Đề xuất giải pháp tấn công mã dòng sử dụng thanh ghi dịch hồi tiếp tuyến tính nhị phân ứng dụng trong hệ thống truyền tin hiện nay

Đoàn Thị Bích Ngọc[1], Đặng Đức Trịnh [2], Lê Văn Tuấn[3*]

[1]Trường Đại học Công nghệ thông tin - Truyền thông, Đại học Thái Nguyên;
[2]Khoa Toán-Tin, Học viện Quân y;
[3]Học viện Khoa học Quân sự.
[*]Email: levantuan71@yahoo.com
Nhận bài ngày 20/5/2023 ; Hoàn thiện: 28/7/2023; Chấp nhận đăng: 08/8/2023; Xuất bản: 25/8/2023.
DOI: https://doi.org/10.54939/1859-1043.j.mst.89.2023.143-152

TÓM TẮT

Bài báo đề xuất phương pháp tấn công hệ mã dòng mà khóa được sinh bởi thanh ghi dịch hồi tiếp tuyến tính đơn tầng dựa trên cặp rõ, mã đã biết, trên cơ sở đó, tác giả sẽ phát triển lý luận khám phá mã dòng với dãy khóa được tạo bởi thanh ghi dịch đa tầng trong các nghiên cứu tiếp theo. Kết quả nghiên cứu có thể ứng dụng để xây dựng những hệ mã dòng tránh được những tấn công mà chúng tôi đã đề xuất trong bài báo này, nhằm nâng cao độ an toàn và bảo mật thông tin trong các hệ thống truyền tin hiện nay.

Từ khóa: Thanh ghi dịch hồi tiếp tuyến tính; Mã dòng.

1. MỞ ĐẦU

Một số chuẩn truyền tin trên thế giới, chẳng hạn như chuẩn STANAG, MIL STD 188-110 (A,B,C), đều sử dụng thanh ghi dịch hồi tiếp tuyến tính với mục đích làm cân bằng kênh, nên cấu trúc và khởi điểm của thanh ghi được công khai thiết kế đến mức chi tiết. Tuy nhiên, với các thanh ghi dịch hồi tiếp tuyến tính sử dụng trong các hệ mật để sinh khóa thì việc công khai cấu trúc và công khai khởi điểm là không thể [12]. Hiện nay, có nhiều công trình khoa học đề cập đến việc ứng dụng thanh ghi dịch hồi tiếp tuyến tính trong mật mã nói chung [1-3, 9] và trong hệ thống mã dòng nói riêng [8, 10, 12, 13]. Trong các công trình nghiên cứu trước đây, kết quả nghiên cứu mới dừng lại ở việc giải thanh ghi khi biết một số bít đầu ra của thanh ghi, chưa gắn việc giải thanh ghi vào khám phá một hệ mã cụ thể. Trong bài báo này, dựa vào các kết quả nghiên cứu trước đó [6, 7, 12] chúng tôi đề xuất giải pháp tấn công hệ mã dòng có khóa được sinh bởi thanh ghi đơn tầng [7, 9] dựa trên cặp (rõ, mã) đã biết. Kết quả nghiên cứu làm cơ sở để khám phá các hệ mã dòng có khóa được sinh bởi nhiều thanh ghi được kết nối với nhau (thanh ghi đa tầng), chẳng hạn như bộ tạo khóa của máy mã H460. Việc đề xuất giải pháp khám phá một hệ mã cũng chính là cơ sở phát hiện các lỗ hổng của hệ mã, từ đó góp phần xây dựng hệ mã dòng an toàn hơn [13] trước kiểu tấn công đã biết. Trong quá trình nghiên cứu, nhóm tác giả đã sử dụng phương pháp nghiên cứu lý thuyết ứng dụng thanh ghi dịch hồi tiếp tuyến tính vào trong các lĩnh vực mật mã và trong các hệ thống truyền tin [1-3, 5-15]; phương pháp xin ý kiến chuyên gia trong lĩnh vực an toàn thông tin và phương pháp thực nghiệm. Một số đóng góp chính của bài báo như sau: đề xuất giải pháp tấn công hệ mã dòng nhị phân với dãy khóa được tạo ra bởi thanh ghi dịch hồi tiếp tuyến tính đơn tầng; đưa ra một số định hướng trong xây dựng và sử dụng hệ mã dòng có khóa được sinh bởi thanh ghi dịch hồi tiếp tuyến tính nhị phân an toàn hơn. Phần tiếp theo, bài báo trình bày một số kiến thức liên quan đến nội dung nghiên cứu; giải pháp tấn công hệ mã dòng và kết luận.

2. CƠ SỞ LÝ THUYẾT

2.1. Thanh ghi dịch hồi tiếp tuyến tính

Định nghĩa 1: Đa thức nguyên thủy [4, 9]

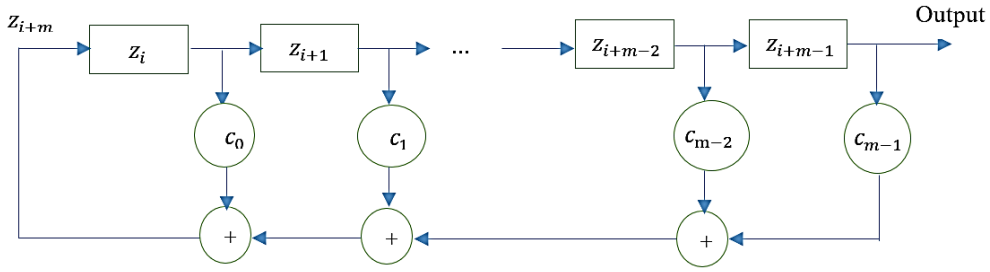
Đa thức p(x) bậc m được gọi là bất khả quy (đa thức tối giản) trên trường $\mathbb{Z}_2$, nếu p(x) không

chia hết cho bất cứ đa thức nào có bậc nhỏ hơn m nhưng lớn hơn không. Hay đa thức bất khả quy là đa thức chỉ chia hết cho đa thức 1 và chính nó. Một đa thức bất khả quy p(x) bậc m được gọi là đa thức nguyên thuỷ nếu đa thức $x^{2^m-1}+1$ là đa thức có bậc nhỏ nhất chia hết cho p(x).

Định nghĩa 2: Thanh ghi dịch hồi quy tuyến tính [6] độ dài m trên trường $\mathbb{Z}_2$ là một automat hữu hạn trạng thái sinh ra một dãy các phần tử thuộc trường $\mathbb{Z}_2$, $z = (z_t)_{t\geq 0}$, thỏa mãn quan hệ hồi quy tuyến tính bậc m trên trường $\mathbb{Z}_2$:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j}, \forall i \geq 1 \quad (1)$$

Trong đó, m hệ số $c_0, c_1, \dots, c_{m-1}$ là các phần tử của trường $\mathbb{Z}_2$ và được gọi là các hệ số hồi quy của thanh ghi dịch. Các hệ số hồi quy sẽ hình thành nên cấu trúc của một thanh ghi dịch.



Hình 1. *Cấu trúc của thanh ghi dịch.*

Trong hình 1, thanh ghi dịch độ dài m gồm m ô nhớ, mỗi ô chứa một phần tử của trường $\mathbb{Z}_2$.

Định nghĩa 3: Khởi điểm của thanh ghi [6].

Các giá trị trong trường $\mathbb{Z}_2$ trong m ô nhớ được gọi là trạng thái của thanh ghi, m giá trị ban đầu của thanh ghi được gọi là các giá trị khởi điểm thanh ghi, ký hiệu $z_1, z_2, \dots, z_m$.

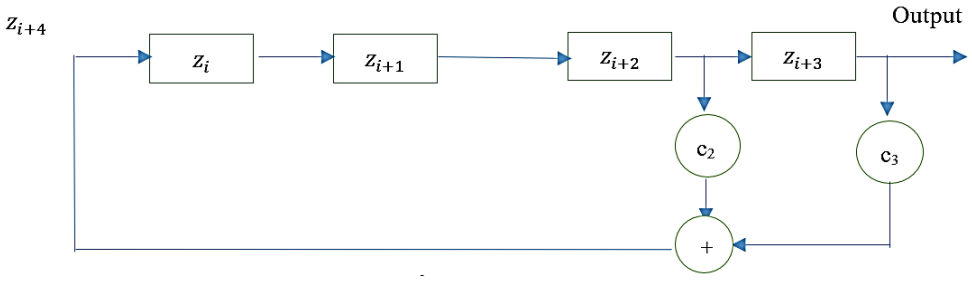
Định nghĩa 4 [6]: Đa thức hồi quy là đa thức mà các hệ số của nó là các giá trị của ô nhớ trong thanh ghi dịch có độ dài m, ký hiệu lần lượt là $c_0, c_1, \dots, c_{m-1}$, đa thức được xác định như sau:

$$P(X) = 1 - \sum_{i=0}^{m-1} c_i X^{i+1} \quad (2)$$

Một cách khác để phản ánh cấu trúc thanh ghi, người ta còn sử dụng đa thức đối ngẫu của đa thức P(X), ký hiệu là $P^*(X)$

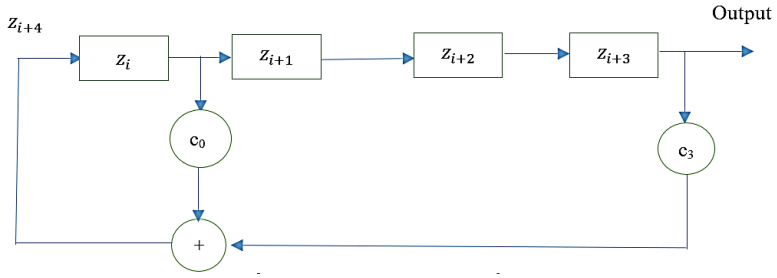
$$P^*(X) = X^m P(1/X) = X^m - \sum_{i=0}^{m-1} c_i X^{m-i+1} \quad (3)$$

Cấu trúc thanh ghi P(X) và $P^*(X)$ là tương đương nhau. Ví dụ xét thanh ghi dịch hồi tiếp tuyến tính trên trường $\mathbb{Z}_2$ có độ dài 4 với các hệ số hồi quy $(c_0, c_1, c_2, c_3) = (0,0,1,1)$. Với hệ số hồi quy này, đa thức hồi quy tương ứng là: P(X)= 1- X^3- X^4. Do các hệ số đa thức trên trường $\mathbb{Z}_2$ nên P(X) = 1+ X^3 + X^4. Cấu trúc thanh ghi như sau:



Hình 2. *Cấu trúc thanh ghi dịch P(X).*

Giả sử khởi điểm thanh ghi trong hình 2 là (0011), khi đó, ta có 30 bit loạn đầu tiên được lấy ra ở tầng cuối cùng (c_4) của thanh ghi như sau: 11000100110101**110001001101011**. Dễ thấy, dãy khóa có chu kỳ tối đa là $2^4 - 1 = 15$ (bít) vì đa thức P(x) là đa thức nguyên thủy. Đa thức đối ngẫu của P(X) là đa thức $P^*(X)$ xác định như sau: $P^*(X) = X^4P(1/X) = 1 + X + X^4$. Khi đó, cấu trúc của thanh ghi của $P^*(X)$ như sau:



Hình 3. *Cấu trúc thanh ghi đa thức đối ngẫu $P^*(X)$.*

Thanh ghi dịch hình 3, lấy khởi điểm thanh ghi là (0011), khi đó, 30 bit loạn đầu tiên như sau: 110010001111010 **110010001111010.** Để chứng minh hai cấu trúc thanh ghi này tương đương ta chứng minh xâu khóa được tạo ra từ hai cấu trúc thanh ghi là tương đương thông qua một số phép biến đổi tương đương là đảo ngược dãy khóa và dịch trái một số bậc, cụ thể là xâu khóa: 110010001111010**110010001111010** có kết quả xâu đảo ngược như sau: 01011110001001101011110001001l. Dịch phải 11 bậc xâu khóa này được kết quả như sau: 11000100110101111000l001101011. Xâu khóa này trùng khớp với xâu khóa được sinh ra từ thanh ghi có cấu trúc trong hình 2.

Cơ chế sinh loạn của thanh ghi dịch: Trong quá trình sinh loạn, thanh ghi dịch được điều khiển bởi một đồng hồ. Tại thời điểm t (còn được gọi là nhịp thứ t), nội dung của ô nhớ bên phải cùng s_t là giá trị đầu ra của thanh ghi. Tiếp đó, giá trị của mỗi ô nhớ trong thanh ghi được chuyển sang ô nhớ bên phải. Giá trị mới của ô trái ngoài cùng là giá trị hồi quy z_{i+m}. Công thức truy hồi như sau:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j}, \forall i \geq 1 \quad (4)$$

Trong đó, biểu thức s_{i+m} là giá trị biểu thức tuyến tính để xác định các giá trị xâu loạn được sinh ra. Chu kỳ dãy khóa tối đa là $2^m - 1$ đạt được khi thanh ghi dịch không bị suy biến.

Chu kỳ của một dãy hồi quy tuyến tính:

Bổ đề 1: Chu kỳ ngắn nhất của một dãy hồi quy tuyến tính bằng giá trị nhỏ nhất e nguyên dương sao cho $X^e + 1$ chia hết cho đa thức hồi quy $P_0(X)$.

Từ bổ đề 1 chúng ta nhận thấy một dãy khóa được sinh ra bởi thanh ghi dịch có chu kỳ lớn nhất $2^{\deg(P_0)} - 1$ khi và chỉ khi đa thức hồi quy P_0 là đa thức nguyên thủy. Dãy sinh ra bởi một thanh ghi dịch với đa thức hồi quy nguyên thủy được gọi là m-dãy.

2.2. Mã dòng nhị phân

Định nghĩa 5[9]: Ký hiệu các tập hợp P, C, K như sau:

P = Z_2 là tập hữu hạn các biểu hình rõ;

C = Z_2 là tập hữu hạn các biểu hình mã;

K = Z_2 là tập hữu hạn các biểu hình khóa.

Được tạo ra bằng thanh ghi dịch hồi quy tuyến tính độ dài m trên trường $\mathbb{Z}_2$ bắt đầu bằng dãy (k_1, k_2,...,k_m) ban đầu gồm m phần tử trên trường Z_2 $z_i = k_i$ với $1 \leq i \leq m$ và z_i vơi $i \geq m + 1$ thỏa mãn quan hệ hồi quy tuyến tính bậc m trên trường Z_2:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j}, \forall i \geq 0 \quad (4)$$

Trong đó, m hệ số $c_0, c_1, \dots, c_{m-1}$ là các phần tử của trường $\mathbb{Z}_2$ và được gọi là các hệ số hồi quy của thanh ghi dịch. Các hệ số hồi quy sẽ hình thành nên cấu trúc của một thanh ghi dịch.

Với khóa $z_i \in K$, $i \geq 1$ tạo lên xâu các phần tử $z = z_1 z_2 \dots$. Giả sử các biểu hình rõ $x_i \in Z_2$, $i \geq 1$ cấu tạo lên xâu $x = x_1 x_2 \dots$, khi đó:

Hàm mã hóa:

$\forall\ x = x_1 x_2 \dots$ với $x_i \in P$, $y = e_z(x) = e_{z1}(x_1) e_{z2}(x_2) \dots = y_1 y_2 \dots$; trong đó $e_{z_i}(x_i) = x_i + z_i \bmod 2$

Hàm giải mã:

$\forall\ y = y_1 y_2 \dots$ với $y_i \in C$, $i \geq 1$; $x = d_z(y) = d_{z1}(y_1) d_{z2}(y_2) \dots = x_1 x_2 \dots$ trong đó $d_{zi}(y_i) = y_i - z_i \bmod 2$

3. KẾT QUẢ NGHIÊN CỨU

Nội dung phần này đề xuất giải pháp tấn công hệ mã dòng mà khóa của nó được tạo bởi thanh ghi dịch hồi tiếp tuyến tính nhị phân trong tình huống biết cặp (rõ, mã).

3.1. Xác định cấu trúc và khởi điểm thanh ghi

Nội dung phần này, nhóm nghiên cứu đề xuất giải pháp xác định cấu trúc của thanh ghi dịch hồi tiếp tuyến tính (tìm đa thức hồi quy) và tìm khởi điểm của nó.

Định lý 1: Cấu trúc của thanh ghi dịch hồi tiếp tuyến tính đơn tầng bậc m được xác định bởi 2m bít đầu ra liên tiếp.

Chứng minh:

Giả sử biết bậc của thanh ghi là m, để xác định cấu trúc thanh ghi cần cần xác định các giá trị hệ số của đa thức hồi quy $(c_0, c_1, \dots, c_{m-1})$. Giả sử thanh ghi có hệ thức truy hồi sau đây:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j}, \forall i \geq 1 \quad (5)$$

Ta triển khai công thức trên dưới dạng hệ m phương trình sau:

$$\begin{cases} z_{m+1} = c_0 z_1 + c_1 z_2 + c_2 z_3 + \dots + c_{m-1} z_m \\ z_{m+2} = c_0 z_2 + c_1 z_3 + c_2 z_4 + \dots + c_{m-1} z_{m+1} \\ \dots \\ z_{2m} = c_0 z_m + c_1 z_{m+1} + c_2 z_{m+2} + \dots + c_{m-1} z_{2m-1} \end{cases} \quad (6)$$

Hệ phương trình (6) có thể viết dưới dạng ma trận sau đây:

$$(z_{m+1}, z_{m+2}, \dots, z_{2m}) = (c_0, c_1, \dots, c_{m-1}) \begin{pmatrix} z_1 & z_2 & \dots & z_m \\ z_2 & z_3 & \dots & z_{m+1} \\ \vdots & \vdots & & \vdots \\ z_m & z_{m+1} & \dots & z_{2m-1} \end{pmatrix} \quad (7)$$

Nếu ma trận hệ số có nghịch đảo trong trường $\mathbb{Z}_2$, hoàn toàn có thể tính toán được các hệ số hồi quy $(c_0, c_1, \dots, c_{m-1})$ như sau:

$$(c_0, c_1, \dots, c_{m-1}) = (z_{m+1}, z_{m+2}, \dots, z_{2m}) \begin{pmatrix} z_1 & z_2 & \dots & z_m \\ z_2 & z_3 & \dots & z_{m+1} \\ \vdots & \vdots & & \vdots \\ z_m & z_{m+1} & \dots & z_{2m-1} \end{pmatrix}^{-1} \quad (8)$$

Khi đó, bộ giá trị $(c_0, c_1, \dots, c_{m-1})$ chính là khởi điểm thanh ghi.

Với m = 5, ta có $(z_{m+1}, z_{m+2} \dots z_{2m}) = (z_6, z_7 \dots z_{10}) = (0,1,0,0,0)$

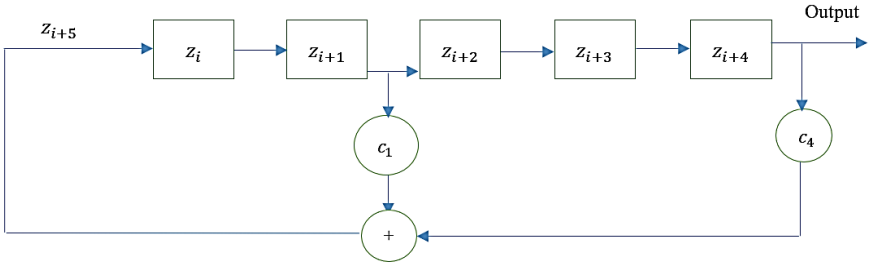
$$(0,1,0,0,0) = (c_1, c_2, c_3, c_4)\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad (9)$$

$$(c_1, c_2, c_3, c_4) = (0,1,0,0,0)\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}^{-1} \quad (10)$$

Dễ thấy:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Vậy $(c_0, c_1, \dots, c_{m-1})$ được xác định theo phương trình sau đây: $z_{i+5} = z_{i+1} + z_{i+4}\ mod\ 2$ với $i \geq 1$ có đa thức hồi quy tuyến tính là $1+x^2+x^5$. Từ công thức truy hồi ta xác định cấu trúc thanh ghi dạng sau:



Hình 4. *Cấu trúc thanh ghi tìm được.*

Với khởi điểm 11010, ta dễ dàng tìm ra 616 bít khóa đầu tiên sau:

```
  0101110110001111100110100100001010111011000111110011010010000101
0101110110001111100110100100001010111011000111110011010010000101010
1110110001111100110100100001010111011000111110011010010000101011101
1000011111001101001000010101110110001111100110100100001010111011000
0111100110100100001010111011000111110011010010000101011101100001111
0011010010000101011101100011111001101001000010101110110000111100110
1001000010101110110001111100110100100001010111011000111100110100100
0010101110110001111100110100100001010111011000111100110100100001010
```

Điều cần chú ý là đa thức hồi quy tuyến tính $1+x^2+x^5$ là nguyên thủy [4], nên chu kỳ dãy khóa được tạo ra có độ dài tối đa là $2^5 - 1 = 31$

Định lý 2: Khởi điểm của thanh ghi dịch hồi tiếp tuyến tính m tầng có đa thức hồi quy P(X) được xác định qua ít nhất m bít đầu ra.

Chứng minh:

Giả sử cho dãy $s^n = s_0, s_1, \dots, s_{n-1}$ là dãy n các bít đầu ra của thanh ghi dịch m tầng, trong

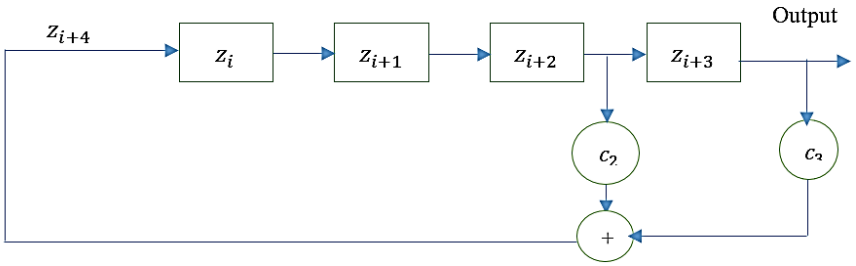
đó $s_i \in \mathbb{Z}_2 \cup \{*\}$, i=0,1,.. và ký hiệu $\{*\}$ là các bít chưa biết. Giả sử đa thức hồi quy $P(X)$ của thanh ghi. Ta xây dựng công thức tìm khởi điểm của thanh ghi dịch sinh ra dãy khóa khớp với dãy s^n đã cho. Gọi số bít đã biết $s_i \in \mathbb{Z}_2$ trong dãy s^n là L, hay $L = \#\{s_i \neq *, 0 \leq i < n\}$. Giả sử đa thức hồi quy của thanh ghi dịch sinh ra dãy khớp với s^n có dạng: $P(X) = 1 - \sum_{i=0}^{m-1} c_i X^{i+1}$ và gọi khởi điểm của thanh ghi dịch là $c = (c_0, c_1, \dots, c_{m-1})$. Như vậy, mỗi giá trị s_i thuộc s^n sẽ là một tổ hợp tuyến tính của $(c_0, c_1, \dots, c_{m-1})$ và được xác định như sau:

$$s_0 = (1,0,\dots,0).c^T;\ s_1 = (0,1,\dots,0).c^T;\dots;\ s_{m-1} = (0,0,\dots,1).c^T$$

$$s_{t+\mathrm{m}} = \sum_{i=0}^{m-1} c_i s_{t+m-i}, \text{ với } t = 0,1,\dots,n-\mathrm{m}-1$$

Với mỗi giá trị $s_i \in Z_2$ ta lập được một phương trình tuyến tính gồm m ẩn $c_0, c_1, \dots, c_{m-1}$. Khi đó, từ dãy s^n ta lập được một hệ L phương trình tuyến tính. Giải hệ phương trình này chúng ta xác định được khởi điểm của thanh ghi dịch. Hệ phương trình này có nghiệm vì theo giả thiết $L \geq \mathrm{m}$.■

Ví dụ: Cho dãy $s^{14} = ****1**0*10**1$ và đa thức hồi quy $P(X) = 1 + X^3 + X^4$ $(m = 4)$. Giả sử cấu trúc thanh ghi dịch như sau:



Hình 5. *Cấu trúc thanh ghi* $P(X) = 1 + X^3 + X^4$.

Đầu ra của thanh ghi dịch được mô tả trong bảng sau:

Bảng 1. *Bảng mô tả đầu ra của thanh ghi dịch 16 nhịp đầu tiên.*

n	Bít đầu ra	Ô nhớ 1	Ô nhớ 2	Ô nhớ 3	Ô nhớ 4
0		c_0	c_1	c_2	c_3
1	$s_0 = c_3$	$c_2 + c_3$	c_0	c_1	c_2
2	$s_1 = c_2$	$c_1 + c_2$	$c_2 + c_3$	c_0	c_1
3	$s_2 = c_1$	$c_0 + c_1$	$c_1 + c_2$	$c_2 + c_3$	c_0
4	$s_3 = c_0$	$c_0 + c_2 + c_3$	$c_0 + c_1$	$c_1 + c_2$	$c_2 + c_3$
5	$s_4 = c_2 + c_3$	$c_1 + c_3$	$c_0 + c_2 + c_3$	$c_0 + c_1$	$c_1 + c_2$
6	$s_5 = c_1 + c_2$	$c_0 + c_2$	$c_1 + c_3$	$c_0 + c_2 + c_3$	$c_0 + c_1$
7	$s_6 = c_0 + c_1$	$c_1 + c_2 + c_3$	$c_0 + c_2$	$c_1 + c_3$	$c_0 + c_2 + c_3$
8	$s_7 = c_0 + c_2 + c_3$	$c_0 + c_1 + c_2$	$c_1 + c_2 + c_3$	$c_0 + c_2$	$c_1 + c_3$
9	$s_8 = c_1 + c_3$	$c_0 + c_1 + c_2 + c_3$	$c_0 + c_1 + c_2$	$c_1 + c_2 + c_3$	$c_0 + c_2$
10	$s_9 = c_0 + c_2$	$c_0 + c_1 + c_3$	$c_0 + c_1 + c_2 + c_3$	$c_0 + c_1 + c_2$	$c_1 + c_2 + c_3$
11	$s_{10} = c_1 + c_2 + c_3$	$c_0 + c_3$	$c_0 + c_1 + c_2$	$c_0 + c_1 + c_2 + c_3$	$c_0 + c_1 + c_2$
12	$s_{11} = c_0 + c_1 + c_2$	c_3	$c_0 + c_3$	$c_0 + c_1 + c_3$	$c_0 + c_1 + c_2 + c_3$
13	$s_{12} = c_0 + c_1 + c_2 + c_3$	c_2	c_3	$c_0 + c_3$	$c_0 + c_1 + c_3$
14	$s_{13} = c_0 + c_1 + c_3$	c_1	c_2	c_3	$c_0 + c_3$
15	$s_{14} = c_0 + c_3$	c_0	c_1	c_2	c_3

Vì $s_4 = 1$, $s_7 = 0$, $s_9 = 1$, $s_{10} = 0$ và $s_{13} = 1$ nên ta có hệ phương trình sau đây:

$$\begin{cases} s_4 = c_2 + c_3 = 1 \\ s_7 = c_0 + c_2 + c_3 = 0 \\ s_9 = c_0 + c_2 = 1 \\ s_{10} = c_1 + c_2 + c_3 = 0 \\ s_{13} = c_0 + c_1 + c_3 = 1 \end{cases} \quad (11)$$

Giải hệ phương trình (*) trên ta được khởi điểm của thanh ghi dịch là $c = (c_0, c_1, \dots, c_3) = (1101)$.

3.2. Tấn công mã dòng khi biết cặp (rõ, mã)

Định lý 3: Hệ mã dòng thanh ghi dịch hồi tiếp tuyến tính bị khám phá khi biết cặp rõ mã tương ứng.

Chứng minh: Giả sử ta biết cặp (rõ, mã) là ($r_0, r_1, \dots, r_3$ ..., $m_0, m_1, \dots, m_3$ ...). Khi đó tiến hành lấy hiệu của (rõ – mã) mod 2 ta được dãy khóa để mã bản rõ và cho bản mã là $z_0, z_1, \dots, z_3$ ... Từ dãy khóa này theo định lý 1 ta xác định được cấu trúc thanh ghi. Áp dụng định lý 2 ta xác định được khởi điểm.

Ví dụ: Xét hệ mã dòng có bậc của thanh ghi hồi tiếp tuyến tính $m = 5$. Giả sử ta có cặp (rõ-mã) là:

Bản Rõ:

```
  01100110000001000110110010101100110011000000110000000100000001
000100110011101100111101000100110000000100010011001000110000001100
000001100000001000001101000000100001011100001011010010110110011100
000001001001011011001110000001001000001011000010000001001111011000
110111010100110010011110
```

Bản mã:

```
  00111011100010111111011011101110011101110001001100110000100000
010011101011010010100111010100011011101000001100000101111000011000
111010100111111011011111000101111100111111110010111011110100110010
011001110111000001011110101010100100010100001111001001011010101111
110000100111100000011000
```

Lấy rõ-mã mod 2 được dãy khóa sau:

```
  01011101100011111001101001000010101110110001111100110100100001
010111011000111110011010010000101011101100011111001101001000010100
111011000111110011010010000101011101100011111001101001000010101111
011000111110011010010000101011101100011111001101001000010101110110
000111110011010010000101011101100011111001101001000010101110110000
111110011010010000101011101100011111001101001000010101110110000111
110011010010000101011101100011111001101001000010101110110001111100
011010010000101011101100011111001101001000010101110110001111100110
```

Với dãy khóa này, áp dụng định lý 1 để tìm cấu trúc thanh ghi, ta hoàn toán xác định được đa thức hồi quy của thanh ghi là: P(X)= 1+x^2+ x^5. Áp dụng định lý 2 tìm ra được khởi điểm thanh ghi là: ($z_0, z_1, \dots, z_4$)= (11010).

Với kết quả sinh ra dãy khóa như sau:

```
  01011101100011111001101001000010101110110001111100110100100001
010111011000111110011010010000101011101100011111001101001000010100
111011000111110011010010000101011101100011111001101001000010101111
011000111110011010010000101011101100011111001101001000010101110110
000111110011010010000101011101100011111001101001000010101110110000
111110011010010000101011101100011111001101001000010101110110000111
110011010010000101011101100011111001101001000010101110110001111100
011010010000101011101100011111001101001000010101110110001111100110
```

01001000010101110110001111100110100100001010111011000111110011010
0100001010111011000111110011010010

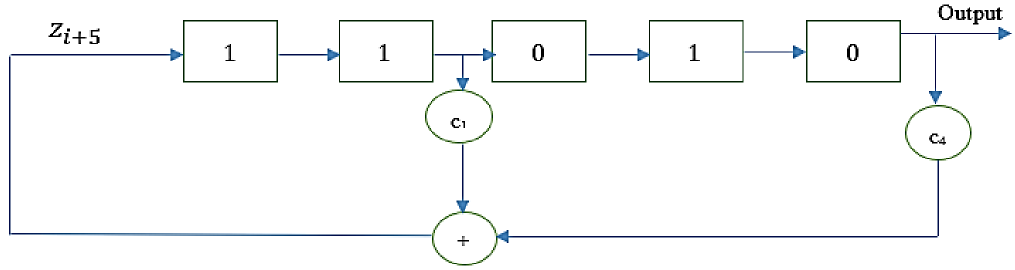
Giả sử bản mã tương ứng như sau:

1000111100000010110001000010010010001011100011011010101100
11010010001101011110010011001010000111010100110111110101010
01001111001101111111010110111101000000000001111011110111111011
10110011010100000101100111000011000000101101110000011001001001
00101100001111100110111001100110011110000011100010011101101
01100111000000010010111001011010100111011110100010011100010
111110101111110011010011110011101111110110001010110111011101
10101101110011100111000100001100001010100000001101111010101010
10111010111100000100100101110110111010000100111011000011000
00111011001000110011010001000111011100000001000001101101101000
000000100110010011101101010110

Áp dụng công thức Rõ = Mã- khóa Mod 2, dễ dàng giải ra bản rõ dạng số như sau:

110100101000101000010010000010111010110000000100011000101110111
00011011001100110000000110000000010001001010100001100111011011100 11
01010011001001110000000100001011000000110000000010000101110111101 10
00000100111010101000011001001110000011101000011000101110110001100
00101100000001000100110010011100011101000000011001000110000000010011
10101010000110010011100000111010000110001011101100011000010110000
00100000101110111101100000001000100101010000110011101101110011 01010
01100100111000000010000101100000011000000001001000011000101110101 00
00101001110101001101000111010101110101001101100111000101110000001
001000101011001010001100100000000100

Giải mã ASCII được bản rõ là: “KQHĐ5 F7630 Ranger 40 to Warpatch 29.01 Warpatch to Ranger 40 at…request QSL”



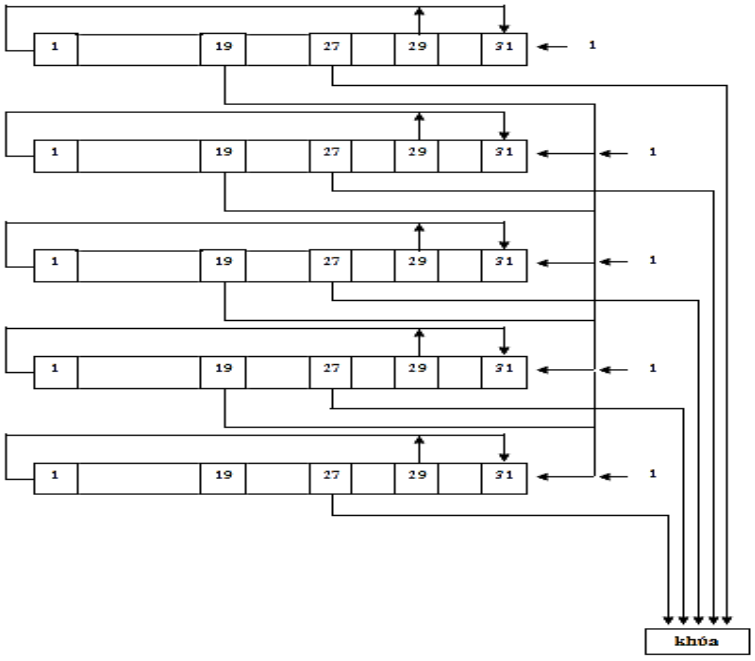
Hình 6. *Cấu trúc thanh ghi tìm được có đa thức hồi quy P(X)= 1+x^2+ x^5.*

3.3. Đề xuất giải pháp nâng cao độ an toàn cho hệ mã dòng

Qua ví dụ trên, chúng tôi kết luận rằng, nếu mã dòng sử dụng thanh ghi dịch hồi tiếp tuyến tính đơn tầng để sinh khóa thì độ mật sẽ không cao. Nếu kẻ tấn công biết trước cặp (rõ, mã) thì lớp hệ mã dòng sử dụng thanh ghi dịch hồi tiếp đơn tầng sinh khóa hầu như bị khám phá. Từ đó, chúng tôi đề xuất giải pháp nâng cao độ an toàn cho hệ mã dòng là bộ tạo khóa bằng các thanh ghi dịch hồi tiếp tuyến tính phải được thiết kế phức tạp hơn, sử dụng nhiều thanh ghi để kết nối với nhau theo một thuật toán phức tạp hơn. Để minh chứng cho lập luận này, dưới đây là ví dụ bộ tạo khóa của máy mã H460 [16], sử dụng 5 thanh ghi dịch hồi tiếp tuyến tính, mỗi thanh ghi dịch có độ dài là 31 bit. Sau mỗi nhịp làm việc tạo ra 5 bít khóa, ký hiệu là $(l_5l_4l_3l_2l_1)_2$.

Với kỹ thuật ghép nối nhiều thanh ghi, mỗi thanh ghi có m ô nhớ, nếu m đủ lớn và đa thức hồi quy P(X) bậc m là đa thức nguyên thủy [4] (đa thức cấu trúc thanh ghi), chu kỳ khóa của mỗi thanh ghi đạt độ dài tối đa là $2^{\deg(P(X))}-1$. Ví dụ, nếu sử dụng đa thức hồi quy P(X) là đa thức nguyên thủy có bậc là 255, thì chu kỳ dãy khóa được sinh ra sẽ có độ dài $2^{255}-1$; kết hợp với việc kết nối nhiều thanh ghi tham gia vào quá trình tạo phần tử khóa (ví dụ hệ thống kết nối thanh ghi của máy mã H460 trên hình 7), khi đó, nếu độ dài chu kỳ khóa mà lớn hơn độ dài thông báo và không để lộ cặp (rõ, mã) thì hệ mã có độ mật cao. Bên cạnh đó, cần xây dựng giao

thức trao đổi khóa, bản rõ và bản mã an toàn tránh để lộ các cặp (rõ, mã) vào tay kẻ tấn công, vì có cặp (rõ, mã) tương ứng thì cấu trúc và các bít khởi điểm thanh ghi sẽ được xác định, khi đó, hệ mã dòng sẽ bị khám phá hoàn toàn.



Hình 7. *Cấu trúc thanh ghi hệ mã H460.*

4. KẾT LUẬN

Dựa vào các kết quả nghiên cứu [1-3, 5-16] liên quan đến than ghi dịch hồi tiếp tuyến tính và mã dòng phương pháp tấn công mật mã [7], bài báo đã đề xuất giải pháp tấn công hệ mã dòng có dãy khóa được tạo bởi thanh ghi dịch hồi tiếp tuyến tính trong trường hợp biết cặp (rõ, mã) [7, 9]. Nội dung cốt lõi của giải pháp là giải thạnh ghi dịch hồi tiếp tuyến tính nhị phân đơn tầng khi biết $2m$ bít không liên tục của dãy khóa được tạo bởi thanh ghi dịch hồi tiếp tuyến tính nhị phân (trong đó m là số tầng của thanh ghi) cho phép xác định được khởi điểm của nó, hoặc chỉ cần biết $2m$ bít khóa có thể xác định được cấu trúc thanh ghi dịch. Kết quả nghiên cứu đã áp dụng tấn công thành công các bản mã thực tế. Kết quả nghiên cứu làm cơ sở để xây dựng các hệ mã nói chung, hệ mã dòng nói riêng mật hơn. Hướng nghiên cứu tiếp theo là đề xuất giải pháp tấn công hệ mã dòng mà khóa của nó sử dụng thanh ghi dịch hồi tiếp tuyến tính đa tầng trong một số tình huống cụ thể, nhằm xây dựng được hệ thống mật mã dòng an toàn hơn trong các hệ thống truyền tin hiện nay.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Thị Thùy Dung, *"Nghiên cứu họ hệ mật WG trong mật mã hạng nhẹ",* Luận văn thạc sĩ, Đại học Công nghệ- ĐHQG HN, (2017).

[2]. Lê Thị Len, *"Mật mã dòng trong mật mã nhẹ và triển vọng trong IoT",* Luận văn thạc sĩ, Đại học Công nghệ- ĐHQG HN, (2017)

[3]. Trần Thị Lượng, *"Sinh các hộp thế phụ thuộc khóa cho AES sử dụng các LFSR và phép hoán vị hàng, cột",* Tạp chí ATTT, Ban cơ yếu Chính phủ, (2021).

[4]. Lều Đức Tân, *"Số nguyên tố và đa thức nguyên thủy",* Hà nội, (2002).

[5]. A. Ahmad and A.M Elabdallai.: *"An Efficient Method to Determine Linear Feedback Connections in Shift Registers That Generate Maximal Length PseudoRandom Up And Down Binary Sequences".* Computer Electronic Engineering Vol.23, No.1 pp. 33-39, (1997).

[6]. Berlekamp-Massey Algorithm Erin Casey University of Minnesota REU Summer 2000
[7]. Chapter 2 Linear Feedback Shift Registers http://www.springer.com/978-1-4471-5078-7
[8]. Chapter 3 LFSR-based Stream Ciphers Error-Correcting Codes and Symmetric Cryptography - A. Canteaut
[9]. D.R Stinson, *"Cryptography: Theory and Practice"*, CRC Press, pp. 194-196, (2003).
[10]. Kencheng Zeng, Chung-Hung Yang, Dah-Yea Wei and T.R.N Rao.: *"Pseudorandom Bit Generators in StreamCipher Cryptography":* IEEE (1991).
[11]. Myat Su Mon Win: *"A New Approach to Feedback Shift Register: World Academy of Science", Engineering* and Technology 48, pp. 185—189, (2008).
[12]. M U Bokhari and Faheem Masoodi.: *"Comparative Analysis of Structures and Attacks on Various Stream Cipher":* Proceedings of the 4th National Conference; INDIACom. pp. 236—238, (2010).
[13]. P. P. Deepthi, Deepa Sara John and P. S. Sathidevi: *"Design and analysis of a highly secure stream cipher based on linear feedback shift register"*, Computers and electrical engineering, Elsevier, pp 235-243, (2009).
[14]. LFSR Reference M-Sequence, Linear Feedback Shift Register.
[15]. http://www.springer.com/978-1-4471-5078-7
[16]. https://www.cryptomuseum.com/crypto/hagelin/h460/index.htm

ABSTRACT

Proposing a solution to attack stream cipher using binary linear feedback shift registers applied in the current communication system

This paper proposes a method of the stream ciphers attack in which its keystream is generated by the linear feedback shift register based on a pair of known plaintext, ciphertext. Based on these studies, the authors will develop the stream cipher attacking theory with its key sequence generated by the multi-layer shift register in the next research. The research results can be applied to build stream ciphers that overcome the disadvantages that we have proposed in this paper in order to improve the safety and security of the current communication systems.

Keywords: Linear feedback shift register; Stream ciphers.