương trình, thời gian thực hiện của toàn bộ chương trình sẽ là thời gian thực hiện của câu lệnh có thời gian thực hiện lớn nhất.

1.4.3.2 Độ an toàn của một hệ mật

Có hai quan niệm chính về độ an toàn của một hệ mật là *độ an toàn tính toán* và *độ an toàn không điều kiện.*

Độ an toàn không điều kiện (unconditional security): Là độ an toàn của các hệ mật khi không có hạn chế nào được đặt ra về khối lượng tính toán mà thám mã được phép thực hiện. Dựa trên quan niệm này, Shannon đã đề xuất khái niệm *độ an toàn hoàn hảo* (perfect secrecy) trong [65]. Tuy nhiên sự phát triển bùng nổ của mật mã

học hiện đại lại không đi theo hướng xây dựng các hệ mật có *độ an toàn không điều kiện*, điều chỉ có thể xảy ra khi độ dài khóa lớn hơn hoặc bằng độ dài bản rõ. Hầu hết các hệ mật hiện đại đều được đánh giá về độ an toàn theo khái niệm *độ an toàn tính toán.*

Độ an toàn tính toán (computational security): Liên quan đến những nỗ lực tính toán cần thiết để phá một hệ mật. Trên thực tế, người ta gọi một hệ mật là *an toàn về mặt tính toán* nếu có một phương pháp tốt nhất phá hệ mật mật này nhưng yêu cầu thời gian lớn đến mức không chấp nhận được. *Độ an toàn ngữ nghĩa (semantically secure)* hay *độ an toàn chứng minh được (provably secure)* thực chất là một trường hợp cụ thể của *độ an toàn tính toán*. Khái niệm này do Goldwasser và Micali đưa ra trong [88]. Cụ thể là, một hệ mật được gọi là *an toàn ngữ nghĩa* nếu với bản mã c cho trước của một bản rõ m nào đó chưa biết (trong không gian bản rõ) cùng với độ dài l của bản rõ, xác suất để kẻ tấn công xác định được bất kỳ một phần thông tin nào của m trong toán thời gian đa thức là *không đáng kể (negligible)*. Nói cách khác, một hệ mật là *an toàn ngữ nghĩa* nếu không tìm được một thuật toán chạy trong thời gian đa thức để khôi phục thông tin về m từ c với một xác suất đủ lớn. Mặc dù có vẻ thực tế hơn *độ an toàn hoàn hảo*, khái niệm *độ an toàn ngữ nghĩa* lại không có công cụ tường minh để đánh giá. Do vậy, trong [87], Goldwasser và Micali đã chứng minh *độ an toàn ngữ nghĩa* là tương đương với một khái niệm độ an toàn khác là *không thể phân biệt bản mã* (ciphertext indistinguishability) *với tấn công bằng bản rõ chọn trước* (IND-CPA: Indistinguishability Under Chossen Plaintext Attack). Khái niệm IND-CPA được sử dụng rộng rãi vì nó cung cấp một công cụ rõ ràng để chứng minh độ an toàn của các hệ mật trên thực tế. Ngoài ra, do có nhiều loại tấn công mạnh hơn CPA như CCA hay mạnh nhất là CCA2, trên thực tế người ta còn sử dụng IND-CCA hay IND-CCA2 là các mức độ *an toàn tính toán* của các hệ mật [60].

Để chứng minh một hệ mật là *an toàn ngữ nghĩa* với một tấn công nào đó, ta cần chỉ ra rằng xác suất để $\mathcal{A}$, bằng thủ tục tấn công đó, là *không đáng kể* và thường thể hiện bằng một *hàm không đáng kể (negligible function)* nào đó.

Định nghĩa 1-10: Một hàm $f(n)$ được gọi là không đáng kể của biến n nếu với mọi hằng số c, luôn tồn tại một một số nguyên N_0 sao cho $f(n) < n^{-c}$ khi $n > N_0$.

Một số hàm không đáng kể quan trọng có thể kể đến là 2^{-n}, $2^{-\sqrt{n}}$ hay $2^{-\log n}$.

Ví dụ với tấn công phân biệt bằng bản rõ được chọn, một hệ mật được coi là an toàn với tấn công này (IND-CPA) nếu như xác suất để $\mathcal{A}$ xác định bản mã trả về

là mã hóa cho một trong hai bản rõ được chọn trước là ½ + $f(n)$, trong đó $f(n)$ là một *hàm không đáng kể* (giá trị $\frac{1}{2}$ là xác suất $\mathcal{A}$ đoán đúng một cách ngẫu nhiên) của biến số giá trị độ dài khóa n được sử dụng.

Định nghĩa 1-11: Một hệ mật khóa bí mật được gọi là không thể phân biệt (IND-EAV) bằng nghe lén nếu xác suất để tấn công $"Sec" \text{ “K”}_{\mathcal{A},\Pi}^{eav}(n)$ thành công là một hàm không đáng kể.

Định nghĩa 1-12: Một hệ mật khóa bí mật được gọi là không thể phân biệt (IND-CPA) bằng nghe lén nếu xác suất để tấn công $"Sec" \text{ “K”}_{\mathcal{A},\Pi}^{cpa}(n)$ thành công là một hàm không đáng kể.

1.4.3.3 Hiệu năng của một hệ mật

Ngoài độ an toàn, một số tham số khác thường được sử dụng để đánh giá một số hệ mật bao gồm [17]:

- Kích thước khoá và không gian khoá: Thường được tính bằng số bit độ dài của khóa và hệ quả là không gian khóa.
- Kích thước khóa cũng ảnh hưởng trực tiếp đến độ phức tạp tính toán của thủ tục mã hóa và giải mã;
- Độ phức tạp tính toán của thủ tục mã hoá và giải mã, thường được tính và so sánh với nhau theo bậc O;
- Hệ số mở rộng bản tin: Là tỉ lệ giữa kích thước bản mã đầu ra trên kích thước bản rõ đầu vào, giá trị này thể hiện hiệu quả mã hóa của hệ mật. Thông thường thì giá trị này luôn lớn hơn 1 và càng nhỏ thì càng tốt.

Ngoài ra, *tính lan truyền sai* cũng là một tham số cần lưu ý khi đánh giá các hệ mật đặc biệt là các hệ mật khóa bí mật.

Việc đánh giá hiệu quả trong cài đặt hệ thống, được đánh giá qua các tham số là:

- Diện tích bề mặt: có thể tính bằng $micro\ m^2$, nhưng giá trị này phụ thuộc vào công nghệ chế tạo và thư viện chuẩn. Diện tích tính theo GE được tính bằng cách chia diện tích theo $micro\ m^2$ cho S cổng $NAND$ 2 đầu vào.
- Số chu kỳ xung nhịp: là số chu kỳ xung nhịp cần để tính toán và đọc dữ liệu ra.

- Thời gian: lượng thời gian cần thiết cho một phép tính cụ thể được tính bằng cách chia số chu kỳ xung nhịp cho tần số hoạt động t (số chu kỳ xung nhịp)/tần số. Đơn vị tính theo mi ni giây (ms).
- Thông lượng: là số các bit đầu ra chia cho 1 lượng thời gian nào đó. Đơn vị là bps.
- Nguồn: tiêu thụ nguồn được ước lượng ở mức cổng thông qua bộ biên dịch cài đặt; việc ước lượng tiêu thụ ở mức transistor là chính xác nhất.
- Năng lượng: việc tiêu thụ năng lượng được coi là tiêu thụ nguồn qua một khoảng thời gian cụ thể; nó thường được tính toán bằng cách nhân tiêu thụ nguồn với thời gian cần cho phép tính đó.
- Dòng điện: là lượng tiêu thụ nguồn chia cho điện áp thông thường.
- Tính hiệu quả của việc cài đặt: tính bằng diện tích chia cho thông lượng.

1.5 KẾT LUẬN CHƯƠNG

Mật mã hạng nhẹ đã và đang được quan tâm không những trên thế giới mà cả Việt Nam, đặc biệt trong thời gian tới, Việt Nam định hướng xây dựng đô thị thông minh, trong đó thiết bị IoT có vai trò chủ đạo, kèm theo đó việc đảm bảo an toàn thông tin cho thiết bị IoT là vấn đề được ưu tiên hành đầu sau những tính năng mà thiết bị IoT mang lại. 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 MỞ ĐẦU CHƯƠNG

Với mục tiêu là xây dựng các hệ mật trên vành đa thức ứng dụng được vào thiết bị có tài nguyên hạn chế, trên cơ sở nghiên cứu về các đặc điểm của vành đa thức ở chương 1, chương này sẽ trình bày một chuỗi hệ mật trên vành đa thức với những cải tiến kế tiếp nhau, được coi như điển hình trong việc ứng dụng vành đa thức. Đồng thời cũng phân tích, chỉ ra nhược điểm còn tồn tại để từ đó tiếp tục cải tiến, xây dựng hệ mật mới nhằm từng bước hạn chế nhược điểm, gia tăng được lợi thế ứng dụng của vành đa thức trong mật mã, đặc biệt trong lĩnh vực mật mã hạng nhẹ.

Nội dung chương 2 được chia làm 4 phần: phần 2 là chuỗi các hệ mật trên vành đa thức được xây dựng, cải tiến từ hệ mật OTP; phần 3 giới thiệu một cải tiến tiếp theo của hệ mật OTP, đồng thời ứng dụng mô hình hệ mật lai ghép để xây dựng hệ mật QRHE và vấn đề còn tồn tại; phần 4 là nội dung chính của chương, mô tả chi tiết hệ mật CBC-QRHE có khả năng chống tấn công CPA và thử nghiệm, cài đặt đánh giá hệ mật CBC-QRHE trên máy tính.

Các kết của của chương này đã được công bố trong công trình [C1].

2.2 CÁC CẢI TIẾN CỦA HỆ MẬT OTP TRÊN VÀNH ĐA THỨC

2.2.1 Hệ mật khóa bí mật OTP

Hệ mật OTP (One-Time Pad) là một hệ mật học cổ điển và đã được công bố từ thế kỷ thứ 19. Công trình đầu tiên liên quan đến OTP được đưa ra bởi Frank Miller, một nhà mật mã học người Mỹ, vào năm 1882. Tác giả đã mô tả nguyên tắc hoạt động và tính bảo mật của OTP trong công trình [23]. Sau đó, năm 1917, Hệ mật OTP chính thức được công bố trong công trình số [43] bởi Major Joseph Mauborgne và AT&T's Gilbert Vernam.

Hệ mật OTP hoạt động trên trường $GF(2)$ với các phép mã hóa và giải mã đều là các phép tính XOR rất đơn giản với độ phức tạp tính toán là $O(n)$ trong đó n là độ dài khóa. Ngoài ra, OTP hiện vẫn là hệ mật an toàn và vẫn được sử dụng trong các lĩnh vực rất đặc thù đòi hỏi độ an toàn rất cao như quốc phòng, an ninh và ngoại giao.

Tuy nhiên, nhược điểm lớn nhất của OTP là khóa bí mật phải được chọn ngẫu nhiên và chỉ được sử dụng duy nhất một lần để tránh tấn công KPA. Ngoài ra, khóa bí mật của OTP cần có độ dài ít nhất bằng độ dài bản rõ dẫn đến hiệu quả mã hóa không cao. Những nhược điểm này khiến cho OTP không phù hợp với các ứng dụng trong thương mại. Trên thực tế, các nghiên cứu mật mã khóa bí mật cũng đều đi theo hướng xây dựng các hệ mật có khả năng mã hóa những bản tin dài với khóa ngắn và có thể tái sử dụng mà vẫn đảm bảo độ an toàn ngữ nghĩa thay vì xây dựng các hệ mật có độ an toàn hoàn hảo.

Hệ mật OTP cũng đã được đề cập và nghiên cứu trong nhiều công trình về mật mã học và an ninh thông tin. Các công trình nổi tiếng liên quan đến OTP phải kể đến là công trình của Claude Shannon, nhà toán học và kỹ sư điện tử người Mỹ, đã công bố một bài báo quan trọng trong lĩnh vực mật mã học năm 1949 [27] . Trong bài báo này, tác giả nêu rõ nguyên lý hoạt động của OTP và đưa ra một phân tích toán học chi tiết về tính bảo mật của nó, ông đã chứng minh rằng OTP là một trong những hệ mật được coi là một trong những hệ mật an toàn tuyệt đối. Đến năm 1996, trong cuốn [23], Bruce Schneier, một chuyên gia an ninh máy tính nổi tiếng, đã trình bày nhiều khía cạnh của mật mã học, trong đó giải thích cách sử dụng và cung cấp lời khuyên về việc triển khai OTP một cách an toàn.

Thuật toán của hệ mật OTP rất đơn giản, chỉ là một phép XOR đơn giản giữa bản tin cần gửi và khóa, thuật toán này đã được chứng minh là hoàn hảo với điều kiện khóa là hoàn toàn ngẫu nhiên và chiều dài khóa bằng chiều dài bản tin.

Gọi m là bản tin cần gửi, k là khóa, bản mã C được tính như sau:

$$c = E(m,k) = m \oplus k \tag{2.1}$$

Bên nhận giải mã cũng bằng phép tính XOR như sau:

$$D(c,k) = c \oplus k = m \oplus k \oplus k = m \tag{2.2}$$

2.2.2 Hệ mật khóa bí mật RISKE

Ý tưởng cốt lõi của hệ mật OTP rất thú vị, điểm mấu chốt để đảm bảo hệ mật OTP là hoàn hảo là khóa hoàn toàn ngẫu nhiên và được thay đổi theo từng phiên giao dịch. Tuy nhiên, trong thực tế các ứng dụng thương mại, để cân bằng giữa yếu tố chi phí với độ mật, không cần hệ mật có độ mật hoàn hảo, mà chỉ cần hệ mật có độ an toàn ngữ nghĩa là được. Trong quá trình nghiên cứu về mật mã trên vành đa thức chẵn, tác giả Cao Minh Thắng nhận thấy rằng nếu thay thế phép cộng đa thức trong

OTP bằng một phép nhân trong vành đa thức thì có thể sử dụng các phần tử khả nghịch trong R_n để làm khóa cho một hệ mật khóa bí mật và nếu tập này đủ lớn thì hệ mật sẽ đạt mức an toàn ngữ nghĩa nào đó. Ý tưởng này đã được tác giả xây dựng thành một hệ mật khóa bí mật, gọi là RISKE (Random Invertible Secret-Key Encryption scheme) và công bố trong công trình [26]. Trong công trình này, tác giả đã cải tiến hệ mật bằng cách sử dụng vành đa thức chẵn R_{2n} để xây dựng một hệ mật có độ phức tạp mã hóa và giải mã tương đương với OTP nhưng có khóa bí mật ngắn hơn độ dài của bản tin mà vẫn đảm bảo hệ mật có độ an toàn chứng minh được. Thực tế, thuật toán mã hóa và giải mã trong OTP thực ra là một phép cộng trong vành đa thức R_n trong đó độ dài bản rõ, bản mã và khóa đều là n bit. Hệ mật mới đã thay thế phép cộng đa thức trong OTP bằng một phép nhân trong vành đa thức và sử dụng các phần tử khả nghịch trong R_n để làm khóa cho một hệ mật khóa bí mật, tác giả cũng đã chứng minh được nếu tập khóa này đủ lớn thì hệ mật sẽ đạt mức an toàn ngữ nghĩa. Ngoài ra, nếu chọn khóa ngắn hơn bản rõ mà vẫn đảm bảo mức an toàn ngữ nghĩa thì hệ mật mới còn hiệu quả hơn hệ mật OTP. Hơn thế nữa, tác giả cũng đã chứng minh được tất cả các đa thức có trọng số Hamming lẻ trong lớp vành đa thức chẵn tuyệt đối R_{2^k} là khả nghịch, là một tập con của vành đa thức chẵn R_{2n}, hệ mật RISKE có độ phức tạp tính toán $O(n^2)$ với độ dài khóa không nhất thiết phải bằng độ dài bản tin mà vẫn có độ an toàn IND-CPA.

Bảng 2-1: Lưu đồ của hệ mật RISKE

<table>
<tr><td colspan="2">A và B muốn truyền tin bảo mật với nhau, trước khi giao dịch hai bên cần phải thống nhất các tham số:
- Vành đa thức chẵn tuyệt đối $R_n,\ n = 2^k$
- Độ dài của bản tin cần truyền N, với điều kiện $N < n$
- Khóa bí mật K, là một đa thức khả nghịch ngẫu nhiên trong R_n bậc của K là $|K| = 2^{N-1} - 1 = n - 1$</td></tr>
<tr><td>A mã hóa m thành C sau đó gửi sang B</td><td>A chia dữ liệu cần truyền thành các bản tin m có chiều dài N bit, sau đó định dạng bản tin trước khi mã hóa thành bản tin M như sau:
$$M = (w(m) + 1) mod\ 2.x^{n-1} + m$$
Sau đó mã hóa bản tin M thành C như sau:</td></tr>
</table>

	$C = \mathrm{M} * \mathrm{K}$
B nhận được C và giải mã để lấy bản tin m	B giải mã C để lấy M: $\mathrm{C} * \mathrm{K}^{-1} = M * K * K^{-1} = M$ Sau đó, khôi phục m từ M: $m = M_{n-1}.x^{n-1} + M$

Bảng 2-2: Ví dụ về hệ mật RISKE

A và B truyền tin bảo mật với nhau, trước khi giao dịch hai bên thống nhất các tham số: - Vành đa thức chẵn tuyệt đối $R_8,\ n = 2^3 = 8.$ - Độ dài của bản tin cần truyền $N = 7$, thỏa mãn điều kiện $N < n.$ - Khóa bí mật $K = (00111)$ dạng nhị phân hay $K(x) = x^2 + x + 1$ dạng đa thức, khi đó $K^{-1}(x) = x^7 + x^5 + x^4 + x^2 + x.$	
A mã hóa m thành C sau đó gửi sang B	A chia dữ liệu cần truyền thành các bản tin m có chiều dài 7 bit, ví dụ: $m = (1010011)$ hay $m(x) = x^6 + x^4 + x + 1$ sau đó định dạng bản tin trước khi mã hóa thành bản tin M như sau: $M = (w(m) + 1) mod 2.x^{n-1} + m$ $= (4 + 1) mod 2.x^7$ $+ (x^6 + x^4 + x + 1)$ $= x^7 + x^6 + x^4 + x + 1$ Sau đó mã hóa bản tin M thành C như sau: $C = \mathrm{M} * \mathrm{K} = (x^7 + x^6 + x^4 + x + 1) * (x^2 + x + 1)$ $= x^5 + x^4 + x^3 + x + 1$
B nhận được C và giải mã để lấy bản tin m	B giải mã C để lấy M: $\mathrm{M} = \mathrm{C} * \mathrm{K}^{-1} = (x^5 + x^4 + x^3 + x + 1)$ $* (x^7 + x^5 + x^4 + x^2 + x)$ $= x^7 + x^6 + x^4 + x + 1$

	Sau đó, khôi phục m từ M: $M_{n-1}.x^{n-1} + M = x^7 + (x^7 + x^6 + x^4 + x + 1)$ $= x^6 + x^4 + x + 1 = m(x)$

Như vậy, so với hệ mật nguyên gốc OTP, hệ mật RISKE có kích thước khóa nhỏ hơn, điều này sẽ giúp hệ mật hiệu quả hơn khi triển khai trên môi trường thực tế. Đặc biệt, hệ mật RISKE cũng đã được chứng minh là có độ an toàn ngữ nghĩa IND-CPA [26], được coi là đã giải quyết được vấn đề đặt ra ban đầu về việc phù hợp với các ứng dụng thương mại. Tuy nhiên, để đạt được điều này, hệ mật RISKE cần phải đánh đổi một tham số là độ phức tạp tính toán, so với hệ mật OTP có độ phức tạp tính toàn là $O(n)$, thì độ phức tạp tính toán của hệ mật RISKE là $O(n^2)$, nhưng xét về tổng thể, với phần cứng, tốc độ tính toán hiện nay, thì hệ mật RISKE vẫn được coi là một cải tiến hiệu quả so với hệ mật OTP.

Tuy nhiên, hệ mật khóa bí mật RISKE vẫn có một nhược điểm là phải sử dụng khóa phiên (session-key) giống như hệ mật OTP. Do vậy, để phù hợp với các ứng dụng thực tế, RISKE cần phải được sử dụng kết hợp với một hệ mật khóa công khai phù hợp và thường là theo mô hình KEM/DEM như đã giới thiệu ở mục 2.2. Bên cạnh đó, xét về hiệu năng, phép mã hóa và giải mã của RISKE vẫn là phép nhân đa thức có độ phức tạp $O(n^2)$. Để giải quyết vấn đề này, trong công trình [13], tác giả Cao Minh Thắng đã tiếp túc đề xuất một hệ mật lai ghép dựa trên các thặng dư bậc hai và các phần tử liên hợp trong vành đa thức chẵn, gọi là QRHE (Quadratic Residue Hybrid Encryption scheme). Hệ mật lai ghép QRHE có các thuật toán mã hóa và giải mã đơn giản hơn, chủ yếu sử dụng phép cộng trong vành đa thức với độ phức tạp $O(n)$. Ngoài ra, thủ tục tạo khóa được cải tiến so với RISKE làm giảm độ phức tạp khi sử dụng khóa phiên bằng cách sử dụng thặng dư bậc hai và các phần tử liên hợp trong vành đa thức R_{2n}. Với các cải tiến này, hệ mật QRHE cũng được đánh giá là phù hợp với thiết bị có tài nguyên hạn chế.

2.2.3 Hệ mật lai ghép QRHE

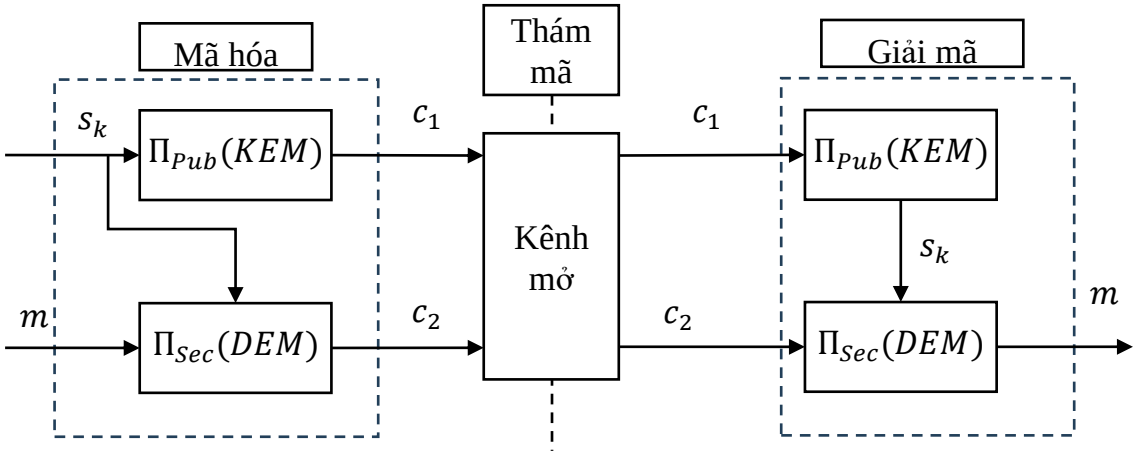
Hệ mật QRHE là hệ mật lai ghép, dựa trện hệ mật RISKE và hoạt động dựa trên đặc tính của các thặng dư bậc hai và các phần tử liên hợp của chúng trong vành chẵn R_{2n}. Phần tiếp theo sẽ giới thiệu về tổng quan về hệ mật lai ghép cũng như ứng dụng mô hình lai ghép để xây dựng hệ mật QRHE.

2.2.3.1 Giới thiệu về hệ mật lai ghép

Các hệ mật khóa bí mật có hiệu quả tính toán cao (chủ yếu sử dụng các phép cộng, AND, OR,…) và có thể mã hóa một bản tin dài bằng một khóa bí mật ngắn. Tuy nhiên, nhược điểm của loại hệ mật này là khóa bí mật cần phải được chia sẻ trước giữa hai bên gửi và nhận [13].

Ngược lại, ưu điểm của các hệ mật khoá công khai là hai bên gửi nhận không phải thoả thuận khoá bí mật. Tuy nhiên, nhược điểm của các hệ mật này là hiệu quả mã hoá thường không cao [13] vì hệ số mở rộng bản tin lớn (luôn lớn hơn 1) và độ phức tạp tính toán của các thuật toán cũng thường cao hơn so với các hệ mật khóa bí mật.

Giải pháp để khắc phục các nhược điểm cũng như tận dụng các ưu điểm của hai loại hệ mật trên là sử dụng mô hình mật mã lai ghép (hybrid cryptography). Ý tưởng này được khởi xướng bởi Cramer và Shoup trong [32] với mô hình KEM/DEM như trên Hình 2-1. Mô hình KEM/DEM là một cách đơn giản để xây dựng các hệ mật khóa công khai hiệu quả và rất được chú ý nghiên cứu. Vì đặc tính đơn giản và linh hoạt mô hình này được sử dụng trong một số tiêu chuẩn mã hóa mới [94].



Hình 2-1: Mô hình mật mã lai ghép KEM/DEM

Với mô hình trên, ở phía mã hóa, khóa bí mật sk của một hệ mật khóa bí mật Π_{Sec} (phần DEM) sẽ được mã hóa bằng một hệ mật khóa công khai Π_{Pub} (phần KEM) với khóa công khai p_k thành bản mã c_1 còn bản tin m sẽ được mã hóa bằng một hệ mật khóa bí mật Π_{Sec} thành bản mã c với khóa bí mật s_k ở trên. Bản mã gửi từ bên mã hóa tới bên giải mã sẽ là (c_1, c_2). Tại phía giải mã, đầu tiên thuật toán giải

mã của phần KEM sẽ được sử dụng để giải mã bản mã c_1 lấy khóa s_k sau đó dùng khóa s_k và thuật toán giải mã của phần DEM để khôi phục bản tin m.

Hệ mật lai ghép được sử dụng phổ biến nhất là OpenPGP (RFC 4880) và PKCS#7 (RFC 2315).

Độ an toàn của các hệ mật lai ghép phụ thuộc vào độ an toàn của các hệ mật thành phần. Cụ thể là, nếu cả hai hệ mật thành phần đều có độ an toàn IND-CPA hay IND-CCA thì hệ mật lai ghép cũng thừa hưởng đặc tính đó [32]. Tuy nhiên, vẫn có thể xây dựng được hệ mật lai ghép có đặc tính IND-CCA dù hệ mật khóa công khai thành phần có độ an toàn thấp hơn [94].

2.2.3.2 Hệ mật lai ghép QRHE

a) Cơ sở toán học

Hệ mật lai ghép QRHE là hệ mật trên vành da thức dựa trên tập các thặng dư bậc hai (QR) và tập các phần tử liên hợp (CE) trong vành đa thức chẵn R_{2n}.

Tập các thặng dự bậc hai trong R_{2n} (ký hiệu là Q_{2n}) được xác định như sau:

$$Q_{2n} = \{f\} |\ g^2 = f, \forall g \in R_{2n} \tag{2.3}$$

Trong đó, đa thức g được gọi là căn bậc hai, đa thức f được gọi là thặng dư bậc hai.

Trong R_{2n} có thể có nhiều căn bậc hai cho cùng thặng dư bậc hai, các căn bậc hai này được gọi là phần tử liên hợp của cùng một thặng dư bậc hai.

Trong công trình [13], tác giả đã chững minh được rằng mọi đa thức g trong trong R_{2n} luôn có thể biểu diễn dưới dạng:

$$g = (1 + x^n) * \sum_{t \in U} x^t + \sqrt{g^2} \tag{2.4}$$

Với U là một tập hợp gồm các tổ hợp tùy ý trong tập $s = \{\overline{0, n-1}\}$.

Công thức (2.4) là ý tưởng chính để xây dựng thuật toán của hệ mật QRHE, cụ thể, nếu ta có thể biểu diễn khối thông tin thành các bản rõ là các đa thức m trong vành R_{2n}, thì các bản rõ có thể được biểu diễn như sau:

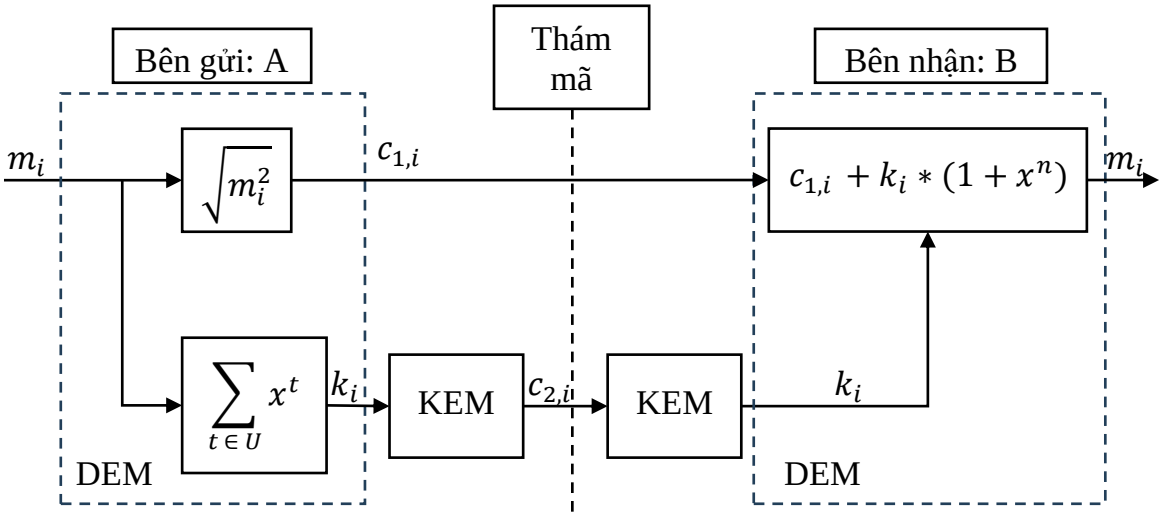
$$m = (1 + x^n) * k + l \tag{2.5}$$

Trong đó l được coi là bản mã 1 ($c_1 = l$), $c_2 = (1 + x^n) * k$ được coi là bản mã 2:

$$l = \sqrt{m^2}\ v\grave{a}\ k = \sum_{t \in U} x^t \qquad (2.6)$$

Ở đây, k được coi là khóa bí mật, chỉ có khóa k mới giải mã để lấy thông tin m từ c_1 và c_2 được.

Với đặc điểm này, công trình [13] đã đề xuất hệ mật QRHE với cấu trúc đại số nền tảng và các tham số của hệ mật được tóm tắt trong Bảng 2-3 và sơ đồ và hoạt động của hệ mật này được mô tả trên Hình 2-2. Có thể thấy, QRHE là một biến thể của sơ đồ lai ghép KEM/DEM [45].



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

Trong đó, tham số:

- i là phiên thứ i của giao dịch.
- j là hệ số thứ j (hoặc bit thứ j) của đa thức.
- U là một tập hợp gồm các tổ hợp tùy ý trong tập $s = \{\overline{0, n-1}\}$.
- t là số ngẫu nhiên thuộc tập U.

Ngoài ra, trong [13], tác giả cũng đã chứng minh được rằng: với mọi đa thức f trong tập các thặng dư bậc hai trong R_{2n} (được ký hiệu và Q_{2n}) có căn bậc hai là tổng của các căn bậc hai chính của các đơn thức trong đa thức f. Điều đó cho thấy căn bậc hai chính của bình phương một đa thức bất kỳ trong vành đa thức chẵn có độ phức tạp tính toán $O(n)$, tương đương với độ phức tạp tính toán của phép cộng đa thức trong vành.

b) Thủ tục tạo khóa

Để hệ mật QRHE hoạt động đúng, trước tiên, các khối thông tin cần được mã hóa thành đa thức m_i trong R_{2n}, m_i có bậc là $2n$ được gọi là bản rõ của hệ mật.

Tiếp theo, A sẽ tính khóa bí mật k_i với các hệ số k_{ij} được xác định như sau:

$$k_{ij} = m_{i(j+n)} \tag{2.7}$$

Bảng 2-3: Cấu trúc đại số nền tảng của QRHE

Tham số	**Giá trị**
Vành đa thức	$R_{2n} = Z_2[x] \setminus (x^{2n}+1), \mathrm{n} \in \mathrm{Z}^*$
Không gian bản rõ	$P = R_{2n}$
Không gian bản mã	$C = R_{2n}$
Kích thước bản rõ	2n
Kích thước bản mã	$\geq$ 2n
Kích thước khóa	n
Không gian khóa	$K = R_n$

khóa này sau đó sẽ được mã hóa bằng một hệ mật khóa công khai nào đó (phần KEM) để tạo từ mã $c_{i,2}$.

c) Thủ tục mã hóa

A sẽ xác định được các hệ số của bản mã $c_{1,i}$ như sau

$$c_{1,ij} = \left(m_{ij} + m_{i(j+n)}\right) mod\ 2 \tag{2.8}$$

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

d) Thủ tục giải mã

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

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

$$m_{ij} = \begin{cases} \left(c_{1,ij} + k_{ij}\right) mod\ 2 & với \quad 0 \leq j \leq (n-1) \\ k_{i(j-n)} & với \quad n \leq j \leq (2n-1) \end{cases} \tag{2.9}$$

2.2.3.3 Ưu, nhược điểm của QRHE

a) Ưu điểm

Ưu điểm rõ rệt nhất của QRHE là độ phức tạp tính toán của các thuật toán chỉ là $O(n)$. Đặc biệt, QRHE không sử dụng các khóa bí mật mà tự sinh khóa từ bản rõ ở mỗi phiên. Ngoài ra, việc mã hóa mỗi bản rõ 2*n* bit quy về việc mã hóa một khóa bí mật chỉ có *n* bit.

Ngoài ra, QRHE còn giúp cải thiện hiệu tỉ lệ giữa kích thước bản mã trên kích thước bản rõ của các hệ mật khóa công khai, vốn có hiệu quả mã hóa không cao. Với đặc điểm này, QRHE được coi là phù hợp với thiết bị có tài nguyên hạn chế.

b) Nhược điểm

Nhược điểm lớn nhất của QRHE là sự bất định (derministic) theo đó mỗi bản rõ m_i sẽ cho một bản mã $c_{1,i}$ tương ứng. Như vậy nếu thám mã sử dụng thủ tục tấn công CPA sẽ biết chính xác bản mã c thu được là của bản rõ nào trong hai bản rõ thách thức (thủ tục tấn công CPA cụ thể được mô tả trong [7] và [8]).

Tất nhiên, việc tìm ra bản rõ tương ứng trong tấn công CPA với QRHE cũng chưa thực sự tìm được đầy đủ thông tin bản rõ vì giá trị này còn phụ thuộc vào n bit khóa ki được che dấu bởi phần KEM là một hệ mật khóa công khai nào đó. Mặc dù vậy, việc biến bản mã $C_{1,i}$ thành ngẫu nhiên ở mỗi phiên mã hóa cũng là rất cần thiết để tránh khai thác thông tin về bản rõ từ các tấn công CPA.

2.2.3.4 Vấn đề còn tồn tại của QRHE

QRHE là một hệ mật lai ghép có hiệu quả mã hóa rất cao nhưng nhược điểm của hệ mật này là không an toàn với các tấn công bằng bản rõ chọn trước (CPA: Chosen Ciphertext Attack). Để khắc phục hạn chế trên, bài báo [C1] trình bày một sơ đồ cải tiến theo chế độ CBC (Cipher Block Chaining) của hệ mật lai ghép QRHE có khả năng chống lại các tấn công CPA đơn giản và có thể sử dụng trong các ứng dụng mã xác thực bản tin (MAC: Message Authentication Code)

Xây dựng các hệ mật có độ phức tạp tính toán thấp và tiêu tốn ít tài nguyên là động lực của khoa học mật mã trong xu hướng IoT. Một trong những giải pháp được sử dụng là lựa chọn cấu trúc đại số vành đa thức để xây dựng các hệ mật. Với các phép tính có độ phức tạp tính toán thấp, các hệ mật dựa trên vành đa thức hầu như đều có thuật toán mã hóa giải mã đơn giản, tốc độ tính toán cao [56].

Ứng dụng của các phần tử khả nghịch trên vành đa thức $R_{n,q} = Z_q[x] \backslash (x^n + 1)$ trong mật mã điển hình là hệ mật khóa công khai xác suất nổi tiếng NTRU [56] và các biến thể như CTRU [45] và đặc biệt là pNE [39], một hệ mật dựa trên vành $R_{2^s,q} \mid s \in Z^*$ cho đến nay có thể coi là biến thể duy nhật của NTRU có độ an toàn chứng minh được.

Đối với các vành đa thức$R_{2n} = Z_2[x]\ (x^{2n} + 1), \mathrm{n} \in \mathrm{Z}^*$ một số hệ mật có độ phức tạp tính toán thấp được xây dựng như trong [25], [26] trong đó đáng chú ý là hệ mật QRHE [13] hoạt động dựa trên các thặng dư bậc hai và lớp các phần tử liên hợp với căn bậc hai chính của thặng dư đó [56]. Đặc điểm nổi bật của hệ mật QRHE là có thuật toán tạo khóa, mã hóa và giải mã rất đơn giản và hiệu quả mã hóa rất cao. So với các hệ mật lai ghép khác, QRHE không cần sử dụng khóa bí mật ngẫu nhiên cho mỗi phiên vì khóa của hệ mật này được sinh từ bản rõ cần mã hóa. Tuy nhiên, hệ mật này có một nhược điểm cố hữu là có thể bị khai thác với các tấn công CPA. Loại tấn công này dù không hoàn toàn phá được QRHE nhưng cũng làm giảm độ tin cậy của hệ mật này. Vấn đề đặt ra là liệu có thể cải tiến QRHE này sao cho vẫn tận dụng được các ưu điểm về hiệu năng mà vẫn đảm bảo an toàn với các tấn công CPA.

Phần tiếp theo trình bày giải pháp có thể chống được tấn công CPA của hệ mật QRHE. Mục [2.3] là sơ đồ đồ cải tiến của hệ mật QRHE nhằm chống tấn công CPA gọi là hệ mật CBC-QRHE.

2.3 HỆ MẬT LAI GHÉP CBC-QRHE

2.3.1 Giới thiệu về hệ mật CBC-QRHE

Theo lý thuyết, để chống được tấn công CPA, thì cần phải thay đổi bản mã với cùng bản rõ tại mỗi một phiên khác nhau; đối với hệ mật QRHE, thì ý tưởng là làm sao ở mỗi phiên mã hóa khác nhau cùng một bản rõ m_i sẽ cho ra các bản mã $c_{1,i}$ khác nhau. Thực tế, giải pháp thường thấy là sử dụng một dòng khóa ngẫu nhiên chung giữa 2 bên gửi và nhận để ngẫu nhiên hóa bản mã $c_{1,i}$. Nhược điểm của giải pháp này là phải có một bộ sinh khóa ngẫu nhiên và đồng bộ khóa này giữa hai bên gửi nhận.

Dựa trên đặc hiểm của vành đa thức chẵn R_{2n}, một khối thông tin đầu vào khi biểu diễn trên vành đa thức R_{2n} sẽ được phân tách thành hai phần, ý tưởng ở đây là lấy một phần thông tin từ bản rõ ở phiên bất kỳ làm một phần của khóa mã hóa dùng ở phiên sau. Hay nói cách khác, có thể sử dụng cơ chế hoạt động chuỗi khối mật mã (CBC: Cipher Block Chaining) của các hệ mật mã khối để xây dựng hệ mật QRHE

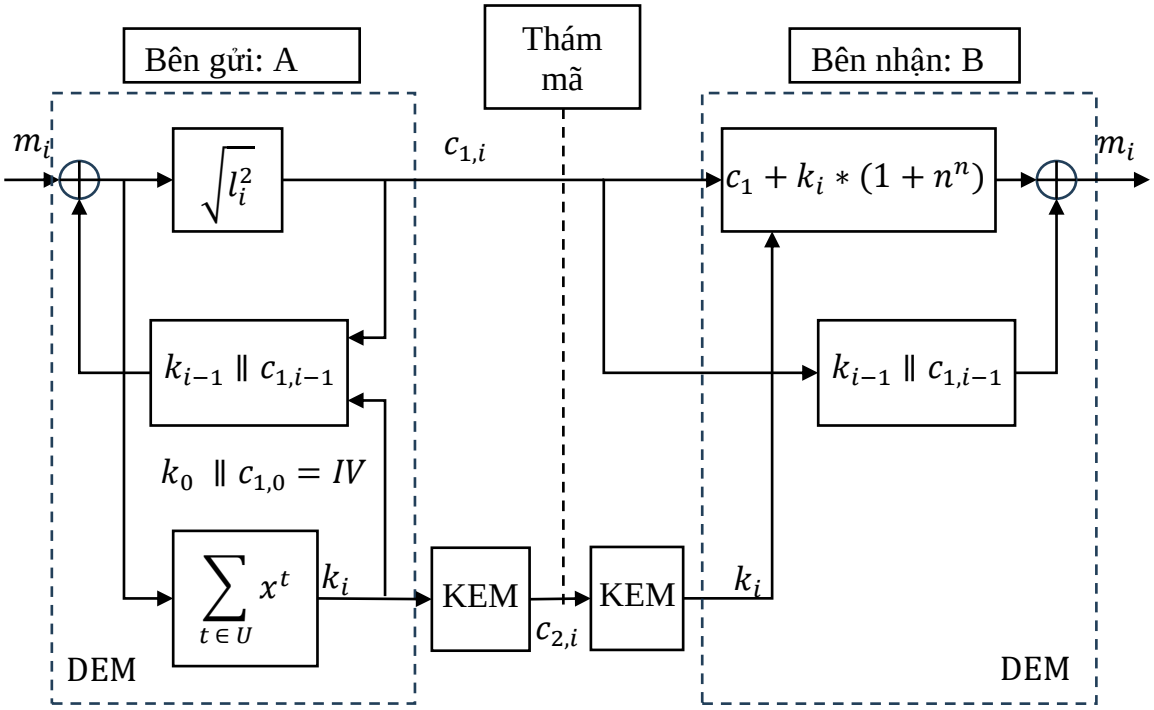
có khả năng chống tấn công CPA. Cơ chế này sẽ giúp loại bỏ khóa bí mật theo từng phiên như một số hệ mật khác như OTP.

Để tiện theo dõi và so sánh, ta gọi biến thể được đề xuất là CBC-QRHE.

2.3.2 Sơ đồ hoạt động của hệ mật CBC-QRHE

Sơ đồ hoạt động của hệ mật QRHE ở chế độ CBC được mô tả trên Hình 2-3.

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 2-3: 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: $Initial\ Vector$):

$$IV = k_0 \parallel c_{1,0} \qquad (2.10)$$

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.

2.3.2.1 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

$$l_i = m_i + k_{i-1} \parallel c_{1,i-1} \tag{2.11}$$

Tiếp đó A tính khóa

$$k_{ij} = l_{i(j+n)} \tag{2.12}$$

như trong QRHE

2.3.2.2 Mã hóa

Đầu tiên, A tính

$$c_{1,ij} = l_{ij} + l_{i(j+n)}\ mod\ 2 \tag{2.13}$$

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.

2.3.2.3 Giải mã

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

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

$$l_{ij} = \begin{cases} (C_{1,ij} + K_{ij})\ mod\ 2 & với \quad 0 \le j \le (n-1) \\ K_{i(j-n)} & với \quad n \le j \le (2n-1) \end{cases} \tag{2.14}$$

3. Tiếp đó, Bob khôi phục

$$m_i = l_i + k_{i-1} \parallel c_{1,i-1} \tag{2.15}$$

2.3.3 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

$$l_i = m_i + k_{i-1} \parallel c_{1,i-1} \tag{2.16}$$

và tương ứng ở phía giải mã là một phép cộng

$$m_i = l_i + k_{i-1} \parallel c_{1,i-1} \tag{2.17}$$

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.

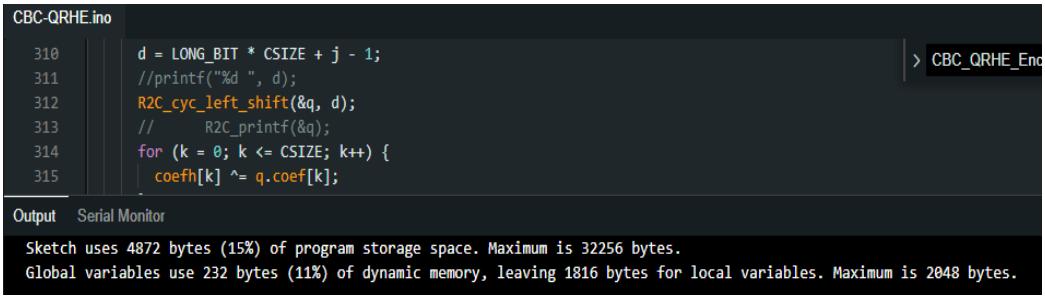
Bên cạnh đó, so với QRHE, sơ đồ CBC-QRHE cần phải lưu thêm $2n$ bit giá trị $k_{i-1} \parallel c_{1,i-1}$ để đảm bảo chế độ hoạt động CBC.

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.

2.4 THỬ NGHIỆM CÀI ĐẶT CBC-QRHE TRÊN THIẾT BỊ CÓ TÀI NGUYÊN HẠN CHẾ

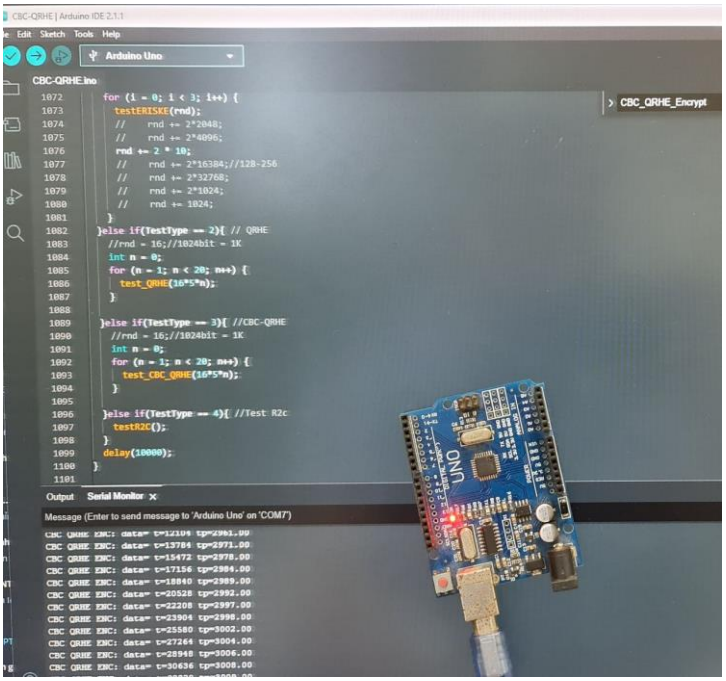
Hệ mật CBC-QRHE được thử nghiệm và đánh giá trên thiết bị Arduino UNO R3, thiết bị này có Vi điều khiển Atmega328 họ 8 bit, RAM 2KB rất nhỏ, hiện nay được coi là thiết bị có tài nguyên hạn chế. Toàn bộ mã nguồn của QRHE và CBC-QRHE được đóng gói và cài đặt trên thiết bị chiếm không gian lưu chữ là 4872 byte như Hình 2-4.



Hình 2-4: 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:

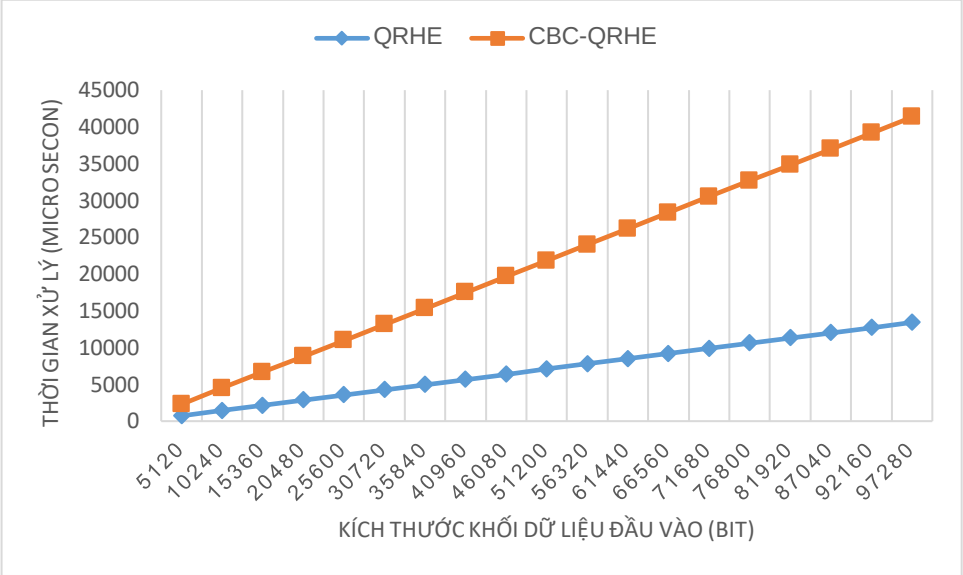
- Hệ mật hoạt động trên vành đa thức chẵn R_{2*32}, tức là mỗi một khối dữ liệu mà module mã hóa và giải mã phải xử lý là 64 bit, trong đó khóa được chọn là 32 bit.
- Các bản rõ đầu vào có kích thước tăng dần, bước nhảy là 5kb tăng dần trong mỗi lần thử.



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 2-5: 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 2-6, 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 2-6: So sánh tốc độ mã hóa 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 $45ms$.

2.5 KẾT LUẬN CHƯƠNG

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). Hệ mật này có độ phức tạp tính toán của thuật toán mã hóa và giải mã là $O(n)$, được coi là có khả năng phù hợp với thiết bị có tài nguyên hạn chế. Hệ mật đã được cài đặt trên thiết bị có tài nguyên hạn chế Arduino UNO R3, kết quả tương đối khả quan. 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, xây dựng hệ mật hoàn chỉnh, ứng dụng trong các giao dịch của các thiết bị có tài nguyên hạn chế trên thực tế trên mạng IoT.

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

3.1 MỞ ĐẦU CHƯƠNG

Hệ mật Omura-Massey (O-M) là một hệ mật tương đối đặc biệt, mỗi bên tham gia phiên giao dịch cần dùng hai khóa có tính chất nghịch đảo với nhau, tương tự như khóa bất đối của các hệ mật khóa công khai thường thấy, nhưng hai khóa của hệ mật O-M lại được giữ bí mật. Hệ mật O-M được xây dựng trên bài toán logarits rời rạc trên trường hữu hạn $GF(p)$, được coi là có nhiều tiềm năng ứng dụng; đến nay đã có nhiều công trình nghiên cứu, tiêu biểu 5 năm gần đây như [38], [68], [90], [93] nhưng chưa được nghiên cứu, xây dựng trên vành đa thức, cho thiết bị có tài nguyên hạn chế.

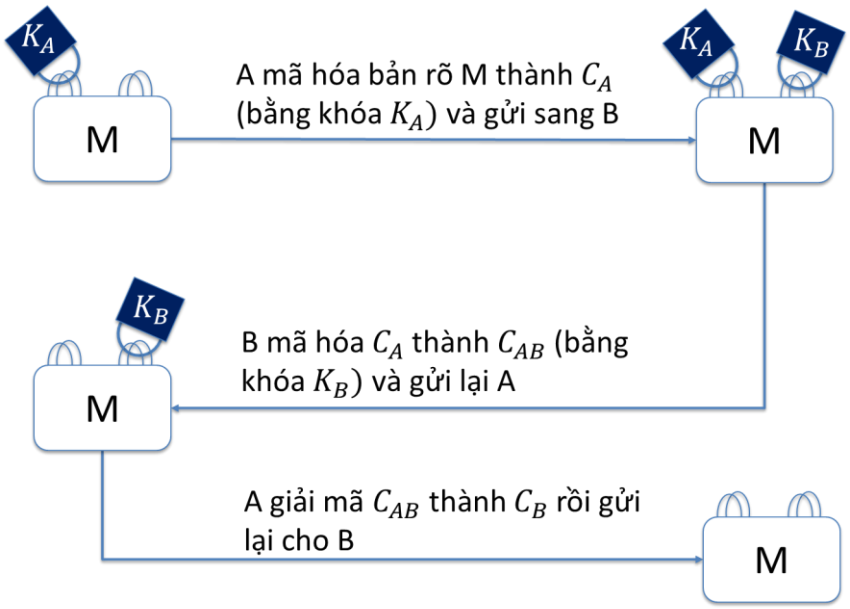
Vành đa thức là một cấu trúc toán học đặc biệt, được phân chia thành nhiều loại khác nhau với các tính chất, đặc điểm khác nhau. Trong đó, vành đa thức hai lớp kề Cyclic có nhiều công trình nghiên cứu được công bố cho đến nay, từ các công trình nghiên cứu về mặt lý thuyết như cấu trúc, tính chất của vành [4], [2], [8] đến ứng dụng vành đa thức hai lớp kề Cyclic để cải tiến, xây dựng các mã, các hệ mật như [2], [9], [13], [14], [16]. Vành đa thức hai lũy đẳng nguyên thủy cũng là một loại vành đặc biệt, nghiên cứu sơ bộ cho thấy vành đa thức hai lũy đẳng nguyên thủy có nhiều tính chất tương tự như vành Cyclic, nhiều tiềm năng nhưng chưa được khai thác.

Nhằm làm phong phú tính ứng dụng của hệ mật Omura-Massey, cũng như trả lời câu hỏi nghiên cứu 3 của luận án, chương này trình bày hai kết quả dùng hai loại vành đa thức khác nhau. Kết quả thứ nhất là hệ mật Omura-Massey trên vành đa thức có xác thực, sau đây gọi tắt là OM-CA. Hệ mật OM-CA là một cải tiến của hệ mật [9] trên vành đa thức hai lớp kề Cyclic, nhược điểm là chưa có tính xác thực, có nguy cơ bị tấn công người đứng giữa (MITM). NCS đã đề xuất bốn phương pháp để cải tiến hệ mật OM-CA để bổ sung tính nhận thực cho hệ mật, toàn bộ nghiên cứu đã được công bố trong công trình [J1], và đã chi tiết hóa trong mục [3.3] của chương này. Kết quả thứ hai là Hệ mật O-M trên vành đa thức hai lũy đẳng nguyên thủy, đây được coi là ứng dụng đầu tiên của vành đa thức hai lũy đẳng nguyên thủy vào mật mã. do đó, trong mục [3.4.2] đã trình bày chi tiết cơ sở toán học của việc dùng vành đa thức hai lũy đẳng nguyên thủy trong việc cải tiến hệ mật trên trường hữu hạn là tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường $GF(p)$,

sau đó mục [3.4.3] chi tiết các thủ tục của hệ mật O-M trên vành đa thức hai lũy đẳng nguyên thủy, toàn bộ nghiên cứu đã được công bố trong công trình [J2].

3.2 GIỚI THIỆU VỀ HỆ MẬT OMURA-MASSEY

Trong lý thuyết mật mã, hệ mật O-M có thuật toán khá thú vị, cũng giống như các hệ mật bất đối xứng khác là mỗi bên tham gia giao dịch đều có hai khóa, nhưng khác là hai khóa này hoàn toàn bí mật. Mô hình hoạt động của hệ mật O-M có thể được ví như là hoạt động trao đổi vật phẩm trong một chiếc hòm có hai chỗ khóa, mỗi bên có khóa và chìa khóa riêng; khi A muốn gửi vật phẩm M sang B, A cho vật phẩm vào hòm và khóa với khóa của mình (K_A) rồi gửi hòm sang B, B nhận được chưa mở ra, mà lại khóa hòm ở chỗ khóa thứ hai bằng khóa K_B rồi gửi lại A, A nhận được thì tháo khóa K_A rồi gửi lại cho B, B chỉ việc tháo khóa K_B là lấy được vật phẩm trong hòm. Mô hình hệ mật O-M được trình bày dạng hòm hai khóa như Hình 3-1 [9].



Hình 3-1: Hoạt động của hệ mật Omura-Massey

Hai bên A và B chọn ngẫu nhiên các khóa bảo mật riêng K_A, K_B bên A cần gửi bản tin M cho bên B, quá trình truyền tin thực hiện theo các bước sau:

- Bước 1: A mã hóa bản rõ M thành bản mã C_A bằng khóa của A là (K_A) và gửi C_A cho B.
- Bước 2: B nhận C_A và mã hóa tiếp bằng khóa của B là (K_B) thành bản mã C_{AB} và gửi lại cho A.

- Bước 3: A nhận C_{AB} và giải mã thành C_B rồi gửi cho B.
- Bước 4: B nhận C_B và giải mã để nhận M.

Các bước thực hiện được mô hình hóa như sau:

4. A chọn ngẫu nhiên cặp số (m, n): $m.n = 1 \; mod \; p$
5. B chọn ngẫu nhiên cặp số (u, v): $u.v = 1 \; mod \; p$

Bảng 3-1: Hoạt động của hệ mật Omura-Massey

$A(m,n) \leftrightarrow B(u,v)$ A muốn gửi bản tin M tới B.	
A mã hóa M thành C_A	A tính $C_A = M.m \; mod \; p$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = (M.m).u \; mod \; p$
A giải mã C_{AB} thành C_B	A tính $C_B = \big((M.m).u\big).n \; mod \; p = M.m.n.u \; mod \; p = M.u \; mod \; p$
B giải mã C_B lấy M	B tính $M.u.v \; mod \; p = M$

Do hệ mật O-M này không có khóa công khai, không có bên quản lý khóa giống như các hệ mật khóa công khai khác, nên còn tồn tại một số nhược điểm:

1. Hệ mật này sẽ an toàn khi thay đổi key trong mỗi một phiên giao dịch, trong trường hợp này, đây là hệ mật xác suất.
2. Hệ mật này không có tính xác thực các bên tham gia giao dịch.
3. Hệ số mở rộng bản tin là 3

Ví dụ: *p = 17*

Bảng 3-2: Hoạt động của hệ mật Omura-Massey với p = 17

$A(3,6) \leftrightarrow B(5,7)$
- A chọn cặp khóa $(3,6)$ vì $3 \times 6 = 18 \; mod \; 17 = 1$
- B chọn cặp khóa $(5,7)$ vì $5 \times 7 = 35 \; mod \; 17 = 1$

- Bản tin muốn gửi từ A sang B là $M = 9$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = 9.3\ mod\ 17 = 10$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = 10.5\ mod\ 17 = 16$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = 16.6\ mod\ 17 = 11$
B giải mã C_B lấy M	B tính $11.7\ mod\ 7 = 9 = M$

3.3 HỆ MẬT OM-CA TRÊN VÀNH ĐA THỨC HAI LỚP KỀ CYCLIC CÓ NHẬN THỰC

3.3.1 Giới thiệu

Ứng dụng của vành đa thức $\frac{Z_q(x)}{(x^n+1)}$ trong mật mã được biết đến đầu tiên là hệ mật xác suất nổi tiếng NTRU [4] và một vài biến thế CTRU [5] và đặc biệt hơn là pNE [8] với các phép tính trên vành đa thức $Z_{2^s}(x)$, đến nay, có thể nói đó là một biến thể có thể chứng minh an toàn của NTRU.

Lợi ích của sử dụng vành đa thức trong mật mã là tốc độ tính toàn nhanh, phép nhân module trên vành đa thức $R_{n,q}$ có độ phức tạp tính toán là $O(n^2)$. Bằng cách khai thác tính năng này, cùng với mức độ an toàn của các bài toán khó dựa trên lý thuyết dàn, NTRU được coi là một giải pháp thay thế hợp lý cho các sơ đồ mã hóa dựa trên phân tích thừa số nguyên tố, logarit rời rạc trên trường hữu hạn và đường cong eclipse và đã được chuẩn hóa trong tiêu chuẩn IEEE P.1363.1 năm 2008.

Vành đa thức hệ số nhị phân $R_n = Z_2(x)\backslash(x^n + 1)$ là một lớp của vành $R_{n,q}$, mặc dù được dùng phổ biến trong mã sửa sai, nhưng chưa được ứng dụng nhiều tỏng mật mã ngoại trừ một lớp vành đã thức chắn tuyệt đối là $R_{2,n}$ với $n = 2^N \mid N \in Z^+$ năm 2002, nhóm nhân Cylic trong $R_{2^s,2}$ đã được khai thác để đề xuất mộ hệ mật mã khóa bí mật [17] được coi như là một biến thể của hệ mật DES [25].

Phần tiếp theo giới thiệu về 4 phương pháp áp dụng để cải tiến một hệ mật thông thường thành hệ mật mã hạng nhẹ, được trình bày cụ thể trên hệ mật Omura Massey.

Để tiện theo dõi, "Hệ mật Omura-Massey trên vành đa thức hai lớp kề Cyclic có nhận thực theo phương pháp xyz" được gọi tắt là "Hệ mật O-M theo phương pháp xyz".

3.3.2 Hệ mật OM-CA trên vành đa thức hai lớp kề Cyclic có nhận thực

3.3.2.1 Hệ mật OM-CA trên vành đa thức hai lớp kề Cyclic có nhận thực 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 nhận (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 gửi 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 3-3: Thủ tục của hệ mật O-M theo phương pháp nhân

$A(mID(B),n) \leftrightarrow B(uID(A),v)$

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

Bảng 3-4: Ví dụ minh họa hệ mật O-M theo phương pháp nhân với n = 5

$A(m,n) \leftrightarrow B(u,v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $$C_A = [034]^2 \ mod \ (x^5 + 1) = [013]$$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $$C_{AB} = [013]^4 \ mod \ (x^5 + 1) = [024]$$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $$C_B = [024]^8 \ mod \ (x^5 + 1) = [012]$$
B giải mã C_B lấy M	B tính

	$[012]^4\ mod\ (x^5+1) = [034] = M$

3.3.2.2 Hệ mật OM-CA trên vành đa thức hai lớp kề Cyclic có nhận thực theo phương pháp cộng

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 nhận (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 gửi 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: $ID(A), ID(B) \in Z_2$(x)\($x^n + 1$))

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 3-5: Thủ tục của hệ mật O-M theo phương pháp 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 $\left[[M(x)]^{u+ID(A)}\right]^v \ mod\ (x^n+1) = M$

c) Ví dụ

Chọn N = 5, ta có

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

Khóa bí mật của A(m,n) = (0,8): (m+ID(B),n) = (2,8) ≡ 1 mod 15

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

A muốn gửi bản tin M = (034) tới B

Bảng 3-6: Ví dụ minh họa hệ mật O-M theo phương pháp cộng (n = 5)

$A(m,n) \leftrightarrow B(u,v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [034]^2\ mod\ (x^5+1) = [013]$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = [013]^4\ mod\ (x^5+1) = [024]$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = [024]^8\ mod\ (x^5+1) = [012]$
B giải mã C_B lấy M	B tính $[012]^4\ mod\ (x^5+1) = [034] = M$

3.3.2.3 Hệ mật OM-CA trên vành đa thức hai lớp kề Cyclic có nhận thực theo phương pháp lũy thừa

a) Tạo khóa

Chọn $Z_2(x)\backslash(x^n+1)$ 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 chọn cặp số ngẫu nhiên (m,n):

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

2. B chọn cặp số ngẫu nghiên (u,v):

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

(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:

$$M(x) \in Z_2(x)\backslash(x^n + 1) \tag{3.7}$$

Bảng 3-7: Thủ tục của hệ mật O-M theo phương pháp 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 $\left[[M(x)]^{u^{ID(A)}}\right]^v \; mod \; (x^n + 1) = M$

c) Ví dụ

Chọn N=5, ta có:

$$Z_2(x)\backslash(x^n + 1) = Z_2(x)\backslash(x^5 + 1) \quad (3.8)$$

và

$$ID(A) = 3;\ ID(B) = 2;$$

Khóa bí mật của A(m,n) = (7,4): $(m^{ID(B)},n) = (7^2,4) \equiv 1 \bmod 15$

Khóa bí mật của B(u,v) = (7,7): $(u^{ID(A)},v) = (7^3,7) \equiv 1 \bmod 15$

A muốn gửi bản tin M = (034) tới B

Bảng 3-8: Ví dụ minh họa hệ mật O-M theo phương pháp lũy thừa (n = 5)

$A(m,n) \leftrightarrow B(u,v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [034]^{7^2}\ mod\ (x^5 + 1) = [034]^4 = [012]$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = [012]^{7^3}\ mod\ (x^5 + 1) = [012]^{13} = [234]$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = [234]^4 = [024]^{14.4} = [024]^{56} = [024]^{11} = [123] mod\ (x^5 + 1)$
B giải mã C_B lấy M	B tính $\left[[123]^7 = [024]^{77}(x^5 + 1) = [034] mod\ (x^5 + 1)\right) = M$

3.3.2.4 Hệ mật Omura-Massey trên vành đa thức hai lớp kề Cyclic có nhận thực theo phương pháp logarit

a) Tạo khóa

Chọn $Z_2(x)\backslash(x^n + 1)$ 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 chọn ngẫu nhiên cặp số (m,n):

$$\left(\left(ID(B)\right)^{m}, n\right) \equiv 1 \; mod \; (2^{N-1} - 1) \tag{3.9}$$

2. B chọn ngẫu nhiên cặp số (u,v):

$$\left(\left(ID(A)\right)^{u}, v\right) \equiv 1 \; mod \; (2^{N-1} - 1) \tag{3.10}$$

(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:

$$M(x) \in Z_2(x)\backslash(x^n + 1) \tag{3.11}$$

Bảng 3-9: Thủ tục của hệ mật O-M theo phương pháp 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 $C_B = \left[[M(x)]^{\left(ID(B)\right)^{m}.\left(ID(A)\right)^{u}}\right]^{n} \; mod \; (x^n + 1) \equiv [M(x)]^{\left(ID(A)\right)^{u}} \; mod \; (x^n + 1)$
B giải mã C_B lấy M	B tính $\left[[M(x)]^{\left(ID(A)\right)^{u}}\right]^{v} \; mod \; (x^n + 1) = M$

c) Ví dụ

Chọn $n = 5$, ta có:

$$Z_2(x)\backslash(x^n + 1) = Z_2(x)\backslash(x^5 + 1) \quad (3.12)$$

$$\text{Và } ID(A) = 3;\ ID(B) = 2;$$

- Khóa bí mật của A(m,n) = (2,4): $((ID(B))^m,n) = (2^2,4) \equiv 1 \bmod 15$
- Khóa bí mật của B B(u,v) = (3,7): $((ID(A))^u,v) = (7^3,7) \equiv 1 \bmod 15$

A muốn gửi bản tin M = (034) tới B

Bảng 3-10: Ví dụ minh họa hệ mật O-M theo phương pháp logarit (n = 5)

$A(m,n) \leftrightarrow B(u,v)$	
A mã hóa M thành C_A sau đó gửi sang B	A tính $C_A = [034]^{7^2}\ mod\ (x^5 + 1) = [034]^4 = [012]$
B mã hóa C_A thành C_{AB} và gửi lại A	B tính $C_{AB} = [012]^{7^3}\ mod\ (x^5 + 1) = [012]^{13} = [234]$
A giải mã C_{AB} thành C_B và lại gửi sang B	A tính $C_B = [234]^4 = [123]\ mod(x^5 + 1)$
B giải mã C_B lấy M	B tính $[123]^7 = [024]^{77} = [034]\ mod\ (x^5 + 1) = M$

3.3.3 Nhận xét

Các ví dụ này đảm bảo tính an toàn bởi kế thừa bài toàn khó logarit rời rạc trên vành đa thức hai lớp kề tương ứng, có bổ sung thêm tính nhận thực so với hệ mật gốc, tuy nhiên hệ số mở rộng bản tin vẫn là 3 (tương tự như hệ mật gốc). Trong tương lai, với 4 phương pháp cải tiến hệ mật này, không những áp dụng cải tiến các hệ mật khác, mà còn tiếp tục nghiên cứu, cải tiến để hệ mật có độ an toàn cao hơn; đồng thời được đánh giá trên thiết bị thực có tài nguyên hạn chế, cũng như so sánh với các hệ mật mã hạng nhẹ khác.

3.4 HỆ MẬT OM-PI TRÊN VÀNH ĐA THỨC CÓ HAI LŨY ĐẲNG NGUYÊN THỦY

3.4.1 Giới thiệu

Do tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường số hữu hạn $GF(p)$, 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 Omura-Massey. 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 Omura-Massey trên vành đa thức hai lũy đẳng nguyên thủy sau đây được gọi tắt là OM-PI.

Nội dung của đề xuất được chia thành 5 phần. Phần 2 trình bày về tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường hữu hạn $GP(p)$. Phần 3 trình bày về hệ mật Omura-Massey nguyên thủy với các vấn đề còn tồn tại. Phần 4 là nội dung chính của đề xuất, trình bày về Hệ mật Omura-Massey trên vành đa thức hai lũy đẳng nguyên thủy. Phần cuối cùng là nhận xét các kết quả của đề xuất.

3.4.2 Vành đa thức có hai lũy đẳng nguyên thủy và tính chất tựa đẳng cấu với trường hữu hạn GF(p)

Vành đa thức hai lũy đẳng nguyên thủy là một loại vành đặc biệt trên vành đa thức, có nhiều tiềm năng nhưng chưa được khai thác hiệu quả, tương tự như vành đa thức hai lớp kề Cyclic, vành đa thức hai lũy đẳng nguyên thủy cũng có những đặc điểm tương tự như vành đa thức hai lớp kề Cyclic; đặc biệt là tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường số, với tính chất này, có thể dùng vành đa thức hai lũy đẳng nguyên thủy để cải tiến hệ mật trên vành số. Phần tiếp theo sẽ trình bày về tính tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường hữu hạn $GF(p)$.

Vành đa thức hai lũy đăng nguyên thủy được giới thiệu tóm tắt như sau:

Định nghĩa 3-1: Vành đa thức hai lũy đẳng nguyên thủy được biểu diễn như sau:

$$\frac{Z_2(x)}{(1+x)g(x)} \tag{3.13}$$

Trong đó, hai lũy đẳng nguyên thủy là 1 và $g(x)+1$, với bậc của $g(x)$ là $\deg\big(g(x)\big) = l$ và $g(x)$ là đa thức bất khả quy.

Với hai lũy đăng nguyên thủy, vành đa thức có hai nhóm nhân như sau:

Nhóm nhân $\mathcal{A}$ có số các phần tử:

$$|\mathcal{A}| = 2^l - 1;$$

$$\mathcal{A} = \{x^i \, mod(1+x) \cdot g(x); i = \overline{1,2^l - 1}\} \quad (3.14)$$

Nhóm nhân $\mathcal{B}$ có số các phần tử:

$$|\mathcal{B}| = 2^l - 1;$$

$$\mathcal{B} = \{[x^i + g(x)] \, mod(1+x) \cdot g(x); i = \overline{1,2^l - 1}\} \quad (3.15)$$

Ví dụ:

Vành đa thức hai lũy đẳng nguyên thủy:

$$\frac{Z_2(x)}{(1+x)(1+x+x^4)} \quad (3.16)$$

Hai lũy đẳng là: 1 và $x + x^4$

Thật vậy:

$$(1)^2 = 1$$

$$(x + x^4)^2 = x^8 + x^5 + x^5 + x^2 \quad (3.17)$$

$$\equiv (x^8 + x^2) \, mod \, (1+x)(1+x+x^4) = x + x^4$$

Trong công thức (3.17), phép tính module $(1+x)(1+x+x^4)$ của đa thức $(x^8 + x^2)$ như sau:

$$\begin{array}{l|l} x^8 + x^2 & x^5 + x^4 + x^2 + 1 \\ \hline x^8 + x^7 + x^5 + x^3 & x^3 + x^2 + x \\ \hline x^7 + x^5 + x^3 + x^2 & \\ x^7 + x^6 + x^4 + x^2 & \\ \hline x^6 + x^5 + x^4 + x^3 & \\ x^6 + x^5 + x^3 + x & \\ \hline x^4 + x & \end{array}$$

Theo *Định nghĩa 3-1*, vành đa thức (5) có hai nhóm nhân là:

$$\mathcal{A} = \left\{ \begin{matrix} (1), (2), (3), (4), (024), (01234), (013), (124), (034), (012), \\ (123), (234), (023), (134), (0) \end{matrix} \right\};$$

$$|\mathcal{A}| = 15 \tag{3.18}$$

$$\mathcal{B} = \begin{Bmatrix} (04), (0124), (0134), (01), (12), (23), (34), (02), (13), (24), \\ (0234), (0123), (1234), (03), (14) \end{Bmatrix};$$

$$|\mathcal{B}| = 15 \tag{3.19}$$

Trong nhóm $\mathcal{A}$, mỗi phần tử trong vành đa thức ta đều có thể tìm được một phần từ trong trường hữu hạn $GF(p)$ như sau:

Bảng 3-11: Bảng ánh xạ các phần từ giữa nhóm nhân $\mathcal{A}$ và trường $GF(p)$

Số thứ tự	**Phần tử trong vành đa thức:** $x^i; i = \overline{1,2^4-1}$	**Các đa thức nhóm $\mathcal{A}$:** $\bmod (1+x)(1+x+x^4)$	**Trường hữu hạn với Module p:** $p = 2^l - 1 = 2^4 - 1 = 15$
1	x^1	(1)	2
2	x^2	(2)	4
3	x^3	(3)	8
4	x^4	(4)	16
5	x^5	(024)	21
6	x^6	(01234)	31
7	x^7	(013)	11
8	x^8	(124)	22
9	x^9	(034)	25
10	x^{10}	(012)	7
11	x^{11}	(123)	14
12	x^{12}	(234)	32
13	x^{13}	(023)	13

14	x^{14}	(134)	26
15	x^{15}	(0)	1

Tương tự, trong nhóm $\mathcal{B}$, mỗi phần tử trên vành đa thức ta đều có thể tìm được một phần tử tương ứng trong trường hữu hạn $GF(p)$ như sau:

Bảng 3-12: Bảng ánh xạ các phần từ giữa nhóm nhân $\mathcal{B}$ và trường $GF(p)$

Số thứ tự	**Phần tử trong vành đa thức:** $x^i + g(x);$ $i = \overline{1,2^4 - 1}$	**Các đa thức nhóm $\mathcal{B}$:** $\bmod (1+x)(1+x+x^4)$	**Trường hữu hạn với Module p:** $p = 2^l - 1$ $= 2^4 - 1$ $= 15$
1	$1 + x^4$	(04)	17
2	$1 + x + x^2 + x^4$	(0124)	23
3	$1 + x + x^3 + x^4$	(0134)	27
4	$1 + x$	(01)	3
5	$1 + x + x^4 + x^5$	(12)	6
6	$1 + x + x^4 + x^6$	(23)	12
7	$1 + x + x^4 + x^7$	(34)	24
8	$1 + x + x^4 + x^8$	(02)	5
9	$1 + x + x^4 + x^9$	(13)	10
10	$1 + x + x^4 + x^{10}$	(24)	20
11	$1 + x + x^4 + x^{11}$	(0234)	29
12	$1 + x + x^4 + x^{12}$	(0123)	15
13	$1 + x + x^4 + x^{13}$	(1234)	30

14	$1 + \mathrm{x} + \mathrm{x}^4 + x^{14}$	(03)	9
15	$1 + \mathrm{x} + \mathrm{x}^4 + x^{15}$	(14)	18

Các phép tính trên vành đa thức hai lũy đẳng nguyên thủy cũng được giữ nguyên tính chất khi chuyển sang trường hữu hạn $GF(p)$:

Bảng 3-13: Bảng ánh xạ các tính chất giữa nhóm nhân và trường $GF(p)$

Phép tính	***Chi tiết***
Trên vành đa thức	$a(x).b(x) = (013)(01234)$ $= (1 + x + x^3)(1 + x + x^2 + x^3 + x^4)$ $= 1 + x^3 + x^4 + x^6 + x^7$ $\equiv (1 + x^3 + x^4 + x^6 + x^7)$ $mod\ (1 + x)(1 + x + x^4)$ $= 1 + x^3 \equiv (03)$
Trên Trường số $GF(15)$	$a.b = 11.31 = 241 \equiv 341\ mod\ 15 = 11$

Như vậy, tương tự như công trình [4], vành đa thức với hai lũy đẳng nguyên thủy và trường số $GF(p)$ với $p = 2^l - 1$ được gọi là tựa đẳng cấu (quasi-isomorphism):

- Mọi phần tử trên vành đa thức hai lũy đẳng nguyên thủy có hai nhóm nhân $\mathcal{A}.$ và $\mathcal{B}$ đều có thể tìm được một phần tử trên trường số $GP(p)$.
- Các tính chất quan trọng như tính giao hoán, tính phân phối, tính kết hợp, phần tử đơn vị, tính nghịch đảo của vành đa thức tương ứng cũng được ánh xạ lên trường hữu hạn $GF(p)$.

3.4.3 Hệ mật OM-PI trên vành đa thức có hai lũy đẳng nguyên thủy

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:

3.4.3.1 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):*

$$m.n \equiv 1 \, mod \, 2^l - 1 \tag{3.20}$$

- Khóa bí mật của B: *(u, v):*

$$u.v \equiv 1 \, mod \, 2^l - 1 \tag{3.21}$$

3.4.3.2 Thủ tục trao đổi thông tin

Bảng 3-14: 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 $C_A = k(x).m \, mod \, (1+x)g(x)$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = k(x).m.u \, mod \, (1+x)g(x)$
A giải mã C_{AB} thành C_B	A tính $C_B = k(x).m.u.n \, mod \, (1+x)g(x)$
B giải mã C_B lấy M	B tính $k(x).u.v \, mod \, (1+x)g(x) = k(x) = M$

3.4.3.3 Lưu ý

Hệ mật này vẫn giữ 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.

3.4.3.4 Ví dụ

Hai bên tham gia giao dịch bảo mật là A và B cùng thống nhất đa thức hai lũy đẳng nguyên thủy:

$$\frac{Z_2[x]}{(1+x)(1+x+x^4)} \tag{3.22}$$

Trong đó:

$$g(x) = 1 + x + x^4 \tag{3.23}$$

$$Modulo: (1+x)(1+x+x^4) = (x^5 + x^4 + x^2 + 1) = (0245)$$

1. Chọn nhóm nhân $\mathcal{A}$:

$$\mathcal{A} = \{(1), (2), (3), (4), (024), (01234), (013), (124), (034), (012), (123), (234), (023), (134), (0)\};$$

$$|\mathcal{A}| = 2^l - 1 = 2^4 - 1 = 15$$

2. A chọn cặp khóa bí mật của A: (m, n)

$$m = (2) = x^2$$

$$n = (023) = 1 + x^2 + x^3 \tag{3.24}$$

Mô tả chi tiết phép tính:

$$m.n = (x^2)(1 + x^2 + x^3)\ mod(1+x)(1+x+x^4)$$
$$= (x^5 + x^4 + x^2)\ mod\ (x^5 + x^4 + x^2 + 1) = 1 \tag{3.25}$$

Trong công thức (3.25), phép tính module được tính như sau:

- $x^5 + x^4 + x^2$ | $x^5 + x^4 + x^2 + 1$
  $x^5 + x^4 + x^2 + 1$ | 1
  1 |

3. B chọn cặp khóa bí mật của B:(u, v)

$$u = (4) = x^4 \tag{3.26}$$

$$v = (123) = x + x^2 + x^3 \quad (3.27)$$

Mô tả chi tiết phép tính:

$$u.v = (x^4)(x + x^2 + x^3) mod (1 + x)(1 + x + x^4)$$
$$= (x^7 + x^6 + x^5)\ mod\ (x^5 + x^4 + x^2 + 1) = 1 \quad (3.28)$$

Trong công thức (3.28), phép tính module được tính như sau:

$$\begin{array}{rll} & x^7 + x^6 + x^5 & x^5 + x^4 + x^2 + 1 \\ - & x^7 + x^6 + x^4 + x^2 & \hline x^2 + 1 \\ \hline & x^5 + x^4 + x^2 & \\ - & x^5 + x^4 + x^2 + 1 & \\ \hline & 1 & \end{array}$$

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

Bảng 3-15: Ví dụ về trao đổi thông 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 $(3)(123) mod\ (0245) = (134) = M$

3.4.4 Nhận xét

Vành đa thức hai lũy đẳng nguyên thủy là một loại vành đặc biệt, có tính chất tựa đẳng cấu với trường số $GF(p)$, do vậy có thể áp dụng để xây dựng, cải tiến các hệ mật mã trên trường số thành hệ mật trên vành đa thức. Kết quả bài báo đã chứng minh được tính chất tựa đẳng cấu này cũng như ứng dụng để cải tiến hệ mật Omura-Massey từ trường số $GF(p)$ sang vành đa thức. Hệ mật Omura-Massey cải tiến này không những giữ nguyên được tính chất của hệ mật nguyên gốc, mà còn tận dụng được khả năng tính toán nhanh với độ phức tạp tính toán $O(n)$, cài đặt đơn giản của vành đa thức để tăng hiệu năng tính toán, tiêu tốn ít tài nguyên hơn khi cài đặt, được coi là phù hợp với thiết bị có tài nguyên hạn chế. Trong tương lai, nhóm sẽ tiếp tục cài đặt và đánh giá trên thiết bị có tài nguyên hạn chế thực tế, cũng như so sánh, đánh giá với các hệ mật mã hạng nhẹ khác trên môi trường thực tế.

3.5 KẾT LUẬN CHƯƠNG

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 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 đề xuất trong 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 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 $O(n)$; về mặt thực tế, các module của hệ mật đã được cài đặt trên thiết bị có tài nguyên hạn chế, 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. Tôi mong rằng luận án sẽ tiếp tục khuyến khích những nỗ lực nghiên cứu sâu hơn và tạo ra những đóng góp đáng kể trong tương lai. 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 có hai lũy đẳng nguyên thủy", *Tạp chí khoa học công nghệ Thông tin và Truyền thông*, số 01 (CS.01) 2023, pages 115-120.

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.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Đặng Hoài Bắc, Nguyễn Bình (2006), "Tạo dãy m bằng phương pháp phân hoạch trên vành đa thức có hai lớp kề cyclic". *Hội nghị khoa học lần thứ* 8, Học viện Công nghệ BCVT, 09/2006.
2. Hồ Quang Bửu, Ngô Đức Thiện, Trần Đức Sự (2012), "Xây dựng hàm băm trên các cấp số nhân cyclic", *Chuyên san các công trình nghiên cứu, phát triển và ứng dụng CNTT và Truyền thông*, Kỳ 3 Tạp chí Thông tin, KHCN của bộ Thông tin và Truyền thông, Tập V-1 số 7 (27), ISSN 1859-3526.
3. Hồ Quang Bửu, Ngô Đức Thiện, Trần Đức Sự (2012), "Xây dựng hệ mật trên các cấp số nhân cyclic của vành đa thức", *Tạp chí Khoa học và Công nghệ, Viện Khoa học và Công nghệ Việt Nam, Chuyên san các công trình nghiên cứu về Điện tử*, Viễn thông và CNTT, Tập 50 số 2A, tháng 9-2012, ISSN 0866 708X.
4. Lê Danh Cường, Nguyễn Bình (2017), "Cấu trúc tựa đẳng cấu giữa vành đa thức có 2 lớp kề cyclic và trường số", *Tạp chí Khoa học và Công nghệ các trường đại học kỹ thuật*, ISSN 2354-1083, số 121, tr. 54-57.
5. Nguyễn Bùi Cường (2015), "Một số kết quả nghiên cứu về mã khối hạng nhẹ", *Tạp chí an toàn thông tin*, số 1 CS (01).
6. Lê Phê Đô, Trần Văn Mạnh (2017), "Nghiên cứu các cuộc tấn công hệ mật mã nhẹ PRESENT", *Hội thảo lần thứ hai: một số vấn đề về chọn lọc an toàn thông tin*.
7. Lê Phê Đô, Mai Mạnh Trừng (2017), "Nghiên cứu một số hệ mật mã nhẹ và ứng dụng trong IoT", *Tạp chí Nghiên cứu Khoa học & Công nghệ Quân sự*, ISSN 1859-1043.
8. Lê Phê Đô, Lê Trung Thực (2017), "Cải tiến mã khối hạng nhẹ họ LED và Neokeon", *Hội thảo quốc gia lần thứ XX:* Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông – Quy Nhơn, 23-24/11/2017.
9. Nguyễn Trung Hiếu, Ngô Đức Thiện (2018), "Hệ mật Omura-Massey xây dựng trên vành đa thức có hai lớp kề cyclic", *Tạp chí Khoa học và Công nghệ các trường Đại học Kỹ thuật*, trang 29-34, số 125, ISSN 2354-1083.

10. Hoàng Đăng Hải (2018), Nghiên cứu, xây dựng hệ thống giám sát, đánh giá cấp độ an toàn, cảnh báo nguy cơ mất an toàn thông tin cho các trang tin / cổng thông tin điện tử, Đề tài cấp nhà nước mã số KC.01.08/16-20.
11. Nguyễn Trung Kiên (2016), Nghiên cứu xây dựng hệ thống công nghệ thông tin thử nghiệm thu thập dữ liệu và phân tích một số chỉ số hiệu năng thực hiện (KPI) của đô thị thông minh phù hợp với điều kiện của Việt Nam nhằm phục vụ cho hoạt động của cơ quan quản lý nhà nước, Đề tài cấp nhà nước mã số KC.01.04/16-20.
12. Cao Minh Thắng, Nguyễn Bình, Hoàng Mạnh Thắng, Nguyễn Ngọc Quân (2015), "E-RISKE, một sơ đồ mật mã khóa bí mật dựa trên các phần tử khả nghịch và khả nghịch mở rộng trong các vành đa thức bậc hữu hạn hệ số nhị phân có hai lớp kề cyclic". *Kỷ yếu hội thảo quốc gia 2015 về điện tử, truyền thông và công nghệ thông tin (REV-ECIT)*, 12-2015, Tp.Hồ Chí Minh, Việt Nam, ISBN: 878-604-67-0635-9, trang 240-247.
13. Cao Minh Thắng, Nguyễn Bình (2015), "Một hệ mật lai ghép dựa trên các thặng dư bậc hai và các phần tử liên hợp trong vành đa thức chẵn". *Tạp chí Khoa học và Công nghệ*, Viện hàn lâm Khoa học và Công nghệ Việt Nam, tập 53 – số 2C năm 2015, ISSN 0866 708X, trang 14-22.
14. Cao Minh Thắng, Nguyễn Bình (2015), "Một hệ mật khóa công khai dựa trên các phần tử khả nghịch trong vành đa thức chẵn - IPKE". *Tạp chí An toàn thông tin*, Ban Cơ yếu chính phủ, số 1.CS (01) - 2015. ISSN 1859-1256, trang 21-27.
15. Ngô Đức Thiện, Nguyễn Trung Hiếu, Nguyễn Toàn Thắng, Đặng Hoài Bắc (2013), "Một phương pháp xây dựng hệ mật mã khối kết hợp sơ đồ Lai-Massey với sơ đồ Feistel và ứng dụng vào hàm băm", *Kỷ yếu Hội nghị Quốc gia về Điện tử -Truyền thông (REV2013-KC01)*, Hà Nội, Việt Nam, ngày 17-18/12/2013, tr. 75-80.
16. Phạm Việt Trung (2005), "Xây dựng hệ mật McEliece trên mã xyclic cục bộ", *Tạp chí nghiên cứu KHKT và công nghệ quân sự*, số 13, pp 63 - 69.

Tiếng Anh

17. Ahmad Mustafa Mohamad Al-Aboosi, Samar Kamil, Siti Norul Huda Sheikh Abdullah, Khairul Akram Zainol Ariffin (2021), "Lightweight Cryptography for Resource Constraint Devices: Challenges and Recommendation", *2021 3rd International Cyber Resilience Conference (CRC)*, ISBN:978-1-6654-1844-7.
18. Alaa Hassan (2022), "State-of-the-Art Lightweight Cryptographic Protocols for IoT Networks", *Proceedings of the Future Technologies Conference (FTC) 2022*, Volume 2, ISBN: 978-3-031-18458-1, pp. 297–310.
19. Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, Charlotte Vikkelsoe, (2007), "Cryptographic Hardware and Embedded Systems-CHES 2007", Springer Berlin Heidelberg, pp 450-466.
20. Axel York Poschmann (2009), "Lightweight cryptography: cryptographic engineering for a pervasive world", in Ph. D. Thesis. 2009. Citeseer.
21. Armknecht, F., Mikhalev, V. (2015), "On Lightweight Stream Ciphers with Shorter Internal States", In: FSE 2015. LNCS, Springer (2015), to appear.
22. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin & C. Vikkelsoe (2007), "PRESENT: An Ultra-Lightweight Block Cipher", *Cryptographic Hardware and Embedded Systems* - CHES 2007 pp 450–466.
23. Bruce Schneier (1996), Applied Cryptography, Wiley, ISBN: 9780471128458,0471128457.
24. Cao Minh Thang, Nguyen Binh (2015), "DTRU, a new NTRU-like cryptosystem based-on dual truncated polynomial rings". *Tạp chí Khoa học và Công nghệ*, Viện hàn lâm Khoa học và Công nghệ Việt Nam, tập 53 – số 2C năm 2015. ISSN 0866 708X, trang 103-118.
25. Cao Minh Thang, Nguyen Binh, Nguyen Minh Trung (2015), "A novel CPA-secure probabilistic encryption scheme based-on pNE cryptosystem", *Proceedings of 2nd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS 2015)*

September 16-18, Ho Chi Minh City, Vietnam, IEEE Catalog Number: CFP15C61-PRT, ISBN: 978-1-4673-6639-7, pp. 119-124.

26. Cao Minh Thang, Nguyen Binh (2015), “RISKE, a novel CPA-Secure secret-key encryption scheme based-on invertible elements in binary quotient polynomial rings”. *Proceedings of the 8th National Conference on Fundamental and Applied Information Technology Research (FAIR’8) July 9-10 2015*, Hanoi, Vietnam, ISBN: 978-604-913-397-8, pp. 620-628.
27. C.E.Shannon (1949), *Communication theory of secrecy systems*, Bell System Tech. J. 28 (1949), 556-715.
28. Cocks, Clifford (1973). "A Note on 'Non-Secret Encryption'", CESG Research Report.
29. Coppersmith, D., Shamir, A. (1997), “Lattice attacks on NTRU”. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 52–61. Springer, Heidelberg (1997).
30. Computer Security Resource Center (2001), "FIPS PUB 197: The official Advanced Encryption Standard"
31. C. Gentry (2001), Key recovery and message attacks on NTRU-composite. In Proceeding of Eurocrypt ’01, LNCS, vol. 2045, Springer-Verlag, pp.182-194, 2001.
32. Cramer, Ronald; Shoup, Victor (2004). "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack" (PDF). *SIAM Journal on Computing* 33 (1): 167–226.
33. Chris Peikert and Brent Waters (2008), “Lossy trapdoor functions and their applications,” in *Proceedings of the 40th annual ACM symposium on Theory of computing* (Victoria, British Columbia, Canada: ACM, 2008), 187-19.
34. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan (2008), “Trapdoors for hard lattices and new cryptographic constructions,” in *Proceedings of the 40th annual ACM symposium on Theory of computing* (Victoria, British Columbia, Canada: ACM, 2008), 197-206.
35. Chris Peikert (2009), “Public-key cryptosystems from the worst-case shortest vector problem: extended abstract,” *in Proceedings of the 41st annual ACM*

symposium on Theory of computing (Bethesda, MD, USA: ACM, 2009), 333-342.

36. Chandrasekaran, J. et al. (2011), "A Chaos Based Approach for Improving Non Linearity in the S-Box Design of Symmetric Key Cryptosystems". *In Meghanathan, N. et al. Advances in Networks and Communications: First International Conference on Computer Science and Information Technology*, CCSIT 2011, Bangalore, India, January 2-4, 2011. Proceedings, Part 2. Springer. p. 516. ISBN 978-3-642-17877-1.
37. Constantinos Patsakis, Panayiotis Kotzanikolaou, Mélanie Bouroche (2015). "Private Proximity Testing on Steroids: An NTRU-based Protocol". *Security and Trust Management* Volume 9331 of the series Lecture Notes in Computer Science pp 172-184. Springer.
38. D. Rachmawati, Mohammad Andri Budiman, M. Adib Rikzan (2019), "Analysis of File Security with Three-Pass Protocol Scheme Using Massey-Omura Algorithm In Android", IOP Conf. Series: Journal of Physics: Conf. Series 1235 (2019) 012075.
39. Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, Young Hoon Kim (2007), "Polynomial rings with two cyclotomic cosets and their applications in Communication", *MMU International Symposium Information and Communications Technologies 2007*, Malaysia, ISBN: 983-43160-0-3.
40. Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh , Young Hoon Kim (2007). "Ploynomial rings with two cyclotomic cosets and their applications in Communication", *MMU International Symposium on Information and Communications Technologies* 2007, Malaysia, ISBN: 983-43160-0-3.
41. Daewan Han, Jin Hong, Jae Woo Han and Daesung Kwon (2003), "Key recovery attacks on NTRU without ciphertext validation routine", *In Proceeding of ACISP '03*, LNCS, vol. 2727, Springer-Verlag, pp.274-284, 2003.
42. Daniel Cabarcas, Patrick Weiden, Johannes Buchmann (2014), "On the Efficiency of Provably Secure NTRU". *Post-Quantum Cryptography* Volume 8772 of the series Lecture Notes in Computer Science, pp 22-39. Springer, 2014.

43. D. Kahn(1967), The Codebreakers: The Story of Secret Writing, *New York: Macmillan Publishing Co.*,
44. Frank Miller (1882), Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams, C.M. Cornwell, 1882.
45. Gaborit, P., Ohler, J., Sole, P. (2002), "CTRU, a Polynomial Analogue of NTRU, INRIA". *Rapport de recherche*, N.4621 (November 2002), (ISSN 0249-6399).
46. Gaborit, P., Ohler, J., Sole, P. (2002), "CTRU, a Polynomial Analogue of NTRU", INRIA. Rapport de recherche, N.4621 (November 2002), (ISSN 0249-6399).
47. Ho Quang Buu, Ngo Duc Thien, Tran Duc Su (2012), "Constructing secretcryptosystem based on cyclic multiplicative progress over polynomial rings", *Journal of Science and Technology*, Posts and Telecommunication Institute of Technology, 50 (2A), pp 109-119. In Vietnamese.
48. Horst Feistel, (1973). "Cryptography and Computer Privacy". Scientific American, 228(5), May 1973, pp 15–23.
49. Hofheinz, Dennis; Kiltz, Eike (2007). "Secure Hybrid Encryption from Weakened Key Encapsulation". *Advances in Cryptology* -- CRYPTO 2007. Springer. pp. 553–571.
50. ÎAshchenko, V. V. (2002), "Cryptography: an introduction". AMS Bookstore. p. 6. ISBN 0-8218-2986-6.
51. ITU-T (2003), *Security architecture for systems providing end-to-end communications*, Recommendation X.805.
52. ISO/IEC 29192-2:2019, *Information security — Lightweight cryptography*
53. ISO/IEC 29167-10:2017, *Information technology — Automatic identification and data capture techniques.*
54. Jonathan Katz, Yehuda Lindell (2007), *Introduction to Modern Cryptography: Principles and Protocols*, Chapman Hall/CRC Cryptography and Network Security Series.
55. Jonathan Katz, Yehuda Lindell (2021), *Introduction to modern cryptography*, Third edition, Chapman & Hall/CRC.

56. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (1998), “NTRU: Alice ringbased public key cryptosystem”, *Lecture Notes in Computer Science* Volume 1423, pp 267-288, Springer Verlag 1998.
57. J. Hoffstein and J.H. Silverman (2003), “Random small hamming weight products with applications to cryptography”. *Discrete Applied Mathematics*, vol. 130, Issue 1 - special issue on the 2000 com2MaC workshop on cryptography, pp. 37 - 49, 2003.
58. Jonathan Katz, Yehuda Lindell (2007), “Introduction to Modern Cryptography: Principles and Protocols”, *Chapman & Hall/CRC Cryptography and Network Security Series*.
59. Katherine Jarvis, Monica Nevins (2013), “ETRU: NTRU over the Eisenstein integers”. Springer Date: 13 Jul 2013.
60. Katz, Jonathan; Lindell, Yehuda (2007), *Introduction to Modern Cryptography: Principles and Protocols*. Chapman and Hall/CRC.
61. Lyubashevsky V., Peikert C., Regev O. (2010), “On ideal lattices and learning with errors over rings”, *In: Gilbert H. (ed.) Advances in Cryptology (EUROCRYPT 2010). Lecture Notes in Computer Science*, vol. 6110, pp. 1–23. Springer, Berlin.
62. Massimo Chenal, Qiang Tang (2015), “Key Recovery Attacks Against NTRU-Based Somewhat Homomorphic Encryption Schemes”. *Information Security Volume 9290 of the series Lecture Notes in Computer Science* pp 397-418. Springer, 27 August 2015.
63. M. Hell, T. Johansson, A. Maximov, and W. Meier (2008), *The Grain Family of Stream Ciphers*, In M. Robshaw and O. Billet Editors, New Stream Cipher Designs, LNCS 4986, pp. 179-190, 2008.
64. Menezes A. J, Van Oorchot P. C. (1998), *Handbook of Applied Cryptography*, CRC Press.
65. Miroslav Knežević (1970), “ KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers”, *Cryptographic Hardware and Embedded Systems* - CHES 2009 (pp.272-288).

66. Michael Coglianese, Bok-Min Goi. MaTRU (2005): “A New NTRU-Based Cryptosystem”, *Lecture Notes in Computer Science* Volume 3797, pp 232-243.

67. Malekian, E. Zakerolhosseini (2010), “OTRU: A non-associative and high speed public key cryptosystem”. *A.Computer Architecture and Digital Systems (CADS)*, 2010 15th CSI International Symposium on, Tehran, pp 83 – 90, ISBN: 978-1-4244-6267-4.

68. Najlae Falah Hameed Al Saffar, Inaam. R. Al-Saiq, Rewayda Razaq Mohsin Abo Alsabeh (2022), “Asymmetric image encryption scheme based on Massey Omura scheme”, International Journal of Electrical and Computer Engineering (IJECE), ISSN: 2088-8708.

69. Nguyen Binh (2002), “Crypto-system based on cyclic geometric progressions over polynomial ring (Part I)”. REV02.2002.

70. Nguyen Binh, Le Dinh Thich (2002), “The order of polynomials and algorithms for defining Oder of Polynomial over polynomial rings”, *VICA-5*, Hanoi, Vietnam.

71. Nguyen Binh, Tran Duc Su, Pham Viet Trung (2001), “Decomposition of polynomial ring according to the classes of conjugate elements”, AIC-26, Hanoi, Vietnam.

72. Nguyen Binh, Le Dinh Thich (2002), “The orders of polynomials and algorithms for defining order of polynomial over polynomial Ring”, VICA-5, Hanoi, Vietnam.

73. Nguyen Binh, Le Dinh Thich (2002), “The Oders of Polynomials and Algorithms for Defining Oder of Polynomial over Polynomial Ping”, VICA-5, Hanoi, Vietnam.

74. Nguyen Binh (2002), *Crypto-system based on cyclic geometric progressions over polynomial ring (Part I).* REV’02.2002.

75. Nguyen Binh, Dang Hoai Bac, (2004). “Cyclic codes over extended rings of polynomial rings with two cyclotomic cosets”. *REV-04*. November 20-23, 2004, Hanoi.

76. NESSIE Final report of European project IST-1999-12324: New European Schemes for Signatures, Integrity, and Encryption, April 2004. Working draft.

77. National Credit Union Administration (2004) "NCUA letter to credit unions" (PDF. July 2004).
78. Network Working Group of the IETF (2006), RFC 4251, The Secure Shell (SSH) Protocol Architecture.
79. N. Howgrave-Graham, J.H. Silverman, W. Whyte (1999), *NTRU Cryptosystems Technical Report #004*, Version 2: A Meet-In-The-Middle Attack on an NTRU Private Key.
80. OKAMURA Toshihiko (2017), "Lightweight Cryptography Applicable to Various IoT Devices", *Special Issue on IoT That Supports Digital Businesses*.
81. Okamura Toshihiko, "Mật mã nhẹ áp dụng cho các thiết bị IoT khác nhau", (2017), https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html
82. Oded Regev (2005), "On lattices, learning with errors, random linear codes, and cryptography," *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing* (Baltimore, MD, USA: ACM, 2005), 84-93.
83. Perlner, R.A., Cooper, D.A. (2009), *Quantum resistant public key cryptography: a survey*. In: Proc. of IDtrust, pp. 85–93. ACM, New York.
84. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weekks, L. Wingers (2015), "SIMONand Speck: Blocks Ciphers for Internet of Things", *Hội thảo về mật mã học nhẹ của NIST* , 20/07/2015.
85. R.L. Rivest, A. Shamir, L. Adleman(1978), "A method for obtaining digital signatures and public key cryptosystems", *Communications of the ACM 21*, 120-126.
86. Stehle, D., Steinfeld, R. (2011), "Making NTRU as secure as worst-case problems over ideal lattices". *In: Paterson, K.G.(ed.) EUROCRYPT 2011*. LNCS, vol. 6632, pp. 27–47. Springer, Heidelberg.
87. S. Goldwasser, S. Micali (1984). "Probabilistic encryption". *Journal of Computer and System Sciences 28* (2): 270–29.
88. S. Goldwasser and S. Micali (1982), *Probabilistic encryption & how to play mental poker keeping secret all partial information*, Annual ACM Symposium on Theory of Computing.

89. Sergei Silvestrov, Anatoliy Malyarenko, Milica Rančić (2017), Algebraic Structures and Applications, *Springer Proceedings in Mathematics & Statistics Volume 317*.

90. Shannon C. Haley (2018), "Non-commutative Massey-Omura Encryption with Symmetric Groups" (2018). Student Research Submissions. 254.

91. Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, Leif Uhsadel (2007), "A Survey of Lightweight-Cryptography Implementations", *ISSN: 0740-7475*, pp. 522 – 533.

92. Tran Xuan Tu, Bui Duy Hieu (2017), "AES datapath optimization strategies for low-power low-energy multi-security-level Internet-of-Thing applications", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, ISSN 1063-8210, pp. 3281-3290.

93. Ulugbek Mardiyev (2021), "Using of R parameter in a Massey-Omura protocol on elliptic curves", 2021 International Conference on Information Science and Communications Technologies (ICISCT).

94. Victor Shoup (2004). *ISO 18033-2: An emerging standard for public-key encryption*, http://shoup.net/iso/std6.pdf, December 2004. Final Committee Draft.

95. Yanbin Pan, Yingpu Deng, Yupeng Jiang, Ziran Tu (2011), "A New Lattice-Based Public-Key Cryptosystem Mixed with a Knapsack", *Lecture Notes in Computer Science* Volume 7092, pp 126-137.

96. Yanbin Pan, Yingpu Deng (2012), "A General NTRU-Like Framework for Constructing Lattice-Based Public-Key Cryptosystems", *Lecture Notes in Computer Science* Volume 7115, 2012, pp 109-120.

97. W. Diffie, M.E. Hellman (1976), "New directions in cryptography", *IEEE Trans on Information Theory* Volume: 22, Issue: 6, (1976), 644-654.