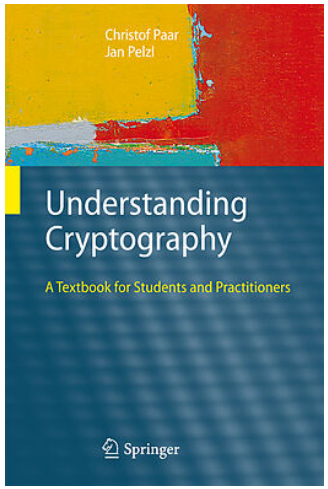
Tài liệu

https://www.crypto-textbook.com

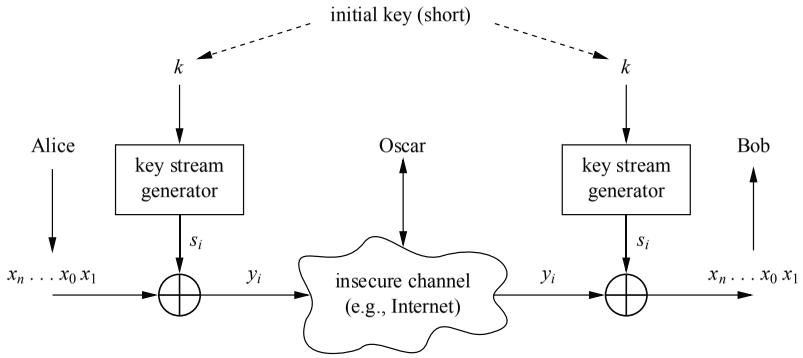


ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Nhập môn An toàn Thông tin

Mã dòng dựa trên thanh ghi dịch

Mã dòng

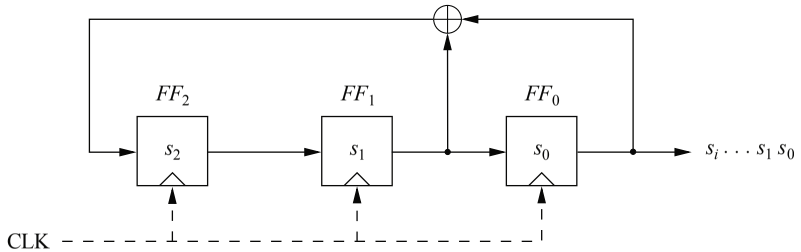


Câu hỏi: Làm thế nào sinh dãy s_i?

Nội dung

Thanh ghi dịch phản hồi tuyến tính

Linear Feedback Shift Register (LFSR)



Hình: LFSR bậc $m = 3$ với ba Flip-flops $FF_2, FF_1 v FF_0$

Công thức truy hồi:

$$s_{i+3} = s_{i+1} \oplus s_i.$$

Ví dụ

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0

$$s_{i+3} = s_{i+1} \oplus s_i$$

Ví dụ

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1

$$s_{i+3} = s_{i+1} \oplus s_i$$

Ví dụ

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0

$$s_{i+3} = s_{i+1} \oplus s_i$$

Ví dụ

$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1

Ví dụ

$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1

Ví dụ

$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0

Ví dụ

$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1

Ví dụ

$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0
8	0	1	0

Nội dung

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Ví dụ

$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
6 / 34

Ví dụ

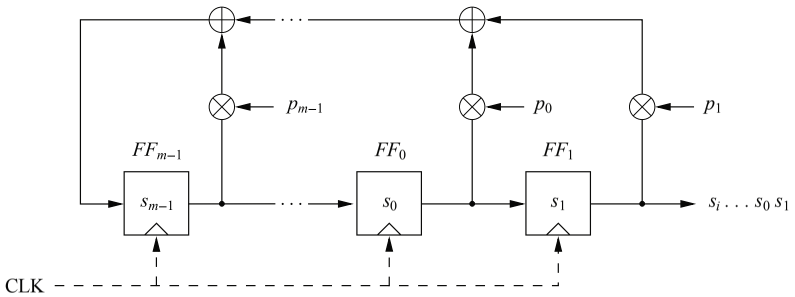
$$s_{i+3} = s_{i+1} \oplus s_i$$

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0
8	0	1	0

Output: 0010111 0010111 0010111 ...

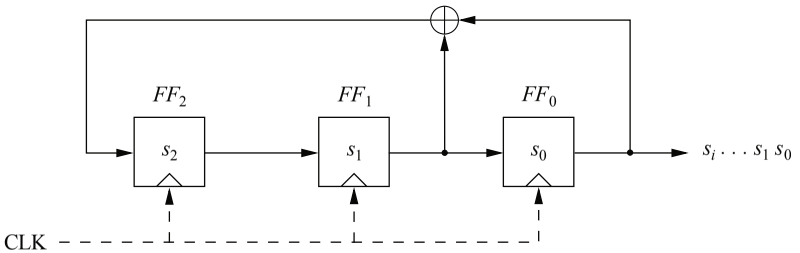
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
6 / 34

LFSR tổng quát



Hình: LFSR với hệ số phản hồi p_i và giá trị ban đầu $s_{m-1}, \ldots, s_0$

Thanh ghi dịch phản hồi tuyến tính

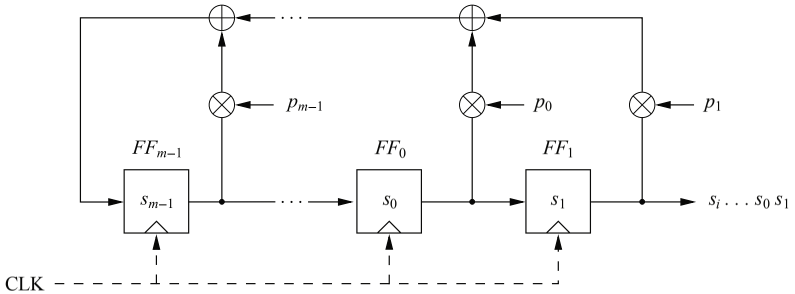


Công thức truy hồi:

$$s_{i+3} = 0 \cdot s_{i+2} + 1 \cdot s_{i+1} + 1 \cdot s_i \mod 2, \quad i = 0, 1, 2, \ldots$$

Công thức truy hồi

$$s_{i+m} = \sum_{j=0}^{m-1} p_j \cdot s_{i+j} \mod 2$$



Bài tập

- Xét LFSR với bậc $m = 4$ và hệ số phản hồi

$$(p_3 = 0, p_2 = 0, p_1 = 1, p_0 = 1).$$

- Bắt đầu từ

$$s_3 = 0,\ s_2 = 1,\ s_1 = 0,\ s_0 = 0$$

hãy tính 15 bit tiếp theo của dãy output.

Độ dài lớn nhất của dãy

- Xét dãy tạo bởi LFSR với công thức truy hồi:

$$s_{i+m} = \sum_{j=0}^{m-1} p_j \cdot s_{i+j} \mod 2; \qquad s_i, p_j \in \{0,1\}; \quad i = 0,1,2,\ldots$$

- Phụ thuộc vào m, dãy này lặp lại theo chu kỳ với độ dài khác nhau.

Định lý

Độ dài (chu kỳ) lớn nhất của dãy sinh bởi LFSR là $2^m - 1$.

Bài tập

- Xét LFSR với bậc $m = 4$ và hệ số phản hồi

$$(p_3 = 1, p_2 = 1, p_1 = 1, p_0 = 1).$$

- Bắt đầu từ

$$s_3 = 0,\ s_2 = 1,\ s_1 = 0,\ s_0 = 1$$

hãy tính 15 bit tiếp theo của dãy output.

LSFR và đa thức

LFSR bậc m với hệ số phản hồi $(p_{m-1}, \ldots, p_1, p_0)$ biểu diễn bởi đa thức

$$P(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0$$

Ví dụ

LFSR với bậc $m = 4$ và hệ số phản hồi

$$(p_3 = 0, p_2 = 0, p_1 = 1, p_0 = 1)$$

biểu diễn bởi đa thức

$$P(x) = x^4 + x + 1.$$

Ví dụ

Xét LFSR với bậc $m = 4$ và hệ số phản hồi

$$(p_3 = 0, p_2 = 0, p_1 = 1, p_0 = 1).$$

Dãy output có chu kỳ $2^4 - 1 = 15$.

Ví dụ

Xét LFSR với bậc $m = 4$ và hệ số phản hồi

$$(p_3 = 1, p_2 = 1, p_1 = 1, p_0 = 1).$$

Dãy output có chu kỳ 5.

Đa thức nguyên thuỷ và LSFR

- Chỉ có LFSR xác định bởi đa thức nguyên thuỷ mới có dãy output với chu kỳ cực đại!
- Đa thức nguyên thuỷ là một trường hợp riêng của đa thức bất khả quy (giống số nguyên tố).
- Ví dụ: Đa thức

$$(0,2,5) \to 1 + x^2 + x^5$$

là đa thức nguyên thuỷ.

Nội dung

Ví dụ

LFSR với bậc $m = 4$ và hệ số phản hồi

$$(p_3 = 1, p_2 = 1, p_1 = 1, p_0 = 1)$$

biểu diễn bởi đa thức

$$P(x) = x^4 + x^3 + x^2 + x + 1.$$

Một số đa thức nguyên thuỷ

(0,1,2)	(0,1,3,4,24)	(0,1,46)	(0,1,5,7,68)	(0,2,3,5,90)	(0,3,4,5,112)
(0,1,3)	(0,3,25)	(0,5,47)	(0,2,5,6,69)	(0,1,5,8,91)	(0,2,3,5,113)
(0,1,4)	(0,1,3,4,26)	(0,2,3,5,48)	(0,1,3,5,70)	(0,2,5,6,92)	(0,2,3,5,114)
(0,2,5)	(0,1,2,5,27)	(0,4,5,6,49)	(0,1,3,5,71)	(0,2,93)	(0,5,7,8,115)
(0,1,6)	(0,1,28)	(0,2,3,4,50)	(0,3,9,10,72)	(0,1,5,6,94)	(0,1,2,4,116)
(0,1,7)	(0,2,29)	(0,1,3,6,51)	(0,2,3,4,73)	(0,11,95)	(0,1,2,5,117)
(0,1,3,4,8)	(0,1,30)	(0,3,52)	(0,1,2,6,74)	(0,6,9,10,96)	(0,2,5,6,118)
(0,1,9)	(0,3,31)	(0,1,2,6,53)	(0,1,3,6,75)	(0,6,97)	(0,8,119)
(0,3,10)	(0,2,3,7,32)	(0,3,6,8,54)	(0,2,4,5,76)	(0,3,4,7,98)	(0,1,3,4,120)
(0,2,11)	(0,1,3,6,33)	(0,1,2,6,55)	(0,2,5,6,77)	(0,1,3,6,99)	(0,1,5,8,121)
(0,3,12)	(0,1,3,4,34)	(0,2,4,7,56)	(0,1,2,7,78)	(0,2,5,6,100)	(0,1,2,6,122)
(0,1,3,4,13)	(0,2,35)	(0,4,57)	(0,2,3,4,79)	(0,1,6,7,101)	(0,2,123)
(0,5,14)	(0,2,4,5,36)	(0,1,5,6,58)	(0,2,4,9,80)	(0,3,5,6,102)	(0,37,124)
(0,1,15)	(0,1,4,6,37)	(0,2,4,7,59)	(0,4,81)	(0,9,103)	(0,5,6,7,125)
(0,1,3,5,16)	(0,1,5,6,38)	(0,1,60)	(0,4,6,9,82)	(0,1,3,4,104)	(0,2,4,7,126)
(0,3,17)	(0,4,39)	(0,1,2,5,61)	(0,2,4,7,83)	(0,4,105)	(0,1,127)
(0,3,18)	(0,3,4,5,40)	(0,3,5,6,62)	(0,5,84)	(0,1,5,6,106)	(0,1,2,7,128)
(0,1,2,5,19)	(0,3,41)	(0,1,63)	(0,1,2,8,85)	(0,4,7,9,107)	
(0,3,20)	(0,1,2,5,42)	(0,1,3,4,64)	(0,2,5,6,86)	(0,1,4,6,108)	
(0,2,21)	(0,3,4,6,43)	(0,1,3,4,65)	(0,1,5,7,87)	(0,2,4,5,109)	
(0,1,22)	(0,5,44)	(0,3,66)	(0,8,9,11,88)	(0,1,4,6,110)	
(0,5,23)	(0,1,3,4,45)	(0,1,2,5,67)			

Dựa trên giả sử rằng

Oscar có:

- Mọi bit bản mã y_i
- Bậc m
- Các bit bản rõ $(x_0, x_1, \ldots, x_{2m-1})$

Bước 1

Tính toán

$$y_i = x_i + s_i \mod 2$$
$$s_i = y_i + x_i \mod 2$$

với $i = 0, 1, \ldots, 2m-1$

Bước 2

- Mục đích: Lấy được dãy bit khoá

$$s_{2m},\ s_{2m+1},\ \ldots$$

- Câu hỏi: Làm thế nào để tính:

$$p_0,\ p_1,\ \ldots,\ p_{m-1}?$$

Nhắc lại:

$$s_{i+m} = \sum_{j=0}^{m-1} p_j \cdot s_{i+j} \mod 2$$

Bước 2: Tính p_i

$$\begin{aligned}
&i = 0, && s_m = p_m s_{m-1} + \cdots + p_1 s_1 + p_0 s_0 && \mod 2\\
&i = 1, && s_{m+1} = p_m s_m + \cdots + p_1 s_2 + p_0 s_1 && \mod 2\\
&\vdots\\
&i = m-1, && s_{2m-1} = p_{m-1} s_{2m-2} + \cdots + p_1 s_m + p_0 s_{m-1} && \mod 2
\end{aligned}$$

- Hệ phương trình tuyến tính m ẩn.
- Dễ giải dùng phương pháp khử Gauss!

Bước 3

- Dùng cấu hình

$$(p_{m-1}, \ldots, p_1, p_0)$$

để xây dựng LFSR.

- Tính dãy bit khoá

$$s_0, s_1, \ldots, s_{2m}, \ldots$$

- Giải mã

$$x_i = y_i + s_i \mod 2.$$

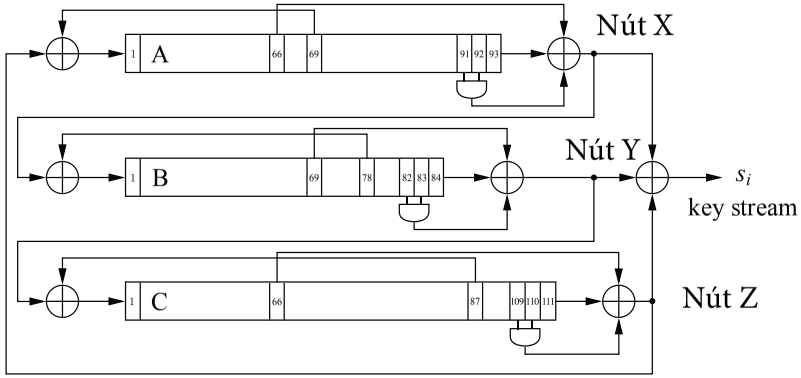
Hệ quả

Nếu kẻ tấn công có (ít nhất) $2m$ giá trị output của LFSR, anh ta có thể lấy được toàn bộ thông tin về cấu hình

$$p_0, p_1, \ldots, p_{m-1}.$$

của LFSR.

Giới thiệu Trivium



Hình: Hệ mã dòng mới với kích thước khoá 80 bit. Dựa trên việc kết hợp ba thanh ghi dịch có phản hồi, và kết hợp với thành phần phi tuyến.

Nội dung

Đặc tả Trivium

	register length	feedback bit	feedforward bit	AND inputs
A	93	69	66	91,92
B	84	78	69	82,83
C	111	87	66	109,110

- Phép toán AND chính là phép nhân theo modun 2, và phương trình không còn là tuyến tính nữa.
- Feedforward paths liên quan đến phép toán AND là thành phần quan trọng cho tính an toàn của hệ.

Mã hoá với Trivium: Khởi tạo

- 80 bit IV được đưa vào 80 bit trái nhất của thanh ghi A. IV không cần giữ bí mật nhưng phải thay đổi sau cho mỗi phiên làm việc.
- 80 bit khoá được đưa vào 80 bit trái nhất của thanh ghi B.
- Mọi bit thanh ghi khác được đặt bằng 0 ngoại trừ ba bit phải nhất của thanh ghi C:

$$c_{109} = c_{110} = c_{111} = 1.$$

Mã hoá với Trivium: Pha khởi động

- Trong pha đầu tiên này, hệ mã được chạy

$$4 \times (93 + 84 + 111) = 1152$$

  lần, nhưng không tạo ra bit đầu ra nào.
- Pha này cần để tạo cho hệ mã đủ ngẫu nhiên.
- Nó đảm bảo dòng khoá phụ thuộc vào cả k và IV.

Mã hoá với Trivium

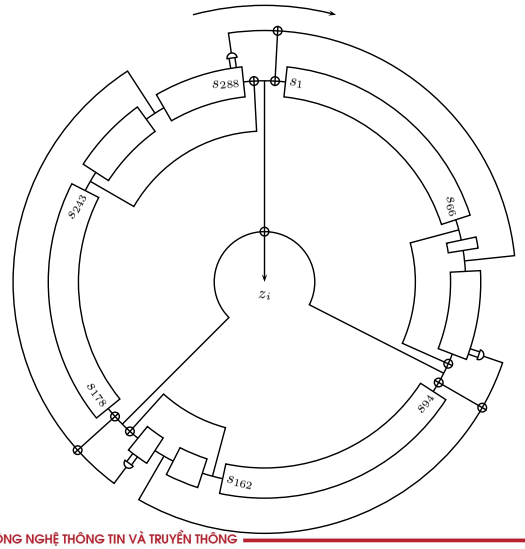
- Dãy bit sau đó, bắt đầu từ chu kỳ 1153, được sử dụng như dòng khoá s_i của hệ mã dòng.
- Tốc độ mã hoá của hệ rất cao: Khoảng 1Gbit/giây trên bộ xử lý 1.5 GHz của Intel.
- Dễ cài đặt trên phần cứng.
- Cho tới nay, chưa có phương pháp tấn công hiệu quả nào được ghi nhận.

Bài tập lập trình

1. Cài đặt hệ mã dòng Trivium.
2. Mã hoá file với Trivium. Bạn có thể sinh IV ngẫu nhiên và đặt vào đầu bản mã.

Tham khảo đặc tả chi tiết Trivium

https://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Cảm ơn!

soict.hust.edu.vn/ fb.com/groups/soict