|  |
| --- |
| BỘ THÔNG TIN VÀ TRUYỀN THÔNG  **HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  **---------------------------------------** |
| https://upload.wikimedia.org/wikipedia/commons/d/d5/Posts_%26_Telecoms_Institute_of_Technology_logo.jpg |
| **CAO MINH THẮNG** |
|  |
| **CÁC HỆ MẬT DỰA TRÊN**  **VÀNH ĐA THỨC CHẴN**  **LUẬN ÁN TIẾN SỸ KỸ THUẬT** |
|  |
| Hà Nội - 2017 |
|  |

|  |
| --- |
| HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  **VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG CDIT**  **---------------------------------------** |
|  |
| **TÀO NGỌC CƯỜNG** |
|  |
| **…**  **BÁO CÁO THỬ VIỆC**  **NGƯỜI HƯỚNG DẪN: TS. CAO MINH THẮNG** |
| Hà Nội – 2020 |

# MỤC LỤC

[MỤC LỤC i](#_Toc31579810)

[DANH MỤC CÁC TỪ VIẾT TẮT iii](#_Toc31579811)

[DANH MỤC CÁC KÝ HIỆU vi](#_Toc31579812)

[DANH MỤC CÁC BẢNG viii](#_Toc31579813)

[DANH MỤC CÁC HÌNH VẼ ix](#_Toc31579814)

[MỞ ĐẦU 1](#_Toc31579815)

[CHƯƠNG 1. 10](#_Toc31579816)

[1.1 MỞ ĐẦU CHƯƠNG 10](#_Toc31579817)

[1.2 TỔNG QUAN VỀ MẬT MÃ 10](#_Toc31579818)

[1.2.1 Mật mã khóa bí mật 10](#_Toc31579819)

[1.2.2 Mật mã khóa công khai 12](#_Toc31579820)

[1.2.3 Mật mã lai ghép 14](#_Toc31579821)

[1.2.4 Độ an toàn của một hệ mật 16](#_Toc31579822)

[1.2.5 Thí nghiệm đánh giá độ an toàn không thể phân biệt 18](#_Toc31579823)

[1.2.6 Phương pháp đánh giá độ an toàn ngữ nghĩa của các hệ mật 21](#_Toc31579824)

[1.2.7 Một số tham số khác được sử dụng để đánh giá các hệ mật 22](#_Toc31579825)

[1.3 CÁC HỆ MẬT DỰA TRÊN VÀNH ĐA THỨC 23](#_Toc31579826)

[1.3.1 Các hệ mật khoá bí mật dựa trên vành đa thức 23](#_Toc31579827)

[1.3.2 Các hệ mật khoá công khai dựa trên vành đa thức 25](#_Toc31579828)

[1.3.3 Các hệ mật lai ghép dựa trên vành đa thức 27](#_Toc31579829)

[1.4 TIỀM NĂNG ỨNG DỤNG CỦA VÀNH ĐA THỨC CHẴN TRONG MẬT MÃ VÀ CÁC VẤN ĐỀ MỞ 27](#_Toc31579830)

[1.4.1 Các vấn đề chung với các hệ mật dựa trên vành đa thức chẵn 27](#_Toc31579831)

[1.4.2 Các tiềm năng ứng dụng của vành đa thức chẵn trong mật mã 28](#_Toc31579832)

[1.5 KẾT LUẬN CHƯƠNG 29](#_Toc31579833)

[CHƯƠNG 2. CÁC HỆ MẬT MỞ RỘNG DỰA TRÊN VÀNH ĐA THỨC CHẴN KẾT HỢP VỚI CÁC VÀNH ĐA THỨC KHÁC 31](#_Toc31579834)

[2.1 MỞ ĐẦU CHƯƠNG 31](#_Toc31579835)

[2.2 HỆ MẬT KHÓA CÔNG KHAI DTRU 32](#_Toc31579836)

[2.2.1 Giới thiệu 32](#_Toc31579837)

[2.2.2 Hệ mật NTRU 32](#_Toc31579838)

[2.2.3 Ý tưởng về hệ mật DTRU 37](#_Toc31579839)

[2.2.4 Hệ mật DTRU 38](#_Toc31579840)

[2.3 KẾT LUẬN CHƯƠNG 51](#_Toc31579841)

[KẾT LUẬN 53](#_Toc31579842)

[TÀI LIỆU THAM KHẢO 56](#_Toc31579843)

# DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| AES | Advanced Encryption Standard | Chuẩn mã hóa tiên tiến |
| CE | Conjugate Element | Phần tử liên hợp (thực chất là các căn bậc hai của một thặng dư bậc hai trong vành đa thức chẵn) |
| COA | Ciphertext Only Attack | Tấn công chỉ bằng bản mã |
| CCA | Chosen Ciphertext Attack | Tấn công bằng bản mã chọn trước |
| CBC | Cipher Block Chaining | Chế độ mật mã khối dạng móc xích |
| CPA | Chosen Plaintext Attack | Tấn công bằng bản rõ chọn trước |
| DES | Data Encryption Standard | Chuẩn mã hóa dữ liệu |
| DHP | Diffie – Hellman Problem | Bài toán khó Diffie – Hellman |
| DLP | Discrete Logarithm Problem | Bài toán logarit rời rạc |
| DSS | Digital Signature Standard | Chuẩn chữ ký số |
| DTRU | Dual Truncated public-key cryptosystem | Hệ mật khóa công khai DTRU dựa trên hai vành đa thức hệ số nhị phân bậc hữu hạn |
| EAV | Eavesdropping Attack | Tấn công kiểu nghe lén |
| ECB | Electronic Codebook | Chế độ hoạt động sổ điện tử mật mã khối |
| E-RISKE | Extended Random Invertible Secret-key Encryption scheme | Hệ mật khóa bí mật RISKE mở rộng trên vành |
| HpNE | Hybrid pNE | Hệ mật lai ghép HpNE dựa trên hai hệ mật RISKE và pNE theo mô hình KEM/DEM |
| IEEE | Institute of Electrical and Electronics Engineers | Viện các kỹ sư điện và điện tử (Hoa Kỳ) |
| IFP | Integer Factorization Problem | Bài toán phân tích số nguyên thành các thừa số nguyên tố |
| IND | Indistinguishable | Không thể phân biệt |
| IND-CCA | Indistinguishable under Chosen Ciphertext Attack | Không thể phân biệt với các tấn công bằng bản mã chọn trước |
| IND-CPA | Indistinguishable under Chosen Plaintext Attack | Không thể phân biệt với các tấn công bằng bản rõ chọn trước |
| IND-EAV | Indistinguishable under Eavesdropping Attack | Không thể phân biệt với các tấn công nghe lén |
| IoT | Internet of Things | Intertnet của vạn vật |
| KEM/DEM | Key Encapsulation Mechanism/ Data 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 cyclic cục bộ |
| LWE | Learning With Errors | Học với lỗi – một bài toán khó trong lĩnh vực học máy |
| MITM | Meet-In-The-Middle | Tấn công gặp ở giữa |
| 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 dựa trên vành đa thức có bậc hữu hạn N |
| OpenPGP | Open Pretty Good Privacy | Tên một chương trình mã hóa dữ liệu trên máy tính |
| OTP | One-Time-Pad | Hệ mật One-Time-Pad |
| QRP | Quadratic Residue Problem | Bài toán thặng dư bậc hai |
| QRHE | Hybrid Encryption scheme based-on Quadratic Residue | Hệ mật lai ghép QRHE dựa trên các thặng dư bậc hai trên vành đa thức  theo mô hình KEM/DEM |
| RISKE | Random Invertible Secret-key Encryption scheme | Hệ mật khóa bí mật RISKE có khóa là các phần tử khả nghịch trên vành đa thức |
| SPN | Substitution-Permutation Network | Mạng Thay thế - Hoán vị |
| SVP | Shortest Vector Problem | Bài toán tìm vector ngắn nhất |
| TCC | Traditional Cyclic Code | Mã cyclic truyền thống |

# DANH MỤC CÁC KÝ HIỆU

|  |  |
| --- | --- |
|  | Kẻ tấn công, hay còn gọi là thám mã |
|  | Tập các đa thức khả nghịch trong ,  và |
|  | Tỉ lệ giữa số đa thức khả nghịch trên tổng số đa thức trong , , và |
|  | Tập các số nguyên dương  là lũy thừa của 2 |
|  | Tập các số nguyên  để  là vành có hai lớp kề cyclic |
|  | Vành đa thức có hệ số nguyên |
|  | Vành đa thức bậc hữu hạn hệ số nguyên dương |
|  | Vành đa thức bậc hữu hạn hệ số nhị phân |
|  | Vành đa thức bậc hữu hạn chẵn hệ số nhị phân , gọi ngắn gọn là vành đa thức chẵn |
|  | Vành đa thức bậc hữu hạn chẵn tuyệt đối hệ số nhị phân  , gọi ngắn gọn là vành đa thức chẵn tuyệt đối |
|  | Vành đa thức bậc hữu hạn hệ số nhị phân có hai lớp kề cyclic, gọi ngắn gọn là vành có hai lớp kề |
|  | Vành các số nguyên modulo |
|  | Ký hiệu hệ mật |
|  | Hệ mật khóa bí mật |
|  | Hệ mật khóa công khai |
|  | Hệ mật lai ghép |
|  | Không gian bản rõ của một hệ mật |
|  | Không gian bản mã của một hệ mật |
|  | Không gian khóa của một hệ mật |
|  | Thuật toán tạo khóa của một hệ mật |
|  | Thuật toán mã hóa của một hệ mật |
|  | Thuật toán giải mã của một hệ mật |
|  | Bậc của một đa thức  trong vành, là một số nguyên dương có giá trị lớn nhất trong các số mũ của các đơn thức có hệ số khác 0 trong biểu diễn của . |
|  | Cấp của một đa thức  trong vành, là một số nguyên dương  nhỏ nhất để  trong vành đó. |
|  | Tập các đa thức  có  hệ số có giá trị ,  hệ số có giá trị  và  hệ số còn lại có giá trị 0. Dùng để mô tả các tập trong hệ mật NTRU. |
|  | Ký hiệu so sánh hai số nguyên.  có nghĩa là  lớn hơn nhiều so với |

# DANH MỤC CÁC BẢNG

[Bảng 3‑1: Cấu trúc đại số nền tảng của hệ mật RISKE và OTP 52](#_Toc503954889)

[Bảng 3‑2: So sánh hiệu năng và độ an toàn của RISKE và OTP 61](#_Toc503954890)

[Bảng 3‑3: Cấu trúc đại số nền tảng của hệ mật QRHE 65](#_Toc503954891)

[Bảng 3‑4: Cấu trúc đại số nền tảng của hệ mật IPKE 73](#_Toc503954892)

[Bảng 3‑5: So sánh hiệu năng lý thuyết của IPKE với RSA và NTRU 80](#_Toc503954893)

[Bảng 3‑6: Các chế độ hoạt động của IPKE 83](#_Toc503954894)

[Bảng 4‑1: Cấu trúc đại số nền tảng của hệ mật DTRU 93](#_Toc503954895)

[Bảng 4‑2: Cấu trúc đại số nền tảng của NTRU và DTRU 103](#_Toc503954896)

[Bảng 4‑3: So sánh hiệu năng lý thuyết của DTRU so với NTRU 104](#_Toc503954897)

[Bảng 4‑4: So sánh trong chế độ an toàn trung bình của NTRU 105](#_Toc503954898)

[Bảng 4‑5: So sánh trong chế độ an toàn cao của NTRU 105](#_Toc503954899)

[Bảng 4‑6: So sánh trong chế độ an toàn cao nhất của NTRU 105](#_Toc503954900)

[Bảng 4‑7: Cấu trúc đại số nền tảng của hệ mật E-RISKE 107](#_Toc503954901)

[Bảng 4‑8: Cấu trúc đại số nền tảng của hệ mật HpNE 120](#_Toc503954902)

[Bảng 4‑9: So sánh các tham số của pNE và HpNE 123](#_Toc503954903)

# DANH MỤC CÁC HÌNH VẼ

[Hình 1‑1: Mô hình mật mã lai ghép KEM/DEM 15](#_Toc503954904)

[Hình 3‑1: Thông lượng mã hóa và giải mã của RISKE trên CPU Intel 2,7 GHz ở với các khóa có độ dài từ 128 đến 2048 bit. 58](#_Toc503954905)

[Hình 3‑2: Thời gian mã hóa của RISKE hoạt động trên vành ở chế độ khóa 128 bit, bản rõ 128 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 59](#_Toc503954906)

[Hình 3‑3: Thông lượng mã hóa và giải mã của RISKE ở chế độ khóa 128 bit, bản rõ 128 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 59](#_Toc503954907)

[Hình 3‑4: Thông lượng mã hóa của RISKE trên phần cứng UNO 16MHz 60](#_Toc503954908)

[Hình 3‑5: Sơ đồ hệ mật QRHE 64](#_Toc503954909)

[Hình 3‑6: Sơ đồ hệ mật QRHE ở chế độ CBC 68](#_Toc503954910)

[Hình 3‑7: Thông lượng mã hóa và giải mã của IPKE trên CPU Intel 2,7 GHz ở với khóa công khai có độ dài từ 128 đến 4096 bit. 81](#_Toc503954911)

[Hình 3‑8: Thời gian mã hóa của IPKE hoạt động trên vành ở chế độ khóa 1024 bit, bản rõ 510 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 82](#_Toc503954912)

[Hình 3‑9: Thông lượng mã hóa và giải mã của IPKE ở chế độ khóa 1024 bit, bản rõ 510 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 82](#_Toc503954913)

[Hình 3‑10: Thông lượng mã hóa của IPKE trên phần cứng UNO 16MHz với khóa công khai có kích thước từ 128 đến 512 bit 83](#_Toc503954914)

[Hình 4‑1: Thông lượng mã hóa và giải mã của DTRU trên CPU Intel 2,7 GHz ở với khóa công khai có độ dài từ 128 đến 4096 bit. 100](#_Toc503954915)

[Hình 4‑2: Thời gian mã hóa của DTRU hoạt động trên vành ở chế độ khóa 1024 bit, bản rõ 510 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 101](#_Toc503954916)

[Hình 4‑3: Thông lượng mã hóa và giải mã của DTRU ở chế độ khóa 1024 bit, bản rõ 269 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 101](#_Toc503954917)

[Hình 4‑4: Thông lượng mã hóa của DTRU trên phần cứng UNO 16MHz với khóa công khai có kích thước từ 128 đến 512 bit 102](#_Toc503954918)

[Hình 4‑5: Thông lượng mã hóa và giải mã của E-RISKE trên CPU Intel 2,7 GHz ở với các khóa có độ dài từ 128 đến 2048 bit. 114](#_Toc503954919)

[Hình 4‑6: Thời gian mã hóa của E-RISKE hoạt động trên vành ở chế độ khóa 128 bit, bản rõ 128 bit so với một số hệ mật khác trên CPU Intel Core i5 2,7GHz 115](#_Toc503954920)

[Hình 4‑7: So sánh thông lượng mã hóa và giải mã của E-RISKE ở chế độ khóa 128 bit, bản rõ 131 bit trên CPU Intel 2,7 GHz so với môt số hệ mật khác 115](#_Toc503954921)

[Hình 4‑8: Thông lượng mã hóa của E-RISKE trên phần cứng UNO 16MHz 116](#_Toc503954922)

[Hình 4‑9: Sơ đồ hệ mật lai ghép HpNE theo mô hình KEM/DEM 120](#_Toc503954923)

# MỞ ĐẦU

Mật mã có lịch sử rất lâu đời và đóng vai trò hết sức quan trọng trong xã hội loài người, đặc biệt trong một số lĩnh vực chính trị, quân sự, tài chính ngân hàng hay truyền thông. Mật mã được coi là công cụ để bảo vệ các bí mật và an ninh quốc gia [61]. Cùng với sự phát triển bùng nổ của máy tính và Internet theo xu hướng IoT, mật mã học ngày càng được quan tâm nghiên cứu.

Mật mã học được phát triển dựa trên lý thuyết toán học và các hệ mật thường dựa được xây dựng dựa trên các phép tính toán cụ thể trong một cấu trúc đại số nền tảng nào đó [42]. Trong lịch sử phát triển của mật mã, có nhiều cấu trúc đại số đã được ứng dụng để xây dựng các hệ mật tiêu biểu như:

* Vành số nguyên modulo , : Đây là cấu trúc đại số được sử dụng rộng rãi trong mật mã. Các hệ mật khóa bí mật cổ điển điển hình như các hệ mật Caesar, Affine, Vigenère [89] sử dụng các phép dịch, hoán vị và thay thế trên bộ chữ cái Latin (tương đương với vành ) làm nền tảng đại số. Đối với mật mã khóa công khai, có nhiều bài toán khó trên vành số nguyên đã được ứng dụng để xây dựng các hệ mật. Cụ thể là, hệ mật RSA [81] hay Rabin [79] dựa trên bài toán phân tích số nguyên (IFP), hệ mật Goldwasser-Micali [37] dựa trên bài toán thặng dư bậc hai (QRP), hệ mật Belanoh dựa trên bài toán thặng dư bậc cao [10], hay hệ mật Merkle-Hellman [63] dựa trên bài toán tổng tập con (SUBSET-SUM);
* Trường nhị phân : Do phép cộng trên trường nhị phân tương đương với phép tính XOR dễ thực hiện bằng phần cứng và có tốc độ tính toán nhanh nên  được ứng dụng khá phổ biến để xây dựng các hệ mật điển hình là hệ mật OTP [88] hay các hệ mật mã lặp như DES [28], IDEA [54];
* Trường hữu hạn : Ứng dụng tiêu biểu của trường hữu hạn trong mật mã khóa bí mật là hệ mật nổi tiếng AES [66] hoạt động trên trường  Trong mật mã khóa công khai, trường hữu hạn với bài toán Logarit rời rạc (DLP) là cơ sở của nhiều hệ mật khóa công khai điển hình là ElGamal [29];
* Các ma trận: Ứng dụng điển hình của các ma trận có các phần tử thuộc  là hệ mật khóa bí mật Hill [56]. Một dạng ma trận đặc biệt, ma trận của các đa thức gần đây đã được khai thác để xây dựng hệ mật khóa công khai MaTRU [23];
* Các đường cong elliptic trên trường hữu hạn: Ứng dụng của các đường cong Elliptic trong mật mã được khởi xướng bởi Miller [63] và Koblitz [52] vào năm 1985. Hướng nghiên cứu này sử dụng nhóm các điểm trên các đường cong elliptic thay vì các nhóm nhân trên trường hữu hạn để xây dựng các bài toán khó Logarit rời rạc (DLP). Với cải tiến này, các hệ mật xây dựng trên đường cong Elliptic thường có khóa nhỏ hơn, tốc độ thực thi nhanh hơn trong khi vẫn đảm bảo độ an toàn tương đương với các hệ mật dựa trên bài toán khó DLP trên trường hữu hạn;
* Các dàn (lattice): Là một cấu trúc đại số tuyến tính nên các phép tính trên dàn có độ phức tạp tính toán thấp (chỉ là ). Với các ưu điểm đó, dàn được xem xét ứng dụng trong mật mã khóa công khai từ những năm 1990 với động lực chính là xây dựng các hệ mật khóa công khai có hiệu năng tính toán cao hơn so với các hệ mật dựa trên bài toán IFP và DLP [41] trên vành số nguyên và các đường cong elliptic. Các bài toán khó trên dàn như SVP (Shortest Vector Problem) và CVP (Closest Vector Problem) đã được ứng dụng trong một số hệ mật như [6], [19], [34], [35], [71]hay [72]. NTRU [40] cũng có thể coi là một hệ mật thuộc nhóm này nếu nhìn từ quan điểm bài toán khó cơ sở.

Bên cạnh các cấu trúc đại số nêu trên, vành đa thức , gọi đầy đủ là vành đa thức có bậc hữu hạn  và các hệ số nằm trong vành , là nền tảng ít được ứng dụng trong mật mã và mới chỉ được quan tâm từ năm 1998 khi hệ mật khóa công khai NTRU được đề xuất bởi Hoffstein, Pipher và Silverman [40]. Mặc dù chưa có độ an toàn ngữ nghĩa (semantical security), hệ mật này đến nay vẫn được coi là an toàn với giả thiết về độ khó của một số bài toán trên dàn như SVP và đã được chuẩn hóa trong các tiêu chuẩn IEEE P.1363.1 [47] năm 2008 và ANSI X9.98 [8] năm 2011. NTRU ra đời đã cho thấy có thể sử dụng các phần tử khả nghịch trên các vành đa thức để xây dựng các hệ mật có khóa nhỏ và tốc độ tính toán nhanh. Tuy nhiên, nhược điểm của NTRU là hệ số mở rộng bản tin (tỉ lệ giữa độ dài của bản mã trên độ dài của bản rõ) khá lớn so với các hệ mật khóa công khai khác, khoảng 3 đến 5 lần. NTRU có nhiều biến thể trên các cấu trúc đại số khác nhau ([8], [74], MaTRU [23], ETRU [50], OTRU [58],…) nhưng đáng chú ý là hệ mật pNE [87], được đề xuất bởi Stehle và Steinfeld năm 2011. pNE hoạt động trên một lớp con của vành đa thức  với  Điểm cải tiến của pNE so với NTRU là có độ an toàn ngữ nghĩa IND-CPA dựa trên bài toán khó R-LWE [57] trên các vành đa thức. Mặc dù vậy, nhược điểm của pNE là hệ số mở rộng bản tin còn cao hơn NTRU [18].

Trong các vành , một lớp con với  còn gọi là lớp vành đa thức có bậc hữu hạn  và hệ số nhị phân ký hiệu bởi  là một cấu trúc đại số rất đáng chú ý. Ưu điểm của cấu trúc đại số này là các phép tính trên vành đa thức được thực hiện rất đơn giản và dễ dàng thực hiện bằng phần cứng, cụ thể là phép cộng đa thức hệ số nhị phân thực chất là  phép tính XOR. Tuy vậy, trước đây  hầu như mới chỉ được ứng dụng trong mã sửa sai tiêu biểu là các mã cyclic [64].

Từ năm 2002 đến nay, một lớp nhỏ của  với  gọi tắt là lớp vành đa thức chẵn tuyệt đối và ký hiệu bởi , đã được nhóm nghiên cứu của GS.TS. Nguyễn Bình ứng dụng để xây dựng một số hệ mật khóa bí mật [15], [3] và một hệ mật khóa công khai [4]. Mặc dù các hệ mật này còn nhiều nhược điểm (thuật toán tính toán còn phức tạp, chưa có độ an toàn ngữ nghĩa,…) nhưng các kết quả ban đầu cho thấy có thể sử dụng một số lớp đặc biệt của vành đa thức  để xây dựng các hệ mật.

Các phân tích như trên cho thấy ứng dụng của các vành đa thức nói chung và đặc biệt là các vành đa thức chẵn  nói riêng trong mật mã vẫn còn một số hạn chế như:

* Các vành đa thức  vẫn chưa được ứng dụng rộng rãi trong việc xây dựng các hệ mật mà chủ yếu được ứng dụng trong xây dựng mã sửa sai;
* Các hệ mật đã được xây dựng trên vành đa thức hiện nay hầu hết chưa có độ an toàn ngữ nghĩa;
* Các hệ mật dựa trên vành đa thức  điển hình như NTRU [40] hay pNE [87] có tốc độ tính toán tốt nhưng hệ số mở rộng bản tin (tỉ lệ giữa độ dài bản mã trên độ dài bản rõ) vẫn khá lớn và không phù hợp với các thiết bị có tài nguyên tính toán hạn chế rất phổ biến trong tương lai theo xu hướng IoT.

Tuy nhiên, trong quá trình nghiên cứu ứng dụng  trong mã sửa sai, lớp vành đa thức chẵn  lại cho thấy những đặc tính đặc biệt phù hợp với mật mã. Cụ thể là:

* Cũng như các vành đa thức khác, các phép tính trên vành  có độ phức tạp tính toán thấp, cụ thể là  với phép cộng và  với phép nhân. Đặc biệt là các phép cộng trong  chỉ là một chuỗi các phép tính XOR rất đơn giản trên trường nhị phân . Đặc tính này rất phù hợp để xây dựng các hệ mật có tốc độ tính toán nhanh và dễ thực thi bằng cả phần mềm lẫn phần cứng;
* Trong  và cụ thể hơn là trong  luôn tồn tại các phần tử khả nghịch [3], bên cạnh những phần tử không khả nghịch. Nếu xác định được các thuật toán mật mã phù hợp, các phần tử khả nghịch sẽ chính là khóa để giải mã thông tin trong khi các phần tử không khả nghịch sẽ là đối tượng để che giấu thông tin, tương tự như trường hợp của hệ mật NTRU [40];
* Trong các vành  với  lẻ, gọi tắt là vành lẻ, tất cả mọi phần tử đều là các thặng dư bậc hai. Trong khi đó, vành  chỉ có  phần tử là thặng dư bậc hai trong tổng số  đa thức thuộc vành [14]. Điểm đáng chú ý mỗi thặng dư bậc hai đó lại có đến  căn bậc hai. Điều này cho thấy là nếu biết một căn bậc hai sẽ dễ dàng suy ra thặng dư bậc hai tương ứng nhưng điều ngược lại là rất khó khăn vì có đến  phương án lựa chọn, đặc biệt khi  lớn. Đặc tính “một chiều” này hoàn toàn có thể khai thác để xây dựng các hệ mật.

Vấn đề đặt ra ở đây là làm thế nào để hiện thực hóa các tiềm năng của vành đa thức chẵn  để giải quyết các vấn đề còn tồn tại đối với các hệ mật dựa trên vành đa thức và rộng hơn là các hệ mật dựa trên các cấu trúc đại số khác.

Với cách đặt vấn đề như trên, **mục đích nghiên cứu** của luận án là xây dựng được các hệ mật (mới hoặc là biến thể của các hệ mật hiện có) có độ phức tạp tính toán thấp, tốc độ tính toán nhanh, tiêu tốn ít tài nguyên và an toàn dựa trên các ưu điểm của cấu trúc đại số vành đa thức mà cụ thể là vành đa thức chẵn .

**Đối tượng nghiên cứu** chính của luận án là các vành đa thức chẵn  cùng một số loại vành đa thức có liên quan và các hệ mật dựa trên các vành đa thức này.

**Phạm vi nghiên cứu** của luận án bao gồm:

1. Nghiên cứu tổng quan về mật mã (phân loại, kỹ thuật xây dựng các hệ mật, tham số đánh giá các hệ mật, các mô hình tấn công cơ bản, phương pháp đánh giá độ an toàn) qua đó đánh giá các hệ mật dựa trên vành đa thức hiện có. Các phân tích này chỉ ra các hạn chế của các kết quả nghiên cứu hiện có và tiềm năng ứng dụng vành đa thức chẵn  trong mật mã.
2. Nghiên cứu các đặc tính của vành đa thức chẵn  (các khái niệm, các phép tính toán, các phần tử đặc biệt) làm cơ sở toán học phục vụ xây dựng các hệ mật.
3. Nghiên cứu đề xuất một cách tường minh (các không gian khóa, bản rõ, bản mã cùng các thuật toán tạo khóa, mã hóa và giải mã) và đánh giá các hệ mật dựa trên vành đa thức chẵn .
4. Nghiên cứu một số vành đa thức đặc biệt (vành đa thức có hai lớp kề cyclic , vành đa thức ) từ đó xem xét đề xuất các hệ mật dựa trên sự kết hợp giữa vành đa thức chẵn  với các vành đa thức này.

**Phương pháp nghiên cứu** chính được sử dụng trong luận án là lý thuyết toán học (lý thuyết số, đại số trừu tượng, xác suất) và độ phức tạp tính toán. Công cụ nghiên cứu chính của luận án là các công cụ toán học và mô phỏng.

**Ý nghĩa khoa học của luận án**:

1. Về mặt toán học, luận án đóng góp một số kết quả nghiên cứu mới về cấu trúc đại số vành đa thức chẵn  nói riêng và vành đa thức  nói chung. Cụ thể là, luận án đã:

* Chỉ ra hai loại vành đa thức đặc biệt (vành đa thức chẵn tuyệt đối  và vành đa thức chỉ có hai lớp kề cyclic ) có tỉ lệ giữa số phần tử khả nghịch trên tổng số đa thức của vành là cực đại;
* Đề xuất được một thuật toán hiệu quả để xác định nghịch đảo của các phần tử khả nghịch trên vành đa thức chẵn tuyệt đối ;
* Đề xuất được một công thức để xác định nghịch đảo mở rộng của các phần tử khả nghịch mở rộng trên các vành  với  lẻ (trong đó có vành ) và chứng minh các phần tử này có thể được sử dụng làm khóa cho các hệ mật tương tự như các phần tử khả nghịch truyền thống.
* Đề xuất các công thức tính căn bậc hai chính của một thặng dư bậc hai trong vành  và các phần tử liên hợp của chúng.

Các kết quả này là nền tảng toán học rất quan trọng cho các ứng dụng của  trong mật mã.

1. Về các ứng dụng mật mã, luận án đã đề xuất được 6 hệ mật bao gồm:
2. Ba hệ mật dựa trên vành đa thức chẵn:

* Hệ mật khóa bí mật RISKE có độ an toàn IND-CPA hoạt động dựa trên các phần tử khả nghịch trên vành đa thức chẵn tuyệt đối ;
* Hệ mật khóa bí mật QRHE, dựa trên các thặng dư bậc hai và lớp các phần tử liên hợp trong vành đa thức chẵn , cùng một ví dụ lai ghép với hệ mật RSA;
* Hệ mật khóa công khai IPKE có độ an toàn IND-CPA dựa trên các phần tử khả nghịch trên vành đa thức chẵn tuyệt đối .

1. Ba hệ mật dựa trên sự kết hợp của vành đa thức chẵn và một số loại vành đa thức đặc biệt khác:

* Hệ mật khóa công khai DTRU, một biến thể với nhiều đặc tính tốt so với hệ mật gốc NTRU, có độ an toàn IND-CPA và hoạt động dựa trên các phần tử khả nghịch đồng thời trên hai vành đa thức, một vành chẵn tuyệt đối  và một vành có hai lớp kề cyclic .
* Hệ mật khóa bí mật E-RISKE, một biến thể mở rộng của hệ mật RISKE hoạt động dựa trên các phần tử khả nghịch mở rộng trong vành đa thức có hai lớp kề cyclic .
* Hệ mật HpNE, có độ an toàn IND-CPA, là một hệ mật lai ghép giữa hệ mật pNE và hệ mật RISKE theo mô hình KEM/DEM.

Về **ý nghĩa thực tiễn**, các hệ mật được đề xuất trong luận án ngoài độ an toàn ngữ nghĩa, còn có độ phức tạp tính toán thấp, tốc độ tính toán nhanh và đòi hỏi ít tài nguyên tính toán do đó có thể được xem xét triển khai trong các thiết bị có tài nguyên tính toán hạn chế trong môi trường IoT.

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

* “Chương 1: Tổng quan về mật mã và các hệ mật dựa trên vành đa thức”: Trình bày một bức tranh tổng quan về mật mã và các hệ mật dựa trên vành đa thức chẵn. Từ đó, nội dung của chương đi sâu phân tích các hạn chế của các hệ mật dựa trên vành đa thức hiện có và đánh giá các tiềm năng ứng dụng của vành đa thức chẵn  trong mật mã cũng như xác định rõ các vấn đề cần nghiên cứu.
* “Chương 2: Vành đa thức chẵn”: Chương này trình bày các nền tảng toán học về vành đa thức chẵn , đặc biệt là một số kết quả toán học mới của luận án về cấu trúc đại số vành đa thức  nói chung và vành đa thức chẵn  nói riêng. Bằng Định lý 2‑3 và Định lý 2‑4, tác giả luận án chứng minh rằng hai lớp vành và  có tỉ lệ các phần tử khả nghịch trên tổng số đa thức trong vành đạt cực đại và đề xuất thuật toán cụ thể (Thuật toán 2‑1) để tính toán nghịch đảo của chúng. Các phần tử khả nghịch này là cơ sở chính để xây dựng các hệ mật ở các chương 3, 4. Cũng trong chương này, bên cạnh các phần tử khả nghịch truyền thống, tác giả luận án chứng minh rằng trong các vành  với  lẻ còn tồn tại một lớp các phần tử khả nghịch mở rộng có tính chất gần tương tự với các phần tử khả nghịch truyền thống (Định lý 2‑1). Các phần tử này cũng có thể sử dụng làm khóa trong các hệ mật tương tự như các phần tử khả nghịch (Định lý 2‑2). Kết quả này cho phép linh hoạt lựa chọn loại vành đa thức để xây dựng các hệ mật và được cụ thể hóa bằng hệ mật khóa bí mật E-RISKE (mục 4.3) hoạt động cả trên và , một cải tiến của hệ mật RISKE (mục 3.2) vốn chỉ hoạt động trên . Ngoài ra, với việc chứng minh hai công thức tính căn bậc hai chính và phần tử liên hợp của một thặng dư bậc hai (Bổ đề 2‑9 và Bổ đề 2‑10), tác giả luận án đã xây dựng một nền tảng để đề xuất hệ mật lai ghép QRHE trong mục 3.3.
* “Chương 3: Các hệ mật dựa trên vành đa thức chẵn”: Đề xuất 03 hệ mật QRHE, IPKE và RISKE) trực tiếp dựa trên lớp vành đa thức chẵn  được công bố lần lượt trong các công trình [C2], [J1] và [J3] của tác giả luận án. Trong đó: Hệ mật RISKE [C2] là một biến thể của hệ mật OTP sử dụng các phần tử khả nghịch trong  làm khóa bí mật và có độ an toàn ngữ nghĩa IND-CPA (Định lý 3‑2); Hệ mật lai ghép QRHE [J1], khai thác đặc tính của các thặng dư bậc hai trong  để khắc phục nhược điểm sử dụng khóa phiên (session-key) của RISKE; Cuối cùng, hệ mật khóa công khai IPKE [J3] cũng hoạt động dựa trên các phần tử khả nghịch trong  và có độ an toàn ngữ nghĩa IND-CPA (Định lý 3‑3).
* “Chương 4: Các hệ mật dựa trên vành đa thức chẵn kết hợp với các vành đa thức khác”: Chương mở rộng này đề xuất 03 hệ mật hoạt động trên vành đa thức chẵn kết hợp với một số loại vành đa thức khác được công bố lần lượt trong các công trình [J2], [C3] và [C1] của tác giả luận án. Trong đó: Hệ mật DTRU [J2] là một biến thể có nhiều ưu điểm của hệ mật NTRU hoạt động dựa trên các phần tử khả nghịch đồng thời trên hai vành  và ; Hệ mật E-RISKE [C3] là một mở rộng của hệ mật RISKE sử dụng các phần tử khả nghịch mở rộng trong  làm khóa bí mật; Cuối cùng, HpNE [C1] là một hệ mật lai ghép theo mô hình KEM/DEM giữa hệ mật RISKE với hệ mật pNE có độ an toàn ngữ nghĩa IND-CPA (Định lý 4‑4) và hệ số mở rộng bản tin linh hoạt.
* “Kết luận”: Tổng hợp đánh giá các kết quả đạt được của luận án đồng thời đề xuất các hướng nghiên cứu tiếp theo.

Nhìn chung, luận án đã đưa ra những đề xuất mang tính khởi đầu cho việc ứng dụng các vành đa thức chẵn  vào lý thuyết mật mã. Các hệ mật này bước đầu đã được chứng minh là có những đặc tính tốt và có thể được xem xét ứng dụng cho các hệ thống đòi hỏi tính toán nhanh hoặc các thiết bị có tài nguyên tính toán hạn chế trong môi trường IoT.

# xxx

## MỞ ĐẦU CHƯƠNG

Mật mã có lịch sử phát triển lâu đời với nhiều loại hệ mật khác nhau với các kỹ thuật trên các cấu trúc đại số khác nhau trong đó có vành đa thức. Để có thể đánh giá rõ hiện trạng ứng dụng của vành đa thức trong mật mã từ đó xác định các vấn đề cần nghiên cứu, chương này sẽ trình bày một bức tranh tổng quan về mật mã và các hệ mật dựa trên vành đa thức chẵn.

Mục 1.2 sẽ hệ thống hóa sự phát triển của mật mã và tập trung phân tích các tham số, phương pháp đánh giá đặc biệt là đánh giá về độ an toàn của các hệ mật. Dựa trên đó, các hệ mật dựa trên vành đa thức chẵn nói riêng và vành đa thức nói chung sẽ được phân tích trong mục 1.3. Từ các phân tích đó, mục 1.4 sẽ đưa ra các vấn đề mở cần nghiên cứu để có thể ứng dụng thành công vành đa thức chẵn trong lý thuyết mật mã.

## CÁC HỆ MẬT DỰA TRÊN VÀNH ĐA THỨC

### Các hệ mật khoá bí mật dựa trên vành đa thức

Trên thế giới, trong các kỹ thuật mật mã khóa bí mật, các phép toán được sử dụng hầu hết đều được thực hiện dựa trên các kỹ thuật thay thế và hoán vị trên các trường nhị phân  với các hệ mật tiêu biểu như DES [28] hay OTP [88]. Điều này là do các phép mã hóa và giải mã trong  đều dựa trên phép tính XOR đơn giản và dễ thực thi bằng cả phần cứng lẫn phần mềm.

Tại Việt Nam, việc ứng dụng các vành đa thức trong mật mã khóa bí mật lại có nguồn gốc từ các nghiên cứu về xây dựng mã sửa sai, cụ thể là mã cyclic cục bộ [13], [14], [16], [17]. Điều này phát sinh từ một số phân tích đặc tính toán học của một số lớp vành đa thức . Hai lớp con quan trọng của  bao gồm lớp vành đa thức chẵn  và lớp vành đa thức chỉ có hai lớp kề cyclic  [17]. Các vành đa thức chẵn  không được sử dụng trong xây dựng mã cyclic truyền thống vì tất cả các mã cyclic truyền thống trên vành này đều được suy ra từ vành lẻ tương ứng [17].

Tuy nhiên, năm 2002, một lớp con của , lớp các vành chẵn tuyệt đối , đã được sử dụng để xây dựng một hệ mật khóa bí mật trong công trình [15]. Hệ mật này khai thác đặc tính của các cấp số nhân cyclic trên lớp vành đa thức . Lớp vành này có điểm đặc biệt là tất cả các đa thức có trọng số lẻ trong vành sẽ tạo thành một nhóm nhân cyclic . Trong nhóm nhân này sẽ có nhiều nhóm con có cấp bằng ước của cấp của . Ý tưởng của hệ mật này là sử dụng một ma trận mã hóa  được tạo bởi hai khóa bí mật là hai đa thức có trọng số lẻ , trong đó  là phần tử sinh của một nhóm nhân cyclic nào đó còn  là một đa thức bất kỳ thuộc . Với cách lựa chọn này, việc giải mã sẽ thực hiện đơn giản bằng cách bình phương ma trận   lần, với  là cấp của đa thức . Ngoài ra, nếu thay  bằng đơn thức , ma trận  sẽ là các ma trận luân hoàn (circulant matrix), ma trận mà trong đó mỗi hàng được xác định bằng cách dịch vòng phải hàng đứng trên nó, và khi đó các phép tính trên vành ma trận phức tạp sẽ tương đương với phép tính đơn giản trên vành đa thức. Nhược điểm của hệ mật này là hiệu năng tính toán không cao vì phải thực hiện nhiều lần phép bình phương đa thức trong khi giải mã. Bên cạnh đó, hệ mật này cũng chưa được đánh giá kỹ lưỡng về độ an toàn.

Tương tự như , các vành đa thức chỉ có hai lớp kề cyclic  cũng mới chỉ được khai thác để xây dựng các m-dãy lồng ghép, một dạng chuỗi giả ngẫu nhiên trong công trình [1].

Dựa trên công trình [15], bài báo [3] đã đề xuất ứng dụng các đa thức trong nhóm nhân cyclic có bậc cực đại của vành  làm khóa trong các vòng lặp của hệ mật DES. Tuy nhiên, hệ mật này chưa được chứng minh là đảm bảo an toàn trong khi DES phiên bản gốc hiện nay đã không còn được sử dụng.

Hệ mật được đề xuất trong [4] này cũng là cơ sở để hai tác giả này đề xuất một loại hàm băm mới trong công trình [2].

Qua phân tích có thể thấy vành đa thức  nói chung và vành đa thức chẵn  nói riêng vẫn chưa được ứng dụng rộng rãi trong các hệ mật khóa bí mật.

### Các hệ mật khoá công khai dựa trên vành đa thức

Tại Việt Nam, hệ mật khóa công khai đầu tiên dựa trên vành đa thức  được đưa ra năm 2005 trong công trình [4]. 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). Ưu điểm đầu tiên của hệ mật này chính là dựa trên các sự linh hoạt lựa chọn tham số của mã cyclic cục bộ. 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.

Ở nước ngoài, việc sử dụng các vành đa thức  để xây dựng các hệ mật khóa công khai được khởi xướng từ những năm 1995 khi hệ mật NTRU lần đầu tiên được giới thiệu tại Crypto’96 [39]. Tại hội thảo ANTS’98, các tác giả của NTRU đã đưa ra phiên bản cải tiến trong đó đã đánh giá về độ an toàn của NTRU đối với các tấn công dựa trên dàn [40]. NTRU được IEEE bắt đầu chuẩn hóa từ năm 2008 [47] trong nhóm tiêu 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 elliptic. Hệ mật này cũng được coi là ứng viên cho thế hệ mật mã khóa công khai có khả năng chống lại các tấn công bằng máy tính lượng tử [77]. 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 [20], [24], [33], [38], [48], [6] và nhiều biến thể khác nhau [8], MaTRU [23], ETRU [50], OTRU [58],...

So với các hệ mật thông dụng như RSA, ECC, NTRU có một số ưu điểm [40]:

* Thuật toán mã hóa và giải mã đơn giản kéo theo tốc độ tính toán rất nhanh, được coi là nhanh nhất hiện nay và còn có thể tối ưu [43];
* Sử dụng khóa ngắn hơn so với các hệ mật khóa công khai khác ở cùng độ an toàn;
* 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 [40]:

* Chưa có độ an toàn ngữ nghĩa;
* Bị tấn công khi phát lại liên tiếp bản mã của cùng một bản rõ;
* Hệ số mở rộng bản tin lớn.

Biến thể đầu tiên của NTRU hoạt động trên vành  được đề xuất năm 2002 có tên là CTRU [32] 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 trên dàn như đối với NTRU. Tuy nhiên hệ mật này năm 2008 đã bị phá bởi các tấn công bằng phương pháp giải hệ phương trình đại số tuyến tính [89].

Một biến thể khác của NTRU, hệ mật pNE [87] được đề xuất năm 2011, hoạt động dựa trên lớp vành đa thức chẵn tuyệt đối hệ số nguyên. 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, theo kết quả phân tích năm 2014 [18], hiệu năng của pNE tính toán thấp hơn NTRU đặc biệt là hệ số mở rộng bản tin.

Gần đây nhất, vào tháng 2 năm 2017, một biến thể cũng có độ an toàn chứng minh được như pNE nhưng lại hoạt động trên vành  với  là số nguyên tố lẻ đã được đề xuất [90]. Biến thể này cho phép lựa chọn linh hoạt hơn cấu trúc đại số vành đa thức để xây dựng các hệ mật có đặc điểm như pNE.

Nhìn chung, xây dựng các hệ mật khóa công khai trên vành đa thức mới chỉ được đề cập đến trong các công trình nêu trên. Hoàn toàn chưa có các hệ mật được xây dựng dựa trên các vành đa thức chẵn .

### Các hệ mật lai ghép dựa trên vành đa thức

Do các hệ mật khóa công khai và khóa bí mật dựa trên các vành đa thức còn chưa phong phú nên các hệ mật lai ghép dựa trên cấu trúc đại số này cũng chưa được xây dựng.

## KẾT LUẬN CHƯƠNG

Từ nội dung tổng quan có thể thấy việc đi tìm các cấu trúc đại số mới để xây dựng và cải tiến các hệ mật là một quá trình liên tục trong lịch sử phát triển của mật mã. Trong các cấu trúc đại số đó, vành đa thức mới được khai thác trong mật mã khoảng 20 năm trở lại đây và có nhiều tiềm năng khi các hệ thống truyền thông phát triển theo xu hướng IoT. Các hệ mật dựa trên vành đa thức vẫn chưa phong phú và còn một số hạn chế như hiệu năng chưa cao, chưa có độ an toàn ngữ nghĩa,… Mặc dù vậy, vành đa thức nói chung và vành đa thức chẵn  nói riêng là các cấu trúc đại số có nhiều tiềm năng ứng dụng trong mật mã. Tuy nhiên, để có thể xây dựng được các hệ mật dựa trên , có hai nhóm vấn đề cần nghiên cứu như sau.

Thứ nhất, để có thể xây dựng các hệ mật dựa trên  trước hết cần nghiên cứu kỹ về đặc tính toán học của cấu trúc đại số này. Một số bài toán cần giải quyết cụ thể như cách thức xác định các phần tử khả nghịch, cách tính nghịch đảo của các phần tử khả nghịch, cách tính các căn bậc hai chính của thặng dư bậc hai và các phần tử liên hợp của chúng,… Đây cũng là nội dung chính trong chương 2 của luận án.

Thứ hai, dựa trên các đặc tính toán học của , cần nghiên cứu xây dựng các giải pháp khắc phục các hạn chế đã phân tích của các hệ mật dựa trên vành đa thức. Cụ thể là, các hệ mật cần được đề xuất với các mô tả tường minh về các không gian (bản rõ, bản mã và khóa), các thuật toán (tạo khóa, mã hóa và giải mã) và đặc biệt là được đánh giá về độ an toàn theo phương pháp đánh giá độ an toàn ngữ nghĩa đã được nêu trong mục 1.2. Các nội dung nghiên cứu này sẽ được trình bày chi tiết trong chương 3 và chương 4.

# …

## MỞ ĐẦU CHƯƠNG

Nội dung chương 3 cho thấy vành đa thức chẵn đứng độc lập đã có thể ứng dụng để xây dựng một số hệ mật có đặc tính tốt. Tuy nhiên, sự kết hợp giữa vành đa thức chẵn  và các vành đa thức khác mở ra nhiều hướng ứng dụng khác của vành đa thức trong mật mã.

Trong chương này, …

## KẾT LUẬN CHƯƠNG

Trong chương này, bằng cách kết hợp vành đa thức chẵn tuyệt đối , một lớp con của các vành đa thức chẵn  với các loại vành đa thức khác, luận án đã đề xuất ba hệ mật mới có nhiều đặc tính cải tiến so với các hệ mật gốc. Hệ mật DTRU, một biến thể mới của hệ mật nổi tiếng NTRU, có thể coi là một ứng viên tiềm năng hơn NTRU trong các ứng dụng cho các thiết bị có tài nguyên tính toán hạn chế. Dựa trên các phần tử nghịch đảo mở rộng trong vành đa thức , hệ mật E-RISKE cho phép lựa chọn các tham số của hệ mật RISKE (độ dài khóa, độ dài bản mã,…) linh hoạt hơn cho các ứng dụng mật mã cụ thể. Cuối cũng, HpNE là một sự lai ghép phù hợp giữa RISKE (dựa trên các vành ) và hệ mật pNE (dựa trên các vành ) theo mô hình KEM/DEM, tận dụng ưu điểm cũng như khắc phục nhược điểm của cả hai hệ mật này.

Các kết quả trong chương này đã khẳng định việc kết hợp vành đa thức chẵn với các vành đa thức có cấu trúc đặc biệt khác để xây dựng các hệ mật là hướng nghiên cứu hữu ích và khả thi.

# KẾT LUẬN

Sau một thời gian nghiên cứu với sự nỗ lực của bản thân và sự hướng dẫn  
tận tình của GS.TS. Nguyễn Bình, luận án “**Các hệ mật dựa trên vành đa thức chẵn**” của tác giả đã hoàn thành với một số kết quả sau đây.

**Về mặt toán học**, luận án đã chứng minh một số đặc tính toán học mới của các vành đa thức chẵn cùng một số loại vành đa thức đặc biệt. Cụ thể là, luận án đã:

1. Chỉ ra hai loại vành đa thức (vành đa thức chẵn tuyệt đối  và vành đa thức chỉ có hai lớp kề cyclic ) có tỉ lệ giữa số phần tử khả nghịch trên tổng số đa thức của vành là cực đại (Định lý 2‑3, Định lý 2‑4).
2. Đề xuất được một thuật toán hiệu quả để xác định nghịch đảo của các phần tử khả nghịch trên vành đa thức chẵn tuyệt đối  (Thuật toán 2‑1).
3. Đề xuất được một công thức (Định lý 2‑1) để xác định nghịch đảo mở rộng của các phần tử khả nghịch mở rộng trên các vành  với  lẻ (trong đó có vành ) và chứng minh các phần tử này có thể được sử dụng để làm khóa cho các hệ mật (Định lý 2‑2).
4. Đề xuất các công thức tính căn bậc hai chính của một thặng dư bậc hai trong vành  và phần tử liên hợp của chúng (Bổ đề 2‑9 và Bổ đề 2‑10).

Các kết quả này là nền tảng rất quan trọng cho các ứng dụng của  trong mật mã.

**Về các ứng dụng trong mật mã**, luận án đã:

1. Đề xuất được ba hệ mật dựa trên vành đa thức chẵn bao gồm:
2. Hệ mật khóa bí mật RISKE có độ an toàn IND-CPA (Định lý 3‑2) hoạt động dựa trên các phần tử khả nghịch trên vành đa thức chẵn tuyệt đối . Hệ mật này là một biến thể của hệ mật OTP nhưng có hiệu quả mã hóa cao hơn. Đặc biệt, hệ mật này rất phù hợp để làm phần DEM trong sơ đồ mật mã lai ghép KEM/DEM.
3. Hệ mật khóa bí mật QRHE, dựa trên các thặng dư bậc hai và lớp các phần tử liên hợp trong vành đa thức chẵn , cùng một ví dụ lai ghép với hệ mật RSA. So với RISKE hay OTP, QRHE có khóa tự sinh từ bản mã trong mỗi phiên mã hóa và hiệu quả mã hóa rất cao.
4. Hệ mật khóa công khai IPKE có độ an toàn IND-CPA (Định lý 3‑3) dựa trên các phần tử khả nghịch trên vành đa thức chẵn tuyệt đối . IPKE có thuật toán mã hóa và giải mã rất đơn giản, sử dụng khóa bí mật nhỏ và có hệ số mở rộng bản tin thấp hơn so với hệ mật NTRU.
5. Đề xuất được ba hệ mật dựa trên sự kết hợp của vành đa thức chẵn và một số loại vành đa thức đặc biệt khác:
6. Hệ mật khóa công khai DTRU, một biến thể với nhiều đặc tính tốt so với hệ mật gốc NTRU. Hệ mật này hoạt động dựa trên các phần tử khả nghịch đồng thời trên hai vành đa thức, một vành chẵn tuyệt đối  và một vành có hai lớp kề cyclic . So với NTRU, DTRU có thuật toán tạo khóa rất đơn giản, kích thước khóa nhỏ hơn, hệ số mở rộng bản tin nói chung là thấp hơn cũng như dễ lựa chọn các tham số và chế độ hoạt động. Ngoài ra, DTRU cũng có độ an toàn IND-CPA (Định lý 4‑1).
7. Hệ mật khóa bí mật E-RISKE, một biến thể mở rộng của hệ mật RISKE hoạt động dựa trên các phần tử khả nghịch mở rộng trong vành đa thức có hai lớp kề cyclic . E-RISKE thừa hưởng tất cả các đặc tính của RISKE đặc biệt là độ an toàn IND-CPA (Định lý 4‑3). Cùng với RISKE, E-RISKE cho phép cho phép lựa chọn linh hoạt cấu trúc đại số cũng như các tham số hoạt động để phù hợp các tình huống ứng dụng mật mã khác nhau.
8. Hệ mật HpNE, một hệ mật lai ghép giữa hệ mật pNE và hệ mật RISKE theo mô hình KEM/DEM, có độ an toàn IND-CPA (Định lý 4‑4) như pNE nhưng có hệ số mở rộng bản tin nhỏ và linh hoạt hơn.

Các hệ mật được đề xuất nhìn chung đều có độ phức tạp tính toán thấp và an toàn ngữ nghĩa với các tấn công phổ biến đã khẳng định ưu điểm của vành đa thức chẵn  nói riêng và vành đa thức  nói chung so với các cấu trúc đại số khác trong các ứng dụng mật mã. Các hệ mật này có thể được xem xét ứng dụng trong các thiết bị có tài nguyên tính toán hạn chế rất phổ biến trong môi trường IoT.

**Một số vấn đề mở** từ các kết quả nghiên cứu của luận án bao gồm:

1. Nghiên cứu xây dựng các hệ mật dựa trên các lớp vành đa thức có tỉ lệ số phần tử khả nghịch hoặc khả nghịch mở rộng trên tổng số đa thức trong vành đạt cực đại hoặc gần cực đại.
2. Nghiên cứu đưa các hệ mật khóa công khai IPKE và DTRU về các bài toán khó cơ sở đã được chứng minh về độ an toàn để tăng cường độ tin cậy của các hệ mật này.
3. Đánh giá thử nghiệm các hệ mật đã đề xuất trên các hệ thống phần cứng cụ thể, đặc biệt là các hệ thống có tài nguyên hạn chế để đánh giá chính xác ưu điểm về tốc độ tính toán của các hệ mật đã xây dựng được cũng như cải tiến các hệ mật này cho phù hợp với các thiết bị có tài nguyên hạn chế trong môi trường IoT.
4. Nghiên cứu độ an toàn của các hệ mật đã đề xuất trong môi trường xử lý song song.

Những kết quả nghiên cứu của luận án về cơ bản đã đạt được mục đích nghiên cứu đề ra với một số đóng góp nhỏ trong lý thuyết mật mã. Tác giả luận án rất mong nhận được các góp ý của các nhà khoa học, các đồng nghiệp và bạn bè để hoàn thiện các công trình nghiên cứu của mình.

Hà Nội, tháng 12 năm 2017

Cao Minh Thắng

# 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”, *Kỷ yếu Hội nghị khoa học lần thứ 8*, Học viện Công nghệ Bưu chính Viễn thông, Hà Nội.
2. Nguyễn Bình, Trần Đức Sự (2007), *Giáo trình Mật mã học*, Nhà xuất bản Bưu điện.
3. 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.
4. 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*, 50 ( 2A), ISSN 0866 708X.
5. 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, trang 63 – 69.

**Tiếng Anh**

1. Ajtai, Miklós; Dwork, Cynthia (1997), "A public-key cryptosystem with worst-case/average-case equivalence", *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, El Paso, Texas, United States: ACM. pp. 284–293.
2. Albrecht, M., Bai, S., Ducas, L., (2016) “A subfield lattice attack on overstretched NTRU assumptions”. *In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS,* vol. 9814, pp. 153–178. Springer, Heidelberg.
3. American National Standards Institute (ANSI) (2010), *X9.98 standard*, *Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry*.
4. Banks W. D., Shparlinski I. E. (2002), “A Variant of NTRU with Non-invertible Polynomials”, *Lecture Notes in Computer Science* Volume 2551, 2002, pp 62-70.
5. Benaloh, Josh, (1994), "Dense Probabilistic Encryption." *(PS). Workshop on Selected Areas of Cryptography,* pages 120–128.
6. Berlekamp, Elwyn R.; McEliece, Robert J.; Van Tilborg, Henk C.A. (1978), "On the Inherent Intractability of Certain Coding Problems", *IEEE Transactions on Information Theory*, IT-24: 203–207.
7. Andrey Bogdanov, Gregor Leander, Lars R. Knudsen, Christof Paar, Axel Poschmann, Matthew J. Robshaw, Yannick Seurin, and Christine Vikkelsoe (2007), “PRESENT - An Ultra-Lightweight Block Cipher”. *In Proceedings of CHES 2007*, LNCS, Springer.
8. Boneh, Dan; Venkatesan, Ramarathnam (1998), "Breaking RSA may not be equivalent to factoring". *Advances in Cryptology — EUROCRYPT'98. Lecture Notes in Computer Science* *1403*, Springer, pp. 59–71.
9. 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 on Information and Communications Technologies 2007*, Malaysia, ISBN: 983-43160-0-3.
10. Nguyen Binh, Tran Duc Su, Pham Viet Trung (2001), “Decomposition of polynomial ring according to the classes of conjugate elements”, *AIC-26*, Hanoi, Vietnam.
11. Nguyen Binh (2002), “Crypto-system based on cyclic geometric progressions over polynomial ring” *(Part I). REV’02*.
12. Nguyen Binh, Le Dinh Thich (2002), “The orders of polynomials and algorithms for defining order of polynomial over polynomial Ring”, *VICA-5*, Hanoi, Vietnam.
13. Nguyen Binh, Dang Hoai Bac (2004), “Cyclic codes over extended rings of polynomial rings with two cyclotomic cosets”, *REV-04*, Hanoi, Vietnam.
14. Cabarcas D., Weiden P., Buchmann J. (2014), “On the Efficiency of Provably Secure NTRU”, [*Post-Quantum Cryptography*](http://link.springer.com/book/10.1007/978-3-319-11659-4) *Volume 8772 of the series*[*Lecture Notes in Computer Science*](http://link.springer.com/bookseries/558), pp 22-39. Springer.
15. Cai Jin-Yi, Cusick Thomas W (1999), “A Lattice-Based Public-Key Cryptosystem”, *Lecture Notes in Computer Science,* Volume 1556, 1999, pp 219-233.
16. Chenal M., Tang Q. (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.
17. Chor B., Rivest R. L. (1988), “A knapsack-type public key cryptosystem based on arithmetic in finite fields”, *IEEE Trans. Inform. Theory* 34, 901–909.
18. Cocks, Clifford (20 November 1973). "A Note on 'Non-Secret Encryption'" (PDF). CESG Research Report.
19. Coglianese M., Goi B.M. (2005), “MaTRU: A New NTRU-Based Cryptosystem”. *Lecture Notes in Computer Science* Volume 3797, 2005, pp 232-243.
20. Coppersmith D., Shamir A. (1997), “Lattice attacks on NTRU”, *In: Fumy, W. (ed.) EUROCRYPT 1997*, LNCS, vol. 1233, pp. 52–61. Springer, Heidelberg.
21. Cramer R. and Shoup V. (1998), "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack." *Proceedings of CRYPTO 1998*, LNCS 1462, p. 13ff.
22. 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), pp. 167-226.
23. W. Diffie, M.E. Hellman (1976), “New directions in cryptography”, *IEEE Trans on Information Theory*, Volume: 22, Issue: 6, (1976), pp. 644-654.
24. Dolev D., Dwork C., and Naor M. (2000), “Non-Malleable Cryptography”, *SIAM Journal on Computing*, 30(2):391–437.
25. ElGamal T. (1985), "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory,* 31 (4): 469–472.
26. Feistel H. (1973), “Cryptography and Computer Privacy". *Scientific American*, 228(5), May 1973, pp 15–23.
27. Fujisaki E., Okamoto T., Pointcheval D., and [Stern](https://en.wikipedia.org/wiki/Jacques_Stern) J. (2001) “RSA-OAEP is secure under the RSA assumption”. In J. Kilian, ed., Advances in Cryptology -- [CRYPTO](https://en.wikipedia.org/wiki/CRYPTO) 2001, vol. 2139 of Lecture Notes in Computer Science, SpringerVerlag.
28. Gaborit, P., Ohler, J., Sole, P. (2002),: “CTRU, a Polynomial Analogue of NTRU”, *INRIA. Rapport de recherche*, N.4621, (ISSN 0249-6399).
29. Gentry C. (2001), “Key recovery and message attacks on NTRU-composite.” In *Proceeding of Eurocrypt ’01*, LNCS, vol. 2045, Springer-Verlag, pp.182-194, 2001.
30. Gentry C., Peikert C., and Vaikuntanathan V. (2008), “Trapdoors for hard lattices and new cryptographic constructions”, *Proceedings of the 40th annual ACM symposium on Theory of computing,* Victoria, British Columbia, Canada: ACM, pp. 197-206.
31. Goldreich O., Goldwasser S., and Halevi S. (1997), “Public-key cryptosystems from lattice reduction problems”. In CRYPTO ’97: *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, pages 112–131, London, UK, Springer-Verlag.
32. Goldwasser S. and Micali S. (1982), “Probabilistic encryption & how to play mental poker keeping secret all partial information”, *Annual ACM Symposium on Theory of Computing*.
33. Goldwasser S. and Micali S. (1984), "Probabilistic encryption", *Journal of Computer and System Sciences* 28 (2): 270–29.
34. Han D., Hong J., Han J. W. and Kwon D. (2003), “Key recovery attacks on NTRU without ciphertext validation routine”. In *Proceeding of* *ACISP ’03, LNCS*, vol. 2727, Springer-Verlag, pp.274-284.
35. Hoffstein J., Pipher J., Silverman J.H. (1996), “NTRU: A new high speed public key”. *Preprint, presented at the rump session of Crypto 1996*.
36. Hoffstein J., Pipher J., Silverman J.H. (1998), “NTRU: A ring-based public key cryptosystem”, *Lecture Notes in Computer Science,* Volume 1423, pp 267-288, Springer Verlag.
37. Hoffstein J., Pipher J., Silverman J.H. (2008), *An Introduction to Mathematical Crytography*. Springer. ISBN: 978-0-387-77993-5.
38. Hoffstein J. and Silverman J.H. (2000), “Optimizations for NTRU”. In *Public-key Cryptography and Computational Number Theory*, DeGruyter.
39. Hoffstein J. and Silverman J.H. (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.
40. Hofheinz, Dennis; Kiltz, Eike (2007), "Secure Hybrid Encryption from Weakened Key Encapsulation" (PDF). *Advances in Cryptology -- CRYPTO 2007*. Springer. pp. 553–571.
41. Howgrave-Graham N., Silverman J.H., Whyte W., “NTRU Cryptosystems Technical Report #004, Version 2: A Meet-In-The-Middle Attack on an NTRU Private Key”.
42. IBM (1997), "A brief history of the data encryption standard". *ACM Press/Addison-Wesley Publishing Co*. New York, NY, USA. pp. 275–280.
43. IEEE (2000), *IEEE Std 1363.1 - Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices*.
44. Internet Engineering Task Force (IETF) (1998), *RFC 2440 - Open PGP Message Format*, November 1998.
45. Jaulmes E. and Joux A. (2000), “A Chosen Ciphertext Attack on NTRU”, In *Proceeding of CRYPTO ’00*, LNCS, vol. 1880, Springer-Verlag, pp. 20-35.
46. Jarvis K., Nevins M. (2013), “ETRU: NTRU over the Eisenstein integers”, *Designs, Codes and Cryptography*, Volume 74, Issue 1, Page 219-242, Springer.
47. Katz J., Lindell Y. (2007), *Introduction to Modern Cryptography: Principles and Protocols*, Chapman & Hall/CRC Cryptography and Network Security Series.
48. Koblitz, N. (1987). "Elliptic curve cryptosystems". *Mathematics of Computation*, 48 (177), pp. 203–209.
49. Lenstra A.K., Lenstra H.W., Lovász L. (1982), “Factoring polynomials with polynomial coefficients”, *Math. Annalen*, 261, pp. 515-534.
50. Lai X., Massey J. L. (1991), “A proposal for a new block encryption standard”, *Advances in Cryptology EUROCRYPT'90*, Aarhus, Denemark, LNCS 473, p. 389-404, Springer.
51. R. Lidl and H. Niederreiter (1983), *Finite Fields*, Addison-Wesley, Reading, Mass.
52. Hill L. S. (1929), “Cryptography in an Algebraic Alphabet”, *The American Mathematical Monthly,* Vol.36, June–July 1929, pp. 306-312.
53. Lyubashevsky V., Peikert C., Regev O. (2010), “On ideal lattices and learning with errors over rings”. *Gilbert H. (ed.) Advances in Cryptology (EUROCRYPT 2010), Lecture Notes in Computer Science*, vol. 6110, pp. 1-23. Springer, Berlin.
54. Malekian, Zakerolhosseini E. (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.
55. Matsumoto T. and IMAI H.(1988), “Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption”, *EUROCRYPT’88*, Springer Verlag, pp. 419–453.
56. McEliece R. J. (1978), "A public-key cryptosystem based on algebraic coding theory", *DSN Progress Report*, pp. 114-116.
57. Menezes A. J, Van Oorchot P. C. (1996), *Handbook of Applied Cryptography*, CRC Press.
58. Merkle R. and Hellman M. (1978), "Hiding information and signatures in trapdoor knapsacks", *IEEE Trans. Inform. Theory*, vol. IT-24, no. 5, pp.525 -530.
59. Miller, V. (1985), "Use of elliptic curves in cryptography", *CRYPTO. Lecture Notes in Computer Science,* 85, pp. 417–426.
60. Moon, Todd K. (2005), *Error Correction Coding*, Wiley-Interscience, a John Wiley & Sons, Inc., Publication.
61. Naccache D. and Stern J. (1998), "Proceedings of the 5th ACM Conference on Computer and Communications Security", *CCS '98*, ACM. pp. 59–66.
62. National Institute of Standards and Technology (NIST) (2001), *Advanced Encryption Standard (AES), Federal Information Processing Standard (FIPS) Publication 197*.
63. National Institute of Standards and Technology (NIST) (1977), *Data Encryption Standard (DES), Federal Information Processing Standard (FIPS) Publication 46*.
64. National Institute of Standards and Technology (NIST) (2001), *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A*.
65. Network Working Group of the IETF, (2006), *RFC 4251, The Secure Shell (SSH) Protocol Architecture*.
66. Okamoto, Tatsuaki; Uchiyama, Shigenori (1998). "A new public-key cryptosystem as secure as factoring". *Advances in Cryptology — EUROCRYPT'98*. Lecture Notes in Computer Science 1403. Springer. pp. 308–318.
67. Pan Y., Deng Y., Jiang Y., Tu Z. (2011), “A New Lattice-Based Public-Key Cryptosystem Mixed with a Knapsack”, *Lecture Notes in Computer Science,* Volume 7092, pp 126-137.
68. Pan Y., Deng Y. (2012), “A General NTRU-Like Framework for Constructing Lattice-Based Public-Key Cryptosystems”, *Lecture Notes in Computer Science,* Volume 7115, pp 109-120.
69. Patarin J. (1996), “Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms”, *Eurocrypt’96*, Springer Verlag, pp. 33–48.
70. Patsakis C., Kotzanikolaou P., Bouroche M. (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, 2015.
71. Peikert C. and Waters B. (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.
72. Peikert C. (2009), “Public-key cryptosystems from the worst-case shortest vector problem: extended abstract”, *Proceedings of the 41st annual ACM symposium on Theory of computing* (Bethesda, MD, USA: ACM, 2009), 333-342.
73. Perlner, R.A., Cooper, D.A. (2009), “Quantum resistant public key cryptography: a survey”, *Proc. of IDtrust*, pp. 85–93. ACM, New York.
74. Rabin, Michael (1979), “Digitalized Signatures and Public-Key Functions as Intractable as Factorization”, *MIT Laboratory for Computer Science*.
75. Regev O., “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.
76. Rivest R.L., Shamir A., Adleman L. (1978), “A method for obtaining digital signatures and public key cryptosystems”, *Communications of the ACM* 21, 120-126.
77. Shamir, Adi (1984), "A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem". *Information Theory, IEEE Transactions on* 30 (5): 699–704.
78. Shannon C.E. (1949), “Communication theory of secrecy systems”, *The Bell System Technical Journal*, Volume 28, Issue 4, pp. 656-715.
79. Wayner, Peter (24 December 1997), "British Document Outlines Early Encryption Discovery", *New York Times*.
80. Singh, Simon (1999), *The Code Book*, Doubleday, pp. 279–292.
81. Shoup V. (2001), A proposal for an ISO standard for public key encryption (version 2.1), <http://www.shoup.net/papers/iso-2_1.pdf>, ngày 5/11/2017.
82. Shoup V. (2004), “ISO 18033-2: An emerging standard for public-key encryption, http://shoup.net/iso/std6.pdf, ngày 6/11/2017.
83. Stehle, D., Steinfeld, R. (2011), “Making NTRU as secure as worst-case problems over ideal lattices”, *Paterson, K.G.(ed.) EUROCRYPT 2011*, LNCS, vol. 6632, pp. 27–47, Springer, Heidelberg.
84. Stinson, D., R. (2006), *Cryptography. Theory and Practice (Third ed.)*, Chapman & Hall/CRC. ISBN 1584885084.
85. Vats N. (2008), “Algebraic Cryptanalysis of CTRU Cryptosystem”, *In: Hu X., Wang J. (eds) Computing and Combinatorics. COCOON 2008. Lecture Notes in Computer Science*, vol 5092, Springer, Berlin, Heidelberg.
86. Yu Y., Xu G., Wang X. (2017), “Provably Secure NTRU Instances over Prime Cyclotomic Rings”, In: *Fehr S. (eds) Public-Key Cryptography – PKC 2017*. *Lecture Notes in Computer Science*, vol 10174. Springer, Berlin, Heidelberg.