MỘT HỆ MẬT KHÓA BÍ MẬT DỰA TRÊN CÁC THẶNG DƯ BẬC HAI VÀ CÁC PHẦN TỬ LIÊN HỢP TRONG VÀNH ĐA THỨC CHẴN

ThS. Cao Minh Thắng, GS.TS. Nguyễn Bình

Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: *Vành đa thức chẵn $Z_2[x]/(x^{2n}+1)$ trước đây ít được sử dụng trong việc xây dựng mã sửa sai. Tuy nhiên, do các đặc tính toán học đặc biệt, các vành này lại có nhiều ứng dụng tiềm năng trong mật mã. Bài báo này đề xuất một hệ mật khóa bí mật dựa trên các đặc điểm của các thặng dư bậc hai và các phần tử liên hợp trên vành đa thức chẵn và trình bày một số đánh giá về hệ mật này.*

Từ khóa: Mật mã, khóa bí mật, vành đa thức chẵn, thặng dư bậc hai, phần tử liên hợp.

A SECRET-KEY CRYPTOSYSTEM BASING ON QUADRATIC RESIDUES AND CONJUGATE ELEMENTS IN EVEN POLYNOMIAL RINGS

Abstract: *Even polynomial rings $Z_2[x]/(x^{2n}+1)$ are not widely used in correcting-coding theory. However, with special mathematical characteristics, thoses rings have some potential applications in cryptography. In this paper, a secret-key cryptosystem basing on the features of quadratic residues and conjugate elements in even polynomial rings is proposed with brief security evaluation.*

Keyword: Cryptography, secret-key, polynomial ring, quadratic residue, conjugate element.

I. GIỚI THIỆU

Trong lý thuyết mã sửa sai cyclic truyền thống, các vành đa thức chẵn $Z_2[x]/(x^{2n}+1)$ không được sử dụng vì các mã này được xây dựng trên các Ideal trong khi các Ideal của vành chẵn chính là Ideal của vành lẻ tương ứng bình phương. Gần đây, với phương pháp phân hoạch vành đa thức chẵn thành các lớp các phần tử liên hợp (Conjugate Element) [1], lớp các phần tử liên hợp của lũy đẳng nuốt trong vành này đã được ứng dụng để xây dựng một số lớp mã cyclic cục bộ [2] có đặc tính tốt. Ngoài ra, với các vành $Z_2[x]/(x^{2^k}+1)$ đã được ứng dụng để xây dựng các hệ mật dựa trên các cấp số nhân cyclic của vành [3], hệ mật này đang được phát triển như một phiên bản mới của chuẩn mã dữ liệu DES [4].

Bài báo này tập trung khai thác đặc tính của các phần tử liên hợp của các thặng dư bậc hai trên vành đa thức chẵn để xây dựng một hệ mật khóa bí mật mới.

Trong mục 2, bài báo trình bày các định nghĩa về các thặng dư bậc hai trên vành đa thức chẵn và các phần tử liên hợp của chúng cũng như phân tích các đặc tính của các đối tượng này. Dựa trên các phân tích đó, mục 3 của bài báo mô tả chi tiết một hệ mật khóa bí mật bao gồm các thuật toán tạo khóa, mã hóa, giải mã cùng một ví dụ thử nghiệm và các đánh giá kết quả sơ bộ. Mục 4 sẽ trình bày một số đưa ra kết luận và định hướng nghiên cứu tiếp theo.

II. CÁC THẶNG DƯ BẬC HAI VÀ CÁC PHẦN TỬ LIÊN HỢP TRONG VÀNH ĐA THỨC CHẴN

Định nghĩa 1: Đa thức $f(x)$ được gọi là thặng dư bậc hai, ký hiệu là QR (Quadratic Residue) trong $Z_2[x]/(x^{2n}+1)$ nếu tồn tại đa thức $g(x)$ thỏa mãn $g^2(x) \equiv f(x) \bmod (x^{2n}+1)$.

Khi đó $g(x) \in Z_2[x]/(x^{2n}+1)$ và được gọi là căn bậc hai của $f(x)$. Đa thức $\sqrt{f(x)}$ được gọi là căn bậc hai chính của $f(x)$. Ví

dụ, căn bậc hai chính của $f(x)=1+x^2+x^4$ là $\sqrt{f(x)}=1+x+x^2$. Tập các QR trong $Z_2[x]/(x^{2n}+1)$ được ký hiệu là Q_{2n}.

Bổ đề 1 : *Đa thức* $f(x)$ *nằm trong tập các thặng dư bậc hai* Q_{2n} *khi và chỉ khi* $f(x)$ *chứa các đơn thức có số mũ chẵn* [1].

Bổ đề 2: Số các QR trong $Z_2[x]/(x^{2n}+1)$ *được xác định như sau* [1]*:*

$$|Q_{2n}|=\sum_{i=0}^{n}C_n^i=C_n^1+C_n^2+C_n^3+...+C_n^{n-1}+C_n^n=2^n$$

Bổ đề 3: *Các căn bậc hai của một QR trong* $Z_2[x]/(x^{2n}+1)$ *được xác định như sau* [1]*:*

$$g(x)=(1+x^n)\sum_{t\in U}x^t+\sqrt{f(x)}$$

Trong đó U là một tập gồm các tổ hợp tuỳ ý các giá trị trong tập $s=\{\overline{0,n-1}\}$. Do vậy lực lượng của U sẽ bằng $|U|=2^n-1$. Như vậy đối với mỗi QR trong vành $Z_2[x]/(x^{2n}+1)$ có tất cả 2^n căn bậc hai (kể cả căn bậc hai chính).

Các căn bậc hai của một đa thức là tổng của nhiều đơn thức sẽ bằng tổng các căn bậc hai của từng đơn thức hay nói cách khác khai căn bậc hai của đa thức là thực hiện khai căn từng thành phần của đa thức. Nếu xét các đơn thức có số mũ chẵn dạng $f(x)=\sum_{i=0}^{n-1}f_ix^{2i}$ thì căn bậc hai chính của f(x) sẽ là $\sqrt{f(x)}=\sum_{i=0}^{i<n}f_ix^i$.

Trong vành $Z_2[x]/(x^{2n}+1)$ có 2^n QR, mỗi thặng dư bậc hai có 2^n căn bậc hai, do vậy có tất cả 2^{2n} căn bậc hai trong vành. Mặt khác, ta thấy rằng, trong vành $Z_2[x]/(x^{2n}+1)$ có 2^{2n} đa thức do vậy các căn bậc hai của các QR tạo nên toàn bộ vành này.

Trong trường số đầy đủ, căn bậc hai của (-1) là $\pm j$, chúng được gọi là các phần tử liên hợp của (-1). Tương tự như vậy, các căn bậc hai của cùng một QR trên vành đa thức cũng được gọi là các phần tử liên hợp tương ứng với thặng dư đó ký hiệu là CE (Conjugate Element).

Bổ đề 4: *Nếu* $l(x)=\sum_{i=0}^{n-1}l_ix^i$ *là căn bậc hai chính của* $f(x)=\sum_{i=0}^{2n-1}f_ix^i$, thì

$$l_i=(f_i+f_{i+n})\bmod 2\,|\,0\le i\le n-1$$

Chứng minh:

Vì

$$\begin{aligned}f(x)&=\sum_{i=n}^{2n-1}f_ix^i+\sum_{i=0}^{n-1}f_ix^i\\&=\sum_{i=0}^{n-1}f_{(i+n)}x^{i+n}+\sum_{i=0}^{n-1}f_ix^i\\&=\sum_{i=0}^{n-1}(f_{(i+n)}x^n+f_i)x^i\end{aligned}$$

nên

$$f^2(x)=f(x^2)=\sum_{i=0}^{n-1}(f_{(i+n)}x^{2n}+f_i)x^{2i}.$$

Do $x^{2n}=1\bmod(x^{2n}+1)$ nên

$$f^2(x)=\sum_{i=0}^{n-1}(f_{(i+n)}+f_i)x^{2i}$$

và

$$\begin{aligned}l(x)=\sqrt{f^2(x)}&=\sqrt{\sum_{i=0}^{n-1}(f_{(i+n)}+f_i)x^{2i}}\\&=\sum_{j=0}^{n-1}(f_{(i+n)}+f_i)x^i\end{aligned}$$

hay

$$l_i=(f_i+f_{i+n})\bmod 2\,|\,0\le i\le n-1.$$

Bổ đề 5: *Đa thức* $k(x)=\sum_{t\in U}x^t$ *trong biểu thức* $g(x)=(1+x^n)\sum_{t\in U}x^t+\sqrt{f(x)}$ *có các hệ số* k_i *được xác định bởi* $k_i=f_{i+n}\,|\,0\le i\le n-1$, *trong đó* f_i *là các hệ số của đa thức* $f(x)=\sum_{i=0}^{2n-1}f_ix^i$.

Chứng minh:

Giả sử $l(x)=\sum_{i=0}^{n-1} l_i x^i$ là căn bậc hai chính của $f(x)=\sum_{i=0}^{2n-1} f_i x^i$.

Vì

$$f(x)=(1+x^n)k(x)+l(x)$$
$$=x^n k(x)+k(x)+l(x)$$

hay

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

Nên dễ thấy toàn bộ các hệ số của các đơn thức có bậc từ n đến $(2n-1)$ của $f(x)$ các hệ số chính là $k_i \mid 0\le j\le n-1$ hay $k_i = f_{i+n} \mid 0\le \mathrm{i}\le n-1$.

III. HỆ MẬT KHÓA BÍ MẬT DỰA TRÊN CÁC THẶNG DƯ BẬC HAI VÀ CÁC PHẦN TỬ LIÊN HỢP TRONG VÀNH ĐA THỨC CHẴN

Mỗi trong tổng số 2^{2n} đa thức $m(x)\in Z_2[x]/(x^{2n}+1)$, có trọng số tối đa là $2n$, đều là CE của QR $f(x)=m^2(x)\bmod(x^{2n}+1)$ tức là mọi đa thức trong vành chẵn luôn có thể biểu diễn dưới dạng:

$$m(x)=(1+x^n)\sum_{t\in U}x^t+\sqrt{m^2(x)}$$

Trong đó, $l(x)=\sqrt{m^2(x)}$ và $k(x)=\sum_{t\in U}x^t$ đều là các đa thức trọng số tối đa là n và được biểu diễn bởi các chuỗi n bit. Nếu coi $k(x)$ là một khóa bí mật và che dấu khóa này bằng một phép mã hóa nào đó, ví dụ RSA, thì thám mã sẽ không thể phát hiện ra $m(x)$ dù thu được $l(x)$. Ngoài ra, bản thân $l(x)$ cũng không phải là một phần của bản rõ $m(x)$ mà chính là một bản mã của $m(x)$ được mã hóa theo công thức $l(x)=\sqrt{m^2(x)}$.

Sơ đồ chi tiết hệ mật khóa bí mật theo ý tưởng trên được mô tả chi tiết trong Hình 1.

Ở mỗi phiên ứng với mỗi lần cần truyền đi bản rõ m_i $2n$ bit tương ứng với đa thức:

$$m_i(x)=\sum_{j=0}^{2n-1}m_{ij}x^j$$

A sẽ tính toán và mã hóa khóa $k_i(x)$ thành $\tilde{k}_i(x)$ (độ dài bit phụ thuộc vào phép mã hóa khóa) sau đó ghép n bit $l_i(x)$ vào sau $\tilde{k}_i(x)$ để tạo thành bản mã rồi truyền tới B qua kênh mở. Ở phía nhận, B sẽ tách $\tilde{k}_i(x)$ ra khỏi $c_i(x)$ và dùng thuật toán giải mã khóa để lấy $k_i(x)$ sau đó sử dụng khóa này để khôi phục được bản rõ $m_i(x)$.

A. Thuật toán tạo và phân phối khóa

Tại phiên thứ i, với $2n$ bit $m_i(x)$, dựa trên *Bổ đề 5*, A sẽ tính $k_i(x)$ với các hệ số $k_{ij} \mid 0\le j\le n-1$ được xác định như sau:

$$k_{ij}=m_{i(j+n)} \qquad (1)$$

Khóa bí mật này sẽ được mã hóa bằng một sơ đồ mã hóa thích hợp nào đó, ví dụ như hệ mật RSA.

B. Thuật toán mã hóa

Theo *Bổ đề 4*, A sẽ xác định được các hệ số của $l_i(x)$ như sau:

$$l_{ij}=(m_{ij}+m_{i(j+n)})\bmod 2 \mid 0\le j\le n-1 \quad (2)$$

Chuỗi n bit này sẽ được ghép vào sau $\tilde{k}_i(x)$ để tạo thành bản mã $c_i(x)$ gửi tới B.

C. Thuật toán giải mã

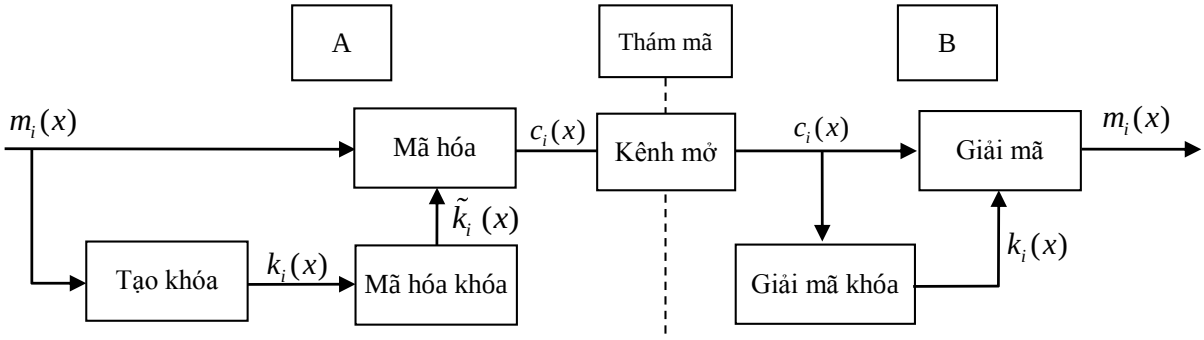
Khi nhận được $c_i(x)$, B sẽ:

1) Tách $l_i(x)$ và $\tilde{k}_i(x)$;

2) Đưa $\tilde{k}_i(x)$ vào giải mã để khôi phục $k_i(x)$;

3) Đưa $l_i(x)$ và $k_i(x)$ vào giải mã để khôi phục $m_i(x)$ với

$$\begin{aligned} m_{ij}&=(l_{ij}+k_{ij})\bmod 2 \mid 0\le j\le n-1\\ m_{ij}&=k_{i(j-n)} \mid n\le j\le 2n-1\end{aligned} \qquad (3)$$



Hình 1: Sơ đồ hệ mật

D. Thuật toán tạo và phân phối khóa

Tại phiên thứ i, với $2n$ bit $m_i(x)$, dựa trên *Bổ đề 5*, A sẽ tính $k_i(x)$ với các hệ số $k_{ij} \mid 0 \le j \le n-1$ được xác định như sau:

$$k_{ij} = m_{i(j+n)} \qquad (4)$$

Khóa bí mật này sẽ được mã hóa bằng một sơ đồ mã hóa thích hợp nào đó, ví dụ như hệ mật RSA.

E. Thuật toán mã hóa

Theo *Bổ đề 4*, A sẽ xác định được các hệ số của $l_i(x)$ như sau:

$$l_{ij} = (m_{ij} + m_{i(j+n)}) \bmod 2 \mid 0 \le j \le n-1 \quad (5)$$

Chuỗi n bit này sẽ được ghép vào sau $\tilde{k}_i(x)$ để tạo thành bản mã $c_i(x)$ gửi tới B.

F. Thuật toán giải mã

Khi nhận được $c_i(x)$, B sẽ:

4) Tách $l_i(x)$ và $\tilde{k}_i(x)$;

5) Đưa $\tilde{k}_i(x)$ vào giải mã để khôi phục $k_i(x)$;

6) Đưa $l_i(x)$ và $k_i(x)$ vào giải mã để khôi phục $m_i(x)$ với

$$\begin{aligned} m_{ij} &= (l_{ij} + k_{ij}) \bmod 2 \mid 0 \le j \le n-1 \\ m_{ij} &= k_{i(j-n)} \mid n \le j \le 2n-1 \end{aligned} \qquad (6)$$

G. Thử nghiệm

Chọn vành đa thức chẵn với $n = 32$. Chọn hệ mật RSA để mã hóa khóa với các tham số: $p = 127487$, $q = 101939$, $e = 65537$, $N = p.q = 12995897293$ (hay viết dưới dạng chuỗi nhị phân 34 bit

11 00000110 10011101

10100111 11001101

để đảm bảo có thể mã hóa tất cả các khóa bí mật 32 bit), khóa giải mã của B là $d_B = 12005580289$.

Giả sử khóa bí mật ở nhip thứ $i-1$ là $k_{i-1} = 0$, ở nhịp thứ i cần mã hóa bản rõ m_i có nội dung là "ptit.edu", viết dưới dạng chuỗi nhị phân 64 bit (mỗi cụm 8 bit với bit đầu là 0 và bảy bit mã ASCII của ký tự tương ứng) là:

m_i = 01110000 01110100 01101001 01110100
00101110 01100101 01100100 01110101

Đa thức tương ứng trong vành là:

$$\begin{aligned} m_i(x) = {} & x^{62} + x^{61} + x^{54} + x^{53} + x^{52} + x^{50} + x^{46} + x^{45} \\ & + x^{43} + x^{40} + x^{38} + x^{37} + x^{36} + x^{34} + x^{29} + x^{27} \\ & + x^{26} + x^{25} + x^{22} + x^{21} + x^{18} + x^{16} + x^{14} + x^{13} \\ & + x^{10} + x^{6} + x^{5} + x^{4} + x^{2} + 1 \end{aligned}$$

Thủ tục tạo khóa:

Sử dụng thuật toán tạo khóa, A sẽ tính được 32 bit khóa:

k_i = 01110000 01110100 01101001 01110100

Giá trị thập phân tương ứng $k_i = 1886677364$.

Do $k_i \ne k_{i-1}$, A mã hóa khóa k_i bằng hệ mật RSA đã chọn như sau:

$$\tilde{k}_i = k_i^e \bmod N$$
$$= 1886677364^{65537} \bmod 12995897293$$
$$= 4016776971$$

Tương ứng với chuỗi khóa 32 bit

$\tilde{k}_i$ = 00010111 11110001 00011101 10000001

Thủ tục mã hóa:

Sử dụng thuật toán mã hóa, A tính được chuỗi 32 bit:

l_i = 01011110 00010001 00001101 00000001

. A ghép chuỗi 32 bit l_i vào sau chuỗi 32 bit $\tilde{k}_i$ để tạo thành bản mã 64 bit

c_i = 00010111 11110001 00011101 10000001
01011100 00010001 00001101 00000001

và gửi đến B.

Thủ tục giải mã:

Nhận được 64 bit c_i, B:

1) Tách 32 đầu để xác định $\tilde{k}_i$ và dùng 32 bit cuối để xác định l_i.

2) Với $\tilde{k}_i = 4016776971$, B sẽ tiến hành giải mã RSA với khóa bí mật d_B để khôi phục

$$k_i = (k_i^{\sim})^{d_B} \bmod N$$
$$= 4016776971^{12005580289} \bmod 12995897293$$
$$= 1886677364$$

hay dưới dạng chuỗi nhị phân 32 bit

k_i = 01110000 01110100
01101001 01110100 .

3) Sử dụng thuật toán giải mã, B khôi phục được

m_i = 01110000 01110100 01101001 01110100
00101110 01100101 01100100 01110101

chính là bản rõ "ptit.edu" ban đầu.

H. Đánh giá

Hệ mật có một số ưu điểm:

1) Có thể dùng nhiều loại hệ mật khóa công khai phổ biến để mã hóa và phân phối khóa $k(x)$, điển hình là RSA [5];

2) Thuật toán tạo khóa, mã hóa và giải mã rất đơn giản, có thể dễ dàng thực thi bằng phần cứng và phần mềm;

3) Kích thước bản mã so với bản rõ giảm từ $2n$ xuống còn n bit. Ngoài ra, với các vành $Z_2[x]/(x^{2^k m}+1)$ trong đó m lẻ có thể áp dụng đệ quy sơ đồ mã hóa tối đa k lần để tăng hiệu quả;

4) Nhìn từ quan điểm của mật mã khối, hệ mật này hoạt động ở chế độ ECB (Electronic Code Book). Các bản tin sẽ được mã hóa và giải mã độc lập do vậy các lỗi bit trên đường truyền của các khối chỉ ảnh hưởng đến việc giải mã của khối đó;

5) Với n bit, số khóa khả dụng sẽ là 2^n khóa, trong ứng dụng thực tế nếu dùng $n \geq 1024$ và cỡ khoảng 4096 (tương ứng với độ dài bit của giá trị modulus được khuyến nghị của hệ mật RSA trên thực tế [5]) thì gần như thám mã không thể tấn công bằng phương pháp vét cạn khóa;

6) Vì xác suất để khóa $k_i(x)$ trùng với khóa $k_{i-1}(x)$ là $1/2^n$ nên nếu tách riêng n bit khóa và truyền độc lập với bản mã $c_i(x)$ thì khi xảy ra trùng khóa sẽ không phải truyền lại khóa như một hệ mật mã dòng tổng quát;

7) Việc giảm được kích thước bản rõ đưa vào mã hóa $2n$ xuống còn n bit đem lại nhiều lợi ích cho các hệ thống mật mã ở phía sau như tiết kiệm được tài nguyên xử lý, dùng không gian n bit để khắc phục một số hạn chế cố hữu của các hệ mật đó (ví dụ để bổ sung thêm các bit giả ngẫu nhiên để khắc phục tấn công khi số mũ mã hóa e nhỏ hoặc tấn công bằng bản mã được chọn đối với hệ mật RSA);

Một số nhược điểm của hệ mật:

1) Mặc dù n càng lớn thì hiệu quả mã hóa của hệ mật càng cao nhưng do giá trị này cần phù hợp với tài nguyên xử lý và đặc tính của các hệ mật mã được sử dụng để truyền khóa bí mật. Giá trị $n \geq 1024$ và 4096 là phù hợp với các ứng dụng thực tế.

2) Khi khóa bí mật $k_i = 0$, ứng trường hợp bản rõ là một trong 2^n căn bậc hai chính trong vành, về lý thuyết thì các bản rõ là không thể che dấu vì chỉ cần bình phương bản mã là có ngay bản rõ. Tuy nhiên thám mã cũng không quyết định được bản rõ có

chính xác không vì có 2^n bản rõ có khóa khác nhau chung bản mã này. Mặc dù vậy đây cũng là các trường hợp không an toàn và nên tránh sử dụng.

3) Một sự thay đổi một bit của bản rõ chỉ gây thay đổi đến tối đa hai bit của bản mã, điều này có thể bị khai thác để tấn công bằng bản mã được chọn.

IV. KẾT LUẬN

Bài báo đã giới thiệu một ứng dụng của vành đa thức $Z_2[x]/(x^{2n}+1)$ trong mật mã khóa bí mật. Hệ mật được đề xuất có thuật toán tạo khóa, mã hóa và giải mã rất đơn giản với số bản rõ hiệu dụng rất cao. Đặc điểm nổi bật của hệ mật này là giảm được khối lượng bản mã cần truyền tải mà mà vẫn đảm bảo tính bí mật, đặc biệt khi giá trị $n \geq 1024$ thì rất khó cho thám mã có thể tấn công bằng phương pháp vẹn cạn khóa. Tùy theo việc sử dụng thuật toán mã hóa khóa công khai để truyền khóa mà hệ mật này có nhiều biến thể khác nhau, trong đó RSA là sự lựa chọn rất phù hợp. Tuy nhiên, để có thể khẳng định tính bảo mật, hệ mật này cần phải được xem xét kỹ lưỡng hơn với các kiểu tấn công khác.

V. TÀI LIỆU THAM KHẢO

[1] *Nguyen Binh, Tran Duc Su, Pham Viet Trung (2001), "Decomposition of polynomial ring according to the classes of conjugate elements", AIC-26, Hanoi, Vietnam.*

[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, trang 109-119.*

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

Thông tin tác giả: **Cao Minh Thắng**

Sinh năm: 1981

Lý lịch khoa học:

- Tốt nghiệp đại học ngành Điện tử Viễn thông vào năm 2003 tại Học viện Công nghệ Bưu chính Viễn thông;
- Tốt nghiệp cao học ngành Kỹ thuật Điện tử năm 2010 tại Học viện Công nghệ Bưu chính Viễn thông;
- Hiện đang là nghiên cứu sinh ngành Kỹ thuật Điện tử tại Học viện Công nghệ Bưu chính Viễn thông;
- Hiện đang công tác tại Viện công nghệ Thông tin và Truyền thông CDIT, Học viện Công nghệ Bưu chính Viễn thông.

Lĩnh vực nghiên cứu hiện nay: Mật mã, An toàn thông tin.

Email: thangcm@ptit.edu.vn; thangcm@cdit.com.vn