Hệ mật khóa công khai dựa trên các phần tử khả nghịch trong vành đa thức chẵn - IPKE

Cao Minh Thắng, Nguyễn Bình

***Tóm tắt*— Các vành đa thức chẵn $GF_2[x]/(x^{2n}+1) \mid n \in Z^+$, hay viết ngắn gọn là $R_{2n}[x]$ thường không được sử dụng trong lý thuyết mã sửa sai truyền thống. Tuy nhiên, các đặc tính toán học của các vành này lại phù hợp với mật mã và có thể khai thác để xây dựng các hệ mật. Bài báo đề xuất một hệ mật khóa công khai dựa trên các phần tử khả nghịch trong một loại vành chẵn đặc biệt $R_{2^k}[x] \mid k \in Z^+$ cùng một số phân tích về hiệu năng và khả năng bảo mật.**

***Abstract*— Even quotient polynomial rings $GF_2[x]/(x^{2n}+1) \mid n \in Z^+$, or $R_{2n}[x]$ for short, are not widely used in traditional error-correction coding theory. However, the mathematical characteristics of those rings are suitable for cryptography and can be exploited to construct cryptosystems. In this paper, a public key cryptosystem based on the invertible elements in $R_{2^k}[x] \mid k \in Z^+$ is proposed along with brief analysis on performance and security.**

***Từ khóa*— Mật mã; khóa công khai; hệ mật; vành đa thức chẵn; phần tử khả nghịch.**

I. GIỚI THIỆU

Các phần tử khả nghịch trên vành đa thức có bậc hữu hạn hệ số nguyên $Z_q[x]/(x^n-1) \mid n \in Z^+$ đã được J. Jeffrey Hoffstein, Jill Pipher và Joseph H. Silverman sử dụng để xây dựng hệ mật NTRU trong [1] vào năm 1998. Tại thời điểm ra đời, NTRU không được xây dựng trên một bài toán khó cụ thể nào, nên đã bị cộng đồng mật mã phản đối. Tuy nhiên, cho đến nay, với các phiên bản cải tiến, NTRU vẫn chưa bị phá và được IEEE chuẩn hóa trong tiêu chuẩn P.1363.1, mặc dù độ mật của NTRU vẫn chưa được chính thức quy về một bài toán khó nào (mà chỉ có liên quan đến một số bài toán khó trên dàn). NTRU có rất nhiều biến thể, tuy nhiên, ngoài CTRU được xây dựng trên vành đa thức có bậc hữu hạn và hệ số nhị phân $GF_2[x]/\langle f \rangle$, trong đó f là một đa thức bất khả quy có bậc hữu hạn trên $GF(2)$ thì chưa có biến thể nào được xây dựng trên vành $R_n[x] \mid n \in Z^+$.

Trong lý thuyết mã sửa sai truyền thống, các vành đa thức chẵn $R_{2n}[x]$ không được sử dụng vì các mã xây dựng trên các ideals của các vành này có thể suy ra trực tiếp từ các mã của vành $R_n[x]$ tương ứng. Gần đây, bằng phương pháp phân hoạch $R_{2n}[x]$ thành các lớp các phần tử liên hợp [2], các phần tử liên hợp của lũy đẳng nuốt (Swallowing Idempotent) và phần tử zero trong các vành này đã được sử dụng để xây dựng một số lớp mã cyclic cục bộ có đặc tính sửa sai tốt. Ngoài ra, các cấp số nhân cyclic trong $R_{2^k}[x] \mid k \in Z^+$, một loại vành chẵn đặc biệt, đã được khai thác để xây dựng một hệ mật khóa bí mật [3] và sau đó được ứng dụng trong một biến thể của hệ mật DES [4].

Trong bài báo này, bài toán khó về khôi phục một đa thức từ một tích không khả nghịch trong vành đa thức $R_{2^k}[x] \mid k \in Z^+$ sẽ được khai thác để xây dựng một hàm cửa sập ứng dụng trong một hệ mật khóa công khai mới là IPKE (Invertible Public Key Encryption scheme) với một số đặc tính tốt.

Trong Mục II của bài báo sẽ chỉ ra trên các vành $R_{2^k}[x] \mid k \in Z^+$ tồn tại cả các phần tử khả nghịch và không khả nghịch, đưa ra tiêu chuẩn xác định các phần tử khả nghịch cùng thuật toán để tính toán phần tử nghịch đảo của chúng, cũng như một hàm cửa sập dựa trên các phần tử này. Trong Mục III, một hệ mật khóa công khai mới dựa trên hàm cửa sập sẽ được trình bày chi tiết gồm các thủ tục tạo khóa, mã hóa và giải mã, cùng một số ví dụ minh họa. Mục IV sẽ tập trung phân tích hiệu năng và khả năng bảo mật của hệ mật được đề xuất trước một số loại tấn công phổ biến. Các kết luận và hướng nghiên cứu tiếp theo được đề cập trong Mục V.

II. CƠ SỞ TOÁN HỌC

Trong mục này, chúng tôi tập trung vào các đa thức khả nghịch trên $R_{2^k}[x]$ và đề xuất một hàm cửa sập dựa trên các phần tử đặc biệt này.

A. Các phần tử khả nghịch trong $R_{2^k}[x]$

Ký hiệu II.1: Trọng số Hamming của một đa thức bất kỳ $f \in R_{2^k}[x]$ được ký hiệu là $w(f)$.

Ký hiệu II.2: Trong $R_{2^k}[x]$, tập các đa thức có trọng số lẻ được ký hiệu là $I_{2^k}[x]$.

Rất dễ nhận thấy rằng số phần tử có trọng số lẻ trong các vành này là $\left|I_{2^k}[x]\right| = 2^{2^{k-1}-1}$.

Định nghĩa II.1: Đa thức $f \in R_{2^k}[x]$ khả nghịch nếu tồn tại một đa thức $g \in R_{2^k}[x]$ thỏa mãn $g.f = 1 \bmod (x^{2^k}+1)$.

Bổ đề II.1: Mọi đa thức $f \in R_{2^k}[x]$ là khả nghịch khi và chỉ khi $f \in I_{2^k}[x]$.

Chứng minh: Giả sử f được biểu diễn là

$$f = \sum_{i=0}^{2^k-1} f_i x^i \mid f_i \in GF(2),$$

vì $f_i \in GF(2)$ nên

$$\begin{aligned} f^{2^k} &= \sum_{i=0}^{2^k-1} (f_i\ x)^{i.2^k} \bmod (x^{2^k}+1) \\ &= \sum_{i=0}^{2^k-1} f_i^{2^k} x^{i.2^k \bmod 2^k} = \sum_{i=0}^{2^k-1} f_i \\ &= w(f) \bmod 2. \end{aligned}$$

Nếu $f \in I_{2^k}[x]$ hoặc $w(f) \bmod 2 = 1$ thì $f^{2^k} = 1 \bmod (x^{2^k}+1)$.

Nếu $g = f^{2^k-1} \bmod (x^{2^k}+1)$, ta có $g.f = f^{2^k-1}.f = f^{2^k} = 1 \bmod (x^{2^k}+1)$ và g là nghịch đảo của f. Dễ thấy $g \in I_{2^k}[x]$.

Nếu $f \notin I_{2^k}[x]$ hiển nhiên $w(f) \bmod 2 = 0$.

Giả sử f là khả nghịch và h là nghịch đảo của f ta sẽ có $h.f = 1 \bmod (x^{2^k}+1)$ và $(h.f)^{2^k} = h^{2^k}.f^{2^k} = 1 \bmod (x^{2^k}+1)$. Điều này không thể xảy ra vì $f^{2^k} = w(f) \bmod 2 = 0 \bmod (x^{2^k}+1)$. □

Trong [5], $n = 2^k$ được chứng minh là cấp cực đại của tất cả các đa thức $f \in R_{2^k}[x]$ và $ord(f)$ là ước của 2^k hay $ord(f) = 2^i \mid i \in [1,k]$. Do đó, ta có thể tính nghịch đảo của f bằng thuật toán sau, thay vì phải tính $g = f^{2^k-1} \bmod (x^{2^k}+1)$.

Thuật toán II.1: Thuật toán tính nghịch đảo g của đa thức $f \in I_{2^k}[x]$

VÀO: Đa thức $f \in I_{2^k}[x]$.

RA: Đa thức $g \in I_{2^k}[x]$, $g \in I_{2^k}[x] \mid g.f = 1 \bmod (x^{2^k}+1)$.

THUẬT TOÁN:

1. $g = f$;
2. $a = f^2 \bmod (x^{2^k}+1)$;
3. for $i = 1$ to $k-1$ {
4. if $g.f = 1 \bmod (x^{2^k}+1)$ exit;

   $g = g.a \bmod (x^{2^k}+1)$;

   $a = a^2 \bmod (x^{2^k}+1)$;

   }.

Lấy ví dụ, trong $I_{2^3}[x]$, để tính nghịch đảo của $f = x^5 + x^4 + x^3$, vì $ord(f) = 2^2 = 4$, sử dụng thuật toán trên, ta có thể tính $g = f^3 \bmod (x^8+1)$ tại bước $i = 2$, thay vì phải tính $g = f^7 \bmod (x^8+1)$.

Bổ đề II.2: Trong $R_{2^k}[x]$, mọi đa thức có dạng $g = f.(x^p+1) \mid p \in Z, 0 < p < 2^k$ với f là đa thức bất kỳ, là không khả nghịch.

Chứng minh: Vì $w(g)$ luôn là số chẵn nên $w(g) \bmod 2 = 0$. Theo Bổ đề II.1, g không khả nghịch.

Bổ đề II.3: Trong $R_{2^k}[x]$, giả sử f một đa thức có bậc $\deg f \le p-1$, với $p \in Z, 0 < p < 2^{k-1}$, nếu

$$g = \sum_{i=0}^{2^k-1} g_i x^i = f.(1+x^p)$$

thì

$$f = \sum_{i=0}^{p-1} g_i x^i.$$

Chứng minh: Vì $\deg f \le p-1$, ta có thể biểu diễn

$$f = \sum_{i=0}^{p-1} f_i x^i \mid f_i \in GF(2)$$

và

$$\begin{aligned} g &= \sum_{i=0}^{p-1} f_i x^i + x^p . \sum_{i=0}^{p-1} f_i x^i \\ &= \sum_{i=0}^{p-1} f_i x^i + \sum_{i=0}^{p-1} f_i x^{i+p}. \end{aligned}$$

Đổi biến $i = j - p$, vì $2p - 1 < 2^k - 1$ ta có:

$$\sum_{i=0}^{p-1} f_i x^{i+p} = \sum_{j=p}^{2p-1} f_j x^{j+p}$$

và $g = \sum_{i=0}^{p-1} f_i x^i + \sum_{i=p}^{2p-1} f_i x^{i+p}$.

Rõ ràng $f_i = g_i \mid i \in [0, p-1]$ hay

$$f = \sum_{i=0}^{p-1} g_i x^i.$$

B. Hàm cửa sập dựa trên các phần tử khả nghịch trong $R_{2^k}[x]$

Đặt $K = s.(1 + x^p) \bmod (x^{2^k} + 1)$ và $c = m.K \bmod (x^{2^k} + 1)$ với K, s, m, c là các đa thức tùy ý trong $R_{2^k}[x]$. Theo Bổ đề II.2, không thể tìm được $K_I \in R_{2^k}[x]$ để $K_I.K = 1 \bmod (x^{2^k} + 1)$. Do đó, chỉ với K, ta không thể tính được m từ c bằng công thức

$$m = K_I.c \bmod (x^{2^k} + 1).$$

Tuy nhiên, nếu biết τ, phần tử nghịch đảo của s, ta có thể tính

$$d = \tau.c \bmod (x^{2^k} + 1)$$
$$= m.(x^p + 1) \bmod (x^{2^k} + 1)$$

và nếu $\deg m \le p - 1$, ta dễ dàng khôi phục m từ d theo Bổ đề II.3.

Qua phân tích trên cho thấy biểu thức

$$c = m.K \bmod (x^{2^k} + 1) \quad (1)$$

giống như một hàm cửa sập, trong đó, dễ dàng tính c từ m nhưng không thể tính ngược m từ c nếu không biết cửa sập τ.

C. Không gian các cửa sập trong $R_{2^k}[x]$

Để tránh lộ s từ K, bậc của s cần lớn hơn $p-1$, khi đó s có dạng:

$$s = s_1.x^q + s_2 \mid q \in Z, p \le q < 2^k \quad (2)$$

với $s_1 \in R_{2^k - q}[x]$ và $s_2 \in R_q[x]$.

Ngoài ra, như đã đề cập ở trên, cửa sập τ tồn tại khi và chỉ khi s khả nghịch hay theo Bổ đề II.2, $s \in I_{2^k}[x]$. Khi đó s có trọng số lẻ hay

$$w(s) = w(s_1) + w(s_2) = 2l + 1 \mid l \in Z^+. \quad (3)$$

Bổ đề II.4: Gọi $S_{2^k}[x]$ là tập các đa thức $s \in R_{2^k}[x]$ thỏa mãn hai điều kiện (2) và (3), khi đó

$$N = \left|S_{2^k}[x]\right| = 2^{2^k + p - q - 1} - 2^{2^k - q - 1} - 2^{p-1}.$$

Chứng minh: Trong $R_n[x]$, có tổng số 2^{n-1} phần tử có trọng số lẻ và $2^{n-1} - 1$ phần tử khác zero (đa thức $f = 0$) có trọng số chẵn.

Điều kiện (3) được thỏa mãn khi $w(s_1)$ hoặc $w(s_2)$ lẻ còn giá trị kia chẵn. Do đó, có:

$$N_1 = 2^{(2^k - q) - 1}.(2^{q-1} - 1)$$

cách chọn s_1, s_2 để $w(s_1)$ lẻ và $w(s_2)$ chẵn và có

$$N_2 = (2^{2^k - q - 1} - 1).2^{q-1}$$

cách chọn s_1, s_2 để $w(s_1)$ chẵn và $w(s_2)$ lẻ. Hệ quả là:

$$N = \left|S_{2^k}[x]\right| = N_1 + N_2 = 2.2^{q-1}.2^{2^k - q - 1} - 2^{2^k - q - 1} - 2^{q-1}$$
$$= 2^{2^k - 1} - 2^{2^k - q - 1} - 2^{q-1}. \square$$

Kết quả này chỉ ra rằng, không phải tất cả $2^{2^k - 1}$ phần tử khả nghịch trong $I_{2^k}[x]$ đều có thể sử dụng để xây dựng hàm cửa sập (1).

III. HỆ MẬT KHÓA CÔNG KHAI IPKE

Điểm đặc biệt của IPKE là khóa bí mật được tạo lập trên cơ sở một đa thức khả nghịch theo một môđun thay vì đồng thời hai môđun khác nhau như trường hợp của NTRU.

Trong mục này, dựa trên hàm cửa sập (1), chúng tôi sẽ mô tả chi tiết hệ mật được đề xuất bao gồm các thủ tục tạo khóa, mã hóa và giải mã và hai ví dụ minh họa.

A. Tạo khóa

Để xây dựng hệ mật, Bob tiến hành các bước như sau:

Chọn một số nguyên dương k và hai số nguyên dương $p < 2^{k-1}$ và $p \le q \le 2^k - 1$ để xây dựng hệ mật trên vành $s_2 \in R_{2^k}[x]$;

Chọn hai đa thức khác zero $s_1 \in R_{2^k - q}[x]$ và $s_2 \in R_q[x]$ tính $s_B = (s_1 x^q + s_2) \bmod (x^{2^k} + 1)$;

Sử dụng Thuật toán II.1 để tính 2^k bit khóa bí mật τ_B với đầu vào s_B;

Tính 2^k bit

$$K_B = s_B.(x^p + 1) \bmod (x^{2^k} + 1) \quad (4)$$

và gửi bộ ba khóa công khai (k, p, K_B) tới Alice.

B. Mã hóa

Để mã hóa p bit bản rõ m, Alice tính

$$c = m.K_B \bmod (x^{2^k} + 1) \quad (5)$$

và gửi 2^k bit bản mã c tới Bob.

C. Giải mã

Khi nhận được c, Bob dùng khóa bí mật τ_B tính

$$d = \tau_B.c \bmod (x^{2^k} + 1) \quad (6)$$

và khôi phục m bằng cách tính

$$m = \sum_{i=0}^{p-1} d_i x^i \quad (7)$$

với $d_i \mid i \in [0, p-1]$ là các hệ số của đa thức d trong biểu diễn

$$d = \sum_{i=0}^{2^k-1} d_i x^i .$$

D. Chứng minh hoạt động giải mã

Thay thế c trong (5) vào (4) ta có

$$d = \tau_B.c = \tau_B.m.K_B \bmod (x^{2^k} + 1)$$

$$= \tau_B.s_B.m.(x^{2^{k-1}} + 1) \bmod (x^{2^k} + 1).$$

Theo (1), ta có

$$d = m.(x^p + 1) \bmod (x^{2^k} + 1).$$

Cuối cùng, theo Bổ đề II.3, ta có

$$m = \sum_{i=0}^{p-1} d_i x^i .$$

E. Ví dụ một hệ mật 8 bit

Bob chọn $k = 3, p = 3, q = 5$ để xây dựng hệ mật trên vành $R_8[x]$.

1. Tạo khóa:

Đầu tiên, Bob chọn $p = 3$ và $q = 5$;

Tiếp theo, Bob chọn

$$s_1 = x^2 + 1 \in R_3[x] \text{ và } s_2 = x^4 \in R_5[x]$$

để tính $s_B = s_1.x^3 + s_2 = x^7 + x^5 + x^4$ và khóa bí mật

$$\tau_B = x^6 + x^4 + x^3 + x^2 + x;$$

Dễ thấy $\tau_B.s_B = 1 \bmod (x^8 + 1)$;

Tiếp đó, Bob tính khóa công khai

$$K_B = x^5 + x^4 + x^2 + 1$$

và gửi k, p, q cùng K_B tới Alice.

2. Mã hóa:

Sau khi nhận được k và K_B, để mã hóa bản tin 3 bit $m = (011)$ dạng nhị phân hay $m = x + 1$ dạng đa thức, sử dụng công thức (5), Alice tính

$$c = x^6 + x^4 + x^3 + x^2 + x + 1$$

và gửi 8 bản mã $c = (01011111)$ dạng nhị phân đến Bob.

3. Giải mã:

Khi nhận được c từ Alice, áp dụng công thức (6), Bob tính

$$d = x^4 + x^3 + x + 1$$

và sử dụng công thức (7) để khôi phục $m = x + 1$.

F. Ví dụ một hệ mật 64 bit

Bob chọn $k = 6$, $p = 31$ và $q = 37$ để xây dựng hệ mật trên vành $R_{64}[x]$.

1. Tạo khóa:

Bob chọn

$$s_1 = x^{26} + x^{15} + x^3 + 1 \in R_{27}[x] \quad \text{và}$$

$$s_2 = x^{36} + x^{26} + x^{11} + x^6 + x^5 \in R_{37}[x]$$

để tính

$$s_B = x^{63} + x^{52} + x^{40} + x^{37} + x^{36} + x^{26} + x^{11} + x^6 + x^5.$$

Vì $w(s_B) = 9$, Bob dùng s_B tính khóa bí mật

$$\tau_B = x^{63} + x^{61} + x^{59} + x^{58} + x^{55} + x^{54} + x^{53} + x^{50} + x^{49}$$
$$+ x^{46} + x^{45} + x^{42} + x^{41} + x^{37} + x^{36} + x^{30} + x^{28} + x^{27}$$
$$+ x^{17} + x^{15} + x^{13} + x^{12} + x^5 + x^4 + x^3 + x + 1.$$

Không khó để có thể kiểm tra $\tau_B.s_B = 1 \bmod (x^{64} + 1)$.

Sau đó, Bob tính khóa công khai

$$K_B = x^{63} + x^{57} + x^{52} + x^{42} + x^{40} + x^{30} + x^{26}$$
$$+ x^{19} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^3$$

và gửi k, p cùng K_B tới Alice.

2. Mã hóa:

Sau khi nhận được k, p và K_B, để mã hóa bản rõ 31 bit dạng đa thức

$$m = x^{30} + x^{28} + x^{22} + x^{20} + x^{18}$$
$$+ x^{14} + x^{11} + x^8 + x^6 + x^4 + x^2$$

Alice sử dụng công thức (5) tính

$$c = x^{61} + x^{59} + x^{58} + x^{56} + x^{54} + x^{53} + x^{52} + x^{51} + x^{49} + x^{47}$$
$$+ x^{46} + x^{42} + x^{41} + x^{40} + x^{38} + x^{37} + x^{32} + x^{29} + x^{25}$$
$$+ x^{21} + x^{20} + x^{19} + x^{18} + x^{13} + x^9 + x^3 + x^2 + 1$$

và gửi c tới Bob.

3. Giải mã:

Khi nhận được c từ Alice, sử dụng công thức (6), Bob tính

$$d = (x^{61} + x^{59} + x^{53} + x^{51} + x^{49} + x^{45} + x^{42} + x^{39} + x^{37} + x^{35} + x^{33}) + (x^{30} + x^{28} + x^{22} + x^{20} + x^{18} + x^{14} + x^{11} + x^{8} + x^{6} + x^{4} + x^{2})$$

sau đó sử dụng công thức (7) khôi phục

$$m = x^{30} + x^{28} + x^{22} + x^{20} + x^{18} + x^{14} + x^{11} + x^{8} + x^{6} + x^{4} + x^{2}.$$

IV. HIỆU NĂNG VÀ KHẢ NĂNG BẢO MẬT CỦA IPKE

Trong mục này, một số loại tấn công phổ biến sẽ được sử dụng để chứng minh hệ mật được đề xuất là an toàn về mặt tính toán. Ngoài ra, các phân tích lý thuyết cho thấy hệ mật này phù hợp với các ứng dụng đòi hỏi tốc độ tính toán nhanh.

A. Các loại tấn công

1. Tấn công kiểu vét cạn

Người thám mã nhận được c có thể thử vét cạn $M = 2^p$ bản rõ m cho đến khi đạt được $m.K_B = c \bmod (x^{2^k} + 1)$ hoặc thử vét cạn

$$N = 2^{2^k - 1} - 2^{2^k - q - 1} - 2^{q-1}$$

khóa bí mật τ_B cho đến khi $\tau_B.K_B = (x^p + 1) \bmod (x^{2^k} + 1)$.

2. Tấn công bằng bản mã được chọn dựa trên đặc tính tuyến tính của hàm cửa sập

Do hàm cửa sập là tuyến tính, có thể thấy, nếu khóa công khai K_B không thay đổi theo từng phiên mã, với m_1, m_2 là hai bản rõ bất kỳ và c_1, c_2 là các bản mã tương ứng của chúng, dễ thấy

$$c_3 = (m_1 + m_2).K_B \bmod (x^{2^k} + 1) = c_1 + c_2.$$

Do vậy, khi nhận được một bản mã c nào đó, người thám mã sẽ chọn một bản rõ tùy ý $m^* \in M$ và thực hiện thủ tục mã hóa

$$c' = c + m^*.K_B = (m + m^*).K_B \bmod (x^{2^k} + 1),$$

sau đó sử dụng thủ tục giải mã (lưu ý rằng, điều kiện của các tấn công bằng bản mã được chọn là ứng với mỗi phiên mã hóa, người thám mã có khả năng truy cập đến cả bộ (oracle) mã hóa và giải mã của hệ mật) và tính được

$$m' = (m + m^*) \bmod (x^{2^k} + 1)$$

từ đó khôi phục được

$$m = (m' + m^*) \bmod (x^{2^k} + 1).$$

Để ngăn chặn các kiểu tấn công này, khóa công khai K_B cần phải được thay đổi ngẫu nhiên trong không gian khóa theo từng phiên mã hóa. Điều này có được bằng cách chọn khóa bí mật s_B ngẫu nhiên trong $S_{2^k}[x]$. Cụ thể hơn, giả sử trong phiên mã hóa c' khóa công khai là K_B^*, kẻ tấn công sẽ không thể tính được m theo cách trên, vì khi đó

$$c' = m.K_B + m^*.K_B^* \bmod (x^{2^k} + 1).$$

Chú ý: Loại tấn công gần tương tự như trên cũng xảy ra đối với hệ mật RSA [7] nhưng dựa trên đặc tính của phép nhân môđun thay vì phép cộng của hệ mật IPKE. Ngoài ra, nếu không sử dụng khóa phiên như trên, ta có thể áp dụng phương pháp theo sơ đồ đệm OAEP [8] tương tự như giải pháp OAEP-RSA [9] để chống lại loại tấn công này.

B. Lựa chọn các tham số

Một nhược điểm của hệ mật được đề xuất là bản mã có độ dài gấp $2^k / p$ lần bản rõ. Vì $p < 2^{k-1}$ nên hệ số mở rộng bản mã luôn lớn hơn 2. Do vậy, có thể chọn

$$p = 2^{k-1} - 1$$

để tối ưu hiệu quả mã hóa. Khi đó, độ mật bản tin cũng đạt giá trị tối ưu

$$M = 2^{2^{k-1} - 1}.$$

Giá trị q là không công khai và có thể chọn theo điều kiện $p \le q \le 2^k - 1$. Tuy nhiên, để cân bằng độ mật của bản tin M và độ mật của khóa N cần chọn q sao cho giá $|M - N|$ càng nhỏ càng tốt.

C. Phân tích hiệu năng trên lý thuyết

Mặc dù k càng lớn thì cả M và N càng lớn, tức khả năng an toàn của hệ mật càng cao, ta cần phải chọn k phù hợp để đảm bảo hiệu quả mã hóa.

Thuật toán tính khóa bí mật τ_B cần nhiều nhất $k - 1$ bước. Cho nên, trong trường hợp độ dài khóa công khai rất lớn, cỡ 4096 ứng với $k = 12$ cũng không ảnh hưởng đến thủ tục tạo khóa.

Bảng 1 tóm tắt các đặc tính trên lý thuyết của hệ mật được đề xuất so sánh với hệ mật RSA khi sử dụng cùng khóa công khai có độ dài 2^k.

Một ưu điểm quan trọng của hệ mật IPKE là tốc độ tính toán. Cả hai thủ tục mã hóa và giải mã đều sử dụng phép nhân đa thức môđun rất đơn giản trong khi RSA phải sử dụng hàm mũ môđun.

BẢNG 1. HIỆU NĂNG TRÊN LÝ THUYẾT CỦA HỆ MẬP IPKE KHI SO SÁNH VS RSA

	IPKE	**RSA**
Độ dài khóa công khai (bit)	2^k	2^k
Độ dài bản rõ (bit)	2^p	2^k
Độ dài bản mã (bit)	2^k	2^k
Độ phức tạp mã hóa (bit operation)	$O(k^2)$	$O(k^2)^{(*)}$
Độ phức tạp giải mã (bit operation)	$O(k^2)$	$O(k^3)$
Hệ số mở rộng bản tin (c (bit) / m (bit))	$2^k / p$	$1/1^{(**)}$

(*): Độ phức tạp mã hóa của RSA là $O(k^3)$ trừ khi số mũ mã hóa là nhỏ.

(**): Trên thực tế, độ mở rộng của RSA thường lớn hơn 1 vì phải dành không gian cho phần đệm dữ liệu (padding).

D. Một số chế độ hoạt động

BẢNG 2. CÁC CHẾ ĐỘ HOẠT ĐỘNG CỦA HỆ MẬT IPKE

Độ mật	**Thấp**	**Trung bình**	**Cao**
k, p, q	7, 63, 65	10, 1023, 1025	12, 2047, 2049
Độ dài khóa	128	1024	4096
Hệ số mở rộng bản tin	2.0158	2.0020	2.0005
M	1024	$6{,}70 \times 10^{153}$	$1{,}62 \times 10^{616}$
N	4096	$8{,}99 \times 10^{307}$	$5{,}22 \times 10^{1232}$

Trong Bảng 2 đưa ra ba chế độ hoạt động của IPKE với ba mức độ bảo mật khác nhau.

Để đơn giản trong tính toán, ta có thể chọn $k = 7$. Chế độ này phù hợp với các hệ thống hạn chế về tài nguyên (CPU, bộ nhớ, pin…).

Tương đương với giá trị khuyến nghị về độ dài khóa của RSA [7] và NTRU [5], IPKE sử dụng khóa có độ dài 1024 cho các ứng dụng thông thường và 4096 cho các ứng dụng yêu cầu bảo mật cao.

Trong chế độ bảo mật cao, các kiểu tấn công đã phân tích đều rất khó thực thi vì N và M đều là các số nguyên rất lớn. Các giá trị k lớn hơn cần được xem xét kỹ để đảm bảo cân bằng giữa mức độ bảo mật và hiệu quả mã hóa.

So với NTRU ở các chế độ khác nhau, IPKE chỉ sử dụng một khóa bí mật và có độ mở rộng bản tin thấp hơn nhiều.

V. KẾT LUẬN

Trong các vành đa thức chẵn $R_{2^k}[x]$, tính toán nghịch đảo của một đa thức khả nghịch là dễ dàng nhưng khôi phục một đa thức từ một tích không khả nghịch là một bài toán khó khi k đủ lớn. Một số phân tích trên lý thuyết cho thấy mặc dù được xây dựng trên một nền tảng tuyến tính, IPKE có một số ưu điểm nhất định và có thể xem xét để đưa vào các ứng dụng thực tế (đảm bảo cân bằng giữa M và N, mở rộng không gian khóa, thử các loại tấn công khác…) đặc biệt là các ứng dụng đòi hỏi tốc độ tính toán cao với tài nguyên hạn chế.

TÀI LIỆU THAM KHẢO

[1]. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, "NTRU: Alice ring-based public key cryptosystem", Lecture Notes in Computer Science, vol. 1423, pp .267-288, Springer Verlag 1998.

[2]. Nguyễn Bình, Trần Đức Sự, "Local cyclic codes constructed on conjugate elements of swallowing idempotent", REV' 02.2002.

[3]. Nguyễn Bình, "Crypto-system based on cyclic geometric progressions over polynomial ring" (Part I), REV' 02.2002.

[4]. 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, Chuyên san năm thứ 3, Học viện Công nghệ Bưu chính viễn thông số 50 (2A), 2012, tr. 109-119.

[5]. Nguyen Binh, Le Dinh Thich (2002), "The Oders of Polynomials and Algorithms for Defining Oder of Polynomial over Polynomial Ping", VICA-5, Hanoi, Vietnam.

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

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

[8]. M. Bellare, P. Rogaway. "Optimal Asymmetric Encryption -- How to encrypt with RSA". Extended abstract in Advances in Cryptology -Eurocrypt '94 Proceedings, Lecture Notes in Computer Science, vol. 950, A. De Santis ed, Springer-Verlag, 1995.

[9]. Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern, "RSA-- OAEP is secure under the RSA assumption", In J. Kilian, ed., Advances in Cryptology - CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, SpringerVerlag, 2001.

SƠ LƯỢC VỀ TÁC GIẢ

GS. TS. Nguyễn Bình

Đơn vị công tác: Học viện Công nghệ Bưu chính Viễn thông, Bộ TT&TT, Hà Nội.

E-mail: nguyenbinh1999@yahoo.com

Tốt nghiệp Học viện Kỹ thuật Quân sự năm 1973. Nhận bằng Tiến sĩ năm 1984. Được phong hàm Phó Giáo sư năm 1996, Giáo sư năm 2006 tại Học viện Kỹ thuật Quân sự.

Hướng nghiên cứu hiện nay: Lý thuyết và kỹ thuật Mật mã.

ThS. Cao Minh Thắng

Đơn vị công tác: Viện Công nghệ Thông tin và Truyền thông CDIT, Học viện Công nghệ Bưu chính viễn thông, Hà Nội.

E-mail: thangcm@ptit.edu.vn

Nhận bằng Kỹ sư Điện tử Viễn thông năm 2003 và Thạc sĩ Kỹ thuật Điện tử tại Học viện Công nghệ Bưu chính Viễn thông (PTIT) Việt Nam năm 2010. Hiện đang là Nghiên cứu sinh ngành Kỹ thuật điện tử tại PTIT khóa 2012-2016.

Hướng nghiên cứu hiện nay: Lý thuyết mật mã, An toàn thông tin.