OMURA-MASSEY CYPTOSYSTEM WITH AUTHENTICATION OVER POLYNOMIAL RINGS WITH TWO CYCLOTOMIC COSETS

Hoang Manh Thang, Nguyen Binh, Cao Minh Thang
Post and Telecommunications Institute of Technology

Abstract: With the advantage of Polynomial rings, it is possible to calculate fast, simple installation, researching the application of polynomial rings for lightweight cryptography systems is considered suitable. Continuing the idea of applying polynomials to improve the Omura-Massey cryptosystem as a cryptosystem that can be applied on a constraint device in article [2]; This article continues to improve the Omura-Massey cryptosystem by using polynomial polynomials to add an authentication attribute to the cryptosystem (1,2,3,4 corresponding to multiplication, addition, exponential, logarithmic on Polynomial ring).

Keyword: Omura Massey, authentication, polynomial rings.

I. INTRODUCTION

The applications polynomial rings $Z_q[x]/(x^n + 1)$ in cryptography are typically in constructing a famous probabilistic public-key cryptosystem NTRU [4] and some variants such as CTRU [5] and especially pNE [8] which operates in $Z_{2^s}(x)$ and is so far the unique provably-secure variant of NTRU.

The advantage of using polynomial rings in encryption schemes is the computation speed. The modular multiplication in polynomial rings $R_{n,q}$ takes $O(n^2)$ operations. By exploiting this feature, along with security related to some hard problems over lattices, NTRU is faster and generally considered as a reasonable alternative to the encryption schemes based on integer factorization and discrete logarithm over finite fields and elliptic curves and is standardized in IEEE P.1363.1 standard in 2008.

Binary quotient polynomial rings $R_n = Z_2[x]/(x^n + 1)$, a class of $R_{n,q}$, although popularly used in error-correcting codes, have been not widely applied in cryptography except a class of $R_{2,n}$ where $n = 2^N | N \in Z^+$. In 2002, the cyclic multiplicative groups in $R_{2^s,2}$ are exploited to propose a secret-key cryptosystem and in [9] which is then developed as a new variant of DES in [10].

In section II, briefly reintroduce some ideas and some theoretical evidence in applying polynomial to improve the existing cryptosystem into a new cryptosystem that can be applied on a constraint device through five versions on Omura-Massey

II. ADDING AUTHENTICATION FEATURE TO EXPONENTIAL OMURA-MASSEY CRYPTO SYSTEM OVER POLYNOMIAL RINGS WITH TWO CYCLOTOMIC COSETS

A. Exponential Omura-Massey crypto-system with Multiplication over PRs

a. Key generation

Public key: $Z_2[x]/(x^N + 1)$ – PRs with two cyclotomic cosets

+ A chooses ID(A) – authentication parameter of A, ID(A) is made public
+ Also, B choose ID(B) – authentication parameter of B, ID(B) is made public

Private key:

+ A chooses randomly (m,n): $(mID(B), n) \equiv 1\ mod\ (2^{N-1} - 1)$
+ B chooses randomly (u,v): $(uID(A), v) \equiv 1\ mod\ (2^{N-1} - 1)$

(Over PRs with two cyclotomic cosets, we can choose as following:$ID(A), ID(B) \in Z_2[x]/(x^N + 1)$)

b. Communication process

A wants to send a message

$$M(x) \in Z_2[x]/(x^n + 1)$$

Corresponding author: Hoang Manh Thang
Email: thanghm@ptit.edu.vn
Manuscript received: 6/2018 , revised: 8/2018 , accepted: 9/2018

$A(mID(B),n) \leftrightarrow B(uID(A),v)$	
A -> B	A computer $[M(x)]^{mID(B)} \ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{mID(B)}]^{uID(A)} \ mod\ (x^N+1)$
A -> B	A computer $\left[[M(x)]^{mID(B).uID(A)}\right]^n \ mod\ (x^N+1) \equiv [M(x)]^{uID(A)} \ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{uID(A)}]^n \ mod\ (x^N+1)$

c. Example

Let $Z_2[x]/(x^N+1) = Z_2[x]/(x^5+1)$ and
$ID(A) = 4;\ ID(B) = 2;$

Private key of A(m,n) = (1,8):
(mID(B),n) = (1.2,8) ≡ 1 mod 15

Private key of B(u,v) = (1,4):
(uID(A),v) = (1.4,4) ≡ 1 mod 15

A want to send a message M = (034) to B

$A(m,n) \leftrightarrow B(u,v)$	
A -> B	A computer $[034]^2 \ mod\ (x^5+1) = [013]$
B -> A	B computer $[013]^4 \ mod\ (x^5+1) = [024]$
A -> B	A computer $[024]^8 \ mod\ (x^5+1) = [012]$
B -> A	B computer $[012]^4 \ mod\ (x^5+1) = [034]$

B. Exponential Omura-Massey crypto-system with Additive over PRs

a. Key generation

Public key: $Z_2[x]/(x^N+1)$ – PRs with two cyclotomic cosets

+ A chooses ID(A) – authentication parameter of A, ID(A) is made public
+ Also, B choose ID(B) – authentication parameter of B, ID(B) is made public

Private key:

+ A chooses randomly (m,n): $(m+ID(B),n) \equiv 1 \ mod\ (2^{N-1}-1)$
+ B chooses randomly (u,v): $(u+ID(A),v) \equiv 1 \ mod\ (2^{N-1}-1)$

(Over PRs with two cyclotomic cosets, we can choose as following:$ID(A), ID(B) \in Z_2[x]/(x^N+1)$)

b. Communication process

A wants to send a message
$M(x) \in Z_2[x]/(x^n+1)$

$A(mID(B),n) \leftrightarrow B(uID(A),v)$	
A -> B	A computer $[M(x)]^{m+ID(B)} \ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{m+ID(B)}]^{u+ID(A)} \ mod\ (x^N+1)$
A -> B	A computer $\left[[M(x)]^{(m+ID(B)).(u+ID(A))}\right]^n \ mod\ (x^N+1) \equiv [M(x)]^{u+ID(A)} \ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{u+ID(A)}]^v \ mod\ (x^N+1)$

c. Example

Let $Z_2[x]/(x^N+1) = Z_2[x]/(x^5+1)$ and
$ID(A) = 4;\ ID(B) = 2;$

Private key of A(m,n) = (0,8):
(m+ID(B),n) = (2,8) ≡ 1 mod 15

Private key of B(u,v) = (1,4):
(u+ID(A),v) = (4,4) ≡ 1 mod 15

A want to send a message M = (034) to B

$A(m,n) \leftrightarrow B(u,v)$	
A -> B	A computer $[034]^2 \ mod\ (x^5+1) = [013]$
B -> A	B computer $[013]^4 \ mod\ (x^5+1) = [024]$
A -> B	A computer $[024]^8 \ mod\ (x^5+1) = [012]$
B -> A	B computer $[012]^4 \ mod\ (x^5+1) = [034]$

C. Exponential Omura-Massey crypto-system with Exponential over PRs

a. Key generation

Public key: $Z_2[x]/(x^N+1)$ – PRs with two cyclotomic cosets

+ A chooses ID(A) – authentication parameter of A, ID(A) is made public
+ Also, B choose ID(B) – authentication parameter of B, ID(B) is made public

Private key:

+ A chooses randomly (m,n): $\left(m^{ID(B)},n\right) \equiv 1 \ mod\ (2^{N-1}-1)$
+ B chooses randomly (u,v): $\left(u^{ID(A)},v\right) \equiv 1 \ mod\ (2^{N-1}-1)$

(Over PRs with two cyclotomic cosets, we can choose as following:$ID(A), ID(B) \in Z_2[x]/(x^N+1)$)

b. Communication process

A wants to send a message
$M(x) \in Z_2[x]/(x^n+1)$

$A(mID(B),n) \leftrightarrow B(uID(A),v)$	
A -> B	A computer $[M(x)]^{m^{ID(B)}} \ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{m^{ID(B)}}]^{u^{ID(A)}} \ mod\ (x^N+1)$
A -> B	A computer

	$\left[\left[M(x)\right]^{m^{ID(B)}u^{ID(A)}}\right]^{n} \ mod\ (x^N+1)$ $\equiv [M(x)]^{u^{ID(A)}}\ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{u^{ID(A)}}]^{v}\ mod\ (x^N+1)$

c. Example

Let $Z_2[x]/(x^N+1) = Z_2[x]/(x^5+1)$ and $ID(A)=3;\ ID(B)=2;$

Private key of A(m,n) = (7,4):

$(m^{ID(B)},n) = (7^2,4) \equiv 1 \bmod 15$

Private key of B(u,v) = (7,7):

$(u^{ID(A)},v) = (7^3,7) \equiv 1 \bmod 15$

A want to send a message M = (034) to B

$A(m,n) \leftrightarrow B(u,v)$	
A -> B	A computer $[034]^{7^2}\ mod\ (x^5+1) = [034]^4 = [012]$
B -> A	B computer $\left[012\right]^{7^3}\ mod\ (x^5+1) = [012]^{13} = [234]$
A -> B	A computer $[234]^4 = [024]^{14.4} = [024]^{56} = [024]^{11} = [123]\ mod\ (x^5+1)$
B -> A	B computer $\left[\begin{matrix}123]^7 = [024]^{77} \\ = [034] mod\ (x^5+1\end{matrix}\right)$

D. Exponential Omura-Massey crypto-system with Logarithm over PRs

a. Key generation

Public key: $Z_2[x]/(x^N+1)$ – PR with two cyclotomic cosets, $p = 2^N - 1$ is Mersenne prime

+ A chooses ID(A) – authentication parameter of A, ID(A) is made public
+ Also, B choose ID(B) – authentication parameter of B, ID(B) is made public

Private key:

+ A chooses randomly (m,n): $((ID(B))^m, n) \equiv 1\ mod\ (2^{N-1}-1)$
+ B chooses randomly (u,v): $((ID(A))^u, v) \equiv 1\ mod\ (2^{N-1}-1)$

(Over PRs with two cyclotomic cosets, we can choose as following:$ID(A), ID(B) \in Z_2[x]/(x^N+1)$)

b. Communication process

A wants to send a message $M(x) \in Z_2[x]/(x^n+1)$

$A(mID(B),n) \leftrightarrow B(uID(A),v)$	
A -> B	A computer $[M(x)]^{(ID(B))^m}\ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{(ID(B))^m}]^{(ID(A))^u}\ mod\ (x^N+1)$
A -> B	A computer $\left[\left[M(x)\right]^{(ID(B))^m.(ID(A))^u}\right]^n\ mod\ (x^N+1) \equiv [M(x)]^{(ID(A))^u}\ mod\ (x^N+1)$
B -> A	B computer $[[M(x)]^{(ID(A))^u}]^{v}\ mod\ (x^N+1)$

c. Example

Let $Z_2[x]/(x^N+1) = Z_2[x]/(x^5+1)$ and $ID(A)=3;\ ID(B)=2;$

Private key of A(m,n) = (2,4):

$((ID(B))^m,n) = (2^2,4) \equiv 1 \bmod 15$

Private key of B(u,v) = (3,7):

$((ID(A))^u,v) = (7^3,7) \equiv 1 \bmod 15$

A want to send a message M = (034) to B

$A(m,n) \leftrightarrow B(u,v)$	
A -> B	A computer $[034]^{7^2}\ mod\ (x^5+1) = [034]^4 = [012]$
B -> A	B computer $\left[012\right]^{7^3}\ mod\ (x^5+1) = [012]^{13} = [234]$
A -> B	A computer $[234]^4 = [123]\ mod\ (x^5+1)$
B -> A	B computer $[123]^7 = [024]^{77} = [034]\ mod\ (x^5+1)$

III. CONCLUSION

These crypto-system is secure provided DLP in PRs with two cyclotomic cosets are intractive, there are authentication but Message expansion factor of this cypto-system is 3 (the same with original crypto-system). In the future, we will prove in other aspects of the variant of the cryptosystem like as CPA-secure; and installing on constraint devices, comparison, evaluation with other lightweight cryptography systems.

REFERECES

[1] 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;

[2] 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, , trang 29-34, số 125, 2018, ISSN 2354-1083.

[3] Jonathan Katz, Yehuda Lindell (2007), Introduction to Modern Cryptography: Principles and Protocols, Chapman Hall/CRC Cryptography and Network Security Series.

[4] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. NTRU: Alice ringbased public key cryptosystem.

Lecture Notes in Computer Science Volume 1423, pp 267-288, Springer Verlag 1998.

[5] Gaborit, P., Ohler, J., Sole, P.: CTRU, a Polynomial Analogue of NTRU, INRIA. Rapport de recherche, N.4621 (November 2002), (ISSN 0249-6399).

[6] 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

[7] Nguyen Binh, Le Dinh Thich (2002), The order of polynomials and algorithms for defining Oder of Polynomial over polynomial rings, VICA-5, Hanoi, Vietnam.

[8] Stehle,D., Steinfeld,R.:Making NTRU as secure as worst-case problems over ideal lattices. In:Paterson,K.G.(ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 2747. Springer, Heidelberg (2011).

[9] Nguyen Binh. Crypto-system based on cyclic geometric progressions over polynomial ring (Part I). REV02.2002.

[10] Ho Quang Buu, Ngo Duc Thien, Tran Duc Su. Constructing secretcryptosystem based on cyclic multiplicative progress over polynomial rings, Journal of Science and Technology, Posts and Telecommunication Institute of Technology, 50 (2A), 2012, pp 109-119. In Vietnamese.

[11] Menezes A. J, Van Oorchot P. C. (1998), Handbook of Applied Cryptography, CRC Press.

MỘT SỐ Ý TƯỞNG CẢI TIẾN HỆ MẬT OMERA MASSEY SỬ DỤNG VÀNH ĐA THỨC HAI LỚP KỀ CYCLIC

Tóm tắt: Với ưu điểm của vành đa thức là khả năng tính toán nhanh, cài đặt đơn giản, việc nghiên cứu ứng dụng vành đa thức cho các hệ mật mã hạng nhẹ được coi là phù hợp. Tiếp nối ý tưởng về việc áp dụng vành đa thức để cải tiến hệ mật O-M thành hệ mật có thể ứng dụng được trên thiết bị có tài nguyên hạn chế như bài báo số [2]; bài báo này tiếp tục nghiên cứu, cải tiến hệ mật O-M bằng cách sử dụng vành đa thức để bổ sung thuộc tính xác thực vào hệ mật (1,2,3,4 tương ứng sử dụng phép nhân, cộng, mũ, logarit trên vành đa thức).

Từ khóa: Omura Massey, xác thực, vành đa thức.

Hoàng Mạnh Thắng, nhận học vị Thạc sỹ 2012; 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, Blockchain, AI.

Nguyễn Bình, nhận học vị Tiến 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.

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.