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 ngành: 9.52.02.03

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI - 2022

Công trình được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học:

TS. Ngô Đức Thiện

TS. Nguyễn Lê Cường

Phản biện 1:

Phản biện 2:

Phản biện 3:

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

……..

……..

……..

vào hồi: ngày tháng năm 2022.

Có thể tìm hiểu luận án tại:

1. Thư viện Quốc gia
2. Thư viện Học viện Công nghệ Bưu chính Viễn thông

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.

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

- 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

1.1.2. Mã hóa thông tin

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].

1.2.2. Mô hình mã mạng đơn giản

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.

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

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.

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 số 1, 2, 3, 4 trong danh mục công trình công bố của tác giả.

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

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

a) Thuật toán Euclid

b) Thuật toán Euclid mở rộng

2.1.1.3. Các số nguyên modulo n

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

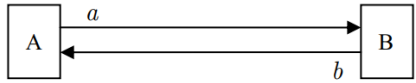
a) Thuật toán tính số nghịch đảo trong $\mathbb{Z}_n$

b) Thuật toán bình phương và nhân có lặp

2.1.2. Một số cấu trúc đại số

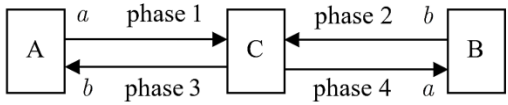
2.1.3. Đề xuất xây dựng mã mạng trên các vành số

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

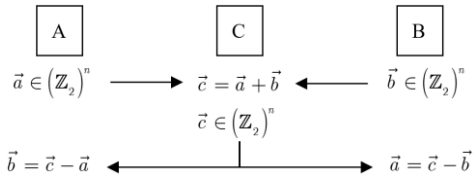
Trên thực tế, để đảm bảo việc truyền tin tin cậy giữa A và B người ta có thể dùng hệ thống vô tuyến cộng tác (cooperative radio - CR). Hệ thống này cho phép cung cấp tốc độ truyền dẫn cao hơn trên hệ thống truy nhập vô tuyến cũng như khả năng tạo vùng phủ rộng hơn. Xét hai nút A và B của một mạng không 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

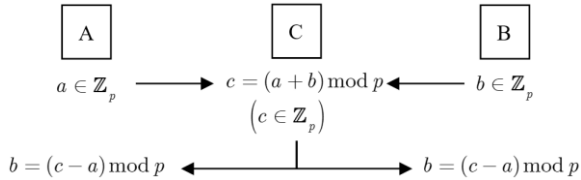
- Pha thứ ba: Nút A và B nhận sau khi nhận được $\vec{c}$ sẽ tiến hành giải mã $\vec{c}$ khôi phục thông tin: $\vec{b} = \vec{c} - \vec{a}$ và $\vec{a} = \vec{c} - \vec{b}$

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

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 được thực hiện như sau:

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

- Pha 2: C tính: $c = (a + b) \bmod p$ (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:

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

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

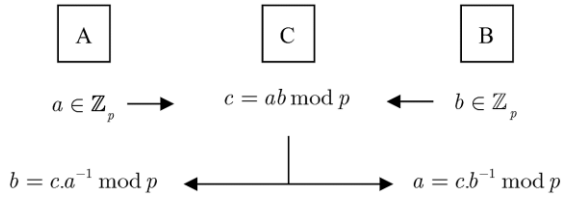
Chú ý:

– 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 vành số $\mathbb{Z}_p$, với p nguyên tố , khi đó $\mathbb{Z}_p = GF(p)$. 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: $c = a.b \bmod p$ (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.

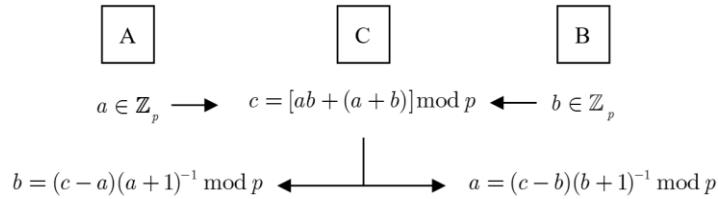
Tại nút A: $b = c.a^{-1} \bmod p$

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.

2.1.3.3. Mã mạng Affine trên vành số

Xét $\mathbb{Z}_p$ trong đó p là số nguyên tố, $\mathbb{Z}_p = \mathrm{GF}(p)$. Chúng ta có thể sử dụng cả phép cộng và phép nhân để thực hiện mã mạng Affine, như 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: $c = [ab + (a + b)] \bmod p$ (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: $$a = (c - b)(b + 1)^{-1} \quad (2.10)$$

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

2.2.1.2. Vành đa thức có 2 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 $\mathrm{Z}_2[x]/(x^n + 1)$. Trong vành đa thức này tồn tại nhóm nhân cyclic có cấp cực đại [13, 14]:

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

Với [13, 14]: $$k = \mathrm{maxord}a(x) = 2^{n-1} - 1 \quad (2.15)$$

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 $\mathrm{Z}_p^* = \mathrm{Z}_p/\{0\}$ có cấp $\left|\mathrm{Z}_p^*\right| = 2^n - 2$, với $\forall \mathrm{a} \in \mathrm{Z}_p^* \rightarrow \exists a^{-1} \in \mathrm{Z}_p^* : aa^{-1} \equiv 1 \mathrm{mod} p$.

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 $Z_2[x]/(x^n + 1)$ 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.

- **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].

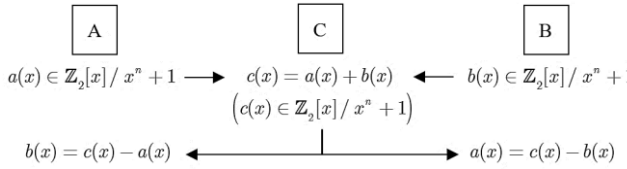
+ Xây dựng mã cyclic và cyclic cục bộ [2, 6, 12, 13, 14]

+ Một số hệ mật mã [4, 5]...

2.2.2. Thuật toán tính lũy thừa đa thức

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

Mô hình thực hiện mã mạng như hình 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:

$$c(x) = a(x) + b(x) \tag{2.16}$$

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: $a(x) = c(x) - b(x)$

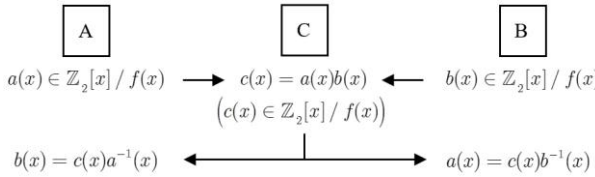
Chú ý: các phép cộng và trừ ở đây là cho các đa thức.

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:

$$c(x) = a(x).b(x) mod\ f(x) \tag{2.17}$$

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 $c(x)$:

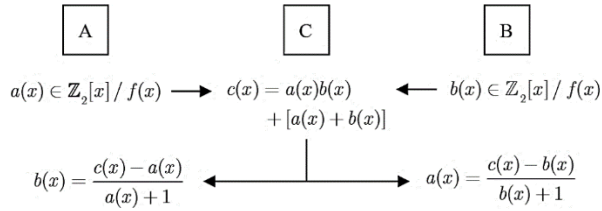
Tại nút A: $b(x) = c(x).a^{-1}(x) mod\ f(x)$

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 $b(x)$.

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:

$$c(x) = a(x).b(x) + [a(x) + b(x)] \tag{2.18}$$

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:

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

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

Hoặc: $$b(x) = [c(x) - a(x)].[a(x) + 1]^{-1} \tag{2.19}$$

Tại nút B:

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

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

Hoặc: $$a(x) = [c(x) - b(x)].[b(x) + 1]^{-1} \tag{2.20}$$

2.3. Mã mạng trên đường cong elliptic

2.3.1.1. Đường cong elliptic

2.3.1.2. Đường cong elliptic trên trường Galois

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:

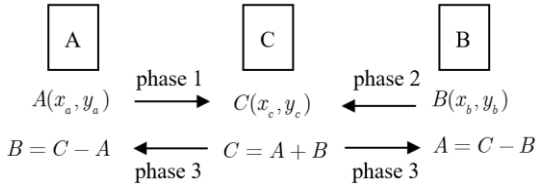
$$y^2 = x^3 + ax + b \bmod p$$

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 $P(x,y)$.

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 (2.22) với a, b thỏa mãn (2.23) 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:

$$C(x_c, y_c) = A(x_a, y_a) + B(x_b, y_b) \quad (2.26)$$

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: $B(x_b, y_b) = C(x_c, y_c) - A(x_a, y_a)$ (2.27)

Nút B nhận $C(x_c, y_c)$ và tính: $A(x_a, y_a) = C(x_c, y_c) - B(x_b, y_b)$ (2.28)

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.

3.1. Bài toán logarit rời rạc

3.1.1. Bài toán logarit trên trường số thực R

3.1.2. Bài toán logarit trên trường hữu hạn

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].

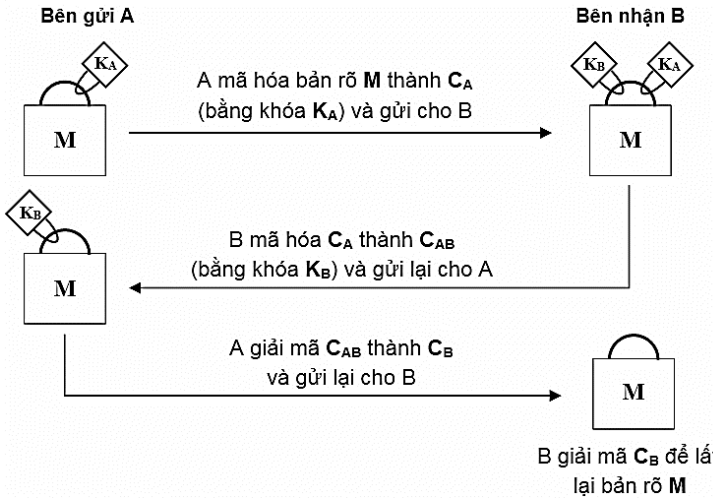
Hoạt động của hệ mật O-M được mô tả như trong Hình 3.1. Hai bên liên lạc A và B sẽ tự tạo cho mình các khóa bảo mật riêng (K_A, K_B), bên A cần gửi bản rõ M cho bên B, quá trình truyền tin thực hiện theo các bước sau:

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.



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

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]:

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

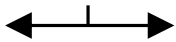
A	C	B
$x_A \xrightarrow{ElGamal}$	Giải mã lấy lại x_A, x_B và tạo x_C: $x_C = x_A x_B$ (hoặc $x_C = x_A + x_B$)	$\xleftarrow{ElGamal} x_B$

+ 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:

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

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

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

- *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:

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

+ 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:

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

- *Bước 4*:

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

$$x_C = D(C_A, k'_A)$$
$$x_B = x_C . x_A^{-1} \quad (3.17)$$

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

$$x_C = D(C_B, k'_B)$$
$$x_A = x_C . x_B^{-1} \quad (3.18)$$

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: $g^{kc} = 5^9 mod \, 23 = 11$

+ *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:

$$\gamma_A^{-k_C} = 17^{-9} = 17^{13}\ mod\ 23 = 10$$

$$\gamma_A^{-k_C}\ \delta_A = 10.21 \bmod 23 = \mathbf{3} = \boldsymbol{x_A}$$

- 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 VÀ KIẾN NGHỊ

** 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 CÁC 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.