HỆ MẬT OMURA-MASSEY TRÊN VÀNH ĐA THỨC CÓ HAI LŨY ĐẲNG NGUYÊN THỦY

Hoàng Mạnh Thắng[*], Nguyễn Bình[#], Nguyễn Trung Hiếu[#], Cao Minh Thắng[#], Hoàng Thị Thu[#]
[*]Ban Chiến lược sản phẩm, VNPT-IT
[#]Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: Vành đa thức có tốc độ tính toán nhanh, cài đặt đơn giản, có nhiều tiềm năng trong việc ứng dụng xây dựng các hệ mật có tài nguyên hạn chế. Vành đa thức có hai lũy đẳng nguyên thủy là một loại vành đa thức đặc biệt, có tính chất tựa đẳng cấu với trường hữu hạn GF(p), nhưng chưa được khai thác trong các bài toán về mật mã. Bài báo này làm rõ tính chất tựa đẳng cấu của vành đa thức hai lũy đẳng nguyên thủy với trường hữu hạn GF(p), đồng thời, ứng dụng tính chất này để cải tiến hệ mật Omura-Massey trên trường hữu hạn GF(p)thành hệ mật trên vành đa thức.

Từ khoá: vành đa thức, hệ mật, lũy đẳng nguyên thủy.

I. GIỚI THIỆU

Hệ mật Omura-Massey (O-M) là một hệ mật tương đối đặc biệt, mỗi bên tham gia phiên giao dịch cần dùng hai khóa có tính chất nghịch đảo với nhau, tương tự như khóa bất đối xứng của các hệ mật khóa công khai thường thấy, nhưng hai khóa của hệ mật O-M lại được giữ bí mật. Nguyên gốc, hệ mật O-M được xây dựng trên bài toán logarits rời rạc trên trường hữu hạn $GF(p)$. Cho đến nay, đã có nhiều nghiên cứu, cải tiến hệ mật O-M nhưng vẫn chủ yếu trên trường số.

Vành đa thức là một cấu trúc toán học đặc biệt, có nhiều tiềm năng ứng dụng. Vành đa thức được phân chia thành nhiều loại khác nhau với các tính chất, đặc điểm khác nhau. Điển hình nhất là vành đa thức hai lớp kề Cyclic, đã có nhiều công trình nghiên cứu được công bố, điển hình như các công trình nghiên cứu về mặt toán học, cấu trúc, tính chất của vành như [1], [2], [8] và việc ứng dụng vành đa thức hai lớp kề Cyclic để cải tiến, xây dựng các mã, các hệ mật như [3], [4], [5], [6], [7], [9], [10].

Tiếp theo các công trình nghiên cứu này, với đặc điểm của vành đa thức có hai lũy đăng nguyên thủy được đánh giá tiềm năng tương đương với vành đa thức có hai lớp kề Cyclic, bài báo này làm rõ về tính chất tựa đẳng cấu giữa Vành đa thức hai lũy đẳng nguyên thủy với trường hữu hạn $GF(p)$, đồng thời ứng dụng tính chất tựa đẳng cấu này để cải tiến hệ mật Omura-Massey trên trường số $GP(p)$ thành hệ mật trên vành đa thức.

Tác giả liên hệ: Hoàng Mạnh Thắng,
Email: hoangthang@vnpt.vn
Đến tòa soạn: 10/2022, chỉnh sửa: 11/2022, chấp nhận đăng: 12/2022.

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

II. TÍNH CHẤT TỰA ĐẲNG CẤU GIỮA VÀNH ĐA THỨC HAI LŨY ĐẲNG NGUYÊN THỦY VÀ TRƯỜNG HỮU HẠN $GF(p)$

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

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

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

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

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

Với hai lũy đẳng nguyên thủy này, vành đa thức có hai nhóm nhân là:

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

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

biểu diễn dạng:

$$\boldsymbol{\mathcal{A}} = \begin{Bmatrix} x^i \, mod(1+x)\, g(x); \\ i = \overline{1,2^l-1} \end{Bmatrix} \tag{3}$$

Nhóm nhân B: số các phần tử là

$$|B| = 2^l - 1 \quad (4)$$

biểu diễn dạng:

$$\boldsymbol{\mathcal{B}} = \left\{ \begin{matrix} [x^i + g(x)]\, mod(1+x)\, g(x); \\ i = \overline{1,2^l - 1} \end{matrix} \right\} \quad (5)$$

Ví dụ:

Vành đa thức hai lũy đẳng nguyên thủy:

$$\frac{Z_2(x)}{(1+x)(1+x+x^4)} \quad (6)$$

Hai lũy đẳng là: 1 và $x + x^4$

Thật vậy:

$$(1)^2 = 1 \quad (7)$$

$$(\boldsymbol{x + x^4})^{\boldsymbol{2}} = \boldsymbol{x^8 + x^5 + x^5 + x^2}$$
$$\equiv (\boldsymbol{x^8 + x^2})\ \boldsymbol{mod}\ (\boldsymbol{1+x})(\boldsymbol{1+x+x^4}) = \boldsymbol{x + x^4} \quad (8)$$

Ví dụ về phép module $(1+x)(1+x+x^4)$ của đa thức $(x^8 + x^2)$ Chi tiết phép tính như sau:

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

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

$$\mathcal{A} = \{(1), (2), (3), (4), (024), (01234),$$
$$(013), (124), (034), (012), (123), (234),$$
$$(023), (134), (0)\};\ |A| = 15$$
$$\mathcal{B} = \{(04), (0124), (0134), (01), (12),$$
$$(23), (34), (02), (13), (24), (0234),$$
$$(0123), (1234), (03), (14)\};\ |B| = 15$$

Nhóm nhân $\mathcal{A}$ có thể được biểu diễn trong trường số $GF(p)$ như trong Bảng 1:

Bảng 1: Ánh xạ phần tử nhóm nhân A với các phần tử trong trường hữu hạn GF(p)

Phần tử trong vành đa thức: x^i	***Các đa thức nhóm $\mathcal{A}$:*** $x^i \bmod (1+x)(1+x+x^4)$	***Trường hữu hạn $GF(p)$:*** $p = 2^l - 1 = 2^4 - 1 = 15$
x^1	(1)	2
x^2	(2)	4
x^3	(3)	8
x^4	(4)	16
x^5	(024)	21
x^6	(01234)	31
x^7	(013)	11
x^8	(124)	22
x^9	(034)	25
x^{10}	(012)	7
x^{11}	(123)	14
x^{12}	(234)	32
x^{13}	(023)	13
x^{14}	(134)	26
x^{15}	(0)	1

Nhóm nhân $\mathcal{B}$ có thể được biểu diễn trong trường số $GF(p)$ như Bảng 2:

Bảng 2: Ánh xạ phần tử nhóm nhân B với các phần tử trong trường hữu hạn GF(p)

Phần tử trong vành đa thức: $x^i + g(x)$	***Các đa thức nhóm $\mathcal{B}$:*** $x^i \bmod (1+x)(1+x+x^4)$	***Trường hữu hạn $GF(p)$:*** $p = 2^l - 1 = 2^4 - 1 = 15$
$1 + x^4$	(04)	17

$1+x+x^2+x^4$	(0124)	23
$1+x+x^3+x^4$	(0134)	27
$1+x$	(01)	3
$1+x+x^4+x^5$	(12)	6
$1+x+x^4+x^6$	(23)	12
$1+x+x^4+x^7$	(34)	24
$1+x+x^4+x^8$	(02)	5
$1+x+x^4+x^9$	(13)	10
$1+x+x^4+x^{10}$	(24)	20
$1+x+x^4+x^{11}$	(0234)	29
$1+x+x^4+x^{12}$	(0123)	15
$1+x+x^4+x^{13}$	(1234)	30
$1+x+x^4+x^{14}$	(03)	9
$1+x+x^4+x^{15}$	(14)	18

Ví dụ về phép ánh xạ các phép tính nhân giữa trường số và vành đa thức như trong Bảng 3.

Bảng 3: Ánh xạ phép tính nhóm nhân với các phép tính trong trường hữu hạn GF(p)

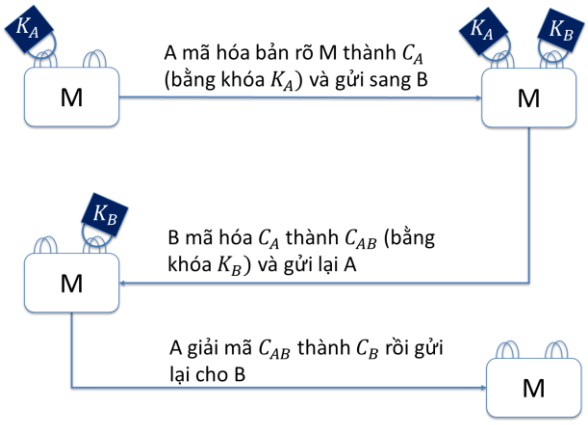
Phép tính	***Chi tiết***
Trên vành đa thức	$a(x).b(x) = (013)(01234)$ $= (1+x+x^3)(1+x+x^2+x^3+x^4)$ $= 1+x^3+x^4+x^6+x^7$ $\equiv (1+x^3+x^4+x^6+x^7)$ $mod\ (1+x)(1+x+x^4)$ $= 1+x^3 \equiv (03)$
Trên Trường số $GF(15)$	$a.b = 11.31 = 241$ $\equiv 341\ mod\ 15$ $= 11$

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

- Mọi phần tử trên vành đa thức hai lũy đẳng nguyên thủy có hai nhóm nhân A. và B đều có thể tìm được một phần tử trên trường số $GP(p)$.
- Các tính chất quan trọng như tính giao hoán, tính phân phối, tính kết hợp, phần tử đơn vị, tính nghịch đảo của vành đa thức được giữ nguyên trên trường số.

III. HỆ MẬT OMURA-MASSEY TRÊN TRƯỜNG HỮU HẠN

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



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

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

- Bước 1: A mã hóa bản rõ M thành bản mã C_A bằng khóa của $A(K_A)$ 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.

Khóa bí mật được lựa chọn như sau:

1) A chọn ngẫu nhiên cặp số *(m, n):*

$$m.n \equiv 1\ mod\ p \quad (9)$$

2) B chọn ngẫu nhiên cặp số *(u, v):*

$$u\,.v = 1\ mod\ p \quad (10)$$

Bảng 4: Thủ tục trao đổi thông tin của hệ mật O-M

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

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

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

Ví dụ: *p = 17*

Bảng 5: Ví dụ thủ tục trao đổi thông tin của hệ mật O-M

$A(3,6) \leftrightarrow B(5,7)$ Bản tin muốn gửi từ A sang B là $M = 9$	
A mã hóa M thành C_A	A tính $C_A = 9.3 \; mod \; 17 = 10$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = 10.5 \; mod \; 17 = 16$
A giải mã C_{AB} thành C_B	A tính $C_B = 16.6 \; mod \; 17 = 11$
B giải mã C_B lấy M	B tính $11.7 \; mod \; 7 = 9 = M$

IV. CẢI TIẾN HỆ MẬT OMURA-MASSEY BẰNG VÀNH ĐA THỨC HAI LŨY ĐẲNG NGUYÊN THỦY

Do tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy và trường số nguyên $GF(p)$, nên các phần tử và phép tính nhân trên vành đa thức có thể thay thế được các số nguyên và phép tính nhân trong trường số $GF(p)$ của hệ mật Omura-Massey. Phần tiếp theo trình bày chi tiết việc thay thế này như là một cải tiến của hệ mật O-M trên vành đa thức.

Để tiện theo gõi, Hệ mật O-M cải tiến được trình bày theo các bước của giao dịch như sau:

A. Tạo khóa

Trước tiên, hai bên A và B cần thống nhất đa thức hai lũy đẳng nguyên thủy cũng như nhóm nhân sẽ sử dụng, cụ thể là đa thức $g(x)$ và nhóm nhân như công thức (3) hay (4), ở đây chọn nhóm nhân(3) để trình bày chi tiết.

Khi chọn đa thứ bất khả quy $g(x)$ sẽ xác định được bậc cao nhất của đa thức là l.

Sau đó, A và B chọn cặp khóa bí mật như sau:

- Khóa bí mật của A: *(m, n):*

$$m.n \equiv 1 \; mod \; 2^l - 1 \qquad (11)$$

- Khóa bí mật của B: *(u, v):*

$$u.v \equiv 1 \; mod \; 2^l - 1 \qquad (12)$$

B. Thủ tục trao đổi thông tin

Bảng 6: Thủ tục trao đổi thông tin của hệ mật O-M trên vành đa thức hai lũy đăng nguyên thủy

$A(m,n) \leftrightarrow B(u,v)$ Bản tin A muốn gửi cho B được trình bày dạng: $M = k(x)$	
A mã hóa M thành C_A	A tính $C_A = k(x).m \; mod \; (1+x)g(x)$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = k(x).m.u \; mod \; (1+x)g(x)$
A giải mã C_{AB} thành C_B	A tính $C_B = k(x).m.u.n \; mod \; (1+x)g(x)$
B giải mã C_B lấy M	B tính $k(x).u.v \; mod \; (1+x)g(x) = k(x) = M$

C. Ghi chú

Hệ mật này vẫn giữa nguyên các đặc tính của hệ mật gốc là

- Để đảm bảo độ mật, cần phải thay khóa trong mỗi một phiên.
- Chưa có tính xác thực các bên tham gia hệ mật.
- Hệ số mở rộng bản tin vẫn bằng 3.

D. Ví dụ

- A và B thống nhất đã thức hai lũy đẳng nguyên thủy:

$$\frac{Z_2[X]}{(1+x)(1+x+x^4)} \quad (13)$$

Trong đó:

$$g(x) = 1 + x + x^4 \quad (14)$$

$$(1+x)(1+x+x^4) = (x^5 + x^4 + x^2 + 1) = (0245) \quad (15)$$

- Chọn nhóm nhân $\mathcal{A}$:

$$\mathcal{A} = \{(1), (2), (3), (4), (024), (01234), (013), (124), (034), (012), (123), (234), (023), (134), (0)\}; \quad (16)$$

$$|\mathcal{A}| = 2^l - 1 = 2^4 - 1 = 15 \quad (17)$$

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

$$m = (2) = x^2 \quad (18)$$

$$n = (023) = 1 + x^2 + x^3 \quad (19)$$

Vì:

$$m.n = (x^2)(1 + x^2 + x^3)\ mod\ (1+x)(1+x+x^4) = (x^5 + x^4 + x^2)\ mod\ (x^5 + x^4 + x^2 + 1) = 1 \quad (20)$$

Chi tiết phép tính:

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

- B chọn cặp khóa bí mật của B:(u, v)

$$u = (4) = x^4 \quad (21)$$

$$v = (123) = x + x^2 + x^3 \quad (22)$$

Vì:

$$u.v = (x^4)(x + x^2 + x^3) mod\ (1+x)(1+x+x^4) = (x^7 + x^6 + x^5)\ mod\ (x^5 + x^4 + x^2 + 1) = 1 \quad (23)$$

Chi tiết phép tính:

-	$x^7 + x^6 + x^5$	$x^5 + x^4 + x^2 + 1$
	$x^7 + x^6 + x^4 + x^2$	$x^2 + 1$
-	$x^5 + x^4 + x^2$	
	$x^5 + x^4 + x^2 + 1$	
	1	

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

Bảng 7: Ví dụ về trao đổi bản tin của hệ mật O-M trên vành đa thức hai lũy đẳng nguyên thủy

$A((2),(023)) \leftrightarrow B((4),(123))$ Bản tin A muốn gửi cho B được trình bày dạng: $M(x) = (134)$	
A mã hóa M thành C_A	A tính $C_A = (134)(2)\ mod\ (0245) = (1)$
B mã hóa C_A thành C_{AB}	B tính $C_{AB} = (1)(4) mod\ (0245) = (024)$
A giải mã C_{AB} thành C_B	A tính $C_B = (024)(023)\ mod\ (0245) = (3)$
B giải mã C_B lấy M	B tính $(3)(123) mod\ (0245) = (134) = M$

V. KẾT LUẬN

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

REFERENCES

[1] 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.

[2] 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.

[3] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, Young Hoon Kim (2007). Polynomial rings with two cyclotomic cosets and their applications in Communication, MMU International Symposium Information and Communications Technologies 2007, Malaysia, ISBN: 983-43160-0-3

[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, 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.

[6] 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.

[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] 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.

[9] Nguyễn Trung Hiếu, Ngô Đức Thiện, "Hệ mật OmuraMassey xây dựng trên vành đa thức có hai lớp kề cyclic", Tạp chí Khoa học và Công nghệ các trường Đại học Kỹ thuật, , trang 29-34, số 125, 2018, ISSN 2354-1083.

[10] Hoang Manh Thang, Nguyen Binh, Cao Minh Thang, "Omura-Massey cryptosystem with authentication over polynomial rings with two cyclotomic cosets", Journal of Science and Technology, Posts and Telecommunication Institute of Technology, CS.01, 2018, pp 17-20, In Vietnamese..

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

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

THE OMURA-MASSEY CRYPTOSYSTEM BUILT ON POLYNOMIAL RINGS WITH TWO PRIMITIVE IDEMPOTENTS

Abstract: Polynomial rings have fast computational speed, simple implementation, and great potential in constructing cryptographic systems with limited resources. The polynomial ring with two primitive idempotents is a special type of polynomial ring that shares isomorphism properties with the finite field $GF(p)$, but has not been fully utilized in cryptographic problems. This paper clarifies the isomorphism properties of the polynomial ring with two primitive roots and the finite field $\boldsymbol{GF(p)}$. Furthermore, it applies these properties to enhance the cryptographic system from the $GF(p)$ to the polynomial ring.

Keywords: polynomial ring, cryptosystem, primitive idempotent.

Hoàng Mạnh Thắng, nhận học vị Thạc sỹ 2012; Hiện công tác tại Tập đoàn Bưu chính Viễn thông Việt Nam. Lĩnh vực nghiên cứu: Mật mã hạng nhẹ, An toàn bảo mật hệ thống thông tin, Blockchain, AI.

Email: hoangthang@vnpt.vn

Nguyễn Bình, nhận học vị Tiễn sĩ năm 1984, học hàm Giáo sư năm 2006; Hiện đang làm trưởng ban thường trực Hội đồng tiến sĩ của Học viện CNBCVT, và là ủy viên Hội đồng chức danh Nhà nước liên ngành Điện – Điện tử - Tự động hóa 2014-2019.

Email: nguyenbinh@ptit.edu.vn

Nguyễn Trung Hiếu, nhận học vị Tiến sĩ năm 2019; Hiện đang công tác lại Học viện Công nghệ Bưu chính Viễn thông.

Email: hieunt@ptit.edu.vn

Cao Minh Thắng, nhận học vị Tiến sĩ năm 2018; Hiện công tác tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Mật mã hạng nhẹ, An toàn bảo mật hệ thống thông tin.

Email: thangcm@ptit.edu.vn

Hoàng Thị Thu, Hiện đang công tác lại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: IoT, WSN, Mạng viễn thông, Điện toán biên

Email: thuht@ptit.edu.vn