Hệ mật Omura-Massey xây dựng trên vành đa thức có hai lớp kề cyclic

The Omura-Massey Cryptosystem Built on Polynomial Rings with Two Cyclotomic Cosets

Nguyễn Trung Hiếu*, Ngô Đức Thiện

Học viện Công nghệ Bưu chính Viễn thông – Số 122, Hoàng Quốc Việt, Cầu Giấy, Hà Nội

Đến Tòa soạn: 06-12-2017; chấp nhận đăng: 28-3-2018

Tóm tắt

Hệ mật Omura-Massey là một hệ mật khóa bất đối xứng (hệ mật khóa công khai) chủ yếu được xây dựng trên bài toán logarit rời rạc trên trường hữu hạn GF(p). Từ các kết quả nghiên cứu gần đây về sự tương đương của một số vành đa thức có hai lớp kề cyclic với trường hữu hạn GF(p), bài báo đề xuất phương pháp xây dựng hệ mật Omura-Massey vẫn dựa trên bài toán logarit rời rạc nhưng trên một số vành đa thức có hai lớp kề cyclic đặc biệt. Ngoài ra, dựa trên cơ sở các nhóm cộng và nhóm nhân trên vành đa thức có hai lớp kề cyclic, bài báo đề xuất thêm hai biến thể mới của hệ mật Omura-Massey.

Từ khóa: Mật mã khóa công khai, hệ mật Omura-Massey, vành đa thức, trường hữu hạn.

Abstract

The Omura-Massey Cryptosystem is an asymmetric key cryptosystem (public-key cryptosystem) that is mainly studied on the discrete logarithm problem in finite field GF(p). Based on recent research results on the equivalence of some polynomial rings with two cyclic cyclotomic cosets with Galois Field GF(p), the paper proposes the method of constructing the Omura-Massey cryptosystem that is also based on the discrete logarithm problem but in some special polynomial rings with two cyclotomic cosets. In addition, on the basic of additive groups and multiplicative groups of polynomial rings with two cyclotomic cosets, the article also proposes two new variants of the Omura-Massey cryptosystem.

Keywords: Public-key cryptography, Omura-Massey cryptosystem, polynomial ring, finite field.

1. Giới thiệu

Hệ mật Omura-Massey (O-M) được công bố vào năm 1982 [1], cho đến nay chủ yếu được nghiên cứu xây dựng trong trường số [2]. Các kết quả nghiên cứu được công bố về nhóm nhân cyclic, cấp số nhân cyclic, mã cyclic cục bộ xây dựng trên vành đa thức ([3], [4]) cho thấy mối quan hệ giữa mã sửa sai và vành đa thức, trong khi một số kết quả nghiên cứu bước đầu về mật mã ([5], [6], [7]) liên quan đến các hệ mật được thực hiện trên cấp số nhân cyclic của vành đa thức chẵn, và bước đầu gợi mở việc ứng dụng xây dựng hệ mật trên vành đa thức có hai lớp kề cyclic [8]. Cho tới gần đây, đã có nghiên cứu liên quan đến sự tương đương của một số vành đa thức có hai lớp kề cyclic và trường hữu hạn $GF(p)$ [9].

Để tiếp nối các nghiên cứu này, bài báo đề xuất xây dựng hệ mật O-M kết hợp giữa trường số và một số vành đa thức có hai lớp kề cyclic đặc biệt. Ngoài ra, cũng trên các vành đa thức kiểu này, bài báo sẽ đề xuất thêm hai biến thể của hệ mật O-M với cách che giấu dữ liệu khác nhau.

Nội dung bài báo được chia làm bốn phần. Phần 2, trình bày mối quan hệ giữa vành đa thức có hai lớp kề cyclic và trường số. Trong phần 3, trình bày cách xây dựng hệ mật O-M trên vành đa thức có hai lớp kề cyclic và một số biến thể của hệ mật này và phần cuối cùng là kết luận của bài báo.

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

Định nghĩa 1: Vành đa thức theo modulo $\mathbb{Z}_2[x]/(x^n+1)$ được gọi là vành đa thức có hai lớp kề cyclic nếu phân tích x^n+1 có dạng sau [5], [9]:

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

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

Trong vành đa thực này tồn tại nhóm nhân cyclic có cấp cực đại [5], [6], [9]:

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

$$\text{Với: } k=\max ord\, a(x)=2^{n-1}-1 \qquad (3)$$

** Mối quan hệ giữa $\mathbb{Z}_2[x]/(x^n+1)$ và $GF(p)$ [9]*

* Địa chỉ liên hệ: Tel.: (+84) 916.566.268
Email: hieunt@ptit.edu.vn

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

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

$$a(x)a^{-1}(x) \equiv 1 \bmod (x^n+1) \quad (4)$$

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

$$a(x) = \sum_{i \in I} f_i x^i \in \mathbb{Z}_2[x]/(x^n+1)$$
$$\mapsto a = \sum_{i \in I} f_i 2^i \in \mathbb{Z}_p^*$$

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 $\mathbb{Z}_2[x]/(x^n+1)$ 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). Ta có thể so sánh việc thực hiện các phép toán cộng và nhân trên hai cấu trúc này như bảng 1 [9].

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 [5], [6], [7]:

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

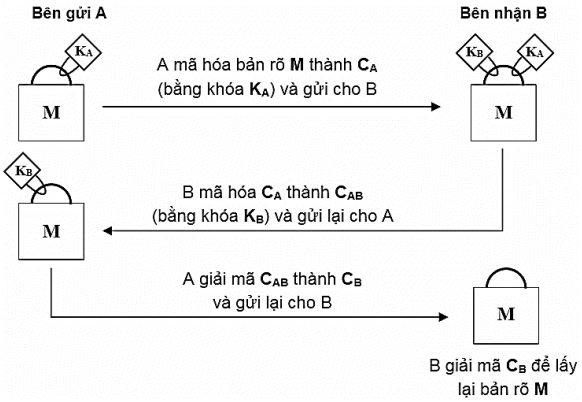
Bảng 1: Phép toán cộng và nhân trên hai cấu trúc vành đa thức và trường số.

Phép tính	Vành đa thức $\mathbb{Z}_2[x]/(x^n+1)$	Trường số $GF(p)$
Phép cộng	$a(x) = \sum_{i \in I \subset \mathbb{Z}_n} a_i x^i$; $b(x) = \sum_{i \in J \subset \mathbb{Z}_n} b_j x^j$ $c(x) = a(x) + b(x)$ $= \sum_{k \in K \subset \mathbb{Z}_n} c_k x^k$ $K = (I \cup J) - (I \cap J)$	$a, b \in GF(p)$ $c = a + b$ $\equiv (a+b) \bmod p$
Phép nhân	$c(x) = a(x)b(x)$ $\equiv a(x)b(x) \bmod (x^n+1)$	$c = a.b$ $\equiv a.b \bmod p$

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.

3. Xây dựng hệ mật Omura-Massey trên vành đa thức có hai lớp kề cyclic

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 [1].



Hình 1. Minh họa hoạt động của hệ mật O-M

Hoạt động của hệ mật O-M được mô tả như trong hình 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 (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 nhận C_{AB} và giải mã thành C_B rồi gửi cho B.
+ Bước 4: B nhận C_B và giải mã để nhận M.

3.1. Hệ mật O-M xây dựng trên bài toán logarit rời rạc

Bài toán logarit rời rạc (DLP) là một trong các bài toán một chiều khó, được sử dụng để xây dựng một số hệ mật khóa công khai, ví dụ như thủ tục trao đổi và thỏa thuận khóa Diffie – Hellman, hệ mật O-M, hệ mật ElGamal,… Phần sau đây sẽ trình bày cơ bản về hệ mật O-M xây dựng trên bài toán logarit rời rạc.

3.1.1 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: $m.n \equiv 1 \bmod (p-1)$.

+ Khóa riêng của B: B chọn cặp số ngẫu nhiên (u,v) thỏa mãn: $u.v \equiv 1 \bmod (p-1)$.

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:

$$\mathbb{Z}_{p-1}^* = \{i,\ i < (p-1),\ \gcd(i, p-1) = 1\} \qquad (5)$$

3.1.2 Quá trình truyền tin bảo mật

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

+ Bước 1: A tính: $C_A \equiv M^m \bmod p$ và gửi C_A cho B

+ Bước 2: B nhận C_A và tính $C_{AB} \equiv (M^m)^u \bmod p$ và gửi C_{AB} cho A.

+ Bước 3: A nhận C_{AB} và tính:

$C_B \equiv (M^{m.u})^n \bmod p \equiv M^u \bmod p$ và gửi C_B cho B

+ Bước 4: B nhận C_B và tính $(M^u)^v \bmod p \equiv M$

3.1.3 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 thảo 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 phép tấn công "Kẻ đứng giữa" (Man in the middle) có thể sử dụng thêm các phương pháp xác thực khác.

– Hệ số mở rộng bản tin của hệ mật O-M là 3 (phải truyền 3 lần giữa A và B).

3.2. Hệ mật O-M trên vành đa thức có hai lớp kề cyclic

Trong phần này, chúng tôi sẽ đề xuất xây dựng hệ mật O-M được xây dựng dựa trên trường số và vành đa thức có hai lớp kề cyclic.

3.2.1 Tạo khóa

+ Khóa công khai: Vành đa thức có hai lớp kề $\mathbb{Z}_2[x]/(x^n+1)$ cyclic.

+ Khóa riêng của A: A chọn ngẫu nhiên (m,n) thỏa mãn: $m.n \equiv 1 \bmod (2^{n-1}-1)$.

+ Khóa riêng của B: B chọn ngẫu nhiên (u,v) thỏa mãn: $u.v \equiv 1 \bmod (2^{n-1}-1)$.

Chú ý: $m,n,u,v \in \mathbb{Z}_q^*; q = 2^{n-1}-1$, với $\mathbb{Z}_q^*$ là nhóm nhân cyclic của vành số theo modulo $\mathbb{Z}_q$, cách xây dựng $\mathbb{Z}_q$ như biểu thức (5). Sở dĩ ta lấy theo modulo của $q = 2^{n-1}-1$ vì đây là cấp cực đại của nhóm nhân cyclic trên vành đa thức có hai lớp kề, như biểu thức (3).

3.2.2 Quá trình truyền tin bảo mật

Bên A muốn gửi bản rõ $M(x) \in \mathbb{Z}_2[x]/(x^n+1)$ tới bên B. (Chú ý, bản rõ và các bản mã đều được biểu diễn bằng các đa thức).

+ Bước 1: A mã hóa: $C_A(x) = [M(x)]^m \bmod (x^n+1)$ và gửi cho B.

+ Bước 2: B nhận $C_A(x)$ và mã hóa

$$\begin{aligned} C_{AB}(x) &\equiv [C_A(x)]^u \bmod (x^n+1) \\ &= \{[M(x)]^m\}^u \bmod (x^n+1) \end{aligned}$$

sau đó B gửi $C_{AB}(x)$ cho A.

+ Bước 3: A nhận $C_{AB}(x)$ và giải mã:

$$\begin{aligned} C_B(x) &\equiv \left[C_{AB}(x)\right]^n \bmod (x^n+1) \\ &= \{[M(x)]^{m.u}\}^n \bmod (x^n+1) \\ &\equiv [M(x)]^u \bmod (x^n+1) \end{aligned}$$

và gửi $C_B(x)$ cho B.

+ Bước 4: B nhận $C_B(x)$ và giải mã

$$\begin{aligned} [C_B(x)]^v \bmod (x^n+1) &= \{[M(x)]^u\}^v \bmod (x^n+1) \\ &\equiv M(x) \end{aligned}$$

3.2.3 Ví dụ 2

** Tạo khóa:*

+ Khóa công khai: Chọn $n = 5 \Rightarrow q = 2^{5-1}-1 = 15$ và vành đa thức $\mathbb{Z}_2[x]/(x^5+1)$.

+ Khóa riêng của A:

$$(m,n) = (2,8) : 2.8 \equiv 1 \bmod 15$$

+ Khóa riêng của B:

$$(u,v) = (7,13) : 7.13 \equiv 1 \bmod 15$$

** Quá trình truyền tin bảo mật:*

Chú ý, để thuận tiện ta mô tả các đa thức theo dạng số mũ của x, ví dụ $a(x) = 1 + x^3 + x^4 \leftrightarrow (034)$.

Bên A muốn gửi bản rõ $M(x)$ biểu diễn như sau: $M(x) = 1 + x^3 + x^4 \leftrightarrow (034)$ tới bên B, quá trình truyền tin thực hiện như sau:

+ Bước 1: A tính:

$$C_A(x) = (034)^2 \bmod(x^5 + 1) \equiv (013)$$

và gửi cho B.

+ Bước 2: B nhận $C_A(x)$ và tính

$$C_{AB}(x) \equiv (013)^7 \bmod(x^5 + 1) \equiv (134)$$

sau đó B gửi $C_{AB}(x)$ cho A.

+ Bước 3: A nhận $C_{AB}(x) = (134)$ và tính:

$$C_B(x) \equiv (134)^8 \bmod(x^5 + 1) \equiv (234)$$

và gửi $C_B(x)$ cho B.

+ Bước 4: B nhận $C_B(x) = (234)$ và giải mã

$$(234)^{13} \bmod(x^5 + 1) \equiv (034) = M(x)$$

3.2.4 Nhận xét

– Hệ mật là an toàn nếu bài toán logarit rời rạc trên vành đa thức có hai lớp kề cyclic là bài toán khó.

– Hệ mật này không có tính năng xác thực.

– Hệ số mở rộng bản tin của hệ mật này là 3.

– Phương pháp sử dụng che giấu thông tin trong hệ mật này là phương pháp mặt nạ mũ.

3.3. Một số biến thể của hệ mật O-M trên vành đa thức có hai lớp kề cyclic

Trong phần này, chúng tôi sẽ đề xuất xây dựng hai biến thể của hệ mật O-M được xây dựng trên vành đa thức có hai lớp kề cyclic, với hai phương pháp che giấu dữ liệu là mặt nạ cộng và mặt nạ nhân.

3.3.1 Hệ mật O-M mặt nạ cộng

** Tạo khóa*

+ Khóa công khai: $\mathbb{Z}_2[x]/(x^n + 1)$ – Vành đa thức có hai lớp kề cyclic.

+ Khóa riêng của A: chọn một đa thức ngẫu nhiên $a(x) \in \mathbb{Z}_2[x]/(x^n + 1)$, $a(x) \neq 0$.

+ Khóa riêng của B: chọn một đa thức ngẫu nhiên $b(x) \in \mathbb{Z}_2[x]/(x^n + 1), b(x) \neq 0$.

** Quá trình truyền tin*

A muốn gửi bản tin $M(x) \in \mathbb{Z}_2[x]/(x^n + 1)$ tới B

+ Bước 1: A tính:

$C_A(x) \equiv [M(x) + a(x)] \bmod(x^n + 1)$ và gửi cho B.

+ Bước 2: B nhận $C_A(x)$ và tính

$$C_{AB}(x) \equiv \{[M(x) + a(x)] + b(x)\} \bmod(x^n + 1)$$

sau đó B gửi $C_{AB}(x)$ cho A.

+ Bước 3: A nhận $C_{AB}(x)$ và tính:

$$C_B(x) \equiv \{[M(x) + a(x) + b(x)] + a(x)\} \bmod(x^n + 1)$$
$$= [M(x) + b(x)] \bmod(x^n + 1)$$

và gửi $C_B(x)$ cho B.

+ Bước 4: B nhận $C_B(x)$ và giải mã

$$\{[M(x) + b(x)] + b(x)\} \bmod(x^n + 1) = M(x)$$

Chú ý: Phép cộng trên vành đa thức là cộng modulo 2, do đó tổng hai đa thức giống nhau sẽ bằng 0.

Ví dụ 3:

** Tạo khóa:*

+ Khóa công khai: chọn $\mathbb{Z}_2[x]/(x^5 + 1)$.

+ Khóa riêng của A: $a(x) = (013) \in \mathbb{Z}_2[x]/(x^5 + 1)$

+ Khóa riêng của B: $b(x) = (124) \in \mathbb{Z}_2[x]/(x^5 + 1)$

** Truyền tin bảo mật*

A muốn gửi bản tin $M(x) = (034)$ tới B.

+ Bước 1: A tính:

$C_A(x) \equiv [(034)+(013)] \bmod(x^5 + 1) \equiv (14)$

và gửi cho B.

+ Bước 2: B nhận $C_A(x)$ và tính

$$C_{AB}(x) \equiv \big[(14) + (124)\big] \bmod(x^5 + 1) \equiv (2)$$

sau đó B gửi $C_{AB}(x)$ cho A.

+ Bước 3: A nhận $C_{AB}(x)$ và tính:

$$C_B(x) \equiv [(2) + (013)] \bmod(x^5 + 1) = (0123)$$

và gửi $C_B(x)$ cho B.

+ Bước 4: B nhận $C_B(x)$ và giải mã

$$\big[(0123) + (124)\big] \bmod(x^5 + 1) = (034) = M(x)$$

Nhận xét:

- Nếu khóa bí mật được chọn ngẫu nhiên thì hệ mật là an toàn nếu không gian khóa đủ lớn (tức là phải chọn n lớn).
- Hệ mật này không có xác thực.
- Hệ số mở rộng bản tin của hệ mật này là 3.
- Việc tính toán của hệ mật này rất đơn giản.

3.3.2 Hệ mật O-M mặt nạ nhân

Hệ mật này sẽ sử dụng các phần tử trong nhóm nhân cyclic có cấp cực đại làm khóa, việc mã hóa và giải mã thực hiện theo cách nhân các đa thức trong nhóm.

** Tạo khóa:*

+ Khóa công khai: $\mathbb{Z}_2[x]/(x^n+1)$ – Vành đa thức có hai lớp kề cyclic.
+ Khóa riêng của A: chọn một đa thức ngẫu nhiên $a(x) \in \mathbb{Z}_2[x]/(x^n+1)$, $\mathrm{w}(a(x))$ lẻ.
+ Khóa riêng của B: chọn một đa thức ngẫu nhiên $b(x) \in \mathbb{Z}_2[x]/(x^n+1)$, $\mathrm{w}(b(x))$ lẻ.

Trong đó $a(x), b(x) \in G$, G là nhóm nhân cyclic có cấp cực đại như mô tả trong (2); $a(x), b(x)$ có trọng số lẻ để thỏa mãn điều kiện ở biểu thức (4) [3], [4].

** Quá trình truyền tin bảo mật*

A muốn gửi bản tin $M(x) \in \mathbb{Z}_2[x]/(x^n+1)$ tới B

+ Bước 1: A tính:

$C_A(x) \equiv [M(x).a(x)] \bmod (x^n+1)$ và gửi cho B.

+ Bước 2: B nhận $C_A(x)$ và tính:

$$C_{AB}(x) \equiv \{[M(x).a(x)].b(x)\} \bmod (x^n+1)$$

sau đó B gửi $C_{AB}(x)$ cho A.

+ Bước 3: A nhận $C_{AB}(x)$ và tính:

$$C_B(x) \equiv \{[M(x).a(x).b(x)].a^{-1}(x)\} \bmod (x^n+1)$$
$$= [M(x).b(x)] \bmod (x^n-1)$$

và gửi $C_B(x)$ cho B.

+ Bước 4: B nhận $C_B(x)$ và giải mã

$$\{[M(x).b(x)]b^{-1}(x)\} \bmod (x^n+1) = M(x)$$

Ví dụ 4:

** Tạo khóa*

+ Khóa công khai: chọn $\mathbb{Z}_2[x]/(x^5+1)$.

+ Khóa riêng của A: $a(x) = (013) \rightarrow a^{-1}(x) = (123)$

+ Khóa riêng của B: $b(x) = (124) \rightarrow b^{-1}(x) = (012)$

** Truyền tin bảo mật*

A muốn gửi một bản tin $M(x) = (034)$ tới B.

+ Bước 1: A tính:

$C_A(x) \equiv [(034).(013)] \bmod (x^5+1) \equiv (2)$

và gửi cho B.

+ Bước 2: B nhận $C_A(x)$ và tính

$$C_{AB}(x) \equiv \big[(2).(124)\big] \bmod (x^5+1) \equiv (134)$$

sau đó B gửi $C_{AB}(x)$ cho A.

+ Bước 3: A nhận $C_{AB}(x)$ và tính:

$$C_B(x) \equiv [(134).(123)] \bmod (x^5+1) = (3)$$

và gửi $C_B(x)$ cho B.

+ Bước 4: B nhận $C_B(x)$ và giải mã

$$\big[(3).(012)\big] \bmod (x^5+1) = (034) = M(x)$$

Nhận xét

- Nếu các khóa bí mật được chọn ngẫu nhiên thì hệ mật là an toàn nếu không gian khóa đủ lớn.
- Hệ mật không có xác thực.
- Hệ số mở rộng bản tin của hệ mật là 3.
- Việc tính toán hệ mật này khá đơn giản.

4. Kết luận

Bài báo đã đề xuất phương pháp xây dựng hệ mật O-M trên vành đa thức có hai lớp kề cyclic, nhờ việc áp dụng các nghiên cứu về sự tương đương của các vành đa thức này với trường hữu hạn, phương pháp che giấu thông tin trong hệ mật này theo kiểu mặt nạ mũ, tương tự hệ mật O-M xây dựng trên trường hữu hạn và bài toán DLP. Độ an toàn của hệ mật này có thể đánh giá tương đương với hệ mật O-M trên bài toán DLP.

Trong phần tiếp theo, bài báo đề xuất hai biến thể của hệ mật O-M với phương pháp che giấu dữ liệu theo kiểu mặt nạ cộng dùng các phần tử của vành đa thức và mặt nạ nhân dựa trên nhóm nhân cyclic có cấp cực đại. Tuy nhiên, để có các đánh giá đầy đủ về hai hệ mật này cần có các nghiên cứu thêm về độ an toàn, độ khuếch tán (diffusion), tính gây lẫn (confusion)...

Tài liệu tham khảo

[1] D. R. Stinson, Cryptography Theory and Practice, CRC Press, 1995.

[2] Menezes A. J., Van Oorschot P. C., Vanstone S. A, Handbook of Applied Cryptography, CRC Press, 2005.

[3] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, "Novel algebraic structure for cyclic codes," Applied Algebra, Algebraic Algorithms, and Error Correcting Codes – Conf. AAECC 17, LNCS 4851, Springer-Verlag Berlin Heidelberg, 2007, pp. 301-310.

[4] Nguyen Binh, "Cyclic and Local Cyclic Codes over Polynomial Ring," Journal of Science and Technology, vol. 50, (2012) , pp. 735-749.

[5] 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.

[6] Hồ Quang Bửu, Ngô Đức Thiện, Trần Đức Sự, "Xây dựng hệ mật trên các cấp số nhân cyclic của vành đa thức," Tạp chí Khoa học và Công nghệ, Viện Khoa học và Công nghệ Việt Nam, Tập 50 số 2A, 2012.

[7] Ngô Đức Thiện, Nguyễn Trung Hiếu, Nguyễn Toàn Thắng, Đặng Hoài Bắc (2013), "Một phương pháp xây dựng hệ mật mã khối kết hợp sơ đồ Lai-Massey với sơ đồ Feistel và ứng dụng vào hàm băm", Kỷ yếu Hội nghị Quốc gia về Điện tử - Truyền thông (REV2013-KC01), Hà Nội, Việt Nam, ngày 17-18/12/2013, tr. 75-80.

[8] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, "New Algebraic Structure Based on Cyclic Geometric Progressions over Polynomial Ring Applied for Cryptography" IEEE, International Conference on Computational Intelligence and Security (CIS) CIS'07, December 15-19, 2007, Harbin, China.

[9] 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.