CHƯƠNG 6

HỆ MẬT MÃ DÒNG - STREAM CIPHERS

Nội dung

- Hệ mật mã khối và mật mã dòng

Nội dung

- Hệ mật mã khối và mật mã dòng
- Hệ mật mã dòng "one-time pad"

Nội dung

- Hệ mật mã khối và mật mã dòng
- Hệ mật mã dòng "one-time pad"
- Hệ mật mã dòng đồng bộ

Nội dung

- Hệ mật mã khối và mật mã dòng
- Hệ mật mã dòng "one-time pad"
- Hệ mật mã dòng đồng bộ
- Hệ mật mã dòng tự đồng bộ hóa

Nội dung

- Hệ mật mã khối và mật mã dòng
- Hệ mật mã dòng "one-time pad"
- Hệ mật mã dòng đồng bộ
- Hệ mật mã dòng tự đồng bộ hóa
- LFSR và Sinh dòng khóa

Nội dung

- Hệ mật mã khối và mật mã dòng
- Hệ mật mã dòng "one-time pad"
- Hệ mật mã dòng đồng bộ
- Hệ mật mã dòng tự đồng bộ hóa
- LFSR và Sinh dòng khóa

Hệ mật mã khối và mật mã dòng

- **Mật mã khối** là quá trình xử lý mã hóa/ giải mã theo từng khối có kích thước tương đối lớn

Hệ mật mã khối và mật mã dòng

- **Mật mã khối** là quá trình xử lý mã hóa/ giải mã theo từng khối có kích thước tương đối lớn
- **Mật mã dòng** là quá trình xử lý mã hóa/giải mã theo từng khối có kích thước nhỏ xem như từng bit

Hệ mật mã khối và mật mã dòng

- **Mật mã khối** là quá trình xử lý mã hóa/ giải mã theo từng khối có kích thước tương đối lớn
- **Mật mã dòng** là quá trình xử lý mã hóa/giải mã theo từng khối có kích thước nhỏ xem như từng bit
- **Hệ mật mã dòng** đôi khi còn gọi là hệ mật mã trạng thái

Hệ mật mã khối và mật mã dòng

- **Mật mã khối** là quá trình xử lý mã hóa/ giải mã theo từng khối có kích thước tương đối lớn
- **Mật mã dòng** là quá trình xử lý mã hóa/giải mã theo từng khối có kích thước nhỏ xem như từng bit
- **Hệ mật mã dòng** đôi khi còn gọi là hệ mật mã trạng thái
- **Mật mã dòng** có thể được xem là hệ mật mã khóa đối xứng hoặc mật mã khóa công khai

Hệ mật mã dòng **One-time pad**

- **One-time pad** hay còn gọi là hệ mật mã Vernam, biểu diễn bởi:

$$c_i = m_i \oplus k_i, \; for \; i = 1, 2, 3, \ldots$$

với m_i là các ký tự trong văn bản gốc và $k_1, k_2, \ldots$ gọi là dòng khóa.

Hệ mật mã dòng **One-time pad**

- **One-time pad** hay còn gọi là hệ mật mã Vernam, biểu diễn bởi:

$$c_i = m_i \oplus k_i, \; for \; i = 1, 2, 3, \ldots$$

với m_i là các ký tự trong văn bản gốc và $k_1, k_2, \ldots$ gọi là dòng khóa.

- **Dòng khóa** $k_1, k_2, \ldots$ được sinh độc lập và ngẫu nhiên

Hệ mật mã dòng **One-time pad**

- **One-time pad** hay còn gọi là hệ mật mã Vernam, biểu diễn bởi:

$$c_i = m_i \oplus k_i, \; for \; i = 1, 2, 3, \ldots$$

với m_i là các ký tự trong văn bản gốc và $k_1, k_2, \ldots$ gọi là dòng khóa.

- **Dòng khóa** $k_1, k_2, \ldots$ được sinh độc lập và ngẫu nhiên
- **One-time pad** đảm bảo bảo mật không điều kiện nghĩa là H(M|C)=H(M)

Hệ mật mã dòng **One-time pad**

- **One-time pad** hay còn gọi là hệ mật mã Vernam, biểu diễn bởi:

$$c_i = m_i \oplus k_i, \; for \; i = 1, 2, 3, \ldots$$

với m_i là các ký tự trong văn bản gốc và $k_1, k_2, \ldots$ gọi là dòng khóa.

- **Dòng khóa** $k_1, k_2, \ldots$ được sinh độc lập và ngẫu nhiên
- **One-time pad** đảm bảo bảo mật không điều kiện nghĩa là H(M|C)=H(M)
- **One-time pad** có hạn chế là khóa có kích thước như văn bản

Mật mã dòng đồng bộ

- **Mật mã dòng** thường được chia thành **mật mã dòng đồng bộ** (Synchronous stream cipher) và **mật mã dòng tự đồng bộ hóa** (Self-synchronizing stream cipher)

Mật mã dòng đồng bộ

- **Mật mã dòng** thường được chia thành **mật mã dòng đồng bộ** (Synchronous stream cipher) và **mật mã dòng tự đồng bộ hóa** (Self-synchronizing stream cipher)
- **Mật mã dòng đồng bộ** là hệ mật mã mà dòng khóa được sinh độc lập với văn bản gốc và văn bản mã hóa

Mật mã dòng đồng bộ

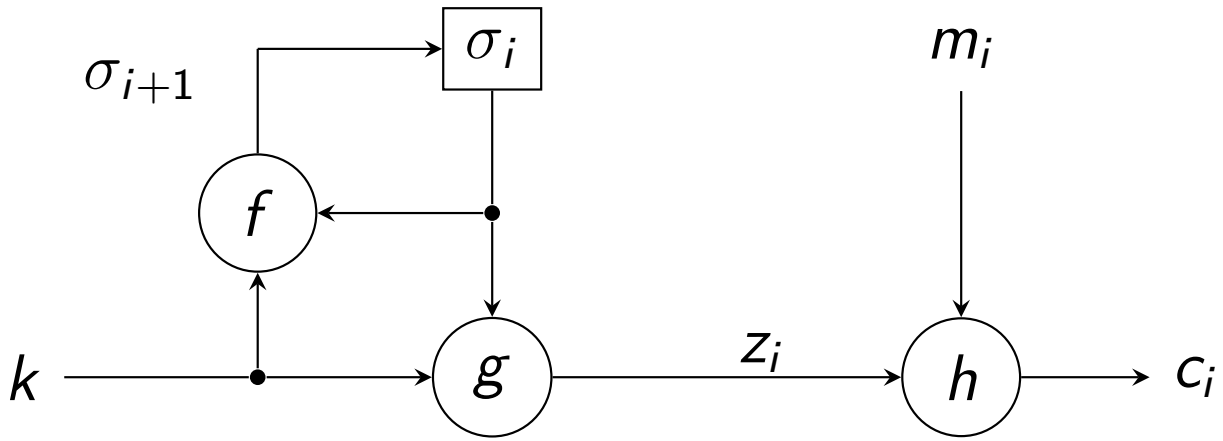
- **Mật mã dòng** thường được chia thành **mật mã dòng đồng bộ** (Synchronous stream cipher) và **mật mã dòng tự đồng bộ hóa** (Self-synchronizing stream cipher)
- **Mật mã dòng đồng bộ** là hệ mật mã mà dòng khóa được sinh độc lập với văn bản gốc và văn bản mã hóa
- **Mật mã dòng đồng bộ** được mô tả bởi:

$$\begin{aligned} \sigma_{i+1} &= f(\sigma_i, k) \\ z_i &= g(\sigma_i, k) \\ c_i &= h(z_i, m_i) \end{aligned}$$

σ_0 là trạng thái ban đầu có thể được xác định từ khóa k và hàm xác định trạng thái tiếp theo f, g là hàm sinh dòng khóa z_i, h là hàm mã hóa.

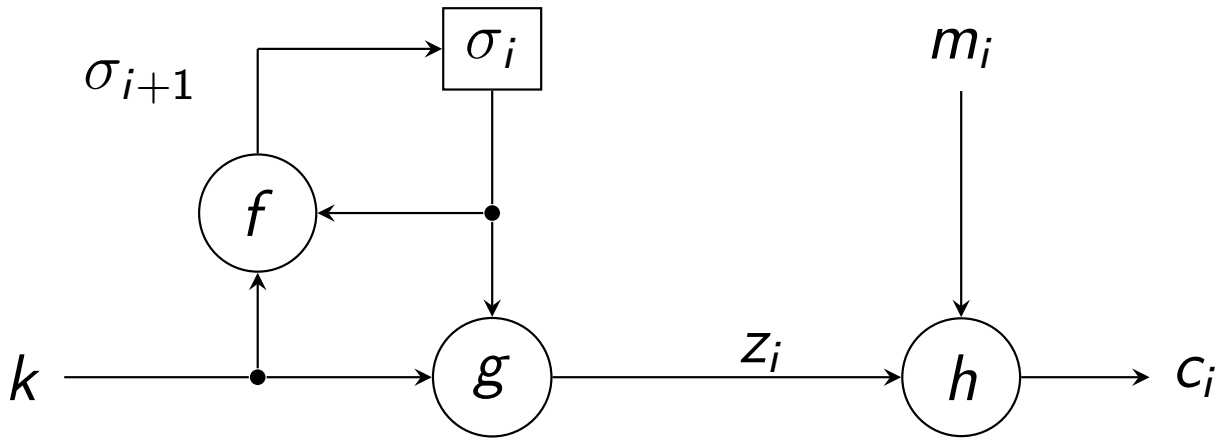
Sơ đồ mật mã dòng đồng bộ

- Quá trình mã hóa

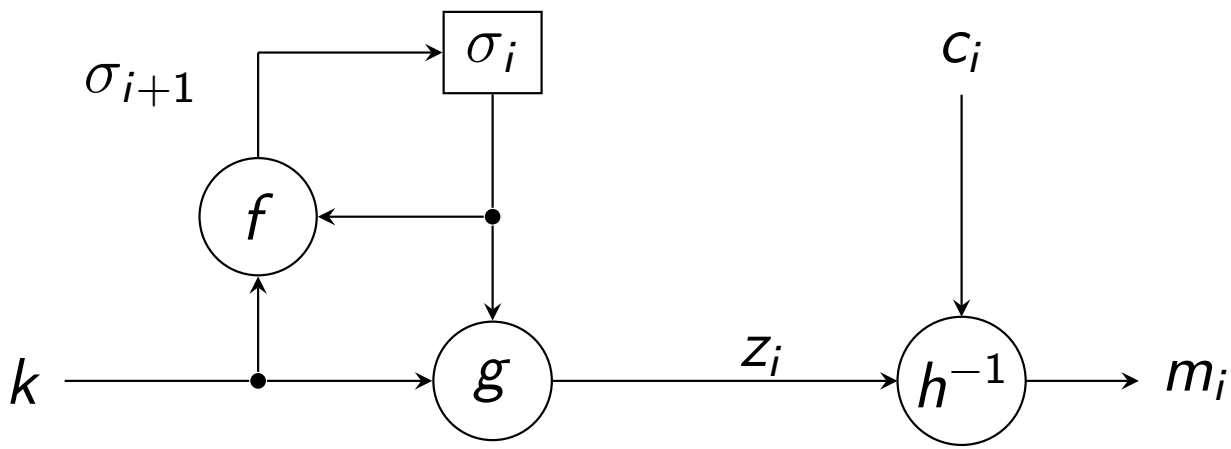


Sơ đồ mật mã dòng đồng bộ

- Quá trình mã hóa



- Quá trình giải mã



Tính chất của mật mã dòng đồng bộ

- Đảm bảo yêu cầu đồng bộ về khóa giữa người gửi và người nhận. Nghĩa là trạng thái vận hành giữa hai bên nhận và gửi là giống nhau.

Tính chất của mật mã dòng đồng bộ

- Đảm bảo yêu cầu đồng bộ về khóa giữa người gửi và người nhận. Nghĩa là trạng thái vận hành giữa hai bên nhận và gửi là giống nhau.
- Không gây lỗi lan truyền từ bước này đến các bước tiếp theo

Tính chất của mật mã dòng đồng bộ

- Đảm bảo yêu cầu đồng bộ về khóa giữa người gửi và người nhận. Nghĩa là trạng thái vận hành giữa hai bên nhận và gửi là giống nhau.
- Không gây lỗi lan truyền từ bước này đến các bước tiếp theo
- Dễ bị tấn công chủ động, nghĩa là nếu thêm, sửa, xóa ký tự trong văn bản mã hóa sẽ gây mất đồng bộ giữa hai bên mã hóa và giải mã do tính chất thứ nhất. Đồng thời kẻ địch cũng chủ động thăm dò sự giải mã trên từng ký tự do tính chất thứ 2

VD: Mật mã dòng cộng nhị phân

- Quá trình mã hóa

VD: Mật mã dòng cộng nhị phân

- Quá trình mã hóa

- Quá trình giải mã

Mật mã dòng tự đồng bộ hóa

- **Mật mã dòng tự đồng bộ hóa** là hệ mật mã dòng mà dòng khóa được sinh bởi hàm của khóa và một số xác định ký tự mã hóa trước đó

Mật mã dòng tự đồng bộ hóa

- **Mật mã dòng tự đồng bộ hóa** là hệ mật mã dòng mà dòng khóa được sinh bởi hàm của khóa và một số xác định ký tự mã hóa trước đó
- **Mật mã dòng tự đồng bộ hóa** được mô tả bởi:

$$\sigma_i = (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1})$$
$$z_i = g(\sigma_i, k)$$
$$c_i = h(z_i, m_i)$$

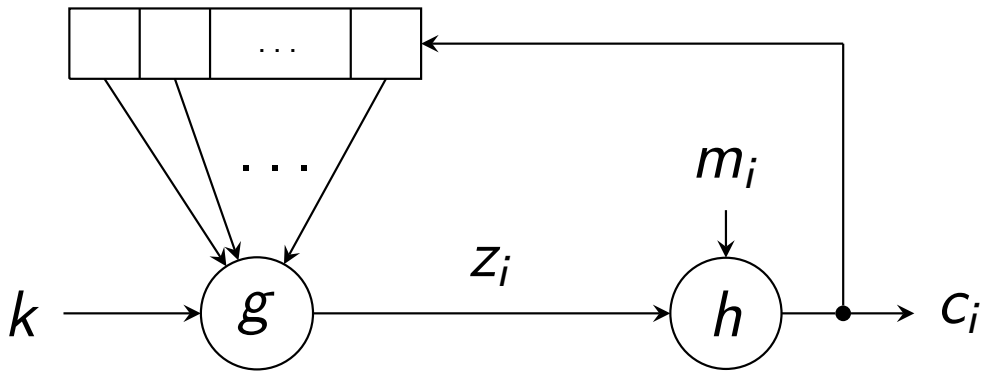
ở đó trạng thái ban đầu $\sigma_0 = (c_{-t}, c_{-t+1}, \ldots, c_{-1})$, khóa k, hàm sinh dòng khóa g và hàm mã hóa h.

Sơ đồ hệ mật mã dòng tự đồng bộ hóa

- Quá trình mã hóa

Sơ đồ hệ mật mã dòng tự đồng bộ hóa

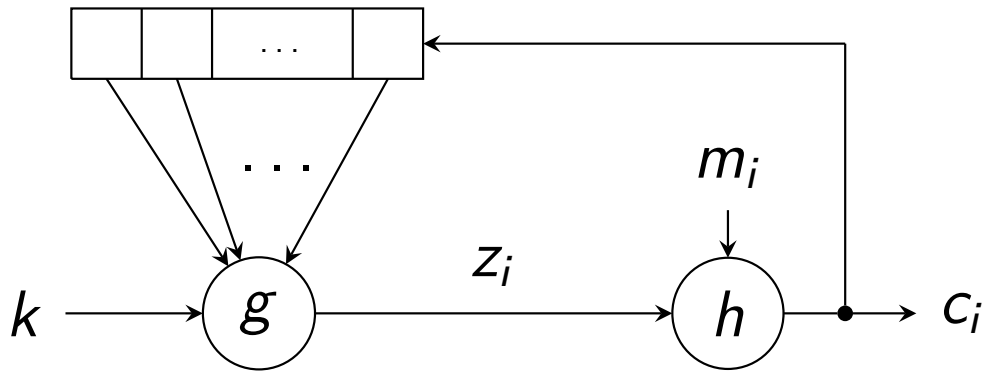
- Quá trình mã hóa



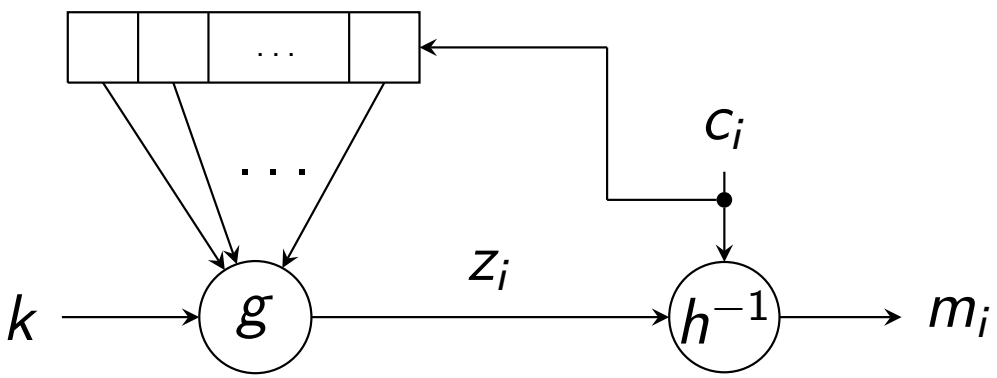
- Quá trình giải mã

Sơ đồ hệ mật mã dòng tự đồng bộ hóa

- Quá trình mã hóa



- Quá trình giải mã



Tính chất của mật mã dòng tự đồng bộ hóa

- Hệ mật mã dòng tự đồng bộ hóa có thể lặp lại việc giải mã chính xác sau khi mất sự đồng bộ mà chỉ một đoạn tin gốc nào đó.

Tính chất của mật mã dòng tự đồng bộ hóa

- Hệ mật mã dòng tự đồng bộ hóa có thể lặp lại việc giải mã chính xác sau khi mất sự đồng bộ mà chỉ một đoạn tin gốc nào đó.
- Việc lan truyền lỗi từ bước này đến các bước tiếp theo bị hạn chế, chẳng hạn giải mã trở lại đúng sau một số ký tự xác định nếu một ký tự mã bị chỉnh sửa.

Tính chất của mật mã dòng tự đồng bộ hóa

- Hệ mật mã dòng tự đồng bộ hóa có thể lặp lại việc giải mã chính xác sau khi mất sự đồng bộ mà chỉ một đoạn tin gốc nào đó.
- Việc lan truyền lỗi từ bước này đến các bước tiếp theo bị hạn chế, chẳng hạn giải mã trở lại đúng sau một số ký tự xác định nếu một ký tự mã bị chỉnh sửa.
- Bị tấn công chủ động. Tuy nhiên kẻ địch sẽ khó phát hiện việc thêm, sửa hay xóa ký tự so với mật mã dòng đồng bộ.

Tính chất của mật mã dòng tự đồng bộ hóa

- Hệ mật mã dòng tự đồng bộ hóa có thể lặp lại việc giải mã chính xác sau khi mất sự đồng bộ mà chỉ một đoạn tin gốc nào đó.
- Việc lan truyền lỗi từ bước này đến các bước tiếp theo bị hạn chế, chẳng hạn giải mã trở lại đúng sau một số ký tự xác định nếu một ký tự mã bị chỉnh sửa.
- Bị tấn công chủ động. Tuy nhiên kẻ địch sẽ khó phát hiện việc thêm, sửa hay xóa ký tự so với mật mã dòng đồng bộ.
- Làm tăng độ nhiễu về thống kê trong văn bản mã hóa vì mỗi ký tự cần mã hóa có thể ảnh hưởng đến các ký tự mã hóa tương ứng quanh nó.

Định nghĩa

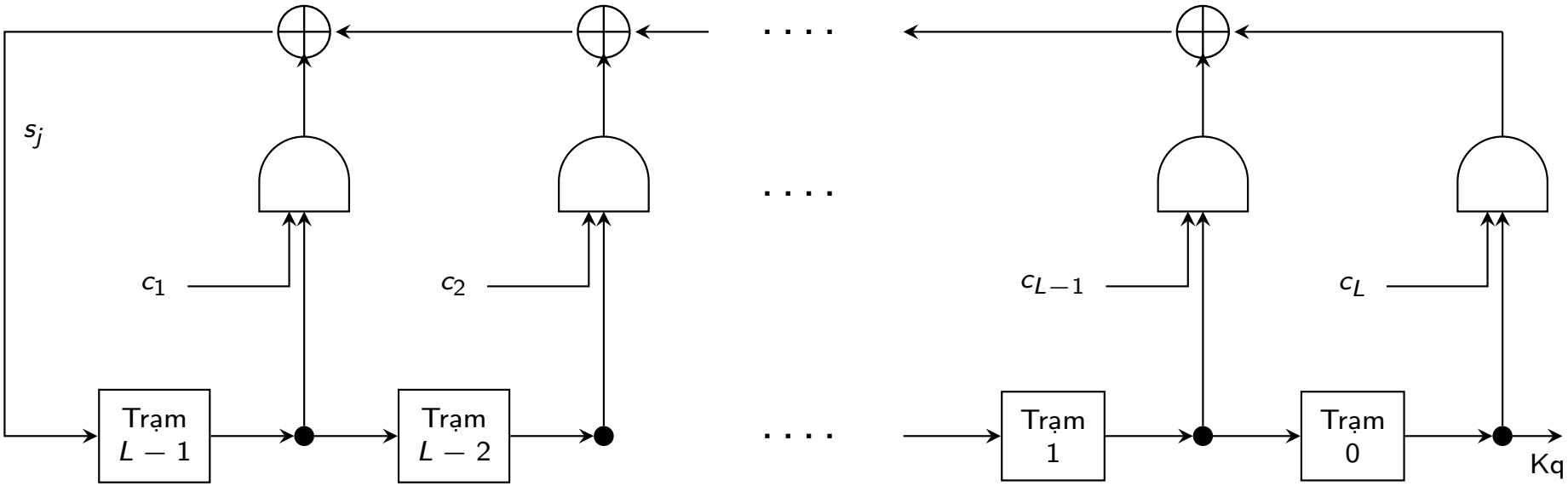
Một LFSR có độ dài L là hệ xử lý gồm có L trạm đánh số 0, 1, . . . , $L-1$, ở mỗi trạm đó có thể lưu trữ, nhận vào, cho ra kết quả là 1 bit và một đồng hồ kiểm soát bước chuyển dữ liệu. Trong đó mỗi đơn vị thời gian thực thi các nhiệm vụ sau:

i) *Kết quả ở trạm 0 là kết quả cho ra của hệ, đồng thời tham gia vào các tính trạng thái các trạm tiếp;*

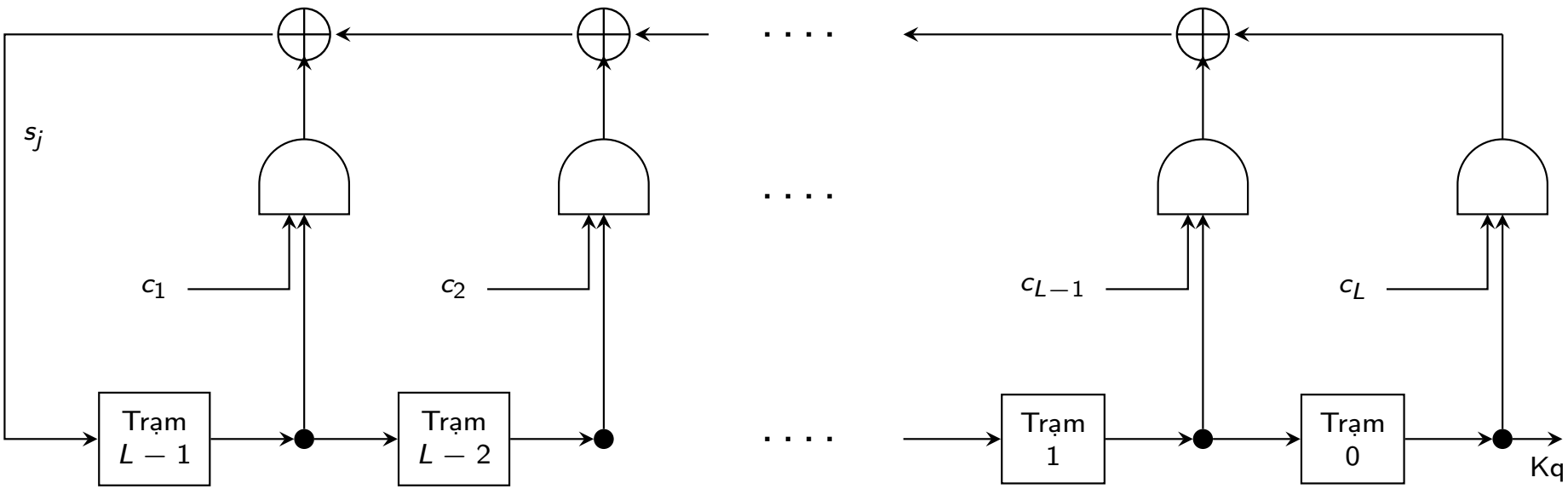
ii) *Kết quả của trạm i được chuyển tới trạm i-1,* $1 \leq i \leq L-1$;

iii) *Kết quả cho vào ở trạm* $L-1$ *là bit phản hồi* s_j *được tính bằng tổ hợp theo modulo 2 của một số kết quả trong các trạm trước.*

Sơ đồ của LFSR

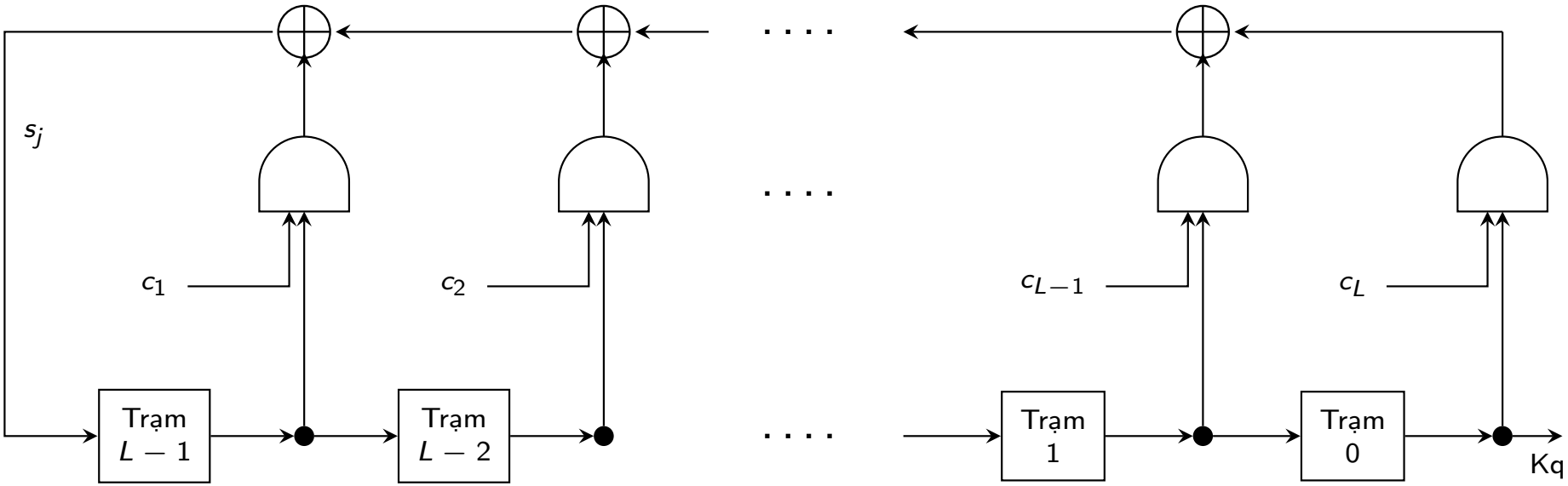


Sơ đồ của LFSR



- Với s_j kết quả thứ j thì:
  $s_j = (c_1 s_{j-1} + c_2 s_{j-2} + \ldots + c_L s_{j-L}) \bmod 2$, $j \geq L$, với $[s_{L-1}, s_{L-2}, \ldots, s_1, s_0]$ là các trạng thái ban đầu ở các trạm.

Sơ đồ của LFSR



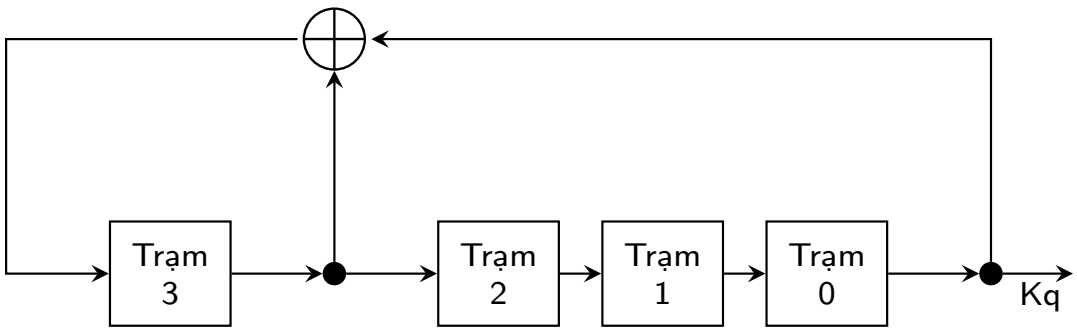
- Với s_j kết quả thứ j thì:
  $s_j = (c_1 s_{j-1} + c_2 s_{j-2} + \ldots + c_L s_{j-L}) \bmod 2$, $j \geq L$, với $[s_{L-1}, s_{L-2}, \ldots, s_1, s_0]$ là các trạng thái ban đầu ở các trạm.
- Ký hiệu LFSR trên là $\langle L, C(D) \rangle$, với $C(D) = 1 + c_1 D + c_2 D^2 + \ldots + c_L D^L \in \mathbb{Z}_2(D)$ là đa thức kết nối với các hệ số và phép toán nhị phân.

Tính chất của LFSR

- Với dãy trạng thái đầu vào thì LFSR sinh ra một chuỗi các bit $s = s_0, s_1, s_2, \ldots$

Tính chất của LFSR

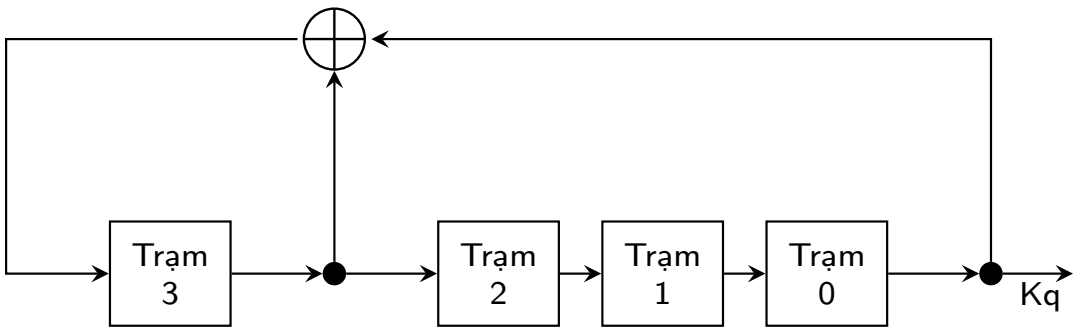
- Với dãy trạng thái đầu vào thì LFSR sinh ra một chuỗi các bit $s = s_0, s_1, s_2, \ldots$
- Ví dụ xét $\langle 4, 1 + D + D^4 \rangle$, có sơ đồ:



Với 4 trạng thái đầu vào in đậm thì được dãy bit là: **0,1,1,0**,0,1,0,0,0,1,1,1,1,...

Tính chất của LFSR

- Với dãy trạng thái đầu vào thì LFSR sinh ra một chuỗi các bit $s = s_0, s_1, s_2, \ldots$
- Ví dụ xét $\langle 4, 1 + D + D^4 \rangle$, có sơ đồ:

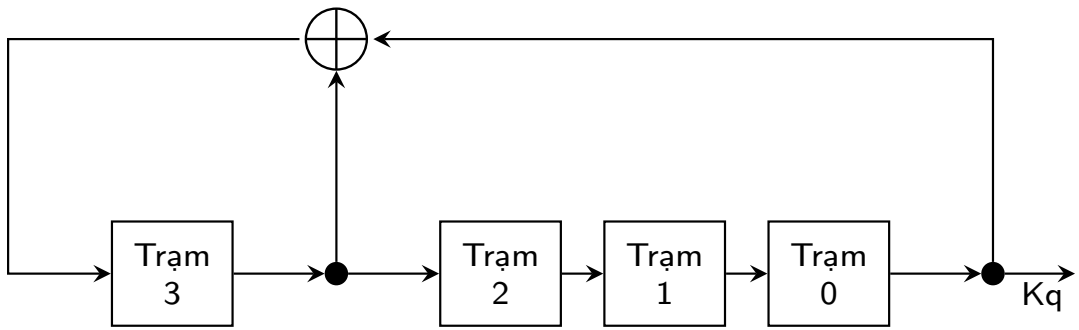


Với 4 trạng thái đầu vào in đậm thì được dãy bit là: **0,1,1,0**,0,1,0,0,0,1,1,1,1,...

- Dãy bit đầu ra của $\langle L, C(D) \rangle$ là tuần hoàn khi và chỉ khi bậc của $C(D)$ bằng L.

Tính chất của LFSR

- Với dãy trạng thái đầu vào thì LFSR sinh ra một chuỗi các bit $s = s_0, s_1, s_2, \ldots$
- Ví dụ xét $\langle 4, 1 + D + D^4 \rangle$, có sơ đồ:

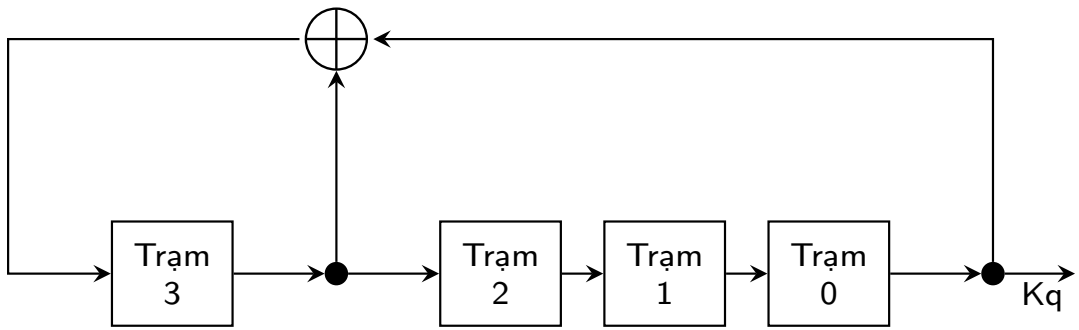


Với 4 trạng thái đầu vào in đậm thì được dãy bit là: **0,1,1,0**,0,1,0,0,0,1,1,1,1,...

- Dãy bit đầu ra của $\langle L, C(D) \rangle$ là tuần hoàn khi và chỉ khi bậc của $C(D)$ bằng L.
- Khi bậc của $C(D)$ nhỏ hơn L thì dãy bit đầu ra của $\langle L, C(D) \rangle$ cũng tuần hoàn nếu bỏ đi một số bit đầu tiên.

Tính chất của LFSR

- Với dãy trạng thái đầu vào thì LFSR sinh ra một chuỗi các bit $s = s_0, s_1, s_2, \ldots$
- Ví dụ xét $\langle 4, 1 + D + D^4 \rangle$, có sơ đồ:



Với 4 trạng thái đầu vào in đậm thì được dãy bit là: **0,1,1,0**,0,1,0,0,0,1,1,1,1,...

- Dãy bit đầu ra của $\langle L, C(D) \rangle$ là tuần hoàn khi và chỉ khi bậc của $C(D)$ bằng L.
- Khi bậc của $C(D)$ nhỏ hơn L thì dãy bit đầu ra của $\langle L, C(D) \rangle$ cũng tuần hoàn nếu bỏ đi một số bit đầu tiên.

Mã hóa dòng dựa vào LFSRs

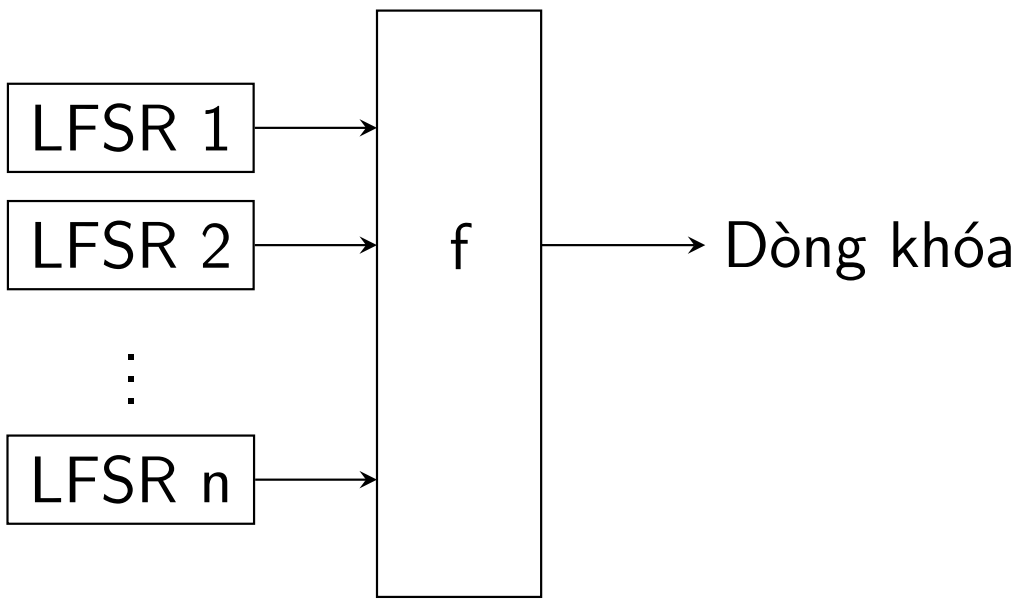
- LFSRs là các thành phần cơ bản trong bộ sinh dòng khóa

Mã hóa dòng dựa vào LFSRs

- LFSRs là các thành phần cơ bản trong bộ sinh dòng khóa
- LFSRs thích hợp cho cài đặt trong phần cứng

Mã hóa dòng dựa vào LFSRs

- LFSRs là các thành phần cơ bản trong bộ sinh dòng khóa
- LFSRs thích hợp cho cài đặt trong phần cứng
- Các LFSR thường được cài đặt và kết hợp phi tuyến với nhau để sinh ra dòng khóa theo mô hình:



Tài liệu tham khảo

Handbook of Applied Crytography, chapter 6

http://cacr.uwaterloo.ca/hac/