HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PHẠM LONG ÂU

MÃ MẠNG TRÊN MỘT SỐ CẤU TRÚC ĐẠI SỐ

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI - 2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

PHẠM LONG ÂU

MÃ MẠNG TRÊN MỘT SỐ CẤU TRÚC ĐẠI SỐ

Chuyên ngành: **Kỹ thuật Điện tử**

Mã số: **9.52.02.03**

LUẬN ÁN TIẾN SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. TS. Ngô Đức Thiện

2. TS. Nguyễn Lê Cường

HÀ NỘI - 2022

LỜI CAM ĐOAN

Nghiên cứu sinh xin cam đoan nội dung trong luận án tiến sĩ này là công trình nghiên cứu khoa học của nghiên cứu sinh và tập thể nghiên cứu, không sao chép nguyên bản từ công trình nghiên cứu hay luận án đã công bố. Tất cả những tham khảo và kế thừa đều được trích dẫn và tham chiếu đầy đủ.

Tác giả Luận án

NCS. Phạm Long Âu

LỜI CẢM ƠN

Sau thời gian học tập và nghiên cứu tại Học viện Công nghệ Bưu chính Viễn thông, nghiên cứu sinh xin trân trọng cảm ơn Ban giám đốc học viện và các thầy cô giáo Học viện Công nghệ Bưu chính Viễn thông; Khoa Quốc tế và Đào tạo sau đại học đã hỗ trợ, giúp đỡ nhiệt tình cho nghiên cứu sinh trong suốt quá trình học tập và thực hiện luận án.

Bằng sự biết ơn và kính trọng, nghiên cứu sinh xin gửi lời cảm ơn chân thành đến TS. Ngô Đức Thiện và TS. Nguyễn Lê Cường, người đã trực tiếp hướng dẫn trong suốt quá trình thực hiện luận án, và đặc biệt là thầy GS.TS. Nguyễn Bình là người đã định hướng, góp ý cho NCS hoàn thành được luận án.

Cuối cùng nghiên cứu sinh xin gửi lời cảm ơn tới gia đình, các đồng chí lãnh đạo của cơ quan đang công tác và bạn bè đã luôn động viên, khuyến khích, tạo điều kiện giúp đỡ nghiên cứu sinh trong suốt thời gian học tập, nghiên cứu và thực hiện luận án này.

Xin chân thành cảm ơn!

Tác giả Luận án

NCS. Phạm Long Âu

MỤC LỤC

DANH MỤC KÝ HIỆU TOÁN HỌC

Ký hiệu	Nghĩa tiếng Việt
$\equiv$	Đồng dư
$\deg(.)$	Bậc của đa thức
$ord\ (.)$	Cấp của một phần tử
$\varphi(.)$	Hàm Phi-Ơle
$\mathbb{Z}$	Tập số nguyên
$\mathbb{Z}_n$	Các số nguyên modulo n
O(.)	Độ phức tạp của thuật toán
G	Nhóm (Group)
R	Vành (Ring)
GF	Trường Galois
$\mathrm{Z}_2[x]/(x^n+1)$	Vành đa thức theo modulo x^n+1

DANH MỤC CÁC TỪ VIẾT TẮT

Ký hiệu	Nghĩa tiếng Anh	Nghĩa tiếng Việt
BCNN (LCM)	Least Common Multiple	Bội chung nhỏ nhất
CC	Channel Coding	Mã hóa kênh
CR	Cooperative radio	Vô tuyến cộng tác
DVR	Discrete Valuation Ring - DVR	Vành giá trị rời rạc
DLP	Discrete Logarithm Problem	Bài toán logarit rời rạc
EC	Elliptic Curve	Đường cong elliptic
ECC	Elliptic Curve Cryptography	Mật mã đường cong elliptic
IP	Internet Protocol	Giao thức Internet
LTE	Long Term Evolution	Tiến hóa dài hạn
Maxflow	Maximum flow	Lưu lượng tối đa
Min-cut	Minimun cut	Dòng cắt tối thiểu
NC	Network Coding	Mã hóa mạng
NCS		Nghiên cứu sinh
NEC	Network Error Correction Coding	Mã hóa sửa lỗi mạng
P2P	Point to Point	Mạng truyền thông điểm - điểm
RANC	Random Affine Network Coding	Mã mạng Affine ngẫu nhiên
RS	Reed - Solomon	Các mã Reed - Solomon
SC	Source Coding	Mã hóa nguồn
RAID	Redundant Array of Inexpensive Disks	Hệ thống đĩa dự phòng
ƯCLN (GCD)	Greatest Common Divisor	Ước chung lớn nhất

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG

MỞ ĐẦU

1. LÝ DO CHỌN ĐỀ TÀI

Các mạng máy tính được thiết kế để truyền tải thông tin từ nút nguồn đến các nút đích. Theo cách truyền thống dữ liệu được truyền theo các *tuyến* theo kiểu unicast (điểm đến điểm) hoặc *dạng cây* theo kiểu multicast (điểm - đa điểm). Khi dữ liệu được định tuyến qua các tuyến unicast, mỗi nút trung gian sẽ chuyển tiếp các gói dữ liệu nhận được từ đầu vào đến đầu ra của nút đó. Trong kết nối multicast qua mạng hình cây, các nút trung gian có thể sao chép các gói dữ liệu và chuyển tiếp đến nhiều đích khác nhau. Đây là cách thực hiện dữ liệu trên mạng theo kiểu truyền thống, không cần xử lý dữ liệu tại các nút trung gian trừ khi cần nhân bản.

Khái niệm cơ bản "*mã mạng"* (Network coding) lần đầu tiên được đưa ra trong mạng thông tin vệ tinh công bố trong bài báo “Distributed source coding for satellite communications” [16] của các tác giả R. W. Yeung and Z. Zhang, và sau đó khái niệm *mã mạng* đã được phát triển đầy đủ trong công bố “Network information flow” [17] của các tác giả R. Ahlswede, N. Cai, S.Y. R. Li, and R. W. Yeung.

Mã mạng là một kỹ thuật mạng, trong đó các gói dữ liệu truyền trong mạng được mã hoá và giải mã tại các nút mạng để tăng lưu lượng mạng, giảm độ trễ và làm cho mạng ổn định hơn. Kỹ thuật mã mạng sử dụng phép toán học nào đó tác động lên các gói dữ liệu với mục đích làm giảm thiểu số phiên truyền dẫn giữa nút nguồn và nút đích, tuy nhiên sẽ đòi hỏi các nút trung gian vá các nút đầu cuối phải xử lý nhiều hơn.

Từ sự đóng góp tiên phong của Ahlswede và đồng nghiệp, mã mạng đã được nghiên cứu và phát triển ứng dụng trong nhiều ứng dụng trong kỹ thuật mạng và truyền thông [24]. Có thể kể đến như: thông tin vô tuyến [25, 26]; truyền thông hợp tác [27]; LTE dựa trên truyền thông hợp tác [28]; truyền thông multicast [29, 30, 31]; truyền thông unicast [32]; truyền thông quảng bá broadcast [33]; mạng phân phối nội dung [34]; mạng cảm biến không dây [35]; mạng P2P [36],...

Một số lợi ích của mã mạng có thể kể đến đó là [20]: trước hết, mã mạng làm tăng thông lượng (throughput) của mạng. Thứ hai, với mã mạng tuyến tính, độ phức tạp tính toán cũng giảm (polynomial time thay vì NP-complete). Thứ ba, mã mạng có tính bền vững (robustness), khi tô-pô mạng bị thay đổi hay khi một số liên kết mạng không hoạt động, do mỗi gói tin mã hóa thì ta có thể thu lại thông tin đã được gửi đi. Thứ tư, mã mạng làm tăng tính bảo mật thông tin, ít nhất bởi chính thông tin truyền đi trên liên kết là tổ hợp của nhiều thông tin. Đối với mạng không dây, do tính chất phát quảng bá của mạng và tô-pô mạng phụ thuộc vào công suất phát…

Với sự xuất hiện của mã mạng và các nhận định về các tiềm năng của nó, hiện nay có rất nhiều nhà nghiên cứu trên thế giới quan tâm đến mã mạng. Hội thảo đầu tiên trên thế giới chuyên về mã mạng đã được tổ chức năm 2005 - First Network Coding Workshop (NetCod 2005) và từ sau đó chuyển thành hội nghị thường niên của hiệp hội IEEE - International Symposium on Network Coding.

Bởi vì tính tổng quát và tiềm năng ứng dụng, mã mạng đang là mối quan tâm rất lớn trong lĩnh vực lý thuyết thông tin và mã hóa, chuyển mạch, thông tin vô tuyến, lý thuyết độ phức tạp, mật mã, lý thuyết ma trận… Lý thuyết về mã mạng được phát triển theo nhiều hướng khác nhau và các ứng dụng của mã mạng ngày càng được ứng dụng nhiều trong thực tế.

Trên thế giới, các nhà nghiên cứu về mã mạng được bắt đầu từ công trình quan trọng của Ahlswede và đồng nghiệp năm 2000 [17] đã thu hút được sự quan tâm lớn trong cộng đồng nghiên cứu. Như đã nói trên, công trình này chứng minh rằng dung năng của các mạng multicast (là số gói tin tối đa được truyền từ một nguồn tới một tập các đích trên thời gian) có thể đạt được bằng cách mã hóa phía trong mạng: cho phép trộn dữ liệu tại các nút mạng trung gian của mạng. Năm 2003 Yeung và Cai chứng minh được rằng đối với các mạng multicast chỉ cần sử dụng mã tuyến tính là đủ để đạt được dung năng phương pháp này được gọi là “linear network coding”. Cùng năm này, Koetter và Medard mở rộng kết quả này cho mạng bất kỳ và giới thiệu một khuôn khổ đại số rất mạnh cho mã mạng. Phương pháp này thiết lập một kết nối hữu ích giữa một bài toán mã mạng với nghiệm của một hệ phương trình đa thức [23]. Song song với các phát triển lý thuyết này của mã mạng; Chou, Wu và

Jain trong năm 2003 đề xuất một phương pháp thực tiễn để thực hiện mã mạng mà không cần thông tin tập trung của tô-pô mạng hay là các hàm mã hóa/hàm giải mã; phương pháp này được gọi là "Practical network coding" [22]. Ý tưởng chính họ đưa ra để làm được điều đó là lồng ghép một véc-tơ mã hóa toàn cục (global encoding vector) trong mỗi một gói tin. Như vậy véc-tơ mã hóa này sẽ được lấy ra từ những gói tin nhận được và dùng chính nó để giải mã các gói tin này. Phương pháp này cho phép áp dụng mã mạng trong mạng phân tán (distributed). Năm 2006, T. Ho và đồng nghiệp kết hợp kết quả lý thuyết về mã tuyến tính [28] và mô hình thực tiễn [27] trên để đề xuất một phương pháp phân tán và ngẫu nhiên dùng thiết kế mã mạng, phương pháp này được gọi là "random linear network coding". Mặc dù là ngẫu nhiên, T. Ho và đồng nghiệp chứng minh được rằng dung năng của mạng có thể đạt được với sác xuất tiến đến l với tốc độ lũy thừa theo độ dài của mã.

Sau năm 2008, một lĩnh vực nghiên cứu lý thuyết tổng quát về mã mạng đã được đưa ra. Công trình đầu tiên theo hướng này là "Ring-theoretic foundation of convolutional network coding" (Lý thuyết vành của mã mạng chập) [37] đã tận dụng nhiều kết quả đã được trình bày trước đó. Họ đã chứng minh rằng lý thuyết mã mạng dựa trên trường cổ điển của toán học và do đó mã mạng chập là phiên bản của một khuôn khổ mới dựa trên đại số giao hoán. Đặc biệt, phần mở rộng lý thuyết này là khả thi bằng cách coi thông tin thuộc về một vành giá trị rời rạc (Discrete Valuation Ring - DVR) và không phải từ một trường.

Một sự phát triển khác của các nguyên tắc cơ bản về lý thuyết mã mạng trong trường hợp các mạng tuần hoàn có hướng đơn nguồn cũng được trình bày trong bài báo "A unified framework for linear network codes" [38]. Các định nghĩa cổ điển về phân tán tuyến tính, phát sóng tuyến tính và phát đa hướng tuyến tính được đưa ra trước đây sử dụng kích thước của các nhân mã hóa toàn cầu được liên kết với các nguồn đến để mô tả các loại mã mạng tuyến tính khác nhau. Mặt khác, cách tiếp cận thống nhất mới đã tận dụng lợi thế từ khái niệm về tập độc lập thường xuyên để mô tả với sự gắn kết sự độc lập tuyến tính giữa tập hợp các cạnh. Tiếp theo, các nhà nghiên cứu cải thiện kết quả trước đây bằng cách áp dụng các khái niệm mới để

chứng minh một số điều kiện và mối quan hệ; với khuôn khổ lý thuyết mới này các tác giả đã chứng minh định lý được đưa ra bằng các phương pháp đơn giản hơn.

Bài báo "Multicasting algorithms for deterministic networks" [31] đã cung cấp một thuật toán thời gian đa thức để thiết kế các ma trận nhị phân cho mã mạng đa hướng xác định và nó phát triển khuôn khổ lý thuyết đại số được xác định trong các nghiên cứu trước bằng cách xem xét các phép toán trên ma trận. Sau đó, bài báo "Vector network coding algorithms" [40] mở rộng kết quả bài báo trên và các tác giả cũng đã mở đường cho việc thực hiện một thuật toán thời gian đa thức để thiết kế mã mạng vectơ trong một kịch bản multicast; thuật toán mới đã thay đổi vấn đề tìm thấy giá trị L nhỏ nhất ($L \times L$ là kích thước của ma trận mã hóa) thành vấn đề tìm kiếm các yếu tố gần giống nhau của đa thức đại số. Kết quả mới này đề xuất một thuật toán trong trường hợp mã mạng vô hướng hoạt động trong thời gian đa thức.

Năm 2009, bài báo "Mã mạng đa điểm tuyến tính nhị phân trên các mạng không tuần hoàn: các nguyên tắc và các ứng dụng trong các mạng truyền thông không dây - Binary linear multicast network coding on acyclic networks: principles and applications in wireless communication networks" [30] đã phát triển một mã mạng multicast tuyến tính nhị phân cho các trường hợp mạng không tuần hoàn. Bằng cách thay đổi kích thước của trường hữu hạn và bằng cách mở rộng chiều đa điểm, các tác giả đã làm giảm độ phức tạp của mã mạng tại các nút trung gian và đạt được chi phí thực hiện thấp hơn tại các nút trong mạng. Đặc biệt, kết quả này rất hữu ích cho việc thiết kế cho các mạng không dây. Một năm sau đó, các nhà nghiên cứu cũng trình bày hai phương pháp để xây dựng hệ thống cộng tác bằng cách sử dụng mã mạng không xác định: hai chiến lược được đề xuất trong trường hợp truyền thông đường lên, đường xuống và được coi là cộng tác một phần đơn nguồn và cộng tác nhiều người dùng.

Năm 2011, bài báo "Beyond the cut-set bound: Uncertainty computations in network coding with correlated sources" [47] cho thấy một kỹ thuật dựa trên khái niệm về vùng không chắc chắn của các vectơ biểu diễn cho các biến ngẫu nhiên để

tính toán cho vấn đề truyền thông tin nguồn được tương quan. Cùng năm đó, bài báo "Coding for a network coded fountain" [42] đã định nghĩa một loại mã gọi là BATched Sparse (BATS) - đại diện cho phần mở rộng của mã LT. Ý tưởng chính là sử dụng các phiên, tập các gói chỉ kết hợp các gói tin từ cùng một tập hợp con; hơn nữa, nó đã được chứng minh rằng các phép biến đổi tuyến tính được thực hiện bởi các phiên có thể được phân tích thông qua kênh toán tử tuyến tính được xác định. Mã LT là một họ của các mã nguồn được giới thiệu lần đầu tiên vào năm 2002. Vào năm 2010, các nhà nghiên cứu đã sử dụng mã LT để giảm độ phức tạp của việc mã mạng trong một hệ thống mạng quảng bá thông tin quy mô lớn. Mục đích của mã BATS là giảm độ phức tạp của mã mạng tại các nút trung gian để truyền một tệp lớn thông qua một chương trình mã hóa đầu cuối.

Về mã chập: một thuật toán cho các mã mạng chập cơ bản với thời gian đa thức, được đề xuất vào năm 2009 trong bài báo "Thuật toán xây dựng thời gian đa thức của BCNC để mã mạng trong các mạng tuần hoàn - Polynomial time construction algorithm of BCNC for network coding in cyclic networks" [43]. Các tác giả đã phát triển thuật toán được đề xuất ở bài báo trên và hoàn thành một thuật toán phiên bản mới. Sau đó trong bài báo "Thuật toán xây dựng thống nhất của mã mạng trong các mạng tuần hoàn - Unified construction algorithm of network coding in cyclic networks" [44] đã xem xét các khái niệm về nhân mã hóa toàn cầu và cục bộ trong trường hợp mạng tuần hoàn: nó phân tích các điều kiện để xác định ma trận nhân mã hóa toàn cầu của mã mạng chập trong một kịch bản tuần hoàn. Tiếp theo, bài báo "Localized dimension growth in random network coding: A convolutional approach" [45] đã thiết kế một mã mạng chập ngẫu nhiên hoạt động thích nghi trong một vùng nhỏ và thích nghi với cấu trúc mạng kết hợp; các tác giả đã cho một ví dụ về phương pháp của họ trong các mạng kết hợp. Ngoài ra các nhà nghiên cứu đã mô tả một lớp mã mạng chập mới cho các mạng đa hướng, được gọi là không thay đổi trễ: tên này là do thực tế là mã không phụ thuộc vào độ trễ của mạng. Bài báo "Construction of convolutional network coding for cyclic multicast networks" [50] đã đề xuất một thuật toán đa thức xác suất cho các mạng tuần hoàn

định hướng bằng cách tính toán các nhân được mã hóa toàn cầu bằng cách sử dụng công thức Mason.

Về mã sửa lỗi mạng: năm 2011 bài báo "Phân tích xác suất điểm kỳ dị cho mã mạng tuyến tính ngẫu nhiên phân tán - Singularity probability analysis for sparse random linear network coding" [41] đã thực hiện phân tích xác suất điểm kỳ dị của ma trận chuyển vị ngẫu nhiên trong ngữ cảnh mã mạng không mạch lạc bằng cách sử dụng các mã kích thước không đổi. Họ tìm thấy một mối quan hệ tương ứng giữa sự thiếu hụt mức của không gian con nhận được và mẫu số không của ma trận chuyển vị. Họ cũng bắt nguồn từ giới hạn trên và giới hạn dưới về xác suất bị giải mã sai. Sau đó, bài báo "Network localized error correction: For non-coherent coding" [51] phát triển các mã sửa lỗi cổ điển trong mã hóa không gian con. Đặc biệt, tác giả đã chứng minh phần xuôi và phần ngược của định lý mã hóa để cung cấp một giới hạn trên cho khả năng mã mạng ngẫu nhiên. Bằng cách xem xét các khái niệm lý thuyết về nhân mã hóa toàn cầu được chứng minh trong các nghiên cứu trước cho thấy rằng mã MDS có thể đạt được giới hạn Singleton và yêu cầu kích thước trường nhỏ hơn kết quả đã biết. Các tác giả đã mô tả một thuật toán thời gian đa thức để triển khai các mã MDS trong các mạng tuần hoàn định hướng. Vì vậy, bài báo "Universal network error correction MDS codes" [46] đã nâng cao kết quả trong các nghiên cứu trước để giảm sự phức tạp của hệ thống và lượng không gian lưu trữ cần thiết trong các nút không phải nút nguồn của mạng.

Bài báo "Convolutional codes for network-error correction" [52] đề xuất sử dụng các mã chập cho NEC bằng cách trình bày một số ưu điểm về kích thước trường và độ phức tạp giải mã. Các tác giả cũng nghiên cứu mã NEC bằng cách đưa ra một giới hạn trên, một ràng buộc về xác suất lỗi bit BER và cách thực hiện giải mã. Bài báo "Network-error correcting codes using small fields" [53] đã mở rộng nghiên cứu trước đó bằng cách áp dụng các nghiên cứu trước đó vào kịch bản NEC; hơn nữa, các tác giả đề xuất một thuật toán khác để tính toán đa thức có nguyên tố cùng nhau và có độ phức tạp nhỏ hơn so với nghiên cứu trước đó...

Một số nghiên cứu về mã mạng ở trong nước:

Đối với Việt Nam: mặc dù kỹ thuật mã mạng được thế giới quan tâm từ lâu với nhiều hội nghị thường niên, tuy nhiên chủ đề này vẫn ít được sự quan tâm của các nhà nghiên cứu trong nước. Các công trình công bố không nhiều, có thể kể đến vài công bố như sau: "Network Coding" khóa luận tốt nghiệp hệ chất lượng cao, của tác giả Nguyễn Thị Thùy Dương [7]; "Kết hợp mã hóa mạng lớp vật lý và lựa chọn nút chuyển tiếp cho kênh vô tuyến chuyển tiếp hai chiều" của Vũ Đức Hiệp, Trần Xuân Nam, [8]; "Network coding for LTE-based cooperative communications" của Lưu Cao Cường và các đồng nghiệp [33]...

Cho đến nay, trong kỹ thuật mã mạng phép toán học được sử dụng để tác động lên các gói dữ liệu thường là phép XOR các chuỗi bit nhị phân (vector nhị nhân) [49]. Ít có các nghiên cứu các cách thức thực hiện khác.

Các cấu trúc đại số như vành số, trường số, vành đa thức,... được sử dụng nhiều trong việc xây dựng các mã sửa sai hay mã bảo mật [1, 9, 10, 59, 61], bởi tính tường minh của các cấu trúc và dễ dàng triển khai từ lý thuyết đại số sang các mạch điện phần cứng. Từ các nhận định này, NCS đã đi đến quyết định lựa chọn hướng nghiên cứu là áp dụng một số cấu trúc đại số (nhóm, vành, trường) vào việc thực hiện mã mạng, với tên đề tài luận án là "Mã mạng trên một số cấu trúc đại số".

Trên cơ sở các nghiên cứu đề xuất xây dựng mã mạng trên một số cấu trúc đại số trong chương 2 của luận án, NCS đề xuất thực hiện một mô hình mã mạng an toàn có bảo mật, kết quả thể hiện trong chương 3 của luận án.

2. MỤC TIÊU NGHIÊN CỨU

- Nghiên cứu đề xuất xây dựng mã mạng trên cấu trúc nhóm cộng và/hoặc nhóm nhân của vành số, trường số, vành đa thức, trường đa thức.

- Nghiên cứu đề xuất xây dựng mã mạng dựa trên nhóm cộng các điểm của đường cong elliptic.

- Nghiên cứu đề xuất mô hình thực hiện mã mạng an toàn, dựa trên hai hệ mật khóa công khai.

3. ĐỐI TƯỢNG VÀ PHẠM VI NGHIÊN CỨU

Đối tượng nghiên cứu: Kỹ thuật mã mạng trong truyền thông (Networking).

Phạm vi nghiên cứu: Thực hiện mã mạng trên một số cấu trúc đại số và mã mạng an toàn nhằm nâng cao hiệu quả và bảo mật truyền tin.

4. PHƯƠNG PHÁP NGHIÊN CỨU

Các phương pháp nghiên cứu được sử dụng trong Luận án bao gồm:

- Phân tích, tổng hợp, khái quát hóa và hệ thống hóa các tài liệu khoa học đã công bố trên thế giới và trong nước, kết hợp với việc tự nghiên cứu;

- Sử dụng ngôn ngữ lập trình và công cụ để thử nghiệm các nghiên cứu, đề xuất.

5. Ý NGHĨA KHOA HỌC VÀ THỰC TIỄN

Những kết quả trong luận án này là một đóng góp nhỏ bé vào việc phát triển kỹ thuật mã mạng. Các nghiên cứu trong luận án đưa ra một số cách thức khác để xây dựng mã mạng và làm cơ sở để có thể tiếp tục nghiên cứu thực hiện mã mạng có khả năng bảo mật.

6. CẤU TRÚC CỦA LUẬN ÁN

Ngoài phần mở đầu, danh mục các hình vẽ, đồ thị, danh mục các ký hiệu, các chữ viết tắt, kết luận và kiến nghị, tài liệu tham khảo và phụ lục, nội dung chính của Luận án gồm 03 chương, cụ thể như sau:

Chương 1: Tổng quan về mã mạng

Chương 2: Đề xuất xây dựng mã mạng trên một số cấu trúc đại số

Chương 3: Mô hình mã mạng an toàn

CHƯƠNG 1. TỔNG QUAN VỀ MÃ MẠNG

Chương 1 là các kiến thức lý thuyết, được nghiên cứu sinh tập hợp làm kiến thức nền tảng phục vụ cho các nghiên cứu về sau trong luận án. Các nội dung đề cập tại chương 1 gồm: Tổng quan chung về lý thuyết thông tin và mã hóa; Tổng quan về mã mạng: Định nghĩa, mô hình, cách thực hiện và một số lợi ích của mã mạng.

1.1. TỔNG QUAN CHUNG VỀ LÝ THUYẾT THÔNG TIN VÀ MÃ HÓA

1.1.1. Lý thuyết thông tin

Người đặt viên gạch đầu tiên để xây dựng lý thuyết thông tin là Hartley R.V.L. Năm 1928, ông đã đưa ra số đo lượng thông tin là một khái niệm trung tâm của lý thuyết thông tin. Dựa vào khái niệm này, ta có thể so sánh định lượng các hệ truyền tin với nhau. Năm 1933, V.A Kachenhicov chứng minh một loạt những luận điểm quan trọng của lý thuyết thông tin trong bài báo "Về khả năng thông qua của không trung và dây dẫn trong hệ thống liên lạc điện". Năm 1935, D.V Ageev đưa ra công trình "Lý thuyết tách tuyến tính", trong đó ông phát biểu những nguyên tắc cơ bản về lý thuyết tách các tín hiệu. Năm 1946, V.A Kachenhicov thông báo công trình "Lý thuyết thế chống nhiễu' đánh dấu một bước phát triển rất quan trọng của lý thuyết thông tin.

Trong hai năm 1948 - 1949, Shanon C.E công bố một loạt các công trình vĩ đại, đưa sự phát triển của lý thuyết thông tin lên một bước tiến mới chưa từng có. Trong các công trình này, nhờ việc đưa vào khái niệm lượng thông tin và tính đến cấu trúc thống kê của tin, ông đã chứng minh một loạt định lý về khả năng thông qua của kênh truyền tin khi có nhiễu và các định lý mã hoá. Những công trình này là nền tảng vững chắc của lý thuyết thông tin.

Ngày nay, lý thuyết thông tin phát triển theo hai hướng chủ yếu sau:

Lý thuyết thông tin toán học: xây dựng những luận điểm thuần tuý toán học và những cơ sở toán học chặt chẽ của lý thuyết thông tin. Cống hiến chủ yếu trong lĩnh vực này thuộc về các nhà bác học lỗi lạc như: N.Wiener, A. Feinstain, C.E Shanon, A.N. Kanmôgorov, A.JA Khintrin.

Lý thuyết thông tin ứng dụng (lý thuyết truyền tin): chuyên nghiên cứu các bài toán thực tế quan trọng do kỹ thuật liên lạc đặt ra có liên quan đến vấn đề chống nhiễu và nâng cao độ tin cậy của việc truyền tin. Các bác học C.E Shanon, S.O RiCe, D. Midleton, W. Peterson, A.A Khakevich, V. Kachenhicov đã có những công trình quý báu trong lĩnh vực này.

- Thông tin: Thông tin là những tính chất xác định của vật chất mà con người (hoặc hệ thống kỹ thuật) nhận được từ thế giới vật chất bên ngoài hoặc từ những quá trình xảy ra trong bản thân nó [10].

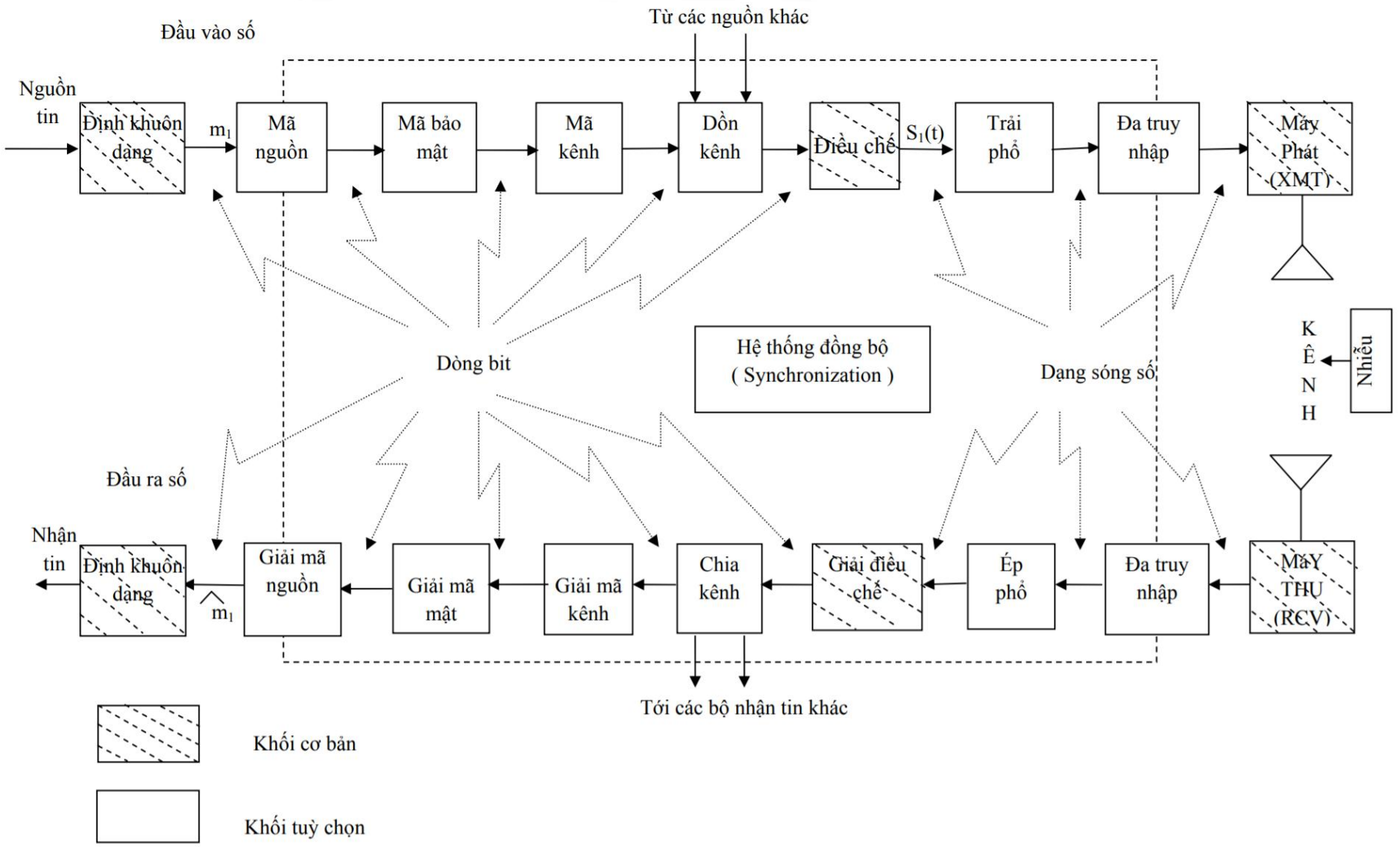
Với định nghĩa này, mọi ngành khoa học là khám phá ra các cấu trúc thông qua việc thu thập, chế biến, xử lý thông tin. Ở đây "thông tin" là một danh từ chứ không phải là động từ để chỉ một hành vi tác động giữa hai đối tượng (người, máy) liên lạc với nhau. Theo quan điểm triết học, thông tin là một quảng tính của thế giới vật chất (tương tự như năng lượng, khối lượng). Thông tin không được tạo ra mà chỉ được sử dụng bởi hệ thụ cảm. Thông tin tồn tại một cách khách quan, không phụ thuộc vào hệ thụ cảm. Trong nghĩa khái quát nhất, thông tin là sự đa dạng. Sự đa dạng ở đây có thể hiểu theo nhiều nghĩa khác nhau: Tính ngẫu nhiên, trình độ tổ chức...

- Tin: Tin là dạng vật chất cụ thể để biểu diễn hoặc thể hiện thông tin. Tin có hai dạng: tin rời rạc và tin liên tục. Ví dụ: Tấm ảnh, bản nhạc, bảng số liệu, bài nói... là các tin.

- Tín hiệu: Tín hiệu là các đại lượng vật lý biến thiên, phản ánh tin cần truyền.

- Nguồn tin: là nơi sản sinh ra tin. Nếu tập tin là hữu hạn thì nguồn sinh ra nó được gọi là nguồn rời rạc. Nếu tập tin là vô hạn thì nguồn sinh ra nó được gọi là nguồn liên tục. Nguồn tin có hai tính chất: Tính thống kê và tính hàm ý. Với nguồn rời rạc, tính thống kê biểu hiện ở chỗ xác suất xuất hiện các tin là khác nhau. Tính hàm ý biểu hiện ở chỗ xác suất xuất hiện của một tin nào đó sau một dãy tin khác nhau nào đó là khác nhau.

- Máy phát: là thiết bị biến đổi tập tin thành tập tín hiệu tương ứng. Phép biến đổi này phải là đơn trị hai chiều (thì bên thu mới có thể "sao lại" được đúng tin gửi đi). Trong trường hợp tổng quát, máy phát gồm hai khối chính.



Hình 1.1. Sơ đồ khối hệ thống truyền tin số

Sơ đồ khối của hệ thống truyền tin số:

- Thiết bị mã hoá: làm ứng mỗi tin với một tổ hợp các ký hiệu đã chọn nhằm tăng mật độ, tăng khả năng chống nhiễu, tăng tốc độ truyền tin.

- Khối điều chế: là thiết bị biến tập tin (đã hoặc không mã hoá) thành các tín hiệu để bức xạ vào không gian dưới dạng sóng điện từ cao tần. Về nguyên tắc, bất kỳ một máy phát nào cũng có khối này.

- Đường truyền tin: là môi trường vật lý, trong đó tín hiệu truyền đi từ máy phát sang máy thu. Trên đường truyền có những tác động làm mất năng lượng, làm mất thông tin của tín hiệu.

- Máy thu: là thiết bị lập lại (sao lại) thông tin từ tín hiệu nhận được. Máy thu thực hiện phép biến đổi ngược lại với phép biến đổi ở máy phát, biến tập tín hiệu thu được thành tập tin tương ứng. Máy thu gồm hai khối: Giải điều chế: biến đổi tín hiệu nhận được thành tin đã mã hoá; Giải mã: biến đổi các tin đã mã hoá thành các tin tương ứng ban đầu (các tin của nguồn gửi đi).

- Nhận tin (có ba chức năng): ghi giữ tin (ví dụ bộ nhớ của máy tính, băng ghi âm, ghi hình...); biểu thị tin: làm cho các giác quan của con người hoặc các bộ cảm biến của máy thụ cảm được để xử lý tin (ví dụ băng âm thanh, chữ số, hình ảnh...); xử lý tin: biến đổi tin để đưa nó về dạng dễ sử dụng. Chức năng này có thể thực hiện bằng con người hoặc bằng máy.

- Kênh truyền tin: là tập hợp các thiết bị kỹ thuật phục vụ cho việc truyền tin từ nguồn đến nơi nhận tin.

- Nhiễu: là mọi yếu tố ngẫu nhiên có ảnh hưởng xấu đến việc thu tin. Những yếu tố này tác động xấu đến tin truyền đi từ bên phát đến bên thu.

1.1.2. Mã hóa thông tin

Việc truyền thông tin qua mạng được hiểu là một sự trao đổi dữ liệu, mà không có khả năng kết hợp hoặc trộn lẫn những dữ liệu đã được gửi. Vào năm 2000, bài báo “Network information flow ” [17] của R. Ahlswede, Ning Cai, S.-R. Li, và R. W. Yeung đã thay đổi quan điểm này bằng cách giới thiệu khái niệm luồng thông tin (information flow) để chứng minh rằng sự kết hợp dữ liệu có thể làm tăng

dung lượng vượt quá giới hạn của một mạng. Phần mở rộng này chứng minh cho sự ra đời của một lĩnh vực nghiên cứu mới đầy hứa hẹn đó là mã mạng (Network Coding). Trước đó, các hoạt động mã hóa của lý thuyết thông tin chỉ được sử dụng trong: mã hóa nguồn (Source Coding) nêu cách nén thông tin tại nguồn để tăng hiệu quả trong truyền dẫn và mã hóa kênh (Channel Coding) thể hiện hoạt động chèn các bit dư thừa trong chuỗi thông tin để làm nó tăng khả năng chống nhiễu và sửa sai trước khi truyền trên kênh truyền.

Mục tiêu của mã hóa nguồn (còn được gọi là nén dữ liệu) là thay thế cho thông tin được tạo ra từ một nguồn thông tin một cách hiệu quả nhất. Kết quả của mã hóa nguồn là các bit độc lập hay là một chuỗi các bit độc lập mỗi bit có thể bằng 0 hoặc 1. Nếu mã hóa nguồn được thực hiện tốt thì sẽ có được số lượng bit nhỏ nhất có thể để biểu diễn nguồn thông tin. Sau đó, chuỗi bit từ mã hóa nguồn cần được truyền từ một điểm này sang điểm khác thông qua một kênh truyền có nhiễu.

Để đạt được thông tin liên lạc tin cậy, mã hóa kênh được áp dụng cho chuỗi bit của mã hóa nguồn sinh ta. Mục tiêu của mã hóa kênh là ở phía máy thu có thể nhận được chuỗi bit và khôi phục chuỗi bit một cách chính xác. Việc mã hóa kênh tương đương với việc chống nhiễu, tức là truyền thông tin trên một kênh có nhiễu như việc truyền thông tin trên một kênh không nhiễu. Hơn nữa, khi chuỗi bit đủ dài, mã hóa nguồn và mã hóa kênh có thể được thực hiện riêng mà vẫn đạt được tính tối ưu.

Lý tưởng nhất, mã hóa nguồn sẽ chuyển đổi tín hiệu ngẫu nhiên được tạo ra bởi nguồn thông tin thành một chuỗi các bit độc lập mà không thể nén thêm được nữa. Đối với mã hóa kênh mục đích là để ngăn chặn chuỗi bit này bị thay đổi bởi nhiễu trên kênh truyền. Điều này được thực hiện mà không cần phải thực hiện bất kỳ tham chiếu hay đồng bộ đến nguồn phát tín hiệu mà chuỗi bit đại diện cho. Do đó, các bit độc lập thường được coi là "information atoms" với ý nghĩa là các yếu tố cơ bản nhất của thông tin.

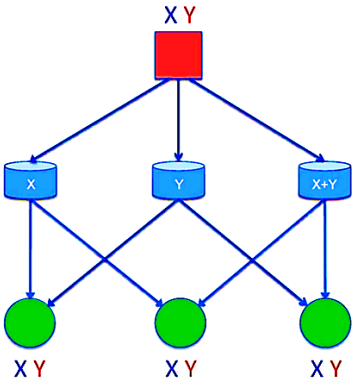
Như vậy, với mục đích truyền thông dữ liệu khi không có ảnh hưởng bởi nhiễu chúng ta chỉ cần quan tâm đến việc thông tin được thể hiện bởi các bit độc lập như

một hàng hóa. Đây là nguyên tắc thiết kế cơ bản cho các mạng máy tính, nơi mà một mạng có nhiễu được chuyển đổi thành một mạng không có nhiễu đầu tiên bằng mã hóa kênh và các bit thông tin được định tuyến thông qua mạng không nhiễu này như một hàng hóa.

1.1.2.1. Hệ thống lưu trữ dữ liệu phân tán

Một thiết kế chung cho các hệ thống lưu trữ dữ liệu số ngày nay là hệ thống lưu trữ có khả năng lưu trữ nhiều dữ liệu và có khả năng khôi phục dữ liệu (Redundant Arrays of Inexpensive Disks - RAID). Một hệ thống như vậy, bao gồm nhiều ổ cứng và cung cấp dự phòng bằng cách sao chép dữ liệu qua các ổ cứng khác nhau. RAID 4/5 có thể được mô hình hóa thành một mạng như trong Hình 1.2. Trong mạng này, chia tập hợp các nút thành ba lớp. Lớp trên đỉnh được gọi là nút nguồn, nơi mà hai bit thông tin X và Y được tạo ra. Lớp ở giữa gồm ba nút, mỗi nút là một ổ cứng có thể lưu trữ một bit. Chúng ta hãy đánh số chúng là ổ số 1-3 từ trái sang phải. Ổ cứng 1 lưu trữ bit X, ổ cứng 2 lưu trữ bit Y và ổ cứng còn lại lưu trữ bit X + Y (cộng modulo 2 hay là phép toán xor) thu được bằng cách mã hóa hai bit X và Y. Lớp dưới cùng là ba nút giải mã, mỗi lần giải mã sẽ truy cập hai ổ cứng khác nhau trong số ba ổ cứng lớp ở giữa.

Hình 1.2 mô tả hệ thống RAID 4/5 có thể lưu trữ hai bit thông tin độc lập là X và Y. Ba nút giải mã là logic, có nghĩa là tùy thuộc vào kịch bản một trong các bộ giải mã có liên quan có thể được sử dụng để giải mã hai bit X và Y; chúng ta hãy gọi chúng là bộ giải mã số 1-3 từ trái sang phải. Trong hoạt động bình thường, cả ba ổ cứng đều luôn sẵn sàng bộ giải mã 1 sử dụng nội dung của ổ cứng 1 và 2 làm đầu vào có thể giải mã X và Y. Thực tế, không cần giải mã thực sự ở đây vì các bit thông tin được lưu trữ không mã hóa. Bây giờ, nếu bất kỳ một trong các ổ cứng bị lỗi thì muốn có hai bit X và Y ta có thể phục hồi từ hai ổ cứng còn lại.

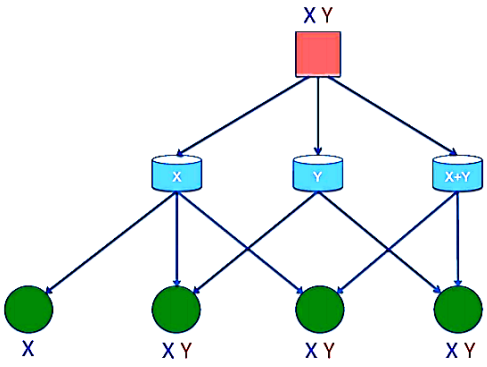


Hình 1.2. Một mạng minh họa cho hệ thống RAID 4/5

Ví dụ: nếu ổ cứng 1 không khả dụng, bị lỗi thì dựa trên hai dữ liệu Y và X + Y được lưu ở hai ổ cứng còn lại bộ giải mã 3 có thể giải mã X là:

$$Y + (X + Y) = (Y + Y) + X = 0 + X = 0$$

Do đó, hệ thống RAID 4/5 có thể khôi phục được dữ liệu khi một ổ cứng bị lỗi. Trong bài toán này, dữ liệu X và Y có thể được coi là một nguồn thông tin vì cả X và Y yêu cầu phải được giải mã bởi mọi bộ giải mã.



Hình 1.3. Hệ thống lưu trữ dữ liệu đa nguồn

Bây giờ chúng ta hãy xem xét hệ thống tổng quát hơn trong Hình 1.4, trong đó hai bit thông tin X và Y được lưu trữ trên ba ổ cứng từ 1-3. Yêu cầu là nếu các ổ cứng đều bị lỗi chỉ còn một ổ cứng bất kỳ nào không bị lỗi thì cả X và Y đều có thể được khôi phục. Nghĩa là nếu một mình ổ cứng 1 hoạt động, bit X có thể được phục hồi. Ở đây X và Y cần phải được phân biệt là hai nguồn thông tin khác nhau bởi vì chúng không cần phải được giải mã cùng nhau bởi mọi bộ giải mã. Các giải pháp

cho vấn đề này là bình thường như được thể hiện trong Hình 1.3. Hóa ra nghiên cứu về vấn đề này là đơn giản và dẫn đến nguồn gốc của mã hóa mạng.

Hãy xem xét hai nguồn thông tin độc lập về mặt thống kê được biểu diễn bằng các biến ngẫu nhiên độc lập X và Y. Giả sử chúng ta muốn gửi X và Y từ một điểm này đến điểm khác bằng cách truyền qua kênh truyền thông điểm-điểm. Từ lý thuyết thông tin cổ điển, chúng ta biết rằng bằng cách nén riêng X và Y chúng ta cần truyền các bit $\mathrm{H}(\mathrm{X}) + \mathrm{H}(\mathrm{Y})$. Ở đây $\mathrm{H}(.)$ biểu thị cho entropy của một biến ngẫu nhiên trong các bit. Nếu thay vào đó chúng ta nén X và Y một cách riêng biệt thì chúng ta cần khoảng $\mathrm{H}(\mathrm{X}, \mathrm{Y})$ bit. Tuy nhiên, vì X và Y là độc lập, chúng ta có:

$$\mathrm{H}(\mathrm{X}) + \mathrm{H}(\mathrm{Y}) = \mathrm{H}(\mathrm{X}, \mathrm{Y})$$

Điều đó có nghĩa là đối với truyền thông điểm-điểm, cho dù chúng ta nén X và Y riêng biệt hay cùng nhau về cơ bản nó không tạo ra sự khác biệt nào. Tức là, thay vì xử lý nhiều nguồn thông tin cùng một lúc chúng ta chỉ cần xử lý một nguồn thông tin tại một thời điểm. Trong trường hợp với nhiều nguồn thông tin, chúng ta đã đề cập đến phương pháp mã hóa xử lý các nguồn riêng biệt như mã hóa phân tách nguồn (source separation coding). Chúng ta đã thấy rằng đối với truyền thông điểm-điểm mã hóa phân tách nguồn là tối ưu.

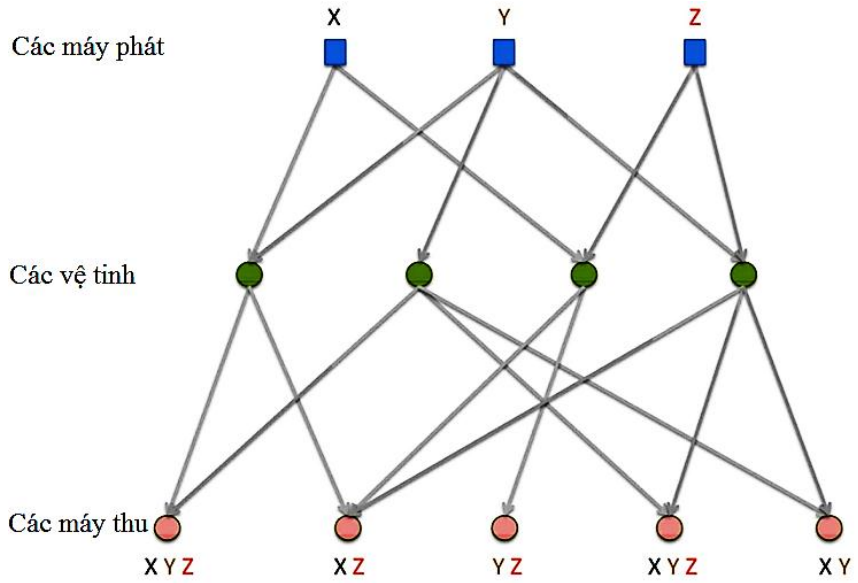
1.1.2.2. Hệ thống thông tin vệ tinh

Vấn đề tiếp theo chúng ta xem xét là một trường hợp phát sinh từ hệ thống truyền thông vệ tinh. Một mạng truyền thông vệ tinh bao gồm các máy phát mặt đất, các vệ tinh và máy thu mặt đất. Một máy phát (máy thu) và vệ tinh có thể giao tiếp với điều kiện là chúng nằm trong tầm nhìn của nhau. Mỗi máy phát phát ra một nguồn thông tin cần phải phát đa hướng đến một bộ thu được lựa chọn thông qua các vệ tinh.

Hiện nay, một vệ tinh không có tính năng gì hơn là chuyển tiếp các gói dữ liệu từ một máy phát đến máy thu bằng cách thu và phát sóng vô tuyến. Tuy nhiên về nguyên tắc, một vệ tinh có thể phát ra một gói tin từ việc mã hóa một số gói tin nhận được có thể từ nhiều hơn một máy phát. Ngoài ra, máy thu có thể giải mã thông tin từ một số

gói dữ liệu được truyền bởi nhiều hơn một vệ tinh. Những bổ sung khả năng mã hóa của các vệ tinh và các máy thu bây giờ được gọi là mã hóa mạng.

Để đơn giản hóa vấn đề, giả sử các đường lên từ các bộ phát tới vệ tinh có băng thông vô hạn, vì vậy người ta có thể giả định rằng vệ tinh biết đầy đủ về nguồn thông tin được tạo ra bởi mỗi máy phát trong vùng bao phủ. Các đường xuống có băng thông hữu hạn, tức là mỗi vệ tinh có thể phát sóng ở một số tốc độ hữu hạn. Đối với một tập hợp các tốc độ cho các nguồn thông tin, chúng tôi quan tâm đến tập hợp tất cả các tốc độ mà các vệ tinh có thể phát để mỗi người nhận có thể khôi phục tất cả các nguồn thông tin dành cho nó. Tập hợp tất cả các tốc độ có thể được gọi là vùng tốc độ mã hóa (coding rate region).



Hình 1.4. Mạng thông tin vệ tinh

Vấn đề này có thể được xây dựng như một hệ thống lưu trữ dữ liệu được thảo luận trong phần trước. Hình 1.4 là minh họa cho một hệ thống vệ tinh vừa được trình bày. Lớp trên cùng là các máy phát, lớp thứ hai là các vệ tinh và lớp dưới cùng là các máy thu. Ở đây, các bộ phát, vệ tinh và bộ thu tương ứng với các nút nguồn, ổ cứng và bộ giải mã trong hệ thống lưu trữ dữ liệu tương ứng. Vấn đề lý thuyết thông tin của hệ thống thông tin vệ tinh là để mô tả vùng tốc độ mã hóa.

1.2. TỔNG QUAN CHUNG VỀ MÃ MẠNG

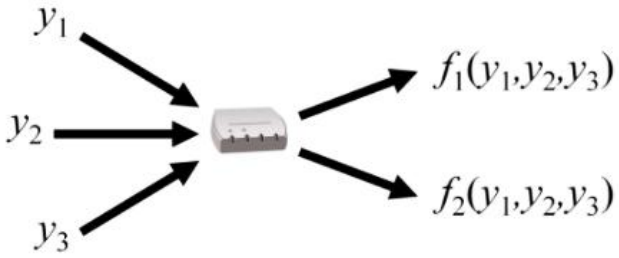
1.2.1. Định nghĩa mã mạng

Định nghĩa mã mạng không đơn giản. Có một số định nghĩa có thể đã được đưa ra và sử dụng. Trong bài báo của Ahlswede, Cai, Li và Yeung nói rằng "việc sử dụng mã hóa tại một nút trong mạng được coi là mã mạng" [17, 18]; Đây là định nghĩa chung nhất về mã mạng. Nhưng nó không phân biệt nghiên cứu về mã mạng từ mạng hoặc nhiều thiết bị đầu cuối, lý thuyết thông tin - một lĩnh vực cũ hơn với vô số các vấn đề khó. Bài báo của Ahlswede và cộng sự có một đặc điểm phân biệt nó với các bài báo lý thuyết thông tin mạng là thay vì nhìn vào các mạng tổng quát nơi mà mọi nút tùy ý có một hiệu ứng xác suất trên mỗi nút khác, chúng có cái nhìn đặc biệt tại các mạng bao gồm các nút liên kết với nhau bằng các liên kết điểm-điểm không có lỗi. Vì vậy, mô hình mạng của Ahlswede và các cộng sự là một trường hợp đặc biệt trong lĩnh vực nghiên cứu lý thuyết thông tin mạng, mặc dù nó rất phù hợp với các mạng hiện tại vì về cơ bản tất cả các mạng có thể được mô hình hóa một khi lớp vật lý được coi như là các đường truyền dẫn không có lỗi thực hiện vận chuyển các bit.

Một định nghĩa khác về mã mạng là việc mã hóa tại một nút trong mạng có các liên kết không có lỗi. Định nghĩa này phân biệt chức năng của mã mạng từ mã hóa kênh với các kết nối có nhiễu. Định nghĩa này thường được sử dụng và theo đó nghiên cứu mã mạng là một lĩnh vực đặc biệt của lý thuyết thông tin mạng. Nhiều nghiên cứu về mã mạng đã tập trung xung quanh một dạng mã mạng cụ thể là mã mạng tuyến tính ngẫu nhiên. Mã mạng tuyến tính ngẫu nhiên được giới thiệu như là một phương thức mã hóa ngẫu nhiên đơn giản cung cấp "một vectơ của các hệ số cho các quá trình nguồn" và được "cập nhật bởi mỗi nút mã hóa". Nói cách khác, mã mạng tuyến tính ngẫu nhiên yêu cầu các bản tin được truyền thông qua mạng được kèm theo một số thông tin bổ sung - trong trường hợp này là một vectơ các hệ số. Trong các mạng truyền thông ngày nay, có một loại mạng được sử dụng rộng rãi dễ dàng chứa các thông tin bổ sung và có các liên kết không có lỗi là mạng gói. Với

các gói tin, thông tin bổ sung hoặc thông tin phụ có thể được đặt trong phần đầu của gói tin (ví dụ: số thứ tự thường được đặt trong tiêu đề gói để theo dõi thứ tự).

Một định nghĩa thứ ba của mã mạng là việc mã hóa tại một nút trong một mạng gói (nơi dữ liệu được chia thành các gói và mã mạng được áp dụng cho các nội dung của gói) hoặc nói chung là việc thực hiện mã hóa ở phía trên lớp vật lý. Điều này không giống như lý thuyết thông tin mạng thường liên quan đến việc mã hóa ở lớp vật lý. Định nghĩa này là hữu ích bởi vì nó căn cứ vào các nghiên cứu của chúng ta trong một trường hợp cụ thể để có thể triển khai thực tế.



Hình 1.5. Mô hình mã mạng

Từ những nội dung trên ta có thể hình dung mã mạng đơn giản như sau: Với một bộ định tuyến trong mạng máy tính chỉ có thể định tuyến hoặc chuyển tiếp gói tin. Mỗi gói tin trên một liên kết đầu ra là một bản sao của gói tin đến trước đó trên một liên kết đầu vào. Mã mạng cho phép mỗi nút trong mạng thực hiện một số phép toán nên mỗi gói tin được gửi trên liên kết đầu ra của nút có thể là một hàm hoặc "trộn" của các bản tin đến trước đó trên các liên kết đầu vào của nút, như được minh họa trong Hình 1.5 [20]. Như vậy, mã mạng nói chung là sự truyền, trộn (hoặc mã hóa) và trộn lại (hoặc mã hóa lại) của các gói tin đến các nút bên trong mạng, sao cho các gói tin được truyền tới đích và có thể giải mã được tại các đích cuối cùng của chúng.

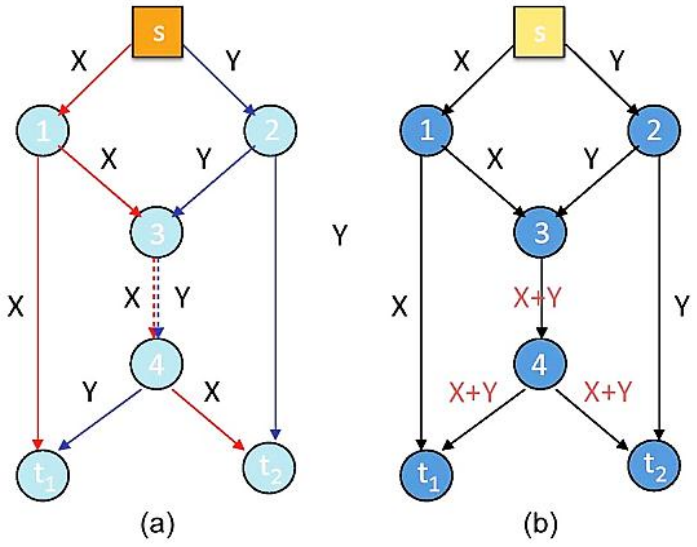
Đơn giản hơn ta có thể hiểu mã mạng qua một trường hợp sau: Trong các mạng định tuyến truyền thống, các gói được lưu trữ một cách đơn giản và sau đó được chuyển tiếp đến nút tiếp theo trong mạng. Như vậy, nếu một nút định tuyến nhận được hai gói từ hai nguồn riêng biệt nó sẽ chuyển tiếp chúng tuần tự, ngay cả

khi chúng được gửi tới cùng một đích, trong khi đưa vào hàng đợi tất cả các gói tin khác mà nó nhận được trong thời gian chờ để gửi xong một gói tin mới tiếp tục gửi tiếp. Điều này dẫn đến việc tạo ra các truyền dẫn riêng biệt cho mỗi bản tin được gửi đi điều này làm giảm hiệu quả của mạng. Mã mạng được sử dụng để giảm thiểu điều này bằng cách hợp nhất các bản tin liên quan với nhau tại một nút chuyển tiếp, sử dụng một phương thức mã hóa đã biết và sau đó chuyển tiếp gói tin sau khi hợp nhất đến nút đích, nút đích nhận được gói tin và tiến hành giải mã thu được thông tin cần thiết.

Khi lĩnh vực mã mạng được đưa ra nghiên cứu dẫn đến những phát triển nhanh chóng và thúc đẩy việc sử dụng các công cụ toán học mới, trong các lĩnh vực như đại số, lý thuyết matroid, hình học, lý thuyết đồ thị, tổ hợp và lý thuyết tối ưu hóa phục vụ cho các phương pháp mã hóa tối ưu hiện nay.

1.2.2. Mô hình mã mạng đơn giản

Mô hình mạng cánh bướm là một mô hình kinh điển, dễ hiểu được sử dụng để mô tả hệ thống mạng sử dụng mã hóa mạng một cách đơn giản nhất [19]. Khi một nguồn thông tin được phát đa hướng trên mạng truyền thông điểm-điểm thì việc mã hóa mạng có thể giúp hoạt động tốt hơn việc định tuyến.



Hình 1.6. Mạng cánh bướm

Xem xét mạng trong Hình 1.6 (a). Hai bit X và Y được tạo ra tại các nút nguồn s. Nhiệm vụ là phát đa hướng cho cả hai bit X và Y tới hai nút đích t_1 và t_2. Trong mạng, mỗi cạnh đại diện cho một kênh truyền dữ liệu không có nhiễu và trên đó một bit có thể được truyền qua. Có một kênh đặc biệt từ nút 3 đến nút 4; Phương pháp tiếp cận định tuyến thông thường cho thấy rằng tác vụ con của phát đa hướng X và tác vụ con của phát đa hướng Y có thể được thực hiện một cách độc lập. Để phát đa hướng X, bit phải được gửi dọc theo các đường dẫn màu đỏ, trong đó bit được nhân bản tại nút 1. Tương tự, bit Y phải được gửi dọc theo các đường dẫn màu xanh và bit được nhân bản tại nút 2.

Rõ ràng, có một xung đột giữa đường dẫn màu đỏ và đường dẫn màu xanh tại kênh từ nút 3 đến nút 4 mà không thể giải quyết được. Do đó, không thể phát đa hướng hai bit từ nút nguồn s đến các nút đích t_1 và t_2 bằng cách định tuyến đơn thuần. Tuy nhiên, xung đột tại kênh từ nút 3 đến nút 4 có thể được giải quyết bằng cách mã hóa hai bit X và Y thành một bit đơn X + Y. Đây chính là giải pháp mã hóa mạng và được hiển thị trong Hình 1.6 (b). Rõ ràng, cả hai nút đích t_1 và t_2 đều có thể giải mã X và Y.

Trong mạng cánh bướm, có hai đường truyền riêng biệt có thể truyền từ nút nguồn s đến nút đích t_i, trong đó $i = 1, 2$. Ví dụ, hai đường phân tách cạnh từ s đến t_1 là:

Đường 1: $s \rightarrow 1 \rightarrow t_1$;

Đường 2: $s \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow t_1$.

Chúng ta nói rằng lưu lượng tối đa (*maximum flow*) từ nút nguồn s đến nút đích t_i là bằng 2. Rõ ràng, không thể gửi nhiều hơn hai bit từ nút nguồn s đến bất kỳ nút nào trong số các nút đích có thể ở dạng mã hóa hoặc không mã hóa. Nếu chúng ta cần gửi hai bit từ nút nguồn s đến bất kỳ một trong các nút đích, thì hai bit có thể được định tuyến dọc theo hai đường truyền riêng biệt tương ứng với hai cạnh. Nói cách khác, số bit có thể được gửi từ nút s đến nút t_i bằng với lưu lượng lớn nhất từ nút s đến nút t_i. Theo nghĩa này, chúng ta nói rằng lưu lượng tối đa từ

nút s đến nút t_i có thể đạt được bằng cách định tuyến. Nếu chúng ta cần phát đa hướng hai bit từ nút nguồn s đến cả hai nút đích, thì lưu lượng tối đa của hai nút đích không thể đồng thời đạt được bằng cách định tuyến. Tuy nhiên, điều này có thể đạt được bằng phương pháp mã hóa mạng như chúng ta đã thấy.

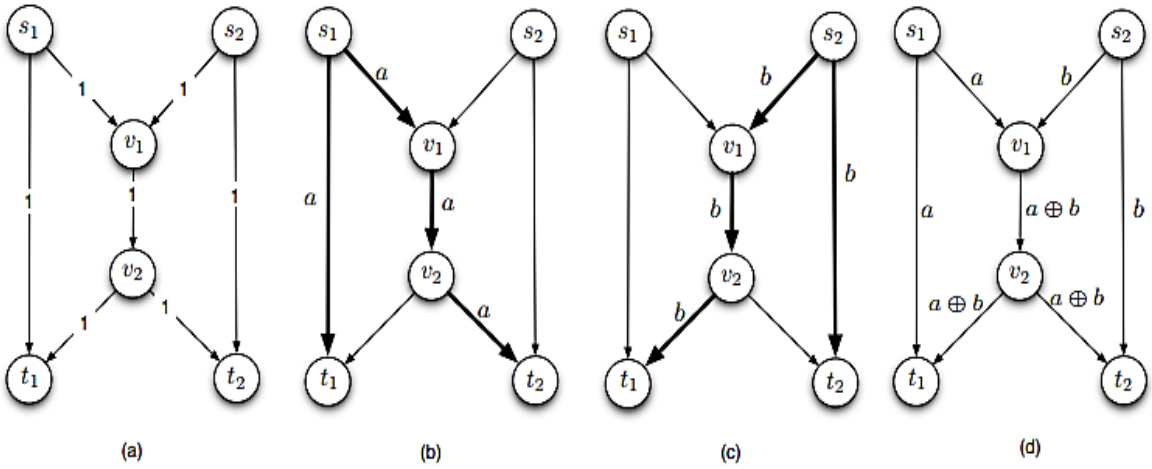
Trong một mạng điểm-điểm, hãy xem xét phát đa hướng nguồn thông tin từ một nút nguồn đến một số lượng cố định các nút đích $t_1; t_2; \dots; t_k$. Biểu thị lưu lượng tối đa từ nút s đến nút t_i bởi luồng tối đa - maxflow (t_i). Như đã thảo luận, tốc độ của nguồn thông tin không thể vượt quá maxflow (t_i) cho mỗi i, hoặc tương đương, tốc độ của nguồn thông tin không thể vượt quá mức tối thiểu của maxflow (t_i) với tất cả $i = 1, 2, \dots, k$. Định lý Max-flow - Min-cut đưa ra giới hạn trên cho luồng thông tin và được gọi là giới hạn dòng chảy tối đa (*Max-flow bound*) hay cũng được gọi là giới hạn Min-cut và nó có thể đạt được bằng mã hóa mạng.

Giải pháp mã hóa mạng trong Hình 1.6 (b) là sự chứng minh định lý Max-flow - Min-cut cho mạng cánh bướm. Trong giải pháp này, cơ chế mã hóa chỉ liên quan đến phép toán cộng modulo 2 tạo thành từ một mã trong mã mạng tuyến tính trên trường nhị phân. Mã mạng tuyến tính là quan trọng nhất trong thực tế vì thuật toán mã hóa và giải mã hiệu quả có thể được thiết kế cho các mã như vậy.

Giải pháp mã hóa mạng cho mạng cánh bướm cho thấy rằng đối với một vấn đề mã hóa mạng đơn nguồn, thì giới hạn Max-flow có thể đạt được bằng mã hóa mạng tuyến tính. Điều này đã được chứng minh bởi Li, sau đó Koetter và Medard đã chứng minh kết quả tương tự bằng phương pháp của một kỹ thuật quen thuộc hơn với các kỹ thuật giao tiếp do đó mở rộng hơn nữa lĩnh vực này.

1.2.3. Một số lợi ích của mã mạng

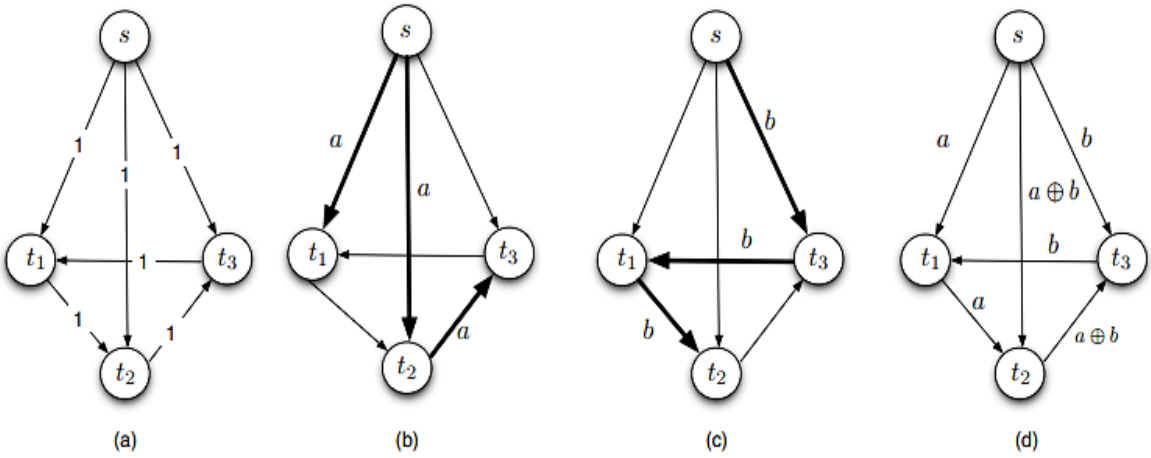
Theo các phân tích trong [21], mã mạng cho phép các nút tạo ra các gói dữ liệu mới bằng cách kết hợp các gói nhận được. Kỹ thuật này có một số lợi ích như tăng thông lượng, cải thiện độ tin cậy và tăng độ ổn định của mạng.



Hình 1.7. Ví dụ cơ bản về mã mạng

Để mô tả lợi thế của kỹ thuật mã mạng, xét mạng được mô tả trong Hình 1.7(a). Xét mạng bao gồm hai nguồn s_1 và s_2, và hai đích t_1 và t_2. Giả sử tất cả các tuyến của mạng đều có dung lượng là đơn vị, mỗi một tuyến chỉ truyền một gói dữ liệu tại một thời điểm. Theo cách truyền thống, các gói được chuyển tiếp qua hai cây Steiner (cây Steiner là cây kết nối nút nguồn với các đích và có thể chứa các nút khác), cây thứ nhất chuyển tiếp các gói tạo bởi s_1, và cây thứ hai chuyển tiếp các gói do s_2 tạo ra. Tuy nhiên, mạng không bao gồm hai tuyến không kết nối Steiner với hai nguồn s_1 và s_2, do đó phương pháp truyền thống kiểu multicast kết nối hai nguồn thông tin này là không thể thực hiện được. Ví dụ, như mô tả trong Hình 1.7(b) và Hình 1.7(c) chia sẻ nút cổ chai (v_1, v_2). Hình 1.7(d) cho thấy xung đột có thể được giải quyết bằng kỹ thuật mã mạng. Giải thích như sau, giả sử a và b là các gói do s_1 và s_2 tương ứng tạo ra. Cả hai gói được gửi đồng thời đến nút v_1, tại đây nó sẽ tạo ra gói mới $a \oplus b$, và gói mới được gửi đến hai nút t_1 và t_2. Dễ dàng nhận thấy cả hai nút có thể giải mã các gói a và b từ các gói nhận được từ các tuyến đến.

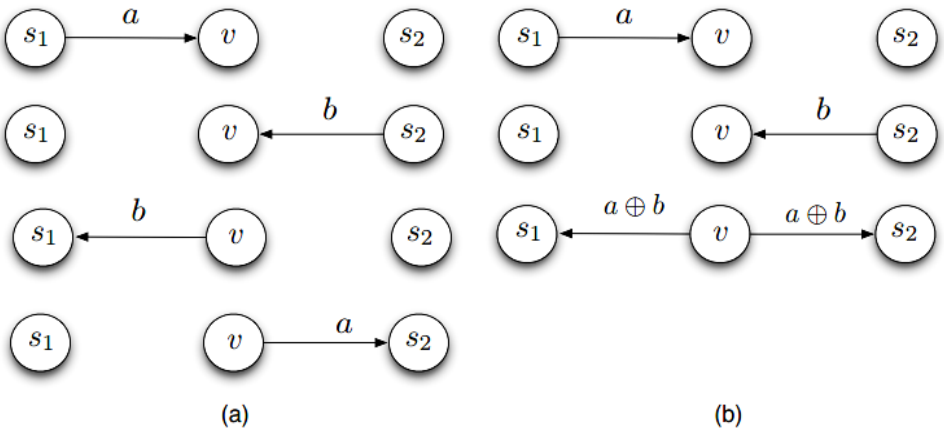
Kỹ thuật mã mạng có thể hữu ích trong việc tối thiểu hóa trễ dữ liệu từ nút nguồn đến các nút đích.



Hình 1.8. Tối thiểu hóa trễ bằng mã mạng

Ví dụ, xét mạng trong Hình 1.8(a). Giả sử tại mỗi thời điểm mỗi tuyến chỉ truyền một gói và trễ của mỗi tuyến là một đơn vị thời gian. Hình 1.8(b) và Hình 1.8(c) mô tả hai tuyến không kết nối của cây Steiner thực hiện kết nối s đến các đích t_1, t_2 và t_3. Tuy nhiên, nút t_2 sẽ nhận một trong các gói bị trễ đi 3 đơn vị thời gian. Ta thấy rằng bất cứ sơ đồ nào không dùng mã mạng sẽ gây ra trễ ba đơn vị thời gian. Hình 1.8(d) là giải pháp dùng mã mạng cho thấy dữ liệu truyền chỉ trễ hai đơn vị thời gian.

Ngoài ra, kỹ thuật mã mạng cũng có thể được dùng để tối thiểu các phiên truyền dẫn, hay là giảm năng lượng tiêu thụ trong mạng không dây.



Hình 1.9. Giảm tiêu thụ năng lượng với mã mạng:

(a) theo cách truyền thống (b) theo mã mạng

Ví dụ, xét mạng không dây trong Hình 1.9. Mạng bao gồm hai nút s_1 và s_2 muốn trao đổi các gói thông qua nút trung gian v. Cụ thể nút s_1 cần gửi gói a cho nút s_2 và nút s_2 cần gửi gói b cho nút s_1. Hình 1.9(a) là cách thực hiện truyền thống và cần đến 4 phiên truyền. Hình 1.9(b) là sơ đồ truyền theo mã mạng mà theo đó nút trung gian v đầu tiên nhận hai gói a và b từ s_1 và s_2 sau đó nó tạo ra gói mới là $a \oplus b$ rồi phát gói này cho cả a và b, theo sơ đồ này thì chỉ cần 3 phiên truyền. Ví dụ này cho thấy kỹ thuật mã mạng có lợi ích để giảm các phiên truyền dẫn trong mạng vô tuyến quảng bá.

Với các ví dụ đã nêu trên đây, cho thấy mã mạng có nhiều lợi ích cho các ứng dụng băng rộng trong các mạng thông tin có dây và không dây. Việc sử dụng kỹ thuật mã mạng cho thấy ưu điểm hơn so với cách truyền thống. Bằng việc mã hóa tại các nút mạng trung gian, kỹ thuật mã mạng tác động lớn đến mạng truyền thông thế hệ mới bởi nhiều lợi ích tiềm năng của nó mà các nhà nghiên cứu đã chỉ ra.

1.3. KẾT LUẬN CHƯƠNG 1

Việc truyền thông tin qua mạng được hiểu là một sự trao đổi dữ liệu, mà không có khả năng kết hợp hoặc trộn lẫn những dữ liệu đã được gửi. Từ các phân tích trong bài báo “Network information flow ” [17] của R. Ahlswede, Ning Cai, S.-R. Li, và R. W. Yeung đã thay đổi quan điểm này bằng cách đưa ra khái niệm *luồng thông tin* để chứng minh rằng sự kết hợp dữ liệu có thể làm tăng dung lượng vượt quá giới hạn của một mạng.

Trong một hệ thống thông tin số, ngoài các loại mã như mã hóa nguồn (với mục đích nén dữ liệu), mã bảo mật, mã hóa kênh (sửa sai); thì kỹ thuật mã mạng (kỹ thuật thuộc lớp mạng) cũng có thể được áp dụng nhằm tăng tính ổn định của mạng, giảm trễ, tăng thông lượng...

Chương 1 đã khái quát chung về lý thuyết thông tin và mã hóa, lý thuyết tổng quan về mã mạng, mô hình cách thức thực hiện mã mạng và các lợi ích khi sử dụng mã mạng.

CHƯƠNG 2. ĐỀ XUẤT XÂY DỰNG MÃ MẠNG TRÊN MỘT SỐ CẤU TRÚC ĐẠI SỐ

Chương 2 trình bày các kiến thức cơ bản về cơ sở toán học về số học modulo, các cấu trúc đại số, trên cơ sở đó, NCS tập trung nghiên cứu đề xuất xây dựng một số phương pháp thực hiện hàm mã hóa mạng bằng các phép cộng, phép nhân các số hoặc đa thức và cấu trúc đại số nhóm cộng các điểm trên đường cong elliptic.

Các kết quả nghiên cứu ở chương 2 đã được công bố trên các bài báo:

Bài báo 1: (2018) Phạm Long Âu, Nguyễn Bình, Ngô Đức Thiện, Nguyễn Lê Cường, "Mã mạng trên một số cấu trúc đại số", Tạp chí Nghiên cứu Khoa học và công nghệ Quân sự, trang 125-132, No 54, 4/2018).

Bài báo 2: (2019) Au Pham Long, Thien Ngo Duc and Binh Nguyen, "About Some Methods of Implementing Network Coding based on Polynomial Rings and Polynomial Fields," 2019 25th Asia-Pacific Conference on Communications (APCC), Ho Chi Minh City, Vietnam, 2019, pp. 507-510, doi: 10.1109/APCC47188.2019.9026530; (PoD) ISSN: 2163-0771, IEEE Xplore.

Bài báo 3: (2019) Pham Long Au, Nguyen Minh Trung, Nguyen Le Cuong, "About Some Methods of Implementation Network Coding over Number Rings", Proceedings of the 12th international conference on advanced technologies for communication, page 371-374, ATC 10/2019; ISSN: 2162-1039 IEEE Xplore;

Bài báo 4: (2019) Pham Long Au, Ngo Duc Thien, "About one method of Implementation Network Coding based on point additive operation on Elliptic curve" Journal of Science and Technology on Information and Communications, No 1 (CS.01) 2019, ISSN 2525- 2224, page 3-6.

2.1. MÔT SỐ PHƯƠNG PHÁP XÂY DỰNG MÃ MẠNG TRÊN VÀNH SỐ

2.1.1. Số học modulo

2.1.1.1. Số nguyên

Tập các số nguyên:

$$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{Z}$$

Định nghĩa 2.1:

Cho $a, b \in \mathrm{Z}$, a là ước của b nếu $\exists c \in \mathbb{Z}: b = a.c$. Ký hiệu: $a|b$.

Các tính chất chia hết

$\forall a, b, c \in \mathrm{Z}$ ta có:

+ $a|a$
+ Nếu $a|b$ và $b|c$ thì $a|c$
+ Nếu $a|b$ và $a|c$ thì $a|(bx + cy)$ với $\forall x, y \in \mathbb{Z}$
+ Nếu $a|b$ và $b|a$ thì $a = \pm b$

Định nghĩa 2.2:

Thuật toán chia đối với các số nguyên:

Nếu a và b là các số nguyên với $b \geq 1$ thì $a = qb + r, 0 \leq r < b, q$ và r là duy nhất.

Phần dư của phép chia a và b được ký hiệu $a \bmod b = r$

Thương của phép chia a và b được ký hiệu $a \operatorname{div} b = q$

Ta có $a \operatorname{div} b = \left[\frac{a}{b}\right], a \bmod b = a - b\left[\frac{a}{b}\right]$

Ví dụ:

$$a = 73, b = 17 \rightarrow 73\mathrm{div}17 = 4, \quad 73\mathrm{mod}17 = 5$$

Định nghĩa 2.3: Ước chung

c là ước chung của a và b nếu $c|a$ & $c|b$

Định nghĩa 2.4: Ước chung lớn nhất (ƯCLN)

Số nguyên dương *d* là ƯCLN của các số nguyên *a* và *b* (Ký hiệu $d = (a, b)$) nếu:

- *d* là ước chung của a và b

- Nếu có $c|a$ và $c|b$ thì $c|d$

Như vậy (a, b) là số nguyên dương lớn nhất ước của cả *a* và *b* không kể $(0, 0) = 0$.

Ví dụ: Các ước chung của 12 và 18 là $\{\pm1, \pm2, \pm3, \pm6\} \rightarrow (12, 18) = 6$

Định nghĩa 2.5: Bội chung nhỏ nhất (BCNN)

Số nguyên dương *d* là bội chung nhỏ nhất (BCNN) của các số nguyên *a* và *b* (Ký hiệu $d = \text{BCNN}(a, b)$) nếu:

(i) $a|d,\ b|d$.

(ii) Nếu có $a|c, b|c$ thì $d|c$.

Như vậy *d* là số nguyên dương nhỏ nhất là bội của cả *a* và *b*.

Tính chất

$$\text{BCNN}(a, b) = \frac{a.b}{(a,b)}$$

Ví dụ:

$$(12, 18) = 6 \rightarrow \text{BCNN}(12, 18) = \frac{12.18}{6} = 36$$

Định nghĩa 2.6: Hai số nguyên dương *a* và *b* được gọi là nguyên tố cùng nhau nếu: $(a, b) = 1$.

Định nghĩa 2.7: Số nguyên $p \geq 2$ được gọi là số nguyên tố nếu các ước dương của nó chỉ là 1 và *p*. Ngược lại *p* được gọi là hợp số.

Định lý 2.1 (Định lý cơ bản của số học):

Với mỗi số nguyên $n \geq 2$ ta luôn phân tích được dưới dạng tích của luỹ thừa của các số nguyên tố.

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \qquad (2.1)$$

Trong đó p_i là các số nguyên tố khác nhau và e_i là các số nguyên dương. Hơn nữa phân tích trên là duy nhất.

Định nghĩa 2.8:

Với $n \geq 2$, hàm $\varphi(n)$ được xác định là số các số nguyên trong khoảng $[1, n]$ nguyên tố cùng nhau với n.

Các tính chất của hàm $\varphi(n)$

Nếu *p* là số nguyên tố thì $\varphi(n) = p - 1$.

Nếu $(m, n) = 1$ thì $\varphi(m.n) = \varphi(m)\varphi(n)$.

Nếu $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ là phân tích ra thừa số nguyên tố của *n* thì:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) \quad (2.2)$$

Với $\forall n \geq 5$:

$$\varphi(n) > \frac{n}{6\ln\ln n}$$

2.1.1.2. Các thuật toán trong $\mathbb{Z}$

Cho a và b là các số nguyên không âm và nhỏ hơn hoặc bằng $a \times b = b \times a$. Cần chú ý rằng số các bit trong biểu diễn nhị phân của *n* là $[\lg n] + 1$ và số này xấp xỉ bằng lg*n*. Số các phép toán bit đối với bốn phép toán cơ bản trên các số là cộng, trừ, nhân và chia sử dụng các thuật toán kinh điển được tóm lược trên bảng sau. Các kỹ thuật tinh tế hơn đối với các phép toán nhân và chia sẽ có độ phức tạp nhỏ hơn.

Độ phức tạp bit của các phép toán cơ bản trong $\mathbb{Z}$

Phép toán		Độ phức tạp bit
Cộng	$a + b$	$0(\lg a + \lg b) = 0(\lg n)$
Trừ	$a - b$	$0(\lg a + \lg b) = 0(\lg n)$
Nhân	$a.b$	$0\big((\lg a).(\lg b)\big) = 0((\lg n)^2)$
Chia	$a = qb + r$	$0\big((\lg a).(\lg b)\big) = 0((\lg n)^2)$

ƯCLN của 2 số nguyên *a* và *b* có thể được tính theo định lý sau:

Định lý 2.2: Nếu $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ trong đó $e_i \geq 0, f_i \geq 0$

Thì $\text{ƯCLN}(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \dots p_k^{\min(e_k,f_k)}$

Và $\text{BCNN}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \dots p_k^{\max(e_k,f_k)}$

Ví dụ: Cho $a = 4864 = 2^8.19, b = 3458 = 2.7.13.19$. Khi đó:

$$\text{ƯCLN}(a,b) = (4864, 3458) = 2.19 = 38$$

$$BCNN(a,b) = (4864, 3458) = 2^8.7.13.19 = 442624$$

Định lý 2.3: Nếu a và b là các số nguyên dương với $a > b$ thì:

$$\text{ƯCLN}(a,b) = \text{ƯCLN}(b, a \bmod b)$$

Thuật toán Euclid sau sẽ cho ta cách tính ƯCLN rất hiệu quả mà không cần phải phân tích ra thừa số nguyên tố.

a) Thuật toán Euclid

Thuật toán Euclid, là một thuật toán giúp tính ƯCLN của hai số một cách hiệu quả. Ở dạng đơn giản nhất, thuật toán Euclid bắt đầu với cặp số nguyên dương và tạo ra một cặp số nguyên dương mới bao gồm số nhỏ hơn và phần dư của phép chia hai số ban đầu. Quá trình được tiếp tục cho đến khi hai số trong cặp bằng nhau, giá trị lúc đó sẽ trở thành ước số chung lớn nhất của cặp số ban đầu. Nguyên lý chính của thuật toán là ước số chung lớn nhất của một cặp số không thay đổi với hiệu của hai số đó. Vì số lớn hơn trong cặp số bị giảm giá trị nên việc lặp đi lặp lại thuật toán này giúp tạo ra những số ngày càng nhỏ và đến một lúc nào đó quá trình này sẽ kết thúc - khi cặp số còn lại hai số bằng nhau (nếu quá trình được thực hiện thêm một bước nữa, sẽ có một trong hai số trở thành số 0).

VÀO: Hai số nguyên không âm a và b với $a > b$ RA : ƯCLN của a và b.
(1) While $b \neq 0$ do $r \leftarrow a \bmod b, a \leftarrow b, b \leftarrow r$ (2) Return (a)

Thuật toán trên có thời gian chạy chừng $O(2\log_2 n)$ các phép toán bit.

Ví dụ: Cho $a = 4864$ và $b = 3458$, các bước của thuật toán Euclid khi tính ƯCLN (a, b) như sau:

+ $b = 3458 \neq 0$:

$r = a \; mod \; b = 4864 \; mod \; 3458 = 1406$

$a = b = 3458; \; b = r = 1406$

+ $b = 1406 \neq 0$:

$r = a \; mod \; b = 3458 \; mod \; 1406 = 646$

$a = b = 1406; \; b = r = 646$

+ $b = 646 \neq 0$:

$r = a \; mod \; b = 1406 \; mod \; 646 = 76$

$a = b = 646; \; b = r = 76$

+ $b = 76 \neq 0$:

$r = a \; mod \; b = 646 \; mod \; 76 = 38$

$a = b = 76; \; b = r = 38$

+ $b = 38 \neq 0$:

$r = a \; mod \; b = 76 \; mod \; 38 = 0$

$a = b = 38; \; b = r = 0$

Kết quả: ƯCLN$(4864,3458) = 78$

Thuật toán trên có thể được mở rộng để không những chỉ tính được ƯCLN của 2 số nguyên *a* và *b* mà còn tính được các số nguyên *x* và *y* thoả mãn $ax + by = d$.

b) Thuật toán Euclid mở rộng

Giải thuật Euclid mở rộng được sử dụng để giải một phương trình vô định nguyên (còn được gọi là phương trình Đi-ô-phăng) có dạng: $ax + by = c$.

Trong đó *a, b, c* là các hệ số nguyên; *x, y* là các ẩn nhận giá trị nguyên. Điều kiện cần và đủ để phương trình này có nghiệm (nguyên) là ƯCLN(a, b) là ước của c. Khẳng định này dựa trên một mệnh đề sau:

Nếu d = ƯCLN(a, b) thì tồn tại các số nguyên *x, y* sao cho $ax + by = d$.

Thuật toán:

VÀO : Hai số nguyên không âm a và b với $a > b$ RA : $d = \text{ƯCLN}(a, b)$ và các số nguyên x và y thoả mãn $ax + by = d$
Nếu $b = 0$ thì đặt $d \leftarrow a, x \leftarrow 1, y \leftarrow 0$ và $return(d, x, y)$. (1) Đặt $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$ (2) While $b > 0$ do (2.1) $q \leftarrow \lfloor a/b \rfloor, r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$ (2.2) $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y$ (3) Đặt $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$ và $return(d, x, y)$

Thuật toán trên có thời gian chạy cỡ $0((\lg n)^2)$ các phép toán bit.

Ví dụ: Bảng sau chỉ ra các bước của thuật toán trên với các giá trị vào $a = 4864$ và $b = 3458$.

Bảng 2.1. Ví dụ thuật toán Euclid mở rộng

Q	r	x	y	a	b	x_1	x_2	y_2	y_1
–	–	–	–	4864	3458	1	0	0	1
1	1406	1	–1	3458	1406	0	1	1	–1
2	646	–2	3	1406	646	1	–2	–1	3
2	114	5	–7	646	114	–2	5	3	7
5	76	–27	38	114	76	5	–27	–7	38
1	38	32	–45	76	38	–27	32	38	–45
2	0	–91	128	38	0	32	–91	–45	128

Bởi vậy ta có:

ƯCLN(4864, 3458) = 38 và (4864)(32) + (3458)(-45) = 38.

2.1.1.3. Các số nguyên modulo n

Định nghĩa 2.9: Nếu a và b là các số nguyên thì a được gọi là đồng dư với b theo modulo (ký hiệu là $a \equiv b \mathrm{mod} n$) nếu $n|(a-b)$.

Số nguyên *n* được gọi là modulo đồng dư.

Ví dụ:

$24 \equiv 9 \mathrm{mod} 5$ vì 24 – 9 = 3.5

$-11 \equiv 17 \mathrm{mod} 7$ vì -11 – 17 = -4.7

Các tính chất

Đối với $a, a_1, b, b_1, c \in \mathbb{Z}$ ta có:

(1) $a \equiv b \mathrm{mod} n$ nếu và chỉ nếu a và b cũng có phần dư khi chia cho *n*.

(2) Tính phản xạ: $a \equiv a \mathrm{mod} n$.

(3) Tính đối xứng: Nếu $a \equiv b (\mathrm{mod} n)$ thì $b \equiv a (\mathrm{mod} n)$

Tính bắc cầu: Nếu $a \equiv b (\mathrm{mod} n)$ và $b \equiv c (\mathrm{mod} n)$ thì $a \equiv c (\mathrm{mod} n)$

(4) Nếu $a \equiv a_1 (\mathrm{mod} n)$ và $b \equiv b_1 (\mathrm{mod} n)$ thì

$a + b \equiv a_1 + b_1 (\mathrm{mod} n)$ và $a.b \equiv a_1.b_1 (\mathrm{mod} n)$

Lớp tương đương của một số nguyên a là tập các số nguyên đồng dư với a modulo n. Từ các tính chất (2), (3) và (5) ở trên ta có thể thấy rằng đối với n cố định, quan hệ đồng dư theo modulo *n* sẽ phân hoạch $\mathbb{Z}$ thành các lớp tương đương.

Nếu $a = qn + r$ với $0 \leq r \leq n$ thì $a \equiv r (\mathrm{mod} n)$.

Bởi vậy mỗi số nguyên a là đồng dư theo modulo n với một số nguyên duy nhất nằm trong khoảng từ 0 tới $n - 1$, số này được gọi là thặng dư tối thiểu của $a \bmod n$. Như vậy a và r có thể được dùng để biểu thị cho lớp tương đương này.

Định nghĩa 2.10: Các số nguyên modulo *n* (ký hiệu $\mathbb{Z}_n$) là tập (các lớp tương đương) của các số nguyên $\{0, 1, 2, \ldots, n-1\}$. Các phép cộng, trừ, nhân trong $\mathbb{Z}_n$ được thực hiện theo modulo *n*.

Ví dụ:

$\mathbb{Z}_{25} = \{0, 1, \dots, 24\}$. Trong Z_{25} ta có:

13 + 16 = 4 và $13 + 16 = 29 \equiv 4(\mathrm{mod}25)$

Tương tự 13.16 = 8 trong $\mathbb{Z}_{25}$.

Định nghĩa 2.11: Phần tử nghịch đảo

Cho $a \in \mathbb{Z}_n$, phần tử nghịch đảo (ngược theo phép nhân) của $a \bmod n$ là một số nguyên $x \in \mathbb{Z}_n$ sao cho: $a.x \equiv 1(\mathrm{mod}n)$

Nếu *x* tồn tại thì nó là duy nhất, a được gọi là khả nghịch. Phần tử nghịch đảo của a được ký hiệu là a^{-1}.

Định nghĩa 2.12:

Phép chia của với a cho $b \bmod n$ là tích của *a* và $b^{-1}\mathrm{mod}n$ tích này được xác định nếu *b* là phần tử khả nghịch.

Định lý 2.4:

Cho $a \in \mathbb{Z}_n$, khi đó *a* là khả nghịch nếu và chỉ nếu: $(a, n) = 1$.

Ví dụ:

Các phần tử khả nghịch trong $\mathbb{Z}_9$ là 1, 2, 4, 5, 7 và 8. Chẳng hạn $4^{-1} = 7$ vì $4.7 \equiv 1(\mathrm{mod}9)$.

Định lý 2.5:

Cho $d = (a, n)$, phương trình đồng dư $ax \equiv b(\mathrm{mod}n)$ có nghiệm *x* nếu và chỉ nếu $d|b$, trong trường hợp này có đúng d nghiệm nằm giữa 0 và n - 1, những nghiệm này là tất cả các đồng dư theo modulo $n|b$.

Định lý 2.6:

Nếu các số nguyên $n_1, n_2, \dots, n_k$ là nguyên tố cùng nhau từng đôi một thì hệ các phương trình đồng dư:

$$x \equiv a_1 \left(\mathrm{mod}\, n_1\right)$$
$$x \equiv a_2 \left(\mathrm{mod}\, n_2\right)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x \equiv a_k \left(\mathrm{mod}\, n_k\right)$$

sẽ có nghiệm duy nhất theo modulo $n (n = n_1, n_2, \ldots, n_k)$.

Thuật toán Gausse

Nghiệm *x* của hệ phương trình đồng dư trong định lý phần dư China có thể được tính bằng:

$$x = \sum_{i=1}^{k} a_i N_i M_i \,\mathrm{mod} n$$

Trong đó $N_i = n/n_i$ và $M_i = N_i^{-1} \mathrm{mod} n_i$

Các tính toán này có thể được thực hiện trong $0((\lg n)^2)$ các phép toán trên bit.

Ví dụ: Cặp phương trình đồng dư $x \equiv 3(\mathrm{mod}7), x \equiv 7(\mathrm{mod}13)$ có nghiệm duy nhất $x \equiv 59(\mathrm{mod}91)$.

Định lý 2.7: Nếu $(n_1, n_2) = 1$ thì cặp phương trình đồng dư.

$x \equiv a(\mathrm{mod} n_1), x \equiv a(\mathrm{mod} n_2)$ có một nghiệm duy nhất $x \equiv a(\mathrm{mod} n_1, n_2)$.

Định nghĩa 2.13: Nhóm nhân của $\mathbb{Z}_n$ là $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | (a, n) = 1\}$.

Đặc biệt, nếu n là số nguyên tố thì $\mathrm{Z}_n^* = \{a | 1 \leq a \leq n - 1\}$.

Định nghĩa 2.14: Cấp của Z_n^* là số các phần tử trong Z_n^* (ký hiệu $|\mathrm{Z}_n^*|$)

Theo định nghĩa của hàm Phi-Euler ta thấy:

$$|\mathrm{Z}_n^*| = \varphi(n) \qquad (2.3)$$

Chú ý: nếu $a \in \mathbb{Z}_n^*$ và $b \in \mathrm{Z}_n^*$ thì $a, b \in \mathbb{Z}_n^*$ và bởi vậy $\mathbb{Z}_n^*$ là đóng đối với phép nhân.

Định lý 2.8: Cho *p* là một số nguyên tố:

(1) Định lý Euler: Nếu $a \in \mathbb{Z}_n^*$ thì $a^{\varphi(n)} \equiv 1(\mathrm{mod} n)$.

(2) Nếu n là tích của các số nguyên khác nhau và nếu $r \equiv s(\mathrm{mod}\varphi(n))$ thì $a^r \equiv a^s(\mathrm{mod}n)$ đối với mọi số nguyên a. Nói một cách khác khi làm việc với modulo *n* thì các số mũ có thể được rút gọn theo modulo $\varphi(n)$.

Định lý 2.9:

Cho *p* là một số nguyên tố:

(1) Định lý Ferma: Nếu $(a,p) = 1$ thì $a^{p-1} \equiv 1(\mathrm{mod}p)$.

(2) Nếu $r \equiv s(\mathrm{mod}p-1)$ thì $a^r \equiv a^s(\mathrm{mod}p)$ đối với mọi số nguyên a. Nói một cách khác khi làm việc với modulo của một số nguyên tố *p* thì các luỹ thừa có thể được rút gọn theo modulo $p - 1$.

(3) Đặc biệt $a^p \equiv a(\mathrm{mod}p)$ với mọi số nguyên a.

Định nghĩa 2.15:

Cho $a \in \mathbb{Z}_n^*$. Cấp của *a* (ký hiệu là $ord(a)$) là số nguyên dương nhỏ nhất *t* sao cho $a^t \equiv 1(\mathrm{mod}n)$.

Định nghĩa 2.16:

Cho $a \in \mathbb{Z}_n^*, ord(a) = t$ và $a^s \equiv 1(\mathrm{mod}n)$ khi đó *t* là ước của *s*.

Đặc biệt $t|\varphi(n)$.

Ví dụ: Cho $n = 21$, khi đó $\mathrm{Z}_{21}^* = \{1,2,3,4,5,8,10,11,13,16,17,19,20\}$

Chú ý rằng $\varphi(21) = \varphi(7).\varphi(3) = 12 = |\mathrm{Z}_{21}^*|$. Cấp của các phần tử trong $\mathbb{Z}_{21}^*$ được nêu trong bảng sau:

$a \in \mathbb{Z}_{21}^*$	1	2	4	5	8	10	11	13	16	17	19	20
$ord(a)$	1	6	3	6	2	6	6	2	3	6	6	2

Định nghĩa 2.17: Cho $\alpha \in \mathbb{Z}_n^*$. Nếu cấp của α là $\varphi(n)$ thì α được gọi là phần tử sinh hay phần tử nguyên thuỷ của $\mathbb{Z}_n^*$. Nếu $\mathbb{Z}_n^*$ có một phần tử sinh thì $\mathbb{Z}_n^*$ được gọi là cyclic.

Các tính chất của các phần tử sinh của Z_n^*

(1) $\mathbb{Z}_n^*$ có phần tử sinh nếu và chỉ nếu $n = 2, 4, p^k$ hoặc là $2p^k$, trong đó p là một số nguyên tố lẻ và $k \geq 1$. Đặc biệt, nếu p là một số nguyên tố thì $\mathbb{Z}_n^*$ có phần tử sinh.

(2) Nếu α là một phần tử sinh của $\mathbb{Z}_n^*$ thì:

$$\mathbb{Z}_n^* = \{\alpha^i \mathrm{mod} n | 0 \leq i \leq \varphi\,(n) - 1\} \qquad (2.4)$$

(3) Giả sử rằng α là một phần tử sinh của $\mathbb{Z}_n^*$ khi đó $b = \alpha^i \mathrm{mod} n$ cũng là một phần tử sinh của $\mathbb{Z}_n^*$ nếu và chỉ nếu $\big(i, \varphi(n)\big) = 1$. Từ đó ta rút ra rằng nếu $\mathbb{Z}_n^*$ là cyclic thì số các phần tử sinh là $\varphi\big(\varphi(n)\big)$.

(4) $\alpha \in \mathbb{Z}_n^*$ là một phần tử sinh của $\mathbb{Z}_n^*$ nếu và chỉ nếu $\alpha^{\varphi(n)/p} \neq 1(\mathrm{mod} n)$ đối với mỗi nguyên tố p của $\varphi(n)$.

Ví dụ: Z_{21}^* không là cyclic vì nó không chứa một phần tử có cấp $\varphi(21) = 12$ (Chú ý rằng 21 không thoả mãn điều kiện (1) ở trên).

$\mathbb{Z}_{25}^*$ là cyclic và có một phần tử sinh $\alpha = 2$.

Định nghĩa 2.18: Cho $a \in \mathbb{Z}_n^*$, a được gọi là thặng dư bậc hai modulo n (hay bình phương của modulo n) nếu tồn tại $x \in \mathbb{Z}_n^*$ sao cho $x^2 \equiv a(\mathrm{mod} n)$. Nếu không tồn tại x như vậy thì a được gọi là thặng dư không bậc hai $mod\ n$. Tập tất cả các thặng dư bậc hai modulo n được ký hiệu là Q_n còn tập tất cả các thặng dư không bậc hai được ký hiệu là $\overline{Q_n}$. Cần chú ý rằng theo định nghĩa $0 \notin \mathrm{Z}_n^*$. Bởi vậy $0 \notin Q_n$ và $0 \notin \overline{Q_n}$.

Định lý 2.10: Cho p là một số nguyên tố và α là một phần tử sinh của $\mathbb{Z}_p^*$. Khi đó $a \in \mathbb{Z}_n^*$ là một thặng dư bậc hai modulo p nếu và chỉ nếu $a = \alpha^i \mathrm{mod}\, p$, trong đó i là một số *nguyên chẵn*. Từ đó rút ra:

$$\big|Q_p\big| = \frac{(p-1)}{2} \text{ và } \big|\overline{Q_p}\big| = \frac{(p-1)}{2}$$

tức là một nửa số phần tử trong $\mathbb{Z}_p^*$ là các thặng dư bậc hai và nửa còn lại thặng dư không bậc hai.

Ví dụ: $\alpha = 6$ là một phần tử sinh của $\mathbb{Z}_{13}^*$. Các luỹ thừa của α được liệt kê ở bảng sau đây:

i	1	2	3	4	5	6	7	8	9	10	11	12
$\alpha^i \bmod 13$	6	10	8	9	2	12	7	3	5	4	11	1

Bởi vậy $Q_{13} = \{1, 3, 4, 9, 10, 12\}, \overline{Q_{13}} = \{2, 5, 6, 7, 8, 11\}$

Định lý 2.11: Cho *n* là tích của hai số nguyên tố lẻ khác nhau *q* và *p*, *n* = *p.q*, khi đó $a \in Z_n^*$ là một thặng dư bậc hai modulo *n* nếu và chỉ nếu $a \in Q_p$ và $a \in Q_q$. Điều đó dẫn tới:

$$|Q_n| = |Q_q||Q_p| = \frac{(p-1)(q-1)}{4}$$

Và

$$|\overline{Q_n}| = \frac{3(p-1)(q-1)}{4}$$

Ví dụ: Cho $n = 21$. Khi đó :

$$Q_{21} = \{1, 4, 16\};\ \overline{Q_{21}} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$$

Định nghĩa 2.19: Cho $a \in Q_n$, nếu $x \in \mathbb{Z}_n^*$ thoả mãn $x^2 \equiv a (\bmod n)$thì *x* được gọi là căn bậc hai của $a \bmod n$.

Định lý 2.12: Nếu *p* là một số nguyên tố lẻ và $a \in Q_n$ thì *a* được gọi là căn bậc hai theo modulo *p*.

Tổng quát hơn, cho $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, trong đó p_i là các số nguyên tố lẻ phân biệt và $e_i \geq 1$. Nếu $a \in Q_n$ thì có đúng 2^k căn bậc hai khác nhau theo modulo *n*.

Ví dụ:

- Các căn bậc 2 của $12\ mod\ 37$ là 7 và 30.

- Các căn bậc 2 của $121\ mod\ 315$ là 11, 74, 101, 151, 164, 214, 241 và 304.

2.1.1.4. Một số thuật toán trong $\mathbb{Z}_n$

Cho *n* là một số nguyên dương. Các phần tử của $\mathbb{Z}_n$ sẽ được biểu thị bởi các số nguyên $Q_{21} = \{1,0, 1, 2, \dots, n-1\}$.

Ta thấy rằng, nếu $a, b \in \mathbb{Z}_n$ thì

$$(a+b) \bmod n \begin{cases} a+b & \text{với } a+b < n \\ a+b-r & \text{với } a+b \geq n \end{cases}$$

Bởi vậy phép cộng (và trừ) theo modulo có thể thực hiện được mà không cần phép chia dài. Phép nhân modulo của *a* và *b* có thể được thực hiện bằng cách nhân các số nguyên thông thường rồi lấy phần dư của kết quả sau khi chia cho *n*. Các phần tử nghịch đảo trong Z_n có thể được tính bằng cách dùng thuật toán Euclid mở rộng (như mô tả tại mục 2.1.1.2).

a) Thuật toán tính số nghịch đảo trong $\mathbb{Z}_n$

Trong lý thuyết số, vành $\mathbb{Z}_n$ được định nghĩa là vành thương của $\mathbb{Z}$ với quan hệ đồng dư theo modulo *n* (là quan hệ tương đương) mà các phần tử của nó là các lớp đồng dư theo modulo *n* (*n* là số nguyên dương lớn hơn 1). Ta cũng có thể xét $\mathbb{Z}_n$ chỉ với các đại diện của nó. Khi đó:

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

Phép cộng và nhân trong $\mathbb{Z}_n$ là phép toán thông thường được rút gọn theo modulo m:

$$a + b = (a + b) \bmod n$$
$$a * b = (a * b) \bmod n$$

Phần tử *a* của $\mathbb{Z}_n$ được gọi là khả nghịch trong $\mathbb{Z}_n$ hay khả nghịch theo modulo *n* nếu tồn tại phần tử a' trong $\mathbb{Z}_n$ sao cho $a * a' = 1$ trong $\mathbb{Z}_n$ hay $a * a' \equiv 1 (\bmod n)$. Khi đó a' được gọi là nghịch đảo modulo *n* của *a*. Trong lý thuyết số đã chứng minh rằng, số *a* là khả nghịch theo modulo *n* khi và chỉ khi ƯCLN của *a* và *n* bằng 1.

Khi đó tồn tại các số nguyên *x, y* sao cho

$$n * x + a * y = 1 \qquad (2.5)$$

Đẳng thức này lại chỉ ra y là nghịch đảo của a theo modulo n. Do đó có thể tìm được phần tử nghịch đảo của *a* theo modulo *m* nhờ thuật toán Euclid mở rộng khi chia n cho a.

VÀO	: $a \in \mathbb{Z}_n$
RA	: $a^{-1} \bmod n$ (nếu tồn tại)

(1) Dùng thuật toán Euclid mở rộng để tìm các số nguyên *x* và *y* sao cho: $ax + ny = d$ trong đó $d = (a, n)$.

(2) Nếu $d > 1$ thì $a^{-1} \bmod n$ không tồn tại.

Ngược lại $return(x)$

Phép luỹ thừa theo modulo có thể được thực hiện có hiệu quả bằng thuật toán nhân và bình phương có lặp. Đây là một thuật toán rất quan trọng trong nhiều thủ tục mật mã. Cho biểu diễn nhị phân của *k* là:

$$\sum_{i=0}^{t} k_i 2^i \text{ trong đó mỗi } k_i \in \{0, 1\}$$

Khi đó:

$$a^k = \prod_{i=0}^{t} a^{k_i 2^i} = (a^{2^0})^{k_0} (a^{2^1})^{k_1} \dots (a^{2^t})^{k_t}$$

b) Thuật toán bình phương và nhân có lặp để lấy luỹ thừa trong $\mathbb{Z}_n$

VÀO: $a \in \mathbb{Z}_n$ và số nguyên $k, (0 \le k \le n)$ có biểu diễn nhị phân:

$$k = \sum_{i=0}^{t} k_i 2^i$$

RA : $a^k \bmod n$

(1) Đặt $b \leftarrow 1$. Nếu $k = 0$ thì $return(b)$

(2) Đặt $A \leftarrow a$

(3) Nếu $k_0 = 1$ đặt $b \leftarrow a$

(4) For *i* from 1 to *t* do

(4.1) Đặt $A \leftarrow A^2 \bmod n$.

(4.2) Nếu $k_i = 1$ thì đặt $b \leftarrow A.b \bmod n$

(5) Return (*b*)

Ví dụ: Bảng sau chỉ ra các bước tính toán $5^{596} \bmod 1234 = 1013$

i	0	1	2	3	4	5	6	7	8	9
k_i	0	0	1	0	1	0	1	0	0	1
A	5	25	625	681	1011	369	421	779	947	925
b	1	1	625	625	67	67	1059	1059	1059	1013

Số các phép toán bit đối với phép toán cơ bản trong $\mathbb{Z}_n$ được tóm lược trong bảng dưới đây.

Phép toán		Độ phức tạp bit
Cộng modulo	$a + b$	$0(\lg n)$
Trừ modulo	$a - b$	$0(\lg n)$
Nhân modulo	ab	$0((\lg n)^2)$
Nghịch đảo modulo	$a^{-1} \mathrm{mod} n$	$0((\lg n)^2)$
Luỹ thừa modulo	$a^k \mathrm{mod} n, k < n$	$0((\lg n)^3)$

Nhận xét

Cho p là một số nguyên tố lẻ. Mặc dù đã biết rằng một nửa các phần tử trong $\mathbb{Z}_p^*$ là các thặng dư không bậc hai theo modulo p nhưng không có một thuật toán xác định theo thời gian đa thức nào được biết để tìm.

Một thuật toán ngẫu nhiên tìm một thặng dư không bậc hai là chọn ngẫu nhiên các số nguyên $a \in \mathbb{Z}_p^*$ cho tới khi số đó thoả mãn $\left(\frac{a}{p}\right) = -1$. Phép lặp đối với số được chọn trước khi tìm được một thặng dư bậc hai là 2 và bởi vậy thuật toán được thực hiện theo thời gian đa thức.

2.1.2. Một số cấu trúc đại số

2.1.2.1. Nhóm: $\langle G, * \rangle$

Nhóm $\langle G, * \rangle$ là một tập hợp G gồm các phần tử với một phép toán 2 ngôi, ký hiệu * (là một ánh xạ từ tập $G \times G \rightarrow G$) thỏa mãn các tính chất sau:

- Tính đóng: Nếu $a, b \in \mathrm{G} \rightarrow a * b = c \in \mathrm{G}$;

- Phần tử đơn vị (trung hòa): Trong G tồn tại một phần tử được gọi là phần tử đơn vị e sao cho với $\forall a \in \mathrm{G}$ thì: $a * e = e * a = a$;

- Phần tử nghịch đảo: Với mỗi phần tử $a \in \mathrm{G}$ tồn tại một phần tử a^{-1}, gọi là phần tử nghịch đảo của a, sao cho: $a^{-1} * a = a * a^{-1} = e$;

- Tính kết hợp: $(a * b) * c = a * (b * c)$ với $\forall a, b, c \in \mathrm{G}$

Nếu $a * b = b * a$ thì nhóm được gọi là nhóm giao hoán.

Ví dụ: Tập các số nguyên $\mathbb{Z}$ với phép toán cộng (+) tạo nên một nhóm giao hoán với phần tử đơn vị là 0.

Nhóm G gọi là hữu hạn nếu như tập G có số lượng phần tử hữu hạn và trường hợp còn lại gọi là vô hạn.

Số lượng phần tử của tập hữu hạn G được gọi là bậc của G, được ký hiệu là $|\mathrm{G}|$.

Nếu $\mathrm{H} \in \mathrm{G}$ và $\langle \mathrm{H}, * \rangle$ tạo nên một nhóm thì H được gọi là nhóm con của G. Cấp của H là ước của cấp của G.

2.1.2.2. Nhóm cyclic

Nói một cách đơn giản, nhóm có biểu diễn vành thì được gọi là nhóm vành.

Nhóm G được gọi là nhóm cyclic, nếu như tồn tại phần tử $a \in \mathrm{G}$, sao cho đối với $\forall b \in G$ tồn tại số nguyên $i \geq 0$, thỏa mãn điều kiện $b = a^i$. Phần tử a gọi là phần tử sinh của nhóm G. Nếu nhóm G sinh ra bởi a, thì ký hiệu $G =< a >$.

Ví dụ: Xét nhóm nhân: $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Ta có:

$$2^0 = 1 \qquad 2^5 = 10$$
$$2^1 = 2 \qquad 2^6 = 9$$
$$2^2 = 4 \qquad 2^7 = 7$$
$$2^3 = 8 \qquad 2^8 = 3$$
$$2^4 = 5 \qquad 2^9 = 6$$

Ta có thể viết: $\mathbb{Z}_{11}^* = \{2^{\mathrm{i}} \mathrm{mod} 11\}$.

Phần tử α được gọi là có cấp k nếu n là số nguyên dương nhỏ nhất thỏa mãn $\alpha^k \equiv 1 \mathrm{mod} n$.

Ở ví dụ trên ta có ord(2) = ord(8) = ord(7) = ord(9) = 10.

2.1.2.3. Vành: $\langle R, +, * \rangle$

Vành R là một tập hợp các phần tử với hai phép toán trong hai ngôi (Phép cộng (+), phép nhân ($*$)) thỏa mãn các tính chất sau:

- $\langle R, + \rangle$ là một nhóm giao hoán đối với phép cộng. Phần tử đơn vị đối với phép cộng (không) được ký hiệu 0;

- $\langle R, * \rangle$ có tính phân phối đối với phép cộng:

$$\forall a, b, c \in R: a * (b + c) = a * b + a * c$$
$$(b + c) * a = b * a + c * a$$

- $\langle R, * \rangle$ có tính kết hợp: $\forall a, b, c \in R: (a * b) * c = a * (b * c)$

- Đối với phép * vành R phù hợp theo các tiên đề đóng kín, kết hợp. Phần tử đơn vị đối với phép nhân (đơn vị) được ký hiệu 1, với $1 \neq 0$.

Vành giao hoán là vành R trong đó phép nhân có tính chất giao hoán.

Vành trong đó phép nhân có phần tử đơn vị được gọi là vành có đơn vị.

Tập con A của R được gọi là vành con của R nếu chính A là một vành với hai phép cộng và nhân trên R.

2.1.2.4. Trường $\langle F, +, * \rangle$

Nếu các phần tử khác không của vành tạo thành nhóm tương ứng với phép nhân thì gọi vành đó là trường [11, 63].

Trường F là một tập hợp các phần tử với hai phép toán trong hai ngôi thỏa mãn:

- $\langle F, + \rangle$ là một nhóm cộng;

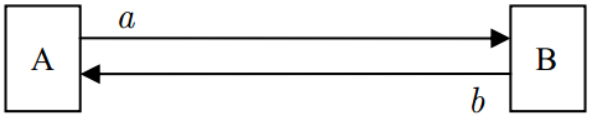
- $\langle F^*, * \rangle$ là một nhóm đối với phép nhân.

Trong đó: $F^* = F \backslash \{0\}$.

Ví dụ: Trường nhị phân GF(2): Trường này chỉ có hai phần tử 0 và 1.

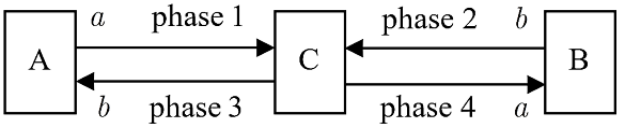
2.1.3. Đề xuất xây dựng mã mạng trên các vành số

Xét mô hình giao tiếp giữa các nút trong một mạng không dây thông thường. Nếu các nút ở xa việc truyền thông tin cậy là khó khăn, ngay cả khi mã hóa kênh được sử dụng. Xét mô hình truyền tin thông thường giữa hai nút là A và B trong Hình 2.1.



Hình 2.1. Mô hình truyền tin giữa hai nút

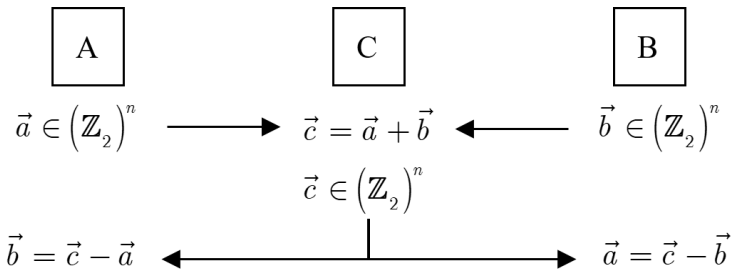
Trên thực tế, để đảm bảo việc truyền tin tin cậy giữa A và B người ta có thể dùng hệ thống vô tuyến cộng tác (cooperative radio - CR). Hệ thống này cho phép cung cấp tốc độ truyền dẫn cao hơn trên hệ thống truy nhập vô tuyến cũng như khả năng tạo vùng phủ rộng hơn. Xét hai nút A và B của một mạng không dây, hệ thống CR sử dụng thêm một nút chuyển tiếp C (nằm giữa A và B), với quá trình truyền tin trải qua 4 pha như mô tả trong Hình 2.2.



Hình 2.2. Mô hình truyền thông vô tuyến cộng tác

Trong đó, *a*, *b* là thông tin tương ứng của A và B.

Theo ý tưởng của Ahlswede, phương thức mã mạng đơn giản có thể được thực hiện trên không gian tuyến tính, như mô tả ở Hình 2.3:



Hình 2.3. Mô hình truyền thông sử dụng mã mạng

Với mô hình này, quá trình truyền thông giữa A và B sẽ được thực hiện qua 3 pha như sau:

- Pha thứ nhất: thông tin truyền từ A, B tới C. Nút A, B lần lượt gửi $\vec{a}, \vec{b}$ tới nút C

- Pha thứ hai: Nút C thực hiện phép tính $\vec{c} = \vec{a} + \vec{b}$ sau đó nút C truyền $\vec{c}$ tới cho cả nút A và nút B

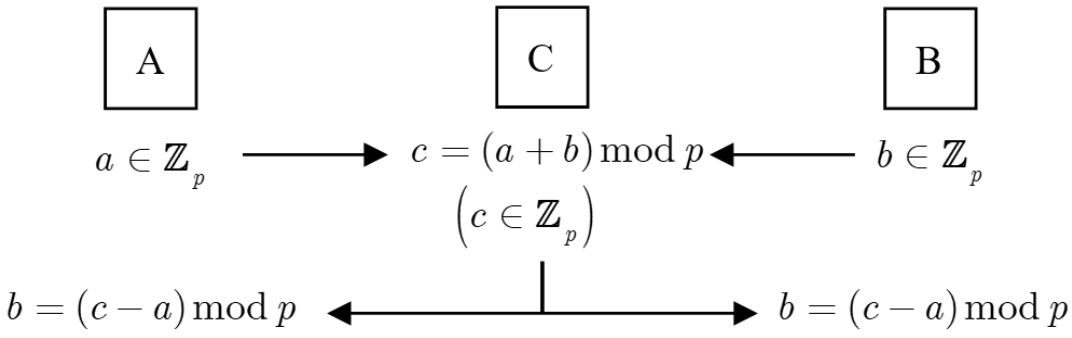
- Pha thứ ba: Nút A và B nhận sau khi nhận được $\vec{c}$ sẽ tiến hành giải mã $\vec{c}$ khôi phục thông tin: $\vec{b} = \vec{c} - \vec{a}$ và $\vec{a} = \vec{c} - \vec{b}$

Thông tin của A và B $(\vec{a}, \vec{b})$ được coi là chuỗi bit hoặc vectơ nhị phân n bit trong không gian tuyến tính n chiều. Phép toán học trong mô hình này là phép cộng vector nhị phân bit.

2.1.3.1. Mã mạng dựa trên phép cộng của vành số

Tiếp tục phát triển phương thức trên, nghiên cứu sinh đã đề xuất phương thức mã hóa thông tin từ A và B bằng các số trong các vành số ($\mathbb{Z}_p$).

Xem xét một số nguyên dương p, tập hợp các số nguyên từ 0 đến p - 1 tạo một vành số $\mathrm{Z}_p = \{0, 1, 2, \ldots, p-1\}$. Có hai phép toán trong $\mathbb{Z}_p$, đó là phép cộng và phép nhân modulo của p. Trong hai phép toán này, phép cộng tạo thành một nhóm đầy đủ. Chúng ta có thể sử dụng nhóm cộng này để thực hiện mã mạng. Mô hình có thể được thực hiện như sau:



Hình 2.4. Mã mạng dựa trên phép cộng của các vành số

Giả sử thông tin của các bên A, B biểu diễn bằng các con số trong vành số $\mathbb{Z}_p$: $a, b \in \mathbb{Z}_p$. Quá trình truyền tin giữa 2 nút A, B theo mã mạng được thực hiện như sau:

- Pha 1: Truyền thông tin: C nhận a, b tương ứng từ A và B.

- Pha 2: C tính

$$c = (a + b) \bmod p \tag{2.6}$$

và sau đó C truyền quảng bá *c* tới cho cả A và B.

- Pha 3: A và B tái tạo lại thông tin cần thiết *a* và *b* sau khi giải mã *c*.

Tại nút A: $b = (c - a) \bmod p$

Tại nút B: $a = (c - b) \bmod p$

Ví dụ, Cho $p = 17 \rightarrow \mathbb{Z}_{17} = \{0,1,2, \dots ,16\}$

$a = 13;\ b = 11.$

Ta có: $c = (13 + 11) \bmod 17 = 7$

A và B khôi phục thông tin từ c = 7:

$$b = (c - a) \bmod 17 = (7 - 13) \bmod 17 = -6 \bmod 17 = 11 \bmod 17$$

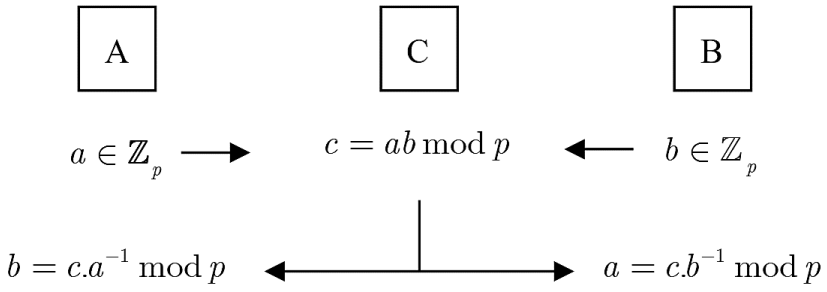
$$a = (c - b) \bmod 17 = (7 - 11) \bmod 17 = -4 \bmod 17 = 13 \bmod 17$$

Chú ý:

- Phương pháp này hiệu quả như phương pháp Ahlswere, nhưng thông tin của A, B và C được thể hiện bằng các số trong Z_p.
- Bất kỳ số (-*n*) nào có thể được tính đơn giản bằng phép tính: $-n \bmod p = (p - n) \bmod p$.

2.1.3.2. Mã mạng dựa trên phép nhân trên vành số

Xét một số nguyên tố p, khi đó vành số $\mathbb{Z}_\mathrm{p}$ trở thành một trường ($\mathbb{Z}_p = GF(p)$). Hai phép cộng và phép nhân trên $\mathbb{Z}_p$ là các nhóm đầy đủ. Chúng ta có thể sử dụng phép nhân để thực hiện mã mạng, như được mô tả trong Hình 2.5.



Hình 2.5. Mã mạng dựa trên phép nhân của các vành số

Xét số nguyên tố p, $a, b \in \mathbb{Z}_p$. Trong đó: a, b tương ứng là thông tin của A, B.

- Pha 1: Truyền thông tin: Nút C nhận a và b từ A và B.

- Pha 2: Nút C thực hiện phép tính:

$$c = a.b \bmod p \tag{2.7}$$

sau đó truyền quảng bá c tới cho cả hai nút A và B.

- Pha 3: A và B lấy lại thông tin cần thiết a và b sau khi giải mã c.

Tại nút A: $b = c.a^{-1} \bmod p$

Tại nút B: $a = c.b^{-1} \bmod p$

Trong đó, a^{-1}, b^{-1} là các số nghịch đảo tương ứng của các số a, b. Các số đó có thể được tính theo thuật toán Euclid mở rộng.

Ví dụ: Xét $\mathbb{Z}_{17}(p = 17)$

- Pha 1: Truyền thông tin:

Giả sử A muốn truyền bản tin a = 3 đến B và B muốn gửi bản tin b = 5 đến A. Nút C nhận được cả hai bản tin a và b.

- Pha 2: Nút C thực hiện phép tính:

$$c = a.b \bmod p = 3 \times 5 \bmod 17 = 15$$

sau đó nút C gửi c = 15 cho cả hai nút A và B.

- Pha 3:

Tại nút A phục hồi bản tin b từ c:

$$b = c.a^{-1} \bmod p = (15 \times 6) \bmod 17 = 5$$

Tại nút B phục hồi bản tin a từ c:

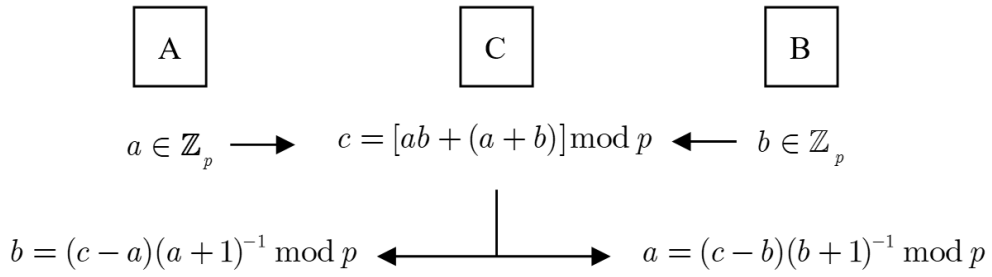
$$a = c.b^{-1}\text{mod}p = (15 \times 7)\text{mod}17 = 3$$

Trong đó: $a^{-1} = 3^{-1}\text{mod}17 = 6$ và $b^{-1} = 5^{-1}\text{mod}17 = 7$ là các số nghịch đảo của a và b.

Chú ý: trong phương thức này a^{-1} và b^{-1} được tính trước theo thuật toán Euclid mở rộng tại mục 2.1.1.2.

2.1.3.3. Mã mạng Affine trên vành số

Xét $\mathbb{Z}_p$ trong đó p là số nguyên tố, $\mathbb{Z}_p = \text{GF}(p)$. Chúng ta có thể sử dụng cả phép cộng và phép nhân trong trường đại số để thực hiện mã mạng Affine, như được mô tả ở Hình 2.6:



Hình 2.6. Mã mạng Affine trên vành số

- Pha 1: Truyền thông tin:

Nút A gửi a tới C và tính $[a + 1]^{-1}$

Tương tự như vậy, nút B gửi b tới C và tính $[b + 1]^{-1}$.

Chú ý: $a, b \neq p - 1$

- Pha 2: Nút C tính:

$$c = [ab + (a + b)]\text{mod}p \tag{2.8}$$

và truyền c tới cho cả hai nút A và B.

- Pha 3: Nút A và B nhận được thông tin cần thiết bằng cách thực hiện phép tính:

Tại nút A:

$$c - a = a.b + b = b(a + 1)$$

$$\Rightarrow b = \frac{c-a}{a+1}$$

Hoặc:

$$b = (c-a)(a+1)^{-1} \quad (2.9)$$

Tại nút B:

$$c - b = a.b + a = a(b+1)$$

$$\Rightarrow a = \frac{c-b}{b+1}$$

Hoặc:

$$a = (c-b)(b+1)^{-1} \quad (2.10)$$

Ví dụ:

Xét $\mathbb{Z}_{17}$ với p = 17 là số nguyên tố.

- *Pha 1:*

Giả sử $a = 7; b = 2, (a, b \in \mathrm{Z}_{17})$

Nút A tính trước:

$$(a+1)^{-1}\mathrm{mod}17 = (7+1)^{-1}\mathrm{mod}17 = 8^{-1}\mathrm{mod}17 = 15$$

Nút B tính trước:

$$(b+1)^{-1}\mathrm{mod}17 = (2+1)^{-1}\mathrm{mod}17 = 3^{-1}\mathrm{mod}17 = 6$$

- *Pha 2:* Nút C nhận được a, b từ hai nút A, B và thực hiện phép tính:

$$c = [a.b + (a+b)]\mathrm{mod}17$$

$$= [7 \times 2 + (7+2)]\mathrm{mod}17$$

$$= 23\mathrm{mod}17 = 6$$

Sau đó C truyền quảng bá $c = 6$ cho cả hai nút A và B.

- Pha 3: Khôi phục thông tin:

Tại nút A (khôi phục b):

$$b = (c-a)(a+1)^{-1}\mathrm{mod}p = (6-7).8^{-1}\mathrm{mod}17$$

$$= (-1 \times 15)\mathrm{mod}17 = -15\mathrm{mod}17 = 2$$

Tại nút B (khôi phục a):

$$a = (c - b)(b + 1)^{-1}\text{mod}p$$
$$= (6 - 2).3^{-1}\text{mod}17$$
$$= (4 \times 6)\text{mod}17 = 7$$

Chú ý:

- Đối với việc thực hiện phép tính các số nghịch đảo, chúng ta có thể sử dụng thuật toán Euclid mở rộng.

- Trong các ví dụ, chúng tôi sử dụng $\mathbb{Z}_p = \text{GF}(p)$, p = 17 (số nguyên tố nhỏ). Mục đích của các ví dụ này là để biết cơ chế thuật toán và dễ dàng trong tính toán.

Trong mã mạng truyền thống, thông tin truyền trong mạng là các vectơ nhị phân. Thông tin trong các nút được mã hóa và giải mã bằng cách thêm các vectơ nhị phân $n - bit$ trong không gian tuyến tính n chiều. Trong mô hình mã hóa mạng dựa trên $\mathbb{Z}_p$, thông tin trong mạng được thể hiện bằng số nguyên. Việc mã hóa và giải mã bản tin được thực hiện bằng cách cộng hoặc nhân các số với modulo của p. Hiệu quả trong việc giảm số phiên truyền của hai phương pháp trên là như nhau nhưng khác nhau về phép toán.

2.2. MÃ MẠNG TRÊN VÀNH ĐA THỨC, TRƯỜNG ĐA THỨC

2.2.1. Vành đa thức

2.2.1.1. Khái niệm vành đa thức

Nếu R là một vành giao hoán thì vành đa thức $R[x]$ là một vành được tạo bởi tập tất cả các đa thức của biến *x* có các hệ số trong R. 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 trường nhị phân $GF(2)$, vành đa thức được ký hiệu $\mathbb{Z}_2[x]/x^n + 1$.

Phép cộng hai đa thức: Xét hai đa thức $a(x) = \sum_{i=0}^{n-1} a_i x^i$ và $b(x) = \sum_{i=0}^{n-1} b_i x^i$, đa thức $c(x)$ là tổng của hai đa thức này và được tính như sau:

$$c(x) = a(x) + b(x) \tag{2.11}$$

Trong đó: $c(x) = \sum_{i=0}^{n-1} c_i x^i$ và $c_i = a_i + b_i$.

Ở đây phép cộng các hệ số a_i và b_i được thực hiện trên trường GF.

Bậc của $c(x)$ được xác định:

$$\deg c(x) = \max(\deg a(x), \deg b(x))$$

Phép nhân hai đa thức:

Xét 2 đa thức $a(x), b(x)$ tích của hai đa thức này được tính như sau:

$$c(x) = a(x).b(x) = (\sum_{i=0}^{n-1} a_i x^i)(\sum_{i=0}^{n-1} a_i x^i) \bmod x^n + 1 \tag{2.12}$$

2.2.1.2. Vành đa thức có 2 lớp kề cyclic

Định nghĩa 2.20: Vành đa thức theo modulo $x^n + 1$ được gọi là vành đa thức có hai lớp kề cyclic nếu phân tích của $x^n + 1$ thành tích của các đa thức bất khả quy trên trường GF(2) có dạng sau [2, 3, 4, 5, 6]:

$$x^n + 1 = (x + 1) \sum_{i=0}^{n-1} x_i \tag{2.13}$$

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

Bổ đề 2.1 (Điều kiện của vành có hai lớp kề)

Vành đa thức theo modulo $x^n + 1$ là một vành đa thức có hai lớp kề cyclic nếu n thoả mãn:

- n phải là một số nguyên tố;

- Phần tử thứ hai phải thoả điều kiện $2^{\varphi(n)/p} \neq 1 \ mod \ n$ với mỗi ước nguyên tố p của $\varphi(n)$. (Trong đó $\varphi(n)$ là hàm phi Euler).

Chứng minh:

Nếu vành đa thức theo modulo $x^n + 1$ là một vành đa thức có hai lớp kề cyclic thì $\mathbb{Z}_n = C_0 \cup C_1$. Trong đó C_0={0}, số lượng các phần tử của C_1 sẽ là : $|C_1| = n - 1$.

Ta thấy rằng C_1 chính là một nhóm nhân cyclic cấp $n - 1$ có phần tử sinh bằng 2. Khi n là một hợp số thì nhóm nhân $\mathbb{Z}_n^*$ của $\mathbb{Z}_n$ sẽ không chứa hết các phần tử khác không của $\mathbb{Z}_n$. Bởi vậy n phải là một số nguyên tố [6].

Từ định nghĩa trên, ta thấy rằng $ord^n 2 = m_1 \leq n - 1$. Để phần tử 2 có cấp $n - 1$, ta thấy rằng phần tử thứ hai phải thoả điều kiện $2^{\varphi(n)/p} \neq 1 \bmod n$, với mỗi p là ước nguyên tố của $\varphi(n)$.

Với $\varphi(n) = n - 1$ khi n là một số nguyên tố.

Căn cứ vào đặc điểm trên của vành đa thức có hai lớp kề cyclic ta sẽ xây dựng thuật toán xác định điều kiện để vành đa thức có hai lớp kề cyclic.

Thuật toán xác định giá trị *n* [2]

Vào: số nguyên tố n **Ra:** Giá trị n thoả mãn.
(1): Tìm phân tích của (n - 1); xác định các ước nguyên tố p_i của phân tích này. (2): Với mỗi p_i tính $2^{n-1/p_i}$ (2.1) Nếu tồn tại p_i sao cho $2^{n-1/p_i} \equiv 1(\bmod n)$ thì n không thoả mãn. (2.2) n thoả mãn trong các trường hợp còn lại.

Theo thuật toán này ta xác định được một số giá trị sau của n đảm bảo vành đa thức theo mod $x^n + 1$ là một vành đa thức có hai lớp kề cyclic.

2.2.1.3. Quan hệ giữa vành đa thức có hai lớp kề cyclic và trường số theo modulo

Xét vành đa thức có hai lớp kề $Z_2[x]/(x^n + 1)$. Trong vành đa thức này tồn tại nhóm nhân cyclic có cấp cực đại [13, 14]:

$$G = \{[a(x)]^i \bmod (x^n + 1), i = 1, 2, 3, \dots, k\} \quad (2.14)$$

Với [13, 14]:

$$k = \max ord a(x) = 2^{n-1} - 1 \quad (2.15)$$

Xét một số nguyên tố p với p có dạng $p = 2^n - 1$. Khi đó vành số modulo Z_p sẽ trở thành trường hữu hạn GF(p) và trên trường này tồn tại một nhóm nhân cyclic $Z_p^* = Z_p/\{0\}$ có cấp $|Z_p^*| = 2^n - 2$, với $\forall a \in Z_p^* \rightarrow \exists a^{-1} \in Z_p^* : aa^{-1} \equiv 1 \bmod p$.

Xét $a(x) \in \mathrm{Z}_2[x]/(x^n+1)$ với $W(a(x))$ lẻ. Khi đó $\exists a^{-1}(x)$ với $W(a^{-1}(x))$ lẻ thỏa mãn:

$$a(x)a^{-1}(x) \equiv 1 \bmod (x^n+1)$$

Do vậy, có thể xây dựng phép tương ứng sau [3]:

$$a(x) = \sum_{i \in I} f_i\, x^i \in \mathrm{Z}_2[x]/(x^n+1)$$

$$\rightarrow a = \sum_{i \in I} f_i\, 2^i \in \mathrm{Z}_p^*$$

và coi $e_0(x) = \sum_{i=0}^{n-1} x^i = 0$.

Khi đó ta có thể coi đây là một ánh xạ 1-1 giữa các phần tử của vành đa thức $\mathrm{Z}_2[x]/(x^n+1)$ với các phần tử của GF(p). Như vậy, vành đa thức có hai lớp kề cyclic và trường GF(p) với $p = 2^n - 1$ (là số nguyên tố) được gọi là tựa đẳng cấu (quasi-isomorphism) [3].

Quan hệ tựa đồng cấu chỉ xảy ra đối với một số vành đa thức có hai lớp kề cyclic đặc biệt, các vành đa thức này được liệt kê dưới đây.

- Số nguyên tố Mersenne: $p = 2^n - 1$

n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 52, 607, 1279, 2203, 3217, 4253, 9689, 9941, 19937,… , 74207281.

- Vành đa thức có hai lớp kề cyclic $Z_2[x]/x^n + 1$:

n = 5, 11, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131,… , 523, 613, 1277, 2213, 3203, 3253, 4253, …, 9941.

Ta có thể so sánh việc thực hiện các phép toán cộng và nhân trên hai cấu trúc này như bảng bên dưới.

Bảng 2.2. Phép toán cộng và nhân trên vành đa thức và trường số.

Phép tính	Vành đa thức $Z_2[x]/(x^n+1)$	Trường số GF(p)
Phép cộng	$a(x)=\sum_{i\in I\subset Z} a_i x^i;\ b(x)=\sum_{i\in J\subset Z} b_j x^i$ $c(x)=a(x)+b(x)=\sum_{k\in J\subset Z_n} c_k x^k$ $K=(I\cup J)-(I\cap J)$	$a,b\in \mathrm{GF}(p)$ $c=a+b$ $\equiv (a+b)\mathrm{mod}p$
Phép nhân	$c(x)=a(x)b(x)$ $\equiv a(x)b(x)\mathrm{mod}(x^n+1)$	$c=a.b$ $\equiv (a.b)\mathrm{mod}p$

Nhận xét: Có thể sử dụng quan hệ tựa đồng cấu này để xây dựng một số hệ mật trên vành đa thức có 2 lớp kề cyclic.

- Một số ứng dụng của vành đa thức có 2 lớp kề cyclic:

+ Tạo m-dãy và m-dãy lồng ghép trên vành đa thức có hai lớp kề cyclic [15].

+ Xây dựng mã cyclic và cyclic cục bộ [2, 6, 12, 13, 14]

+ Một số hệ mật mã [4, 5]...

2.2.2. Thuật toán tính lũy thừa đa thức

Thông thường các hệ mật sử dụng bài toán logarit rời rạc đều phải thực hiện lũy thừa các số theo modulo trên trường số và người ta thường sử dụng thuật toán bình phương và nhân (như trình bày tại mục 2.1.1.4).

Tương tự, với các đa thức, dựa vào một tính chất đặc biệt của đa thức sau đây, có thể thực hiện thuật toán tính lũy thừa cho đa thức như sau [5].

Xét đa thức $a(x)\in \mathbb{Z}_2[x]/(x^n+1)$:

$$a(x)=a_0x^0+a_1x^1+a_2x^2+\ldots+a_{n-1}x^{n-1} \tag{2.16}$$

Biểu diễn dạng số mũ (chỉ cho các $a_i=1$):

$$a(x)\leftrightarrow \hat{a}=\left(a_0 0,\ a_1 1,\ a_2 2,\ldots,\ a_{n-1}(n-1)\right) \tag{2.17}$$

với $a_i\in[0,1]$.

+ Nếu một số k có dạng $k = 2^u$ khi đó:

$$\left[a(x)\right]^k = \left[a(x)\right]^{2^u} = \sum_{i=0}^{n-1} a_i x^{2^u i \bmod n} \tag{2.18}$$

Dạng mũ:

$$\left(\hat{a}\right)^k = \left(a_0 0.2^u \bmod n,\ a_1 1.2^u \bmod n, ..., a_{n-1}(n-1).2^u \bmod n\right) \tag{2.19}$$

Chứng minh:

$$[a(x)]^k = [a(x)]^{2^u} = ((([a(x)]^{\overbrace{2}^{u \text{ lần}}})^2)^{2...2})$$

Mà :

$$[a(x)]^2 = \sum_{i=0}^{n-1} a_i^2 x^{2i \bmod n} + 2 \sum_{\substack{i,j=0; \\ i \neq j}}^{n-1} a_i a_j x^{(i+j) \bmod n}$$

Ta thấy với $i \neq j$:

$$2a_i a_j x^{(i+j) \bmod n} = a_i a_j x^{(i+j) \bmod n} + a_i a_j x^{(i+j) \bmod n} = 0$$

do phép cộng đa thức là cộng modulo 2.

Vì thế: $2 \sum_{\substack{i,j=0; \\ i \neq j}}^{n-1} a_i a_j x^{(i+j) \bmod n} = 0$

Vậy ta có: $[a(x)]^2 = \sum_{i=0}^{n-1} a_i^2 x^{2i \bmod n}$

Tương tự như thế ta tính được:

$$[a(x)]^4 = ([a(x)]^2)^2 = \sum_{i=0}^{n-1} (a_i^2 x^{2i \bmod n})^2 = \sum_{i=0}^{n-1} a_i^4 x^{4i \bmod n}$$

Tổng quát:

$$[a(x)]^{2^u} = \sum_{i=0}^{n-1} a_i^{2^u} x^{2^u i \bmod n} = \sum_{i=0}^{n-1} a_i x^{2^u i \bmod n} \tag{2.20}$$

Chú ý: do $a_i \in [0,1]$ nên $a_i^{2^u} = a_i$

Điều phải chứng minh

Ví dụ: xét $n = 5;\ a(x) = 1 + x^2 + x^4 \leftrightarrow \hat{a} = (0,2,4)$

- Nếu $k = 2$ thì (tính theo dạng đa thức):

$$[a(x)]^2 = 1 + x^{2.2 \bmod 5} + x^{2.4 \bmod 5} = 1 + x^3 + x^4$$

- Nếu $k = 2^3 = 8$ thì (tính theo dạng mũ):

$$\begin{aligned}(\hat{a})^8 &= (0*8 \bmod 5,\ 2*8 \bmod 5,\ 4*8 \bmod 5) \\ &= (0,1,2)\end{aligned}$$

Tức là để tính lũy thừa $[a(x)]^{2^u}$ *ta chỉ việc nhân các số mũ của từng đơn thức* x *trong* $a(x)$ *với* 2^u *rồi lấy modulo theo* n *như biểu thức (2.18), (2.19).*

Dựa vào tính chất này của đa thức ta có thể tính lũy thừa bất kỳ cho đa thức $a(x)$ như sau:

Cho số k nguyên dương và có phân tích như sau:

$$k = \sum_t 2^{u_t} = \sum_t k_t \tag{2.21}$$

Ví dụ: $k = 19 = 2^0 + 2^1 + 2^4 = 1 + 2 + 16$

$\hat{u} = (0,1,4);\ \overline{k} = [k_t] = [1,2,16]$

Khi đó phép lũy thừa $[a(x)]^k \bmod (x^n + 1)$ có thể tính như sau:

$$\left[a(x)\right]^k = \prod_t [a(x)]^{k_t} = \prod_t [a(x)]^{2^{u_t}} \tag{2.22}$$

Thuật toán tính lũy thừa của đa thức theo modulo $x^n + 1$ như trong bảng 2.2.

Bảng 2.3. Thuật toán tính lũy thừa các đa thức theo modulo x^n+1

Vào: n, $\hat{a}=(a_1,a_2,...,a_r)_{1\times r}, \overline{k}=[k_1,k_2,...,k_t]_{1\times t}$ **Ra:** $\hat{b}=(\hat{a})^k \bmod(x^n+1)$
[**1**] $\hat{b}\leftarrow(0)$, if $k=0$ then return $\hat{b}$ [**2**] For i from 1 to t do: [2.1] for j from 1 to r do: $A_j \leftarrow a_j.k_i \bmod n$ [2.2]: $\hat{b}\leftarrow \hat{b}.\hat{A}$ [**3**] **Return** ($\hat{b}$)

Chú thích

+ Số n đảm bảo $\mathbb{Z}_2[x]/(x^n+1)$ là vành đa thức có 2 lớp kề cyclic và $p=2^n-1$ là số nguyên tố (như mô tả trong bảng 2.1).
+ Đa thức $a(x)\in\mathbb{Z}_2[x]/(x^n+1)$; dạng số mũ $a(x)\leftrightarrow\hat{a}=(a_1,a_2,...,a_r)_{1\times r}$ độ dài $\hat{a}$ là $r\le n$.
+ Số nguyên k, $(0\le k\le 2^{n-1}-1)$; k được biểu diễn thành một vector bao gồm t số thập phân $\overline{k}=[k_1,k_2,...,k_t]_{1\times t}$; trong đó $k_i=2^{u_t}$:

$$k=\sum_t k_t \leftrightarrow \overline{k}=[k_t]_{1\times t}$$

+ Mục [1]: $\hat{b}=(0)\leftrightarrow b(x)=2^0=1$;

Mục [2.1] tập các số A_j là biểu diễn dạng mũ của đa thức $A(x)$; $A(x)\leftrightarrow\hat{A}=(A_1,A_2,...,A_r)$. Trong một số ngôn ngữ lập trình (như Matlab) có thể dễ dàng tính được ngay toàn bộ các phần tử trong $\hat{A}$ mà không cần phải dùng vòng lặp. Tức là ta có thể tính trực tiếp

$(A_j)\leftarrow(a_j.k_i \bmod n): j=1,2,...,r$

+ Mục [2.2] là phép *nhân đa thức* theo modulo, đây là phép nhân bình thường trên vành đa thức được lấy theo modulo của $x^n + 1$ (tính như công thức 2.2).
+ Kết quả dạng mũ: $\hat{b} = (\hat{a})^k \bmod(x^n + 1)$

** Ví dụ:*

Xét $n = 5;\ a(x) = 1 + x^2 + x^4 \leftrightarrow \hat{a} = (0,2,4)_{1\times 3}$ và

$k = 13 = 1 + 4 + 8 = 2^0 + 2^2 + 2^3$, biểu diễn k như sau: $\overline{k} = [1,4,8]_{1\times 3}$.

Ta có: $r = 3; t = 3$

Khi đó $\hat{b} = \hat{a}^{13}$ được tính như sau:

[1] $\hat{b} \leftarrow (0)$

[2] For i from 1 to 3 do:

- $i = 1$: (với $k_1 = 1$)

  $+ \hat{A} = (A_1, A_2, A_3) = (0*1 \bmod 5,\ 2*1 \bmod 5,\ 4*1 \bmod 5)$

  $= (0,2,4)$

  $+ \hat{b} \leftarrow (0)*(0,2,4) = (0,2,4)$

- $i = 2$: (với $k_2 = 4$)

  $+ \hat{A} = (A_1, A_2, A_3) = (0*4 \bmod 5,\ 2*4 \bmod 5,\ 4*4 \bmod 5)$

  $= (0,3,1)$

  $+ \hat{b} \leftarrow (0,2,4)*(0,3,1) = (0,1,4)$

- $i = 3$: (với $k_3 = 8$)

  $+ \hat{A} = (A_1, A_2, A_3) = (0*8 \bmod 5,\ 2*8 \bmod 5,\ 4*8 \bmod 5)$

  $= (0,1,2)$

  $+ \hat{b} \leftarrow (0,1,4)*(0,1,2) = (1,3,4)$

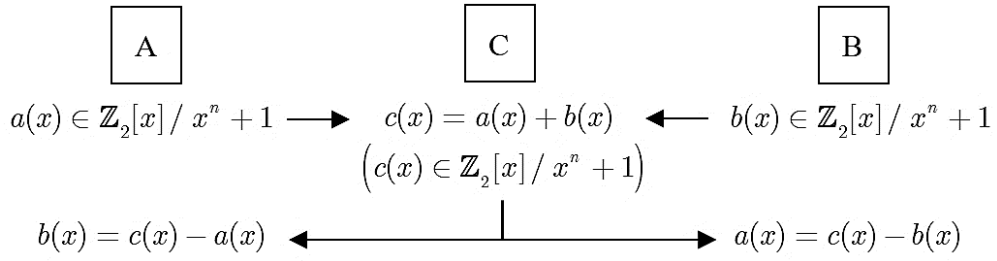
[3] Return $\hat{b} = (1,3,4)$

Vậy kết quả có được là:

$$(1+x^2+x^4)^{13} \bmod (x^5+1) = x+x^3+x^4 \leftrightarrow (1,3,4)$$

2.2.3. Mã mạng dựa trên nhóm cộng của vành đa thức

Theo ý tưởng của Ahlswede, thông tin từ A và B có thể coi như đa thức $a(x)$ và $b(x)$ trong một vành đa thức $\mathbb{Z}_2[x]/x^n+1$. Trong trường hợp này chúng ta thực hiện mã mạng như bên dưới:



Hình 2.7. Mã mạng trên vành đa thức

- Pha thứ nhất: Truyền thông tin:

Nút C nhận thông tin $a(x)$ từ nút A và thông tin $b(x)$ từ nút B.

$a(x), b(x) \in \mathbb{Z}_2[x]\ /(x^n+1)$

- Pha thứ hai: Tại nút C thực hiện phép tính:

$$c(x) = a(x) + b(x) \tag{2.23}$$

sau đó truyền $c(x)$ cho cả nút A và nút B.

- Pha thứ ba: Tại Nút A và B khôi phục thông tin $a(x)$ và $b(x)$ sau khi giải mã $c(x)$:

Tại nút A: $b(x) = c(x) - a(x)$

Tại nút B: $a(x) = c(x) - b(x)$

Chú ý: các phép cộng và trừ ở đây là cho các đa thức.

Ví dụ: Xét vành đa thức $\mathbb{Z}_2[x]/x^5+1$, với $n = 5$.

Giả thiết:

$$a(x) = 1 + x^2 + x^3 \leftrightarrow (023),$$

$$b(x) = 1 + x^2 + x^4 \leftrightarrow (024)$$

Suy ra: $c(x) = a(x) + b(x) = x^3 + x^4 \leftrightarrow (34)$

Nút A và B khôi phục thông tin từ $c(x)$ bằng cách thực hiện phép tính:

$$b(x) = c(x) - a(x) = (34) - (023) = (024),$$
$$a(x) = c(x) - b(x) = (34) - (024) = (023)$$

Chú ý: Ký hiệu $a(x) = (023)$ là biểu diễn dạng số mũ của đa thức: $a(x) = 1 + x^2 + x^3$, nó có nghĩa là: $(023) \leftrightarrow x^0 + x^2 + x^3 = 1 + x^2 + x^3$. Tương tự với các đa thức khác.

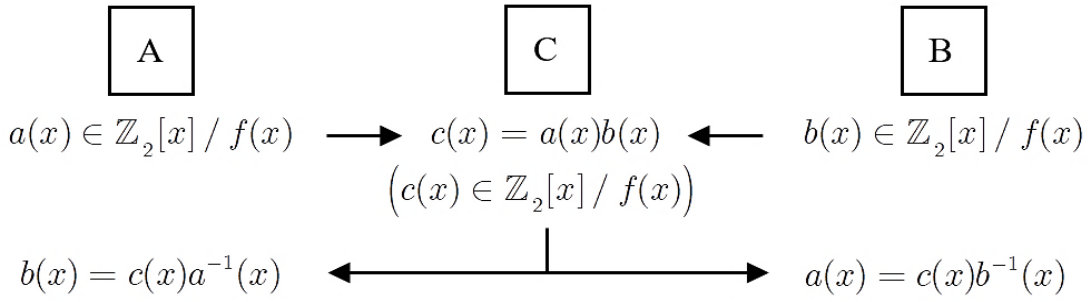
Như vậy, chúng ta thấy phương pháp này hiệu quả như phương pháp của Ahlswere. Tuy nhiên, thông tin của A, B và C được trình bày bởi các đa thức trong vành đa thức.

2.2.4. Mã mạng trên trường đa thức

Xét một đa thức nguyên thủy $f(x)$ có bậc m với các hệ số trong GF(2), từ đó $Z_2[x]/f(x)$ là một trường đa thức [62].

2.2.4.1. Mã mạng sử dụng phép nhân trên trường đa thức

Quá trình mã mạng có thể được mô tả như Hình 2.8 bên dưới:



Hình 2.8. Mã mạng trên trường đa thức

- Pha thứ nhất: Truyền thông tin

Nút C nhận thông tin là các đa thức $a(x)$ và $b(x)$ từ nút A và B.

Trong đó, $a(x), b(x) \in Z_2[x]/f(x)$; $f(x)$ là một đa thức nguyên thủy; $\deg f(x) = m$; $\deg a(x) < m$; $\deg b(x) < m$.

- Pha thứ hai: Tại nút C thực hiện phép tính:

$$c(x) = a(x).b(x) mod\ f(x) \quad (2.24)$$

rồi sau đó phát quảng bá $c(x)$ tới cả nút A và B.

- Pha thứ ba: Tại nút A và B khôi phục được thông tin $a(x), b(x)$ sau khi giải mã $c(x)$:

Tại nút A: $b(x) = c(x).a^{-1}(x) mod\ f(x)$

Tại nút B: $a(x) = c(x).b^{-1}(x) mod\ f(x)$

Chú ý: $a^{-1}(x)$ và $b^{-1}(x)$ là đa thức nghịch đảo tương ứng của $a(x)$ và $b(x)$.

Ví dụ: Xét $f(x) = 1 + x^2 + x^5 \leftrightarrow (025)$ với $\deg f(x) = m = 5$.

- Pha thứ nhất: Giả sử $a(x) = (023)$ và $b(x) = (024)$. Nút C nhận được cả $a(x)$ và $b(x)$. Sau đó chuyển sang pha 2.

- Pha thứ hai: Tại nút C thực hiện phép tính:

$$c(x) = a(x).b(x) mod f(x) = (023)(024) = (14)$$

rồi sau đó phát quảng bả $c(x)$ tới cả nút A và B.

- Pha thứ ba:

Tại nút A khôi phục thông tin $b(x)$ từ $c(x)$:

$$b(x) = c(x).a^{-1}(x) mod f(x) = (14)(0123) = (024)$$

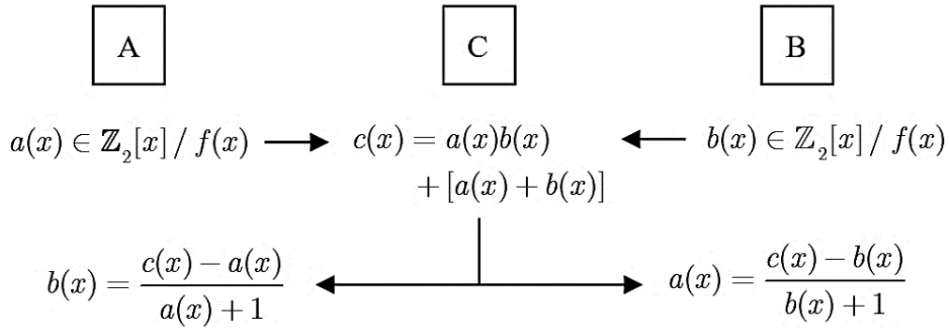
Tại nút B khôi phục thông tin $a(x)$ từ $c(x)$:

$$a(x) = c(x).b^{-1}(x) mod f(x) = (014)(134) = (023)$$

Trong đó, $a^{-1}(x) = (0123)$ và $b^{-1}(x) = (134)$ là đa thức nghịch đảo tương ứng của $a(x)$ và $b(x)$.

2.2.4.2. Mã mạng Affine trên trường đa thức

Trong mô hình mã mạng này, NCS sử dụng cả phép cộng và phép nhân đa thức trên trường đa thức để thực hiện mã mạng.



Hình 2.9. Mã mạng Affine trên trường đa thức

- Pha thứ nhất: Truyền thông tin

Nút C nhận thông tin là các đa thức $a(x)$ và $b(x)$ từ nút A và B.

Trong đó, $a(x), b(x) \in Z_2[x]/f(x)$; $f(x)$ là một đa thức nguyên thủy; $\deg f(x) = m$; $\deg a(x) < m$; $\deg b(x) < m$.

- Pha thứ hai: Tại nút C thực hiện phép tính:

$$c(x) = a(x).b(x) + [a(x) + b(x)] \tag{2.25}$$

rồi sau đó C phát quảng bá $c(x)$ tới cả nút A và B.

- Pha thứ ba: Tại nút A và B khôi phục được thông tin $a(x), b(x)$ sau khi giải mã $c(x)$.

Tại nút A:

$$c(x) - a(x) = a(x).b(x) + b(x) = b(x).[a(x) + 1]$$

$$\Rightarrow b(x) = \frac{c(x) - a(x)}{a(x) + 1}$$

Hoặc:

$$b(x) = [c(x) - a(x)].[a(x) + 1]^{-1} \tag{2.26}$$

Tại nút B:

$$c(x) - b(x) = a(x).b(x) + a(x) = a(x).[b(x) + 1]$$

$$\Rightarrow a(x) = \frac{c(x) - b(x)}{b(x) + 1}$$

Hoặc:

$$a(x) = [c(x) - b(x)].[b(x) + 1]^{-1} \quad (2.27)$$

Ví dụ: Xét trường đa thức $Z_2[x]/f(x)$ với $f(x) = 1 + x^3 + x^5 \leftrightarrow (035)$ là một đa thức nguyên thủy và $\deg f(x) = m = 5$.

- Pha thứ nhất:

Nút A chọn $a(x) = 1 + x + x^2 \in Z_2[x]/f(x)$, $\boldsymbol{a(x)} = (\mathbf{012})$

với $\deg a(x) = 2 < m$; Sau đó A tính trước:

$$[a(x) + 1]^{-1} = [1 + x + x^2 + 1]^{-1} = [x + x^2]^{-1} = x^2 + x^3 \leftrightarrow (23)$$

Nút B chọn $b(x) = x^2 + x^4 \in Z_2[x]/f(x)$, $\boldsymbol{b(x)} = (\mathbf{24})$

với $\deg b(x) = 4 < m$; Sau đó B thực hiện phép tính:

$$[b(x) + 1]^{-1} = [x^2 + x^4 + 1]^{-1} = 1 + x^3 + x^4 \leftrightarrow (034)$$

- Pha thứ hai: Nút C nhận $a(x)$ và $b(x)$ từ nút A và B, rồi C thực hiện phép tính:

$$c(x) = a(x)b(x) + [a(x) + b(x)] = (012)(24) + [(012) + (24)] = (2)$$

Sau khi tính được $c(x)$, nút C phát $c(x) = x^2 \leftrightarrow (2)$ cho cả nút A và B.

- Pha thứ ba: Khôi phục thông tin

Tại nút A:

$$b(x) = [c(x) - a(x)][a(x) + 1]^{-1}$$
$$= [(2) - (012)](23)$$
$$= (01)(23) = (\mathbf{24})$$

Tại nút B sẽ thực hiện phép tính:

$$a(x) = [c(x) - b(x)][b(x) + 1]^{-1}$$
$$= [(2) - (24)](034)$$
$$= (4)(034) = (\mathbf{012})$$

2.3. MÃ MẠNG TRÊN ĐƯỜNG CONG ELLIPTIC

2.3.1.1. Đường cong elliptic

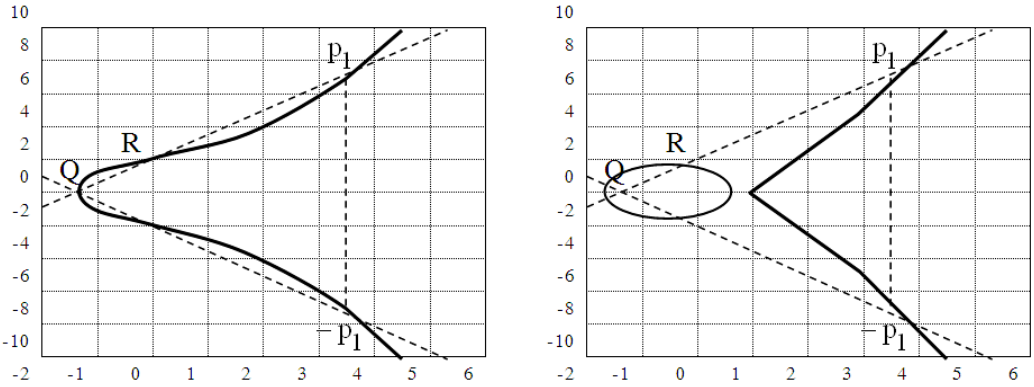
Lý thuyết đường cong Elliptic (EC- Elliptic Curve) được xác định trên trường số hữu hạn và ứng dụng trong lĩnh vực mật mã. Lý do cơ bản của nó là đường cong elliptic trên trường hữu hạn đã cung cấp cho chúng ta một cơ sở xây dựng thuật toán không thể dùng thuật toán vét cạn để thám mã của nhóm Abelian [63].

Đường cong elliptic [54, 55] là tập hợp các điểm có tọa độ (*x*, *y*) thỏa mãn phương trình có dạng sau đây :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.28)$$

Hình 2.10 sau mô tả các đường cong EC:

$$y^2 = x^3 + 2x + 5 \text{ và } y^2 = x^3 - 2x + 1$$



Hình 2.10. Các đường cong $y^2 = x^3 + 2x + 5$ và $y^2 = x^3 - 2x + 1$

Xét đường cong elliptic trên trường nguyên tố hữu hạn F_p (p là số nguyên tố, $p > 3$) với công thức biến đổi như sau:

$$x \to x - \frac{a_2}{3}, y \to y - \frac{a_1x + a_3}{2}$$

Khi đó phương trình Weierstrass có dạng:

$$x^3 + ax + b$$

Vậy trong trường F_p phương trình trở thành:

$$y^2 = x^3 + ax + b \quad (2.29)$$

Giả sử K là một trường có đặc số khác 2, 3 và xét đa thức: $x^3 + ax + b$ với $a, b \in$ K. Khi đó đường cong elliptic trên trường K: $y^2 = x^3 + ax + b$ là tập hợp tất cả các điểm (x, y) với $x, y \in$ K sao cho phương trình không có các nghiệm bội tức là $4a^3 + 27b^2 \neq 0$ theo $mod\ p$ cùng với phần tử O - điểm O này được gọi là điểm vô hạn. Vậy đường cong elliptic là tập hợp S:

$$S = \{(x, y): y^2 = x^3 + ax + b\ ;\ x, y \in K\} \cup \{0\}$$

Với $a, b \in$ K cho trước sao cho $4a^3 + 27b^2 \neq 0$ theo $mod\ p$.

Nếu K là trường đặc số 2 thì ta định nghĩa:

$$S = \{(x, y): y^2 + y = x^3 + ax + b\} \cup \{0\}$$

Nếu K là trường đặc số 3 thì ta định nghĩa:

$$S = \{(x, y): y^2 = x^3 + ax + bx + c\} \cup \{0\}$$

Tính chất

- Nếu hai điểm $P_1(x_1, y_1)$ và $P_2(x_2, y_2)$ với $x_1 \neq x_2$ nằm trên đường cùng một đường cong EC, thì đường thẳng qua hai điểm P_1 và P_2 sẽ cắt một điểm duy nhất $P_3(x_3, y_3)$ có thể xác định thông qua P_1 và P_2 nằm trên đường cong EC.

- Tiếp tuyến tại điểm bất kỳ $P(x, y)$ trên đường cong EC cũng cắt EC tại một điểm duy nhất, điểm này cũng có thể xác định được thông qua P.

Dựa vào những tính chất đó người ta đã nghiên cứu và phát hiện ra một khả năng mới cho kỹ thuật mã bảo mật mới đó là kỹ thuật mật mã đường cong elliptic (ECC).

Người ta đã chỉ ra rằng các hệ mật đường cong elliptic có độ bảo mật cao hơn nhiều so với các hệ mã hóa công khai khác như RSA, Elgamal. Độ bảo mật dựa trên độ khó phân tích số nguyên thành các thừa số nguyên tố cũng như bài toán logarit rời rạc, độ dài khóa giảm đi nhiều lần và do đó tốc độ thực hiện cũng sẽ nhanh hơn rất nhiều. Chính vì vậy người ta áp dụng kỹ thuật mật mã đường cong elliptic vào nhiều lĩnh vực khác nhau đặc biệt là việc xây dựng các giải pháp bảo mật thông tin cho các thiết bị điện tử có khả năng tính toán và không gian bộ nhớ hạn chế.

2.3.1.2. Đường cong elliptic trên trường Galois

Đường cong elliptic $y^2 = x^3 + ax + b$ trên trường hữu hạn $\mathbb{Z}_p$ (với p là nguyên tốt) được định nghĩa là tập hợp tất cả các điểm $(x, y) \in \mathbb{Z}_p$ thỏa mãn phương trình [56, 57, 59, 60, 62]:

$$y^2 = x^3 + ax + b(\text{mod}p) \tag{2.30}$$

với $x \in \mathbb{Z}_p$, a, b: nguyên dương.

Điều kiện tồn tại là:

$$\Delta = 4a^3 + 27b^2(mod\ p) \neq 0 \tag{2.31}$$

Các phép toán cộng và nhân trên các nhóm EC

Giả sử $P(x_1, y_1), Q(x_2, y_2)$ là các điểm trong nhóm $E_p(a, b)$, $O(\infty, \infty)$ là điểm vô cực. Các quy tắc đối với phép cộng trên nhóm con $E_p(a, b)$ như sau:

(1) $P + O = O + P + P$.

(2) Nếu $x_2 = x_1$ và $y_2 = -y_1$
tức là $P(x_1, y_1)$ và $Q(x_2, y_2) = Q(x_1, -y_1) = -P$ thì $P + Q = O$

(3) Nếu $Q \neq -P$ thì tổng $P + Q = K(x_3, y_3)$ với tọa độ x_3, y_3 của K xác định như sau:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \bmod p \\ y_3 &= \lambda(x_1 - x_3) - y_1 \bmod p \end{aligned} \tag{2.32}$$

Trong đó:

$$\lambda \triangleq \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p, \text{ nếu } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \bmod p, \text{ nếu } P = Q \end{cases} \tag{2.33}$$

** Cách xây dựng nhóm cộng trên đường cong elliptic*

Các phần tử của nhóm được tính như sau:

- Phần tử zero: $O(\infty, \infty)$ nằm ngoài tập hợp.
- Các phần tử khác tính theo quy tắc phép cộng các điểm trên đường cong Elliptic như trình bày trên đây.

Ví dụ:

Xây dựng nhóm $E_p(a,b) = E_{17}(1,1)$ từ phần tử nguyên thủy $P(0,1)$ và tìm tất cả các phần tử nguyên thủy của nhóm.

Theo nguyên tắc tính các điểm ở biểu thức (2.32) và (2.33) ta tính được các điểm của nhóm cộng như sau.

+ Điểm $P(0,1)$

+ Điểm $2P = P + P$

$$\lambda = \frac{3.0+1}{2.1} = 2^{-1} \bmod 17 = 9 \bmod 17 \Rightarrow x_3 = 81 \bmod 17 = 13, y_3 = 1$$

Vậy $2P(13,1)$

Chú ý: số 2 và 9 là hai số nghịch đảo, có nhiều cách tính nghịch đảo, sau đây là một cách tính theo nhóm nhân $\mathbb{Z}_{17}^*$ có phần tử sinh là 3.

Bảng 2.4. Nhóm nhân $\mathbb{Z}_{17}^*$ với phần tử sinh $\alpha = 3$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^i mod\ 17$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

+ Điểm $3P = P + 2P$

$$\lambda = \frac{0}{12} = 0 \Rightarrow \begin{cases} x_3 = -13 \bmod 17 = 4 \\ y_3 = -1 \bmod 17 = 16 \end{cases}$$

$$\Rightarrow 3P(4,16)$$

+ Điểm $4P = P + 3P$

$$\lambda = \frac{15}{4} = 15.4^{-1} \bmod 17 = 15.13 \bmod 17 = 8 \Rightarrow \begin{cases} x_3 = 9 \\ y_3 = 12 \end{cases}$$

$$\Rightarrow 4P(9,12)$$

+ Điểm $5P = P + 4P$

$$\lambda = \frac{15}{9} = 15.9^{-1} \bmod 17 = 15.6 \bmod 17 = 5 \Rightarrow \begin{cases} x_3 = 16 \\ y_3 = 4 \end{cases}$$

$$\Rightarrow 5P(16,4)$$

+ Điểm $6P = P + 5P$

$$\lambda = \frac{3}{16} = 3.16^{-1} = 3.16 \bmod 17 = 14 \Rightarrow \begin{cases} x_3 = 10 \\ y_3 = 12 \end{cases}$$

$$\Rightarrow 6P(10,12)$$

+ Điểm $7P = P + 6P$

$$\lambda = \frac{11}{10} = 11.10^{-1} = 11.12 \bmod 17 = 13 \Rightarrow \begin{cases} x_3 = 6 \\ y_3 = 6 \end{cases}$$

$$\Rightarrow 7P(6,6)$$

+ Điểm $8P = P + 7P$

$$\lambda = \frac{5}{6} = 5.6^{-1} = 5.3 \bmod 17 = 15 \Rightarrow \begin{cases} x_3 = 15 \\ y_3 = 12 \end{cases}$$

$$\Rightarrow 8P(15,12)$$

+ Điểm $9P = P + 8P$

$$\lambda = \frac{11}{15} = 11.15^{-1} = 11.8 \bmod 17 = 3 \Rightarrow \begin{cases} x_3 = 11 \\ y_3 = 0 \end{cases}$$

$$\Rightarrow 9P(11,0)$$

Từ điểm $10P$ trở đi có thể tính theo quy tắc sau: $P(x,y) = -P(x,-y)$

+ Điểm $10P = -8P \Rightarrow 10P(15,-12) = 10P(15,5)$.

(Chú ý: $-12 \bmod 17 \equiv 5 \bmod 17$)

+ Điểm $11P = -7P \Rightarrow 11P(6,-6) = 11P(6,11)$.

+ Điểm $12P = -6P \Rightarrow 12P(10,-12) = 12P(10,5)$.

+ Điểm $13P = -5P \Rightarrow 13P(16,-4) = 13P(16,13)$.

+ Điểm $14P = -4P \Rightarrow 14P(9,-12) = 14P(9,5)$.

+ Điểm $15P = -3P \Rightarrow 15P(4,-16) = 15P(4,1)$.

+ Điểm $16P = -2P \Rightarrow 16P(13,-1) = 16P(13,16)$.

+ Điểm $17P = -P \Rightarrow 17P(0,-1) = 17P(0,16)$.

+ Điểm $18P = 0$.

Các điểm nguyên thủy của nhóm nhân được xác định như sau:

Nếu P là một điểm nguyên thủy thì iP sẽ là nguyên thủy với $\left(i, \left|E_p(a,b)\right|\right) = 1$

Trong ví dụ này ta có $\left|E_{17}(1,1)\right| = 18$ vậy các điểm nguyên thủy iP có:

$(i, 18) = 1$ hay $i = (1, 5, 7, 11, 13, 17)$.

Các điểm nguyên thủy là: $P, 5P, 7P, 11P, 13P, 17P$ (6 điểm)

2.3.1.3. Phương pháp mã mạng dựa trên đường cong elliptic

Xét đường cong elliptic dạng Weierstrass trên $\mathbb{Z}_p$ (với p nguyên tố) được mô tả bởi phương trình (2.22) như sau:

$$y^2 = x^3 + ax + b \bmod p$$

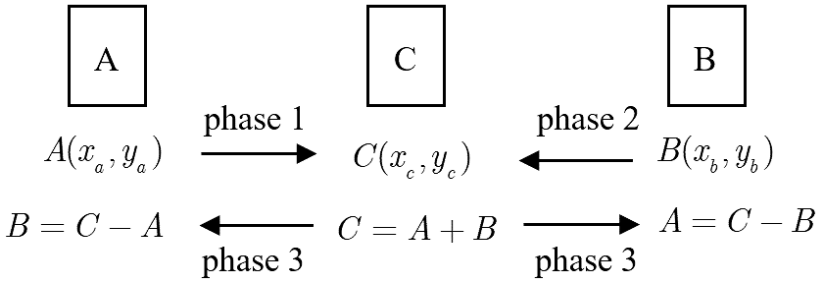
Với $a, b \in \mathbb{Z}_p^*$ (nhóm nhân trên $\mathbb{Z}_p$).

Chú ý: a và b ở đây là hệ số của đường cong elliptic trong biểu thức.

Xét nhóm $E_p(a,b)$ bao gồm tất cả các điểm có tọa độ (x,y) thỏa mãn phương trình (2.22) và điểm zero O. Nhóm $E_p(a,b)$ là một nhóm cộng, các điểm của $E_p(a,b)$ ký hiệu là $P(x,y)$.

Quy tắc thực hiện phép cộng các điểm trên đường cong EC như trình bày ở mục 2.3.1.2.

Bằng cách dùng phép cộng các điểm của EC, NCS đã tiến hành thực hiện mã mạng trên đường cong elliptic như mô tả trong hình 2.11.



Hình 2.11. Mã mạng dựa trên đường cong elliptic

Nếu ta coi thông tin cần truyền là các điểm của nhóm cộng $E_p(a, b)$ trên đường cong elliptic, thì ý tưởng thực hiện mã mạng ta có thể xây dựng một hệ thống CR như Hình 2.2.

Giả sử nút A muốn gửi thông tin (là 1 điểm) $A(x_a, y_a)$ cho B, và B muốn gửi điểm $B(x_b, y_b)$ cho A. Thủ tục truyền được thực hiện như sau:

Nút A, B, C chọn một đường cong elliptic theo dạng (2.30) với a, b thỏa mãn (2.31) và tính $E_p(a, b)$

+ Giai đoạn 1: A phát $A(x_a, y_a)$ cho C

+ Giai đoạn 2: B phát $B(x_b, y_b)$ cho C

+ Giai đoạn 3: Nút C nhận thông tin $A(x_a, y_a)$, $B(x_b, y_b)$ và tính tổng:

$$C(x_c, y_c) = A(x_a, y_a) + B(x_b, y_b) \quad (2.34)$$

Và C phát quảng bá $C(x_c, y_c)$ cho bên A và B.

Nút A nhận $C(x_c, y_c)$ và tính:

$$B(x_b, y_b) = C(x_c, y_c) - A(x_a, y_a) \quad (2.35)$$

Nút B nhận $C(x_c, y_c)$ và tính:

$$A(x_a, y_a) = C(x_c, y_c) - B(x_b, y_b) \quad (2.36)$$

Ví dụ:

Xét đường cong EC: $E_{13}(1,1)$ với $p = 13; a = 1; b = 1$.

$$y^2 = x^3 + x + 1 \ (mod\ 13)$$

Xét điều kiện tồn tại theo (2.23):

$$\Delta = (4.1^3 + 27.1^2) mod\ 13 = 5 \neq 0$$

Vậy Δ thỏa mãn điều kiện tồn tại.

Tất cả các phần tử của $E_{13}(1,1)$ có thể tính như sau:

Xét tập $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ là tập các thặng dư bậc 2 của $\mathbb{Z}_{13}^*$ (theo định nghĩa 2.18), ta có thể tính Q_{13} bằng cách bình phương tất cả các phần tử của $\mathbb{Z}_{13}^*$.

Bảng 2.5. Các phần tử là thặng dư bậc hai của Z_{13}^*.

i	1	2	3	4	5	6	7	8	9	10	11	12
i^2	1	4	9	3	12	10	10	12	3	9	4	1

Mỗi phần tử của Q_{13} có hai căn bậc 2 (định lý 2.10):

$$\sqrt{1} = \{1, 12\};\quad \sqrt{3} = \{4, 9\};\quad \sqrt{2} = \{2, 11\};$$

$$\sqrt{9} = \{3, 10\};\quad \sqrt{10} = \{6, 7\};\quad \sqrt{12} = \{5, 8\};$$

Bảng 2.6. Giá trị các điểm của $E_{13}(1,1)$

x	0	1	2	3	4	5	6	7	8	9	10	11	12
y^2	1	3	11	5	4	1	2	0	1	11	10	4	12
$y^2 \in Q_{13}$?	**Y**	**Y**	N	N	**Y**	**Y**	N	**N**	**Y**	N	**Y**	**Y**	**Y**
y_1	1	4			2	1		0	1		6	2	5
y_2	12	9			11	12		0	12		7	11	8

($Y = yes$, $N = no$; $\sqrt{y^2} = (y_1, y_2)$)

Từ bảng 2.4, ta có:

$$E_{13}(1,1) = \{(0,1), (0,12), (1,4), (1,9), (4,2), (4,11), (5,1), (5,12), (7,0),$$
$$(8,1), (8,12), (10,6), (10,7), (11,2), (11,11), (12,5), (12,8), O\}$$

Với tổng số 18 phần tử: $|E_{13}(1,1)| = 18$

Chú ý::

(a) Với $x = 7$ thì $y = 0$, mặc dù $y = 0$ không phải là thặng dư bậc hai nhưng nó 1 căn bậc hai đó là: $\sqrt{0} = 0$.

(b) Điểm O có tọa độ $O(\infty, \infty)$ đây là điểm vô cùng, thỏa mãn:

$$P + (-P) = 0$$

Thủ tục truyền tin giữa hai nút A và B theo mô hình mã mạng như sau:

Giả sử bên A chọn $A(1,4)$, bên B chọn $B(8,12)$

+ Giai đoạn 1: A gửi $A(1,4)$ cho C

+ Giai đoạn 2: B gửi $B(8,12)$ cho C

+ Giai đoạn 3: C tính $C(x_c, y_c) = A(1,4) + B(8,12)$ theo (2.24) và (2.25):

$$\lambda = \frac{y_b - y_a}{x_b - x_a} mod\ p = \frac{12-4}{8-1} mod\ 13 = 8.7^{-1} = 3$$

$$x_c = (\lambda^2 - x_a - x_b) mod\ p$$

$$= (3^2 - 1 - 8) mod\ 13 = 0$$

$$y_c = [\lambda(x_a - x_c) - y_a] mod\ p$$

$$= [3(1-0) - 4] mod\ 13$$

$$= -1 mod\ 13 = 12$$

Sau đó C gửi $C(0,12)$ cho cả A và B.

Chú ý: trong nhóm nhân $\mathbb{Z}_{13}^* = \{1,2,3,\dots,11,12\}$ có 7 cặp số nghịch đảo như sau: $(1,1)$; $(2,7)$; $(3,9)$; $(4,10)$; $(5,8)$; $(6,11)$; $(12,12)$.

Có nghĩa là: $2 = 7^{-1}$ (và đương nhiên $7 = 2^{-1}$) vì $2.7\ mod\ 13 = 1$, tương tự với các cặp số nghịch đảo khác.

- Nút A khôi phục bản tin:

$$B(x_b, y_b) = C(x_c, y_c) + [-A(x_a, y_a)]$$

Theo tính chất của nhóm nhân:

Nếu $A(1,4)$ thì $-A(1,-4)$ hay $-A(1,9)$, chú ý: $-4 = 13 - 4\ mod\ 13 = 9$

Tọa độ điểm $B(x_b, y_b)$ được bên A tính như sau:

$$\lambda = \frac{9-12}{1-0} mod\ 13 = -3 = 10$$

$$x_c = (\lambda^2 - x_a - x_b) mod\ p = (10^2 - 0 - 1) mod\ 13 = 8$$

$$y_c = [\lambda(x_a - x_c) - y_a] mod\ p = [10(0-8) - 12] mod\ 13$$

$$= -92 mod\ 13 = 12$$

Vậy A đã khôi phục được bản tin $B(8,12)$ được gửi từ B.

Tương tự, nút B khôi phục bản tin:

$$A(x_a, y_a) = C(x_c, y_c) + [-B(x_b, y_b)]$$

Do $B(8,12)$ nên $-B(8,-12)$ hay $-B(8,1)$

Tọa độ (x_a, y_a) được khôi phục tương tự, như sau:

$$\lambda = \frac{1-12}{8-0} mod\ 13 = 10$$

$$x_c = (10^2 - 0 - 8) mod\ 13 = 1$$

$$y_c = [10(0-1) - 12] mod\ 13 = -22 mod\ 13 = 4$$

Nút B khôi phục chính xác $A(1,4)$

2.4. KẾT LUẬN CHƯƠNG 2

Các nghiên cứu trong chương 2 đưa ra được các đề xuất mô hình thực hiện mã mạng trên các cấu trúc đại số cụ thể, đó là: nhóm cộng và/hoặc nhóm nhân trên vành số, trường số. Đặc biệt, từ các nghiên cứu về vành đa thức, vành đa thức có hai lớp kề cyclic và các ứng dụng tiềm năng, NCS cũng đã đề xuất xây dựng mô hình mã mạng trên các vành đa thức và trường đa thức.

Các nghiên cứu đề xuất này là một hướng nghiên cứu tiềm năng và là cơ sở để áp dụng được nhiều cấu trúc đại số khác nhau cho hàm mã hóa trong hệ thống mã mạng.

Về tốc độ xử lý: Khi áp dụng các đề xuất có sử dụng phép cộng trên vành số, vành đa thức có thể nói gần tương đương với phép toán được sử dụng trong mã mạng thông thường. Còn khi sử dụng các phép nhân thì tốc độ xử lý sẽ chậm hơn.

Phần cuối của chương 2 là các nghiên cứu về cấu trúc đại số nhóm cộng các điểm trên đường cong elliptic trên trường hữu hạn và đề xuất xây dựng mã mạng trên nhóm cộng này. Đây chính là một hướng mở để tiếp tục nghiên cứu áp dụng các hệ mật tiên tiến vào mã mạng nhằm hướng tới xây dựng các mô hình mã mạng an toàn và hiệu quả.

CHƯƠNG 3. MÔ HÌNH MÃ MẠNG AN TOÀN

Trong Chương 3, nghiên cứu sinh tập trung nghiên cứu bài toán logarit rời rạc trên trường hữu hạn, hai hệ mật khóa công khai Omura-Massey và ElGamal kết hợp với đề xuất xây dựng mã mạng trên vành số, trương số ở chương 2 để đề xuất xây dựng một mô hình mã mạng an toàn.

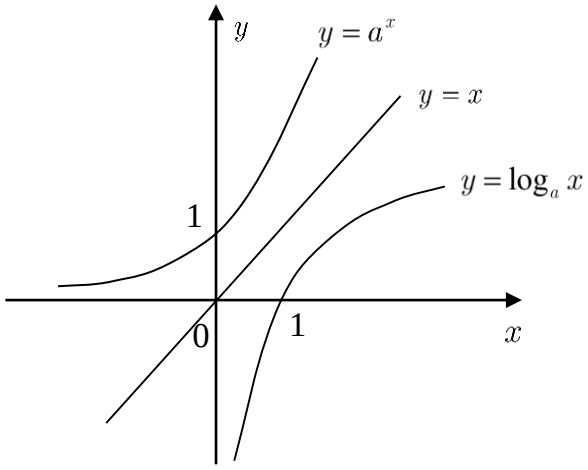
Kết quả nghiên cứu ở chương 3 được thể hiện tại Bài báo 5: (2021) Phạm Long Âu, Nguyễn Bình, Ngô Đức Thiện, "Mã mạng an toàn dựa trên hai hệ mật Omura-Masey và Elgamal trên vành số", Tạp chí Khoa học Công nghệ Thông tin và Truyền thông, Học viện Công nghệ Bưu chính Viễn thông, số 02 (CS.01)2021, ISSN 2525- 2224.

3.1. BÀI TOÁN LOGARIT RỜI RẠC

3.1.1. Bài toán logarit trên trường số thực R

+ *Bài toán thuận*: Hàm số $y = a^x$ với $a, x \in R$, việc tính toán hàm mũ này có thể được thực hiện dễ dàng bằng thuật toán bình phương và nhân.

+ *Bài toán ngược*: như ta đã biết phép tính ngược của hàm mũ chính là hàm logarit $y = \log_a x$, việc tính toán hàm ngược logarit này sẽ khó khăn hơn nhiều so với hàm thuận. Tuy nhiên, cả hai phép hãm mũ và logarit đều là các hàm đồng biến cho nên có thể xác định giá trị tương đối của hàm logarit được (như Hình 3.1).



Hình 3.1. Đồ thị hàm $y = a^x$ và $y = \log_a x$

Một số tính chất của hàm logarit.

+ $y = \log_a bc = \log_a b + \log_a c$

+ $y = \log_a \frac{b}{c} = \log_a b - \log_a c$

+ $\log_a 1 = 0$

+ $y = \log_a x^{-1} = -\log_a x$

3.1.2. Bài toán logarit trên trường hữu hạn

Bài toán logarit rời rạc (DLP) là một trong các bài toán một chiều dùng để xây dựng các hệ mật khóa công khai. Phép tính xuôi là hàm lũy thừa rời rạc, thường là phép tính dễ, được dành cho các bên mã hóa và giải mã hợp pháp. Còn phép tính ngược là phép tính logarit rời rạc, là bài toán khó, được dành cho các bên thám mã (giải mã) bất hợp pháp.

Tóm tắt bài toán logarit rời rạc như sau [9, 58]:

Xét một vành số $\mathbb{Z}_p$, nếu p là nguyên tố thì $\mathbb{Z}_p$ là một trường ($\mathbb{Z}_p = GF(p)$). Tập tất cả các phần tử khác 0 của trường sẽ tạo nên một nhóm nhân cyclic $\mathbb{Z}_p^*$.

$$\mathbb{Z}_p^* = \mathbb{Z}_p / \{0\} = \{1,2, \dots, p-1\}$$

- Cho $g \in \mathbb{Z}_p^*$ là một phần tử sinh (nguyên thủy) của nhóm nhân.

- Cho $y \in \mathbb{Z}_p^*$, yêu cầu hãy tìm x (nếu tồn tại) sao cho:

$$g^x = y, \text{ tức là: } x = \log_g y$$

Nhận xét: $\forall y \in \mathbb{Z}_p^*$ thì:

- Bài toán có nghiệm khi g là phần tử nguyên thủy.

- Bài toán có thể không có nghiệm khi g bất kỳ.

Một số tính chất của hàm logarit rời rạc.

+ $y = \log_a bc = \left(\log_a b + \log_a c\right) \bmod p - 1$

+ $y = \log_a \frac{b}{c} = \left(\log_a b - \log_a c\right) \bmod p - 1$

+ $\log_{a^{-1}} x = -\log_a x = p - 1 - \log_a x$

+ $\log_a 1 = 0 = p-1$ (coi $0 = p-1$)

Ví dụ:

Xét $p = 19, \alpha = 2$ ta có các giá trị bài toán thuận $y = \alpha^x$ như trong bảng 3.1.

Bảng 3.1. Các giá trị của $y = 2^x \bmod 19$ trên $\mathbb{Z}_{19}^*$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Chú ý:

+ *Nếu α là một phần tử nguyên thủy thì α^x sẽ đi qua tất cả các phần tử của nhóm $\mathbb{Z}_p^*$.*
+ *Nếu α là phần tử nguyên thủy thì α^i cũng là nguyên thủy với $(i, p-1) = 1$.*

Trong ví dụ này các giá trị của i thỏa mãn $(i,18) = 1$ là $i = (1,5,7,11,13,17)$.

Số lượng các giá trị của i bằng giá trị hàm $\varphi(p-1)$.

$$N_i = \varphi(p-1) = \varphi(18) = 6$$

Cách tính hàm Phi-Euler φ như trình bày tại định nghĩa 2.8.

Như vậy trong nhóm $\mathbb{Z}_{19}^*$ có 6 phần tử nguyên thủy:

$$2 = 2^1; \quad 13 = 2^5; \quad 14 = 2^7; \quad 15 = 2^{11}; \quad 3 = 2^{13}; \quad 10 = 2^{17}$$

Các phần tử nguyên thủy này tạo thành các cặp nghịch đảo như sau:

$$(2,10) \leftrightarrow 2 = 10^{-1}; \quad (13,3) \leftrightarrow 13 = 3^{-1}; \quad (14,15) \leftrightarrow 14 = 15^{-1}$$

+ *Bài toán ngược:* $y = \log_a x$

Từ bảng 3.1 ta tính được hàm ngược $\log_2 x$ như trong bảng 3.2.

Bảng 3.2. Giá trị $\log_2 x (\bmod 19)$ trên $\mathbb{Z}_{19}^*$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Tương tự ta có thể tính logarit rời rạc của các phần tử nguyên thủy còn lại của $\mathbb{Z}_{19}^*$ như bảng 3.3.

Bảng 3.3. Bài toán logarit rời rạc trên $\mathbb{Z}_{19}^*$

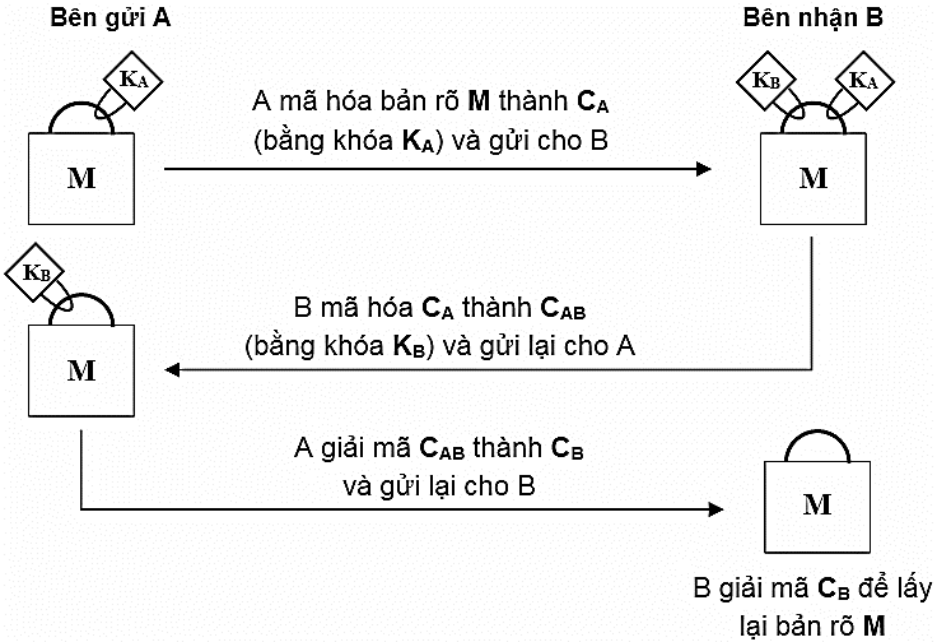
x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9
$\log_{10} x$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9
13^x	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
$\log_{13} x$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9
$\log_3 x$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9
14^x	14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
$\log_{14} x$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9
$\log_{15} x$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Nhận xét: Từ các Bảng 3.1 và Bảng 3.3 ta thấy hai hàm thuận và ngược đều không phải hảm đồng biến, khi biết bài toán thuận thì mời tìm được bài toán ngược. Do đó việc giải bài toán ngược giống bài toán vét cạn, phải thử lần lượt các trường hợp.

Việc xác định logarit của một phần tử bất kỳ trong $\mathbb{Z}_p^*$ là bài toán khó giải khi p là số nguyên tố lớn.

3.2. HỆ MẬT OMURA - MASSEY

Hệ mật Omura-Massey (O-M) được đề xuất bởi James Massey và Jim. K. Omura lần đầu tiên vào năm 1982 được xem như một cải thiện tích cực trên giao thức Shamir [59], [60], [61].



Hình 3.2. Minh họa hoạt động của hệ mật O-M

Hoạt động của hệ mật O-M được mô tả như trong Hình 3.1. Hai bên liên lạc A và B sẽ tự tạo cho mình các khóa bảo mật riêng (K_A, K_B), bên A cần gửi bản rõ 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 (K_B) thành bản mã C_{AB} và gửi lại cho A.

Bước 3: A giải mã C_{AB} được C_B rồi gửi lại cho B.

Bước 4: B nhận C_B và giải mã để nhận M.

+ Hệ mật O-M xây dựng trên bài toán DLP

* *Tạo khóa*

Khóa công khai: chọn p là một số nguyên tố lớn.

Khóa riêng của A: A chọn cặp số ngẫu nhiên (m, n) thỏa mãn:

$$m.n \equiv 1 \, mod(p-1) \tag{3.1}$$

Khóa riêng của B: B chọn cặp số ngẫu nhiên (u, v) thỏa mãn:

$$u.v \equiv 1\ mod(p-1) \tag{3.2}$$

Chú ý: vì $(m, n), (u, v)$ là các cặp số nghịch đảo nên $m, n, u, v \in \mathbb{Z}_{p-1}^*$, $\mathbb{Z}_{p-1}^*$ là nhóm nhân trên vành số $\mathbb{Z}_{p-1}$. Nhóm nhân này là tập các phần tử là nguyên tố cùng nhau với $(p-1)$, cấu trúc $\mathbb{Z}_{p-1}^*$ như sau:

$$\mathbb{Z}_{\boldsymbol{p-1}}^* = \{i, i < (p-1), \gcd(i, p-1) = 1\} \tag{3.3}$$

* *Quá trình truyền tin bảo mật*

Bên A muốn gửi một bản rõ M tới bên B.

+ Bước 1: A tính C_A và gửi cho B:

$$C_A = M^m \bmod p \tag{3.4}$$

+ Bước 2: B nhận C_A và tính C_{AB} rồi gửi cho A.

$$C_{AB} = (M^m)^u \bmod p \tag{3.5}$$

+ Bước 3: A nhận C_{AB} và tính:

$$C_B = (M^{mu})^n \bmod p = M^u \bmod p \tag{3.6}$$

và gửi C_B cho bên B.

+ Bước 4: B nhận C_B và giải mã:

$$(M^u)^v \bmod p = M \tag{3.8}$$

* *Nhận xét*

Để thu được bản rõ thì hệ mật phải có tính đẳng lũy và có tính giao hoán. Với hệ mật O-M các hàm mã hóa và giải mã đều là hàm mũ, với các số mũ là nghịch đảo của nhau nên thoả mãn.

Việc thám mã hệ mật O-M liên quan tới bài toán logarit rời rạc đây là bài toán khó với số p lớn.

Vì hệ mật O-M không có tính năng xác thực, nên để tránh loại hình tấn công "Kẻ đứng giữa" (Man in the middle) có thể sử dụng thêm các phương pháp xác thực khác.

3.3. HỆ MẬT ELGAMAL

Hệ mật ElGamal là một hệ mật khóa công khai dựa trên trao đổi khóa Diffie-Hellman, do Taher ElGamal đưa ra vào năm 1985. Mô tả vắn tắt hệ mật như sau [59, 60, 62]:

+ *Tạo khóa*: Bên liên lạc A tạo cho mình một cặp khóa công khai và bí mật, theo các bước sau:

Bước 1: Chọn p là nguyên tố lớn, $g \in \mathbb{Z}_p^*$ là phần tử nguyên thủy.

Bước 2: Chọn một số x thỏa mãn $1 < x < p-1$ và tính $g^x \ mod \ p$.

Bước 3: Khóa công khai của A: (p, g, g^x)

Khóa bí mật của A là: x

+ *Mã hóa*: B cần gửi bản tin m cho A ($m < p$)

Bước 1: B nhận khóa công khai của A: (p, g, g^x)

Bước 2: B chọn y ngẫu nhiên ($1 < y < p-1$) và tính:

$$\gamma = g^y \ mod \ p \tag{3.9}$$

$$\delta = m(g^x)^y \ mod \ p \tag{3.10}$$

Bước 3: B gửi bản mã $C = (\gamma, \delta)$ cho A

+ *Giải mã*: A nhận bản mã C và giải mã:

Bước 1: A tính

$$\gamma^{-x} = g^{-xy} \ mod \ p \tag{3.11}$$

$$= (g^y)^{p-1-x} mod \ p$$

$$(\gamma^{-x} = \gamma^{p-1-x} mod \ p)$$

Bước 2: A tính

$$\delta . \gamma^{p-1-x} = m . g^{xy} g^{-xy} mod \ p = m \tag{3.12}$$

+ *Nhận xét*: Để giải mã thì thám mã phải biết x (khóa bí mật) tức là phải giải bài toán logarit rời rạc (tính $x = \log_g g^x$) với p lớn không thể giải được, do đó hệ mật là an toàn.

+ Hiệu quả truyền tin thấp, do hệ số mở rộng bản tin $E = 2$ (Bản mã $C = (\gamma, \delta)$ có độ dài bằng 2 lần độ dài bản rõ m).

3.4. XÂY DỰNG MÃ MẠNG AN TOÀN

3.4.1. Mô hình mã mạng an toàn

Trong mô hình mã mạng hai nút như Hình 2.2, thông tin truyền trên mạng (x_A, x_B, x_C) chưa được bảo mật và xác thực. Nội dung này nghiên cứu sinh đề xuất áp dụng hai hệ mật khóa công khai kết hợp với mô hình mã mạng, với mục đích tận dụng ưu điểm của mã mạng và có thêm chức năng xác thực và bảo mật thông tin.

Mô hình mã mạng an toàn đề xuất vẫn được xây dựng như Hình 2.2. Giả sử A cần gửi bản tin x_A cho B; Bên B cần gửi bản tin x_B cho A. Quá trình truyền tin theo hai giai đoạn sau:

Giai đoạn 1: Truyền tin bảo mật từ A, B đến C, dùng hệ mật ElGamal.

Bảng 3.4. Truyền tin bảo mật bằng hệ mật ElGamal

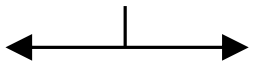
A	**C**	**B**
$x_A \xrightarrow{ElGamal}$	Giải mã lấy lại x_A, x_B và tạo x_C: $x_C = x_A x_B$ (hoặc $x_C = x_A + x_B$)	$\xleftarrow{ElGamal} x_B$

+ A và B dùng khóa công khai của C để mã hóa các bản tin x_A và x_B, sau đó truyền các bản mã cho C.

+ Bên C nhận các bản mã và giải mã để lấy lại x_A, x_B, sau đó kết hợp chúng lại thành bản tin mới x_C.

Giai đoạn 2: Sử dụng kỹ thuật mã mạng kết hợp hệ mật Omura-Massey. Bên C tạo bản tin x_C từ việc kết hợp các bản tin x_A và x_B, có thể kết hợp theo các cách khác nhau của mã mạng. Thông thường, có thể thực hiện bằng phép nhân hoặc phép cộng bá từ C đến A, B.

Bảng 3.5. Truyền tin mã mạng bảo mật bằng hệ mật Omura-Massey

Bên A	**Bên C**	**Bên B**
	Mã hóa x_C bằng khóa k'_C: $C_C = f(x_C, k'_C)$ và phát quảng bá 	
Mã hóa C_C bằng k'_A: $C_{C,A} = f(x_C, k'_C, k'_A)$ và gửi $C_{C,A}$ cho C		Mã hóa C_A bằng k'_B: $C_{C,B} = f(x_C, k'_C, k'_B)$ và gửi $C_{C,B}$ cho C
	Giải mã (gỡ k'_C): : $C_A = f(x_C, k'_A)$ $C_B = f(x_C, k'_B)$:	
+ Giải mã: $x_C = f^{-1}(x_C, k'_A)$ + Tái tạo bản rõ x_B $x_B = x_C x_A^{-1}$ (hoặc $x_B = x_C - x_A$)		+ Giải mã: $x_C = f^{-1}(x_C, k'_B)$ + Tái tạo bản rõ x_A $x_A = x_C x_B^{-1}$ (hoặc $x_A = x_C - x_B$)

- *Bước 1*:

+ Bên C mã hóa bản tin $x_C \rightarrow C_C = E(x_C, k'_C)$ bằng khóa k'_C của C, rồi phát quảng bá cho A và B.

- *Bước 2*:

+ Bên A nhận C_C mã hóa $C_C \rightarrow C_{C,A}$ bằng khóa k'_A và gửi trả C:

$$C_{C,A} = E(C_C, k'_A) = E(x_C, k'_C, k'_A) \tag{3.13}$$

+ Bên B nhận C_C mã hóa $C_C \rightarrow C_{C,B}$ bằng khá k'_B và gửi trả C:

$$C_{C,B} = E(C_C, k'_B) = E(x_C, k'_C, k'_B) \tag{3.14}$$

- *Bước 3*:

+ Bên C nhận $C_{C,A}$ và giải mã $C_{C,A} \rightarrow C_A$ (tháo khóa k'_C), và gửi C_A cho A:

$$C_A = D\left(C_{C,A}, k'_C\right) = E(x_C, k'_A) \tag{3.15}$$

+ Bên C nhận $C_{C,B}$ và giải mã $C_{C,B} \rightarrow C_B$ (tháo khóa k'_C), và gửi C_B cho B:

$$C_B = D\left(C_{C,B}, k'_C\right) = E(x_C, k'_B) \tag{3.16}$$

- *Bước 4*:

+ Bên A nhận C_A và giải mã tái tạo bản rõ x_B:

$$\begin{aligned} x_C &= D(C_A, k'_A) \\ x_B &= x_C . x_A^{-1} \end{aligned} \tag{3.17}$$

+ Bên A nhận C_B và giải mã tái tạo bản rõ x_A:

$$\begin{aligned} x_C &= D(C_B, k'_B) \\ x_A &= x_C . x_B^{-1} \end{aligned} \tag{3.18}$$

Chú ý: $E(.)$ và $D(.)$ là các hàm mã hóa và giải mã. Để thực hiện mã hóa và giải mã không theo quy tắc "bóc bánh" như biểu thức trên tức là có thể thực hiện không theo thứ tự, thì phép mã hóa và giải mã thường dựa trên tính chất đẳng lũy của phép tính lũy thừa.

3.4.2. Mã mạng an toàn sử dụng bài toán logarit rời rạc

Hoạt động của mã mạng an toàn đề xuất xây dựng trên bài toán DLP thực hiện như sau:

* *Tạo khóa*

+ Tham số chung: Các bên A, B, C chọn:

p - số nguyên tố lớn;

g- phần tử nguyên thủy, $g \in \mathbb{Z}_p^*$;

+ Tham số bí mật: các bên chọn số bí mật như sau:

Bên A:

- Số ngẫu nhiên k_A: $(1 < k_A < p - 1)$

- Cặp số: m_A, n_A: $m_A n_A = 1\ mod\ (p - 1)$

Bên B:

- Số ngẫu nhiên k_B: $(1 < k_B < p - 1)$

- Cặp số: m_B, n_B: $m_B n_B = 1\ mod\ (p - 1)$

Bên C:

- Số ngẫu nhiên k_C: $(1 < k_C < p - 1)$; Tính $g^{k_C}\ mod\ p$ và *công khai* g^{k_C} cho A và B.

- Cặp số: u, v: $uv = 1\ mod\ (p - 1)$

Chú thích: các số bí mật k_A, k_B, k_C sử dụng cho hệ mật ElGamal; các cặp số $(m_A, n_A), (m_B, n_B), (u, v)$ sử dụng cho hệ mật O-M (tương ứng với các khóa k'_A, k'_B, k'_C trong mục *3.4.1*).

** Quá trình truyền tin:*

Giai đoạn 1:

Truyền tin bảo mật từ A, B đến C, dùng hệ mật ElGamal. Bản rõ của A là x_A, và của B là x_B.

Bên A tính (theo (3.9), (3.10)):

$$\gamma_A = g^{k_A}\ mod\ p$$

$$\delta_A = x_A (g^{k_C})^{k_A}\ mod\ p$$

và gửi $C_A = (\gamma_A, \delta_A)$ cho C.

Bên B tính:

$$\gamma_B = g^{k_B}\ mod\ p$$

$$\delta_B = x_B (g^{k_C})^{k_B}\ mod\ p$$

và gửi $C_B = (\gamma_B, \delta_B)$ cho C.

Bên C giải mã theo (3.11), (3.12):

- Giải mã x_A

$$\gamma_A^{-k_C} = \gamma_A^{p-1-k_C} = g^{-k_A k_C} \, mod \, p$$

$$\gamma_A^{-k_C} \, \delta_A = x_A (g^{k_C k_A}) g^{-k_A k_C} = x_A$$

- Giải mã x_B

$$\gamma_B^{-k_C} = \gamma_B^{p-1-k_C} = g^{-k_B k_C} \, mod \, p$$

$$\gamma_B^{-k_C} \, \delta_B = x_B (g^{k_C k_B}) g^{-k_B k_C} = x_B$$

Giai đoạn 2: Truyền tin bảo mật quảng bá từ C đến A, B bằng hệ mật Omura-Massey. Sử dụng kỹ thuật mã mạng: Bên C tạo bản tin x_C từ việc kết hợp các bản tin x_A và x_B, có thể kết hợp theo các cách khác nhau của mã mạng. Thông thường, có thể thực hiện bằng phép nhân hoặc phép cộng.

- theo phép nhân: $x_C = x_A x_B \, mod \, p$

- theo phép cộng: $x_C = (x_A + x_B) \, mod \, p$

+ *Bước 1*: Bên C mã hóa bản tin x_C (theo phép nhân) và phát quảng bá bản mã cho A, B:

$$C_C = x_C^u \, mod \, p$$

+ *Bước 2*:

Bên A nhận C_C mã hóa $C_C \rightarrow C_{C,A}$ bằng khóa riêng của A và gửi $C_{C,A}$ cho C:

$$C_{C,A} = C_C^{m_A} \, mod \, p = x_C^{u.m_A} \, mod \, p$$

Bên B nhận C_C mã hóa $C_C \rightarrow C_{C,B}$ bằng khóa riêng của A và gửi $C_{C,B}$ cho C:

$$C_{C,B} = C_C^{m_B} \, mod \, p = x_C^{u.m_B} \, mod \, p$$

+ *Bước 3*:

Bên C nhận $C_{C,A}$, giải mã $C_{C,A} \rightarrow C_A$ và gửi lại C_A cho A:

$$C_A = C_{C,A}^v = x_C^{u.v.m_A} \; mod \; p = x_C^{m_A} \; mod \; p$$

Bên C nhận $C_{C,B}$, giải mã $C_{C,B} \rightarrow C_B$ và gửi lại C_B cho B:

$$C_B = C_{C,B}^v = x_C^{u.v.m_B} \; mod \; p = x_C^{m_B} \; mod \; p$$

+ *Bước 4*:

Bên A nhận C_A và giải mã lấy lại x_C

$$C_A^{n_A} = x_C^{m_A n_A} \; mod \; p = x_C$$

tái tạo bản rõ x_B:

- Theo phép nhân: $x_B = x_C x_A^{-1}$
- Theo phép cộng: $x_B = x_C - x_A$

Bên B nhận C_B và giải mã lấy lại x_C

$$C_B^{n_B} = x_C^{m_B n_B} \; mod \; p = x_C$$

tái tạo bản rõ x_A:

- Theo phép nhân: $x_A = x_C x_B^{-1}$
- Theo phép cộng: $x_A = x_C - x_B$

Ví dụ:

* *Tạo khóa*

+ *Tham số chung*: Các bên A, B, C chọn:

$p = 23$ - số nguyên tố;

$g = 5$ là phần tử nguyên thủy, $g \in \mathbb{Z}_{23}^*$;

Bên C chọn $k_C = 9$ là tham số bí mật của C và tính:

$$g^{k_C} = 5^9 mod \; 23 = 11$$

+ *Tham số bí mật*:

Bên A chọn:

- Số ngẫu nhiên $k_A = 7$: $(1 < 7 < 30)$

- Cặp số: $(m_A, n_A) = (7,19)$ thỏa mãn:

$$7 \times 19 \; mod \; 22 = 1$$

Bên B chọn:

- Số ngẫu nhiên $k_B = 15$: $(1 < 15 < 22)$

- Cặp số: $(m_B, n_B) = (5,9)$ thỏa mãn:

$$5 \times 9 \; mod \; 22 = 1$$

Bên C chọn:

- Số ngẫu nhiên $k_C = 9$: $(1 < 9 < 22)$

- Tính $g^{kc} = 5^9 mod \; 23 = 11$ *và công khai* g^{kc} cho A và B (như ở trên).

- Cặp số: $(u, v) = (13,17)$ thỏa mãn:

$$13 \times 19 \; mod \; 22 = 1$$

Tóm lại:

Tham số công khai: $p = 23; g = 5, \; g^9 = 11$

Tham số bí mật:

- Bên A: $k_A = 7; (m_A, n_A) = (7,19)$
- Bên B: $k_B = 15; \; (m_B, n_B) = (5,9)$
- Bên C: $k_C = 9; \; (u, v) = (13,17)$

* *Quá trình truyền tin:*

Giai đoạn 1: Truyền tin bảo mật từ A, B đến C, dùng hệ mật ElGamal.

Giả sử bản rõ của A là $x_A = 3$, và của B là $x_B = 12$.

Bên A tính:

$$\gamma_A = g^{k_A} = 5^7 mod\ 23 = 17$$

$$\delta_A = x_A(g^{k_C})^{k_A} = 3.11^7 mod\ 23 = 21$$

và gửi $C_A = (17, 21)$ cho C.

Bên B tính:

$$\gamma_B = g^{k_B} = 5^{15}\ mod\ 23 = 19$$

$$\delta_B = x_B(g^{k_C})^{k_B} = 12.11^{15} mod\ 23 = 5$$

và gửi $C_B = (19, 5)$ cho C.

Bên C giải mã:

- Giải mã x_A, C tính:

$$\gamma_A^{-k_C} = 17^{-9} = 17^{13}\ mod\ 23 = 10$$

$$\gamma_A^{-k_C}\ \delta_A = 10.21 \text{ mod } 23 = \mathbf{3} = \boldsymbol{x_A}$$

- Giải mã x_B

$$\gamma_B^{-k_C} = 19^{13}\ mod\ 23 = 7$$

$$\gamma_B^{-k_C}\ \delta_B = 7.5\ mod\ 23 = \mathbf{12} = \boldsymbol{x_B}$$

Chú ý: $\gamma^{-k_C} = \gamma^{p-1-k_C} = \gamma^{22-9}$.

Giai đoạn 2: Truyền tin bảo mật kết hợp mã mạng.

+ *Bước 1*: Bên C kết hợp bản tin theo phép nhân:

$$x_C = x_A x_B = 3.12\ mod\ 23 = 13$$

+ *Bước 2*: Bên C mã hóa bản tin x_C và phát quảng bá bản mã cho A, B:

$$C_C = x_C^u\ mod\ p = 13^{13}\ mod\ 23 = 8$$

+ *Bước 3*:

Bên A nhận $C_C = 8$ và mã hóa $C_C \rightarrow C_{C,A}$, sau đó gửi $C_{C,A}$ cho C:

$$C_{C,A} = C_C^{m_A}\ mod\ p = 8^7\ mod\ 23 = 12$$

Bên B nhận C_C, mã hóa $C_C \rightarrow C_{C,B}$ sau đó gửi $C_{C,B}$ cho C:

$$C_{C,B} = C_C^{m_B} \, mod \, p = 8^5 \, mod \, 23 = 16$$

+ *Bước 4*:

Bên C giải mã $C_{C,A} \rightarrow C_A$ và gửi lại C_A cho A:

$$C_A = C_{C,A}^v = 12^{17} \, mod \, 23 = 9$$

Bên C giải mã $C_{C,B} \rightarrow C_B$ và gửi lại C_B cho B:

$$C_B = C_{C,B}^v = 16^{17} \, mod \, 23 = 4$$

+ *Bước 5*:

Bên A nhận C_A và giải mã lấy lại x_C.

$$C_A^{n_A} = 9^{19} \, mod \, 23 = 13$$

tái tạo bản rõ x_B:

$$x_B = x_C x_A^{-1} = 13 * 8 \, mod \, 23 = \mathbf{12}$$

Bên B nhận C_B và giải mã lấy lại x_C.

$$C_B^{n_B} = 4^9 \, mod \, 23 = 13$$

tái tạo bản rõ x_A:

$$x_A = x_C x_B^{-1} = 13 * 2 \, mod \, 23 = \mathbf{3}$$

Chú ý: $3^{-1} mod \, 23 = 8$; $12^{-1} mod \, 23 = 2$ là các cặp số nghịch đảo. Để tính phép lũy thừa các số lớn theo modulo, có thể sử dụng thuật toán bình phương và nhân.

3.4.3. Đánh giá mô hình mã mạng an toàn

Nghiên cứu sinh đã đề xuất một mô hình mã mạng kết hợp ưu điểm của việc giảm phiên truyền dẫn (của mã mạng) với các hệ mật mã công khai, để tạo ra một mã mạng an toàn. Các bước của mô hình này tóm tắt như sau: Bước 1: xác thực bảo mật dùng hệ mật ElGamal; Bước 2 giải mã và xác thực, kết hợp (che giấu) bản tin bằng mặt nạ cộng hoặc nhân; Bước 3 phát quảng bá bằng hệ mật O-M.

Ưu điểm của mô hình đề xuất đó là: (1) Sử dụng được ưu điểm của mã mạng là giảm số phiên truyền dẫn giữa các nút truyền trên mạng (tăng thông lượng), tăng độ

ổn định của việc truyền tin; (2) thông tin truyền trong mạng được bảo mật an toàn nhờ các hệ mật khóa công khai. Độ an toàn của các hệ mật khóa công khai dựa trên bài toán logarit rời rạc, đã được chứng minh là bài toán an toàn với trường hợp số nguyên tố lớn.

Các đề xuất áp dụng các hệ mật kết hợp vào mã mạng như trong luận án nhằm tạo ra mã mạng có khả năng bảo mật. Các đề xuất này mới là bước đầu để có các nghiên cứu tiếp theo là áp dụng các hệ mật có độ an toàn cao hơn vào mô hình mã mạng an toàn.

3.5. KẾT LUẬN CHƯƠNG 3

Từ các nghiên cứu đề xuất ở chương 2, NCS nhận thấy có thể áp dụng việc thực hiện bảo mật thông tin trên mã mạng, vì lúc này thông tin trong mạng đã có thể được mô tả bằng các con số (trên vành số, trường số), hoặc các đa thức, hoặc các điểm trên đường cong elliptic.

Kết quả nghiên cứu ở chương 3 đã đưa ra một mô hình thực hiện mã mạng an toàn (có bảo mật) kết hợp mô hình mã mạng theo kiểu truyền thông hợp tác (giữa 2 nút ở xa) với 2 hệ mật khóa công khai là Omura-Massey và ElGamal. Có thử nghiệm tính toán với trường hợp hai hệ mật xây dựng trên trường số và trên bài toán logarit rời rạc.

Tuy nhiên, các nghiên cứu mới dừng ở mức đề xuất mô hình và phương pháp thực hiện, độ an toàn bảo mật của phương pháp đề xuất đạt được theo độ an toàn của bài toán logarit rời rạc, cho đến nay bài toán này vẫn là an toàn khi sử dụng số nguyên tố lớn.

KẾT LUẬN

** Các kết quả chính của luận án:*

Với sự định hướng và hướng dẫn của hai hướng dẫn khoa học, nghiên cứu sinh đã tiến hành thực hiện luận án: "Mã mạng trên một số cấu trúc đại số" với các kết quả chính đạt được như sau:

- Đề xuất phương pháp thực hiện mã mạng trên vành số, trường số, vành đa thức, trường đa thức bằng cách sử dụng các nhóm cộng (phép cộng), nhóm nhân (phép nhân) và kết hợp cả nhóm cộng và nhóm nhân để thực hiện hàm mã hóa/giải mã cho mã mạng.

- Đề xuất phương pháp thực hiện mã mạng bằng cấu trúc nhóm cộng các điểm trên đường cong elliptic của trường số.

- Đề xuất một mô hình mã mạng an toàn: nhằm kết hợp các ưu điểm của mã mạng với độ an toàn của các hệ mật mã công khai để thực hiện một mã mạng có bảo mật thông tin.

** Hướng phát triển của luận án:*

Tiếp tục nghiên cứu, phân tích sâu hơn để có thể đánh giá đầy đủ tính hiệu quả các phương thức, thuật toán mã mạng mà NCS đã đề xuất. Đặc biệt là xây dựng hệ thống kiểm thử thông qua mô phỏng hệ thống bằng các phần mềm mô phỏng trên máy tính nhằm đánh giá hiệu năng, độ an toàn bảo mật của mô hình đề xuất, rồi tiến tới thực nghiệm trong thực tế để có thể đưa các phương thức mã mạng hiệu quả.

Tiếp tục nghiên cứu, trao đổi học thuật để có thể đưa ra được nhiều phương thức, thuật toán mã mạng mới hiệu quả hơn.

Trên cơ sở các đề xuất của luận án, hướng phát triển tiếp theo có thể là nghiên cứu áp dụng các hệ mật mã như các hệ mật trên bài toán logarit rời rạc, các hệ mật đường cong elliptic, các hệ mật trên vành đa thức có hai lớp kề... vào mô hình mã mạng nhằm tạo được các mô hình mã mạng an toàn.

Hà Nội, tháng 6 năm 2022

DANH MỤC CÔNG TRÌNH ĐÃ CÔNG BỐ CỦA TÁC GIẢ

[1]. Phạm Long Âu, Nguyễn Bình, Ngô Đức Thiện, Nguyễn Lê Cường, "Mã mạng trên một số cấu trúc đại số", Tạp chí Nghiên cứu Khoa học và công nghệ quân sự, pages 125-132, No 54, 4/2018;

[2] Âu Pham Long, Thien Ngo Duc and Binh Nguyen, "About Some Methods of Implementing Network Coding based on Polynomial Rings and Polynomial Fields," 2019 25th Asia-Pacific Conference on Communications (APCC), Ho Chi Minh City, Vietnam, 2019, pp. 507-510, doi: 10.1109/APCC47188.2019.9026530; (PoD) ISSN: 2163-0771, IEEE Xplore.

[3] Pham Long Au, Nguyen Minh Trung, Nguyen Le Cuong, "About Some Methods of Implementation Network Coding over Number Rings", Proceedings of the 12th international conference on advanced technologies for communication, page 371-374, ATC 10/2019; ISSN: 2162-1039 IEEE Xplore;

[4] Pham Long Au, Ngo Duc Thien, "About one method of Implementation Network Coding based on point additive operation on Elliptic curve" Journal of Science and Technology on Information and Communications, No 1 (CS.01) 2019, ISSN 2525- 2224, page 3-6..

[5]. Phạm Long Âu, Nguyễn Bình, Ngô Đức Thiện, "Mã mạng an toàn dựa trên hai hệ mật Omura-Masey và Elgamal trên vành số", Tạp chí Khoa học Công nghệ Thông tin và Truyền thông, Học viện Công nghệ Bưu chính Viễn thông, số 02 (CS.01)2021, ISSN 2525- 2224.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1]. Hồ Văn Canh, Lê Danh Cường, "Mật mã và an toàn thông tin: Lý thuyết và ứng dụng", NXB Thông tin và Truyền thông, 2018.

[2]. Nguyen Trung Hieu, Ngo Duc Thien, Tran Duc Su, "On Constructing Cyclic Multiplicative Groups with Maximum Order over Polynomial Rings with Two Cyclotomic Cosets", Jounal of scientific research and military technology, Vol. 17, February - 2012, pp. 133-140, ISSN 1859-1043.

[3]. Lê Danh Cường, Nguyễn Bình, "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, 2017, tr. 54-57.

[4]. Nguyễn Trung Hiếu, Ngô Đức Thiện, "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, ISSN 2354-1083, số 125, 2018, tr. 29-34.

[5]. Ngô Đức Thiện, (2020), *Một phương pháp xây dựng hệ Pohlig-Hellman trên vành đa thức*, Tạp chí KHCN Thông tin và Truyền thông, ISSN-2525-2224, Số 02 (CS.01) 2020.

[6]. Đặng Hoài Bắc, (2010) "Các mã cyclic và cyclic cục bộ trên vành đa thức có hai lớp kề cyclic", Luận án TS kỹ thuật.

[7]. Nguyễn Thị Thùy Dương, "Network Coding", khóa luận tốt nghiệp hệ chất lượng cao, Trường Đại học Công nghệ, 6/2010;

[8]. Vũ Đức Hiệp, Trần Xuân Nam, Kết hợp mã hóa mạng lớp vật lý và lựa chọn nút chuyển tiếp cho kênh vô tuyến chuyển tiếp hai chiều, Tạp chí Công nghệ thông tin và Truyền thông (Chuyên san) bộ Thông tin truyền thông, số 10 (30), tháng 12-2013, ISSN 1859-3526

[9]. Nguyễn Bình (2013), Giáo trình Mật mã học, Học viện Công nghệ Bưu chính Viễn thông, Nxb Bưu điện, 2013.

[10]. Nguyễn Bình (2008), Giáo trình Lý thuyết thông tin, Học viện Công nghệ Bưu chính Viễn thông, Nxb Bưu điện, 2008.

[11]. Nguyễn Chánh Tú (2006), Giáo trình Lí thuyết mở rộng trường và Galois", Đại học Sư phạm Huế.

Tiếng Anh

[12]. 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.

[13]. Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh (2007), "Decomposition in polynomial ring with with two cyclotomic cosets", *36th AIC, November 18-23 2007, Manila*.

[14]. Nguyen Binh, Dang Hoai Bac (2004), "Cyclic Codes over Extended Rings of Polynomial Rings with Two Cyclotomic Cosets", REV'04, Vietnam.

[15]. Hồ Quang Bửu, Trần Đức Sự, "Constructing Interleaved M-sequences over Polynomial Rings with Two Cyclotomic Cosets," Tạp chí Khoa học và Công nghệ Quân sự, số 47, 02 (2012), trang 133-140.

[16]. R. W. Yeung and Zhen Zhang, "Distributed source coding for satellite communications," IEEE Trans. Inf. Theory, vol. 45, no. 4, pp. 1111–1120, May 1999, doi: 10.1109/18.761254.

[17]. R. Ahlswede, Ning Cai, S.-R. Li, and R. W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000, doi: 10.1109/18.850663.

[18]. R.W. Yeung, S.-Y.R. Li, N. Cai, and Z. Zang. Network Coding Theory. Foundations and Trends in Communications and Information Theory, NOW publisher 2006.

[19]. S.Y. R. Li, R. W. Yeung, and N. Cai. Linear Network Coding. IEEE Transactions on Information Theory, 49(2):371 – 381, 2003.

[20]. T. Ho and D. S. Lun. Network Coding: An Introduction. Cambridge University Press, Cambrige, UK, 2008.

[21]. Alex Sprintson. Network Coding and its Applications in Communication Networks. In book: Algorithms for Next Generation Networks. pp.343-372. Texas A&M University, College Station, Texas, USA, 2010.

[22]. P. A. Chou, Y. Wu, and K. Jain. Practical Network Coding. In Proceedings of Allerton Conference on Communication, Control, and Computing, Monticello, IL, October 2003.

[23]. R. Koetter and M. Medard. An Algebraic Approach to Network Coding. IEEE/ACM Transactions on Networking, 11(5):782 – 795, 2003

[24]. R. W. Yeung, "Network Coding: A Historical Perspective," Proc. IEEE, vol. 99, no. 3, pp. 366–371, Mar. 2011, doi: 10.1109/JPROC.2010.2094591.

[25]. A. Nosratinia, T. Hunter and A. Hedayat, "*Cooperative communication in wireless networks",* Communication Magazine, IEEE, vol. 42, Oct 2004, pp.74 – 80.

[26]. P. A. Chou and Y. Wu, "Network Coding for the Internet and Wireless Networks," IEEE Signal Process. Mag., vol. 24, no. 5, pp. 77–85, Sep. 2007, doi: 10.1109/MSP.2007.904818.

[27]. X. Tao, X. Xu, and Q. Cui, "*An overview of cooperative communications",* Communications Magazine, IEEE, vol. 50, June 2012, pp. 65-71.

[28]. Cuong Cao Luu, Dung Van Ta, Quy Trong Nguyen, Sy Nguyen Quy, Hung Viet Nguyen, (Oct 15-17, 2014), "*Network coding for LTE-based cooperative communications",* the 2014 International Conference on Advanced Technologies for Communications (ATC), Hanoi, Vietnam.

[29]. T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "*A random linear network coding approach to multicast,"* IEEE Transactions on Information Theory, vol. 52, pp. 4413-4430, Oct, 2006.

[30]. X. Li, T. Jiang, Q. Zhang, and L. Wang, "Binary linear multicast network coding on acyclic networks: principles and applications in wireless communication networks," IEEE J. Sel. Areas Commun., vol. 27, no. 5, pp. 738–748, Jun. 2009, doi: 10.1109/JSAC.2009.090614.

[31]. J. Ebrahimi and C. Fragouli, "Multicasting algorithms for deterministic networks," in 2010 IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo), Jan. 2010, pp. 1–5, doi: 10.1109/ITWKSPS.2010.5503221.

[32]. N. Ratnakar, D. Traskov, and R. Koetter, "*Approaches to network coding for multiple unicast,"* in Communications, 2006 International Zurich Seminar on, pp.70-73, Oct 2006.

[33]. X. Wang, W. Guo, Y. Yang, and B. Wang, "*A secure broadcasting scheme with network coding,"* Communications letters, IEEE, vol. 17, pp.1435-1538, July 2013.

[34]. Q. Li, J.-S Lui, and D.-M Chiu, "*On the security and efficiency of content distribution via network coding,"* Dependable and secure computing, IEEE Transactions on, vol. 9, pp. 211-221, March 2012.

[35]. X. Yang, E. Dutkiewicz, Q. Cui, X. Tao, Y. Guo, and X. Huang, "*Compressed network coding for distributed storage in wireless sensor networks,"* in Communications and Information Technologies (ISCIT), 2012 International Symposium on, pp. 816-821, Oct 2012.

[36]. F. de Asis Lopez-Fuentes and C. Cabrera Medina, "*Network coding for streaming video over P2P networks",* in Multimedia (ISM), 2013 IEEE International Symposium on, pp. 329-332, Dec. 2013.

[37]. S. R. Li and S. T. Ho, “Ring-theoretic foundation of convolutional network coding,” in 2008 Fourth Workshop on Network Coding, Theory and Applications, Jan. 2008, pp. 1–6, doi: 10.1109/NETCOD.2008.4476179.

[38]. M. Tan, R. W. Yeung, and S. T. Ho, “A Unified Framework For Linear Network Codes,” in 2008 Fourth Workshop on Network Coding, Theory and Applications, Jan. 2008, pp. 1–5, doi: 10.1109/NETCOD.2008.4476192.

[39]. S. Kim, T. Ho, M. Effros, and S. Avestimehr, “Network error correction with unequal link capacities,” in 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Sep. 2009, pp. 1387–1394, doi: 10.1109/ALLERTON.2009.5394512.

[40]. J. Ebrahimi and C. Fragouli, “Vector network coding algorithms,” in 2010 IEEE International Symposium on Information Theory, Jun. 2010, pp. 2408–2412, doi: 10.109/ISIT.2010.5513771.

[41]. X. Li, W. H. Mow, and F.-L. Tsang, “Singularity Probability Analysis for Sparse Random Linear Network Coding,” in 2011 IEEE International Conference on Communications (ICC), Jun. 2011, pp. 1–5, doi: 10.1109/icc.2011.5963470.

[42]. S. Yang and R. W. Yeung, “Coding for a network coded fountain,” in 2011 IEEE International Symposium on Information Theory Proceedings, Jul. 2011, pp. 2647–2651, doi: 10.1109/ISIT.2011.6034050.

[43]. J. Huang, L. Wang, W. Cheng, and H. Li, “Polynomial Time Construction Algorithm of BCNC for Network Coding in Cyclic Networks,” in 2009 Eighth IEEE/ACIS International Conference on Computer and Information Science, Jun. 2009, pp. 228–233, doi: 10.1109/ICIS.2009.52.

[44]. J. Huang, L. Wang, T. Zhang, and H. Li, “Unified construction algorithm of network coding in cyclic networks,” in 2009 15th Asia-Pacific Conference on Communications, Oct. 2009, pp. 749–753, doi: 10.1109/APCC.2009.5375495.

[45]. W. Guo, N. Cai, Xiaomeng Shi, and M. Médard, “Localized dimension growth in random network coding: A convolutional approach,” in 2011 IEEE International Symposium on Information Theory Proceedings, Jul. 2011, pp. 1156–1160, doi: 10.1109/ISIT.2011.6033714.

[46]. X. Guang, F.-W. Fu, and Z. Zhang, “Universal Network Error Correction MDS Codes,” in 2011 International Symposium on Networking Coding, Jul. 2011, pp. 1–6, doi: 10.1109/ISNETCOD.2011.5979063.

[47]. A. A. Gohari, S. Yang, and S. Jaggi, “Beyond the cut-set bound: Uncertainty computations in network coding with correlated sources,” in 2011 IEEE International Symposium on Information Theory Proceedings, Jul. 2011, pp. 598–602, doi: 10.1109/ISIT.2011.6034199.

[48]. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros. Resilient Network Coding in the Presence of Byzantine Adversaries. IEEE Transactions on Information Theory, 54(6):2596–2603, June 2008.

[49]. R. Koetter and M. Medard. An Algebraic Approach to Network Coding. IEEE/ACM Transactions on Networking, 11(5):782 – 795, 2003.

[50]. “Construction of convolutional network coding for cyclic multicast networks |Request PDF.” https://www.researchgate.net/publication/251963081_Construction_of_convolutional_network_coding_for_cyclic_multicast_networks (accessed May 10, 2020).

[51]. “Network localized error correction: For non-coherent coding - IEEE Conference Publication.” https://ieeexplore.ieee.org/document/6033711 (accessed May 10, 2020).

[52]. K. Prasad and B. S. Rajan, “Convolutional Codes for Network-Error Correction,” in GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, Nov. 2009, pp. 1–6, doi: 10.1109/GLOCOM.2009.5425892.

[53]. K. Prasad and B. S. Rajan, “Network-error correcting codes using small fields,” in 2011 IEEE International Symposium on Information Theory Proceedings, Jul. 2011, pp. 1930–1934, doi: 10.1109/ISIT.2011.6033888.

[54]. D. Hankerson, A. Menezes and S. Vanstone, "Guide to Elliptic Curse Cryptography", Berlin: Springer-Verlag, 2004.

[55]. Koblitz, N. (1987), "Elliptic curve cryptosystems", Mathematics of Computation. 48 (177): 203–209. doi:10.2307/2007884. JSTOR 2007884.

[56]. Brown, M.; Hankerson, D.; Lopez, J.; Menezes, A. (2001). "Software Implementation of the NIST Elliptic Curves Over Prime Fields". Topics in Cryptology – CT-RSA 2001. Lecture Notes in Computer Science. Vol. 2020. pp. 250–265. CiteSeerX 10.1.1.25.8619. doi:10.1007/3-540-45353-9_19. ISBN 978-3-540-41898-6.

[57]. "The Case for Elliptic Curve Cryptography". National Security Agency (NSA - 2009).

[58]. Frederik Vercauteren, "Discrete Logarithms in Cryptography", ESAT/COSIC - K.U. Leuven ECRYPT Summer School 2008.

[59]. D. R. Stinson, "Cryptography Theory and Practice", CRC Press, 1995.

[60]. Jean-Yves Chouinard - ELG 5373, “Secure Communications and Data Encryption, School of Information Technology and Engineering”, University of Ottawa, April 2002.

[61]. William Stallings “Cryptography and Network Security Principles and Practice”, Sixth edition, Pearson Education, Inc., 2014.

[62]. A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[63]. Rudolf Lidl, Harald Niederreiter, “*Finite Fields*”, (Encylopedia of Mathematics and Its Appliaction; Volume 20. Section, Algebra), Addison-Wesley Publishing Company, 1983.