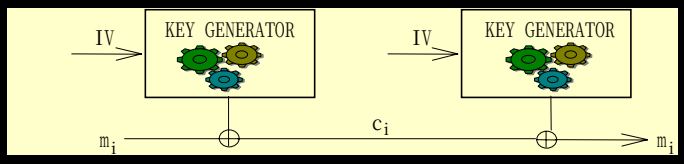
❑ 분류

Synchronous Stream Cipher

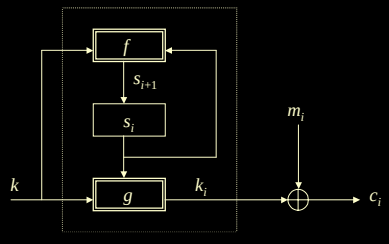
Self-Synchronous Stream Cipher

❑ Synchronous Stream Cipher



- Keystream Generator의 최초상태는 **IV**로 초기화 된다.
- No Error Propagation
- 송수신자간의 Perfect Synchronization 요구

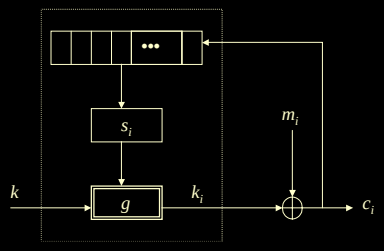
❑ Synchronous Stream Cipher



$s_{i+1} = f(k, s_i)$
$k_i = g(k, s_i)$
$c_i = m_i \oplus k_i$, $i = 0, 1, 2, \ldots$

키 수열 생성기가 맨 처음 기동이 되어 비밀키 k와 그 비밀키로부터 일정한 방식에 의해서 도출되어질 수 있는 초기 상태 s_0이 유입되면 함수 $g(\,)$를 적용하여 평문 m_0과 XOR되어질 키 수열 $k_0 = g(k, s_0)$을 생성한다. 동시에 함수 $f(\,)$가 적용되어 다음 상태 $s_1 = f(k, s_0)$이 생성되면서 키 수열 생성기의 암호화 상태는 다음 상태로 변하게 된다. 키 수열 k_0이 생성될 때 s_0은 현재 상태가 된다.

❑ Self-Synchronous Stream Cipher



$s_i = (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1})$
$k_i = g(k, s_i)$
$c_i = m_i \oplus k_i, i = 0, 1, 2, \ldots.$

키 수열의 생성에 있어서 비밀키 k와 상태 s_i가 사용된다는 측면에서는 동기식과 유사하지만 현재 상태를 생성하는 데에는 이전에 이미 생성된 t개의 암호문 비트나 문자가 이용된다는 점에 있어서 차이가 난다. 키 수열을 생성할 때의 상태 s_i는 이미 이전에 생성되었던 암호문 비트나 문자 $c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}$ 들이 된다. $c_{-t}, c_{-t+1}, \ldots, c_{-1}$은 키 수열 생성기가 처음 기동이 될 때 사용되는 초기 상태로서 공개될 수도 있고 또는 비밀키의 일부로 간주되어질 수도 있다.

❑ 키 수열의 안전성

키 수열의 주기(period)

유사-난수열

선형 복잡도

키 수열의 주기가 너무 짧다면 평문의 서로 다른 부분들이 동일한 방식으로 암호화될 것이며 결국 이것은 매우 심각한 취약점을 나타내게 된다. 즉, 관측된 암호문 일부에 해당하는 평문의 내용이 암호분석가에게 알려진다면 해당 키 수열의 일부가 노출되어질 수가 있게 되고 또한 암호분석가는 그 키 수열의 일부가 평문의 다른 부분을 암호화하는 데에 사용되어졌다는 사실을 이용하여 암호문의 다른 부분을 성공적으로 분석할 가능성은 높아지게 된다.

키 수열의 주기는 어느 정도가 되어야 안전할까? 이 질문은 많은 암호학자들 사이에서 논란의 대상이 되어왔지만 궁극적으로 스트림 암호가 적용되는 응용분야에 전적으로 의존한다고 할 수 있다. 예를 들어 **초당 1M 바이트**를 암호화할 수 있는 스트림 암호를 사용하는 경우에 주기가 2^{32}인 키 수열은 단지 **2^9초 ≈ 8.5분** 만에 반복되게 된다. 안전한 키 수열의 주기는 동일한 키 수열이 암호화에 두 번 이상 참여하지 않게끔 매우 길어야 한기 때문에 이것은 일반적으로 적절한 길이의 주기라고 할 수 없다. 2^{64}의 주기를 갖는 스트림 암호의 경우에는 동일 조건하에서 **2^{41}초 ≈ 69,730년** 만에 반복된다.

❑ 키 수열의 안전성

키 수열의 주기(period)

유사-난수열

선형 복잡도

첫째, 매 주기마다 발생되는 '1'의 개수와 '0'의 개수의 차이는 기껏해야 1이다. **둘째**, 매 주기마다 '00 ... 0' 또는 '11 ... 1'과 같이 연속적인 '1' 또는 '0'이 종종 나타나는 데 길이가 짧은 연속적인 값들이 길이가 긴 연속적인 값들보다 더 자주 나타난다. 좀 더 자세히 표현하면 연속적인 값들의 1/2이상은 길이가 1, 연속적인 값들의 1/4이상은 길이가 2, 연속적인 값들의 1/8이상은 길이가 3과 같이 나타난다. **셋째**, p를 수열의 주기라고 할 때 두 가지의 값을 가지는 다음과 같은 자기상관 함수(auto -correlation function) $C(t)$가 존재한다

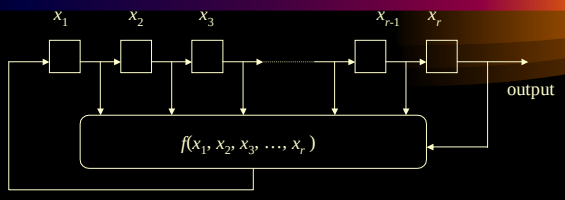
자기상관(auto -correlation) 함수의 개념은 2개의 동일한 수열이 존재하고 그 중 하나가 다른 수열과 t, $0 \le t \le p-1$만큼의 위치적인 차이가 있을 때 두 수열이 동일한 위치에 같은 값을 가지는 위치의 개수 A_t와 서로 상이한 값을 가지는 위치의 개수 D_t를 각각 계산하여 p로 나눈 $(A_t - D_t) / p$를 의미한다. *Golomb*의 공리계에서는 이 자기상관 함수의 값이 오직 2가지의 값만을 가진다.

[예] 주기가 $p = 15$인 다음의 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1
'1'이 개수는 8, '0'의 개수는 7이기 때문에 첫번째 조건을 만족한다. 위의 수열에는 다음과 같이 모두 8개의 연속적인 값들이 존재한다.

{ 0 }, { 1, 1 }, { 0, 0 }, { 1 }, { 0, 0, 0 }, { 1, 1, 1, 1 }, { 0 }, { 1 }

길이가 1인 것이 4개, 길이가 2인 것이 2개, 길이가 3인 것이 1개, 길이가 4인 것이 1개 존재하므로 두 번째 조건도 만족한다. 자기상관 함수 값은 $C(0) = 1$, $C(t) = K = -1/15$, $1 \le t \le 14$이기 때문에 두 가지의 값만을 가짐으로 역시 세 번째 조건을 만족한다.

❑ Linear Feedback Shift Register



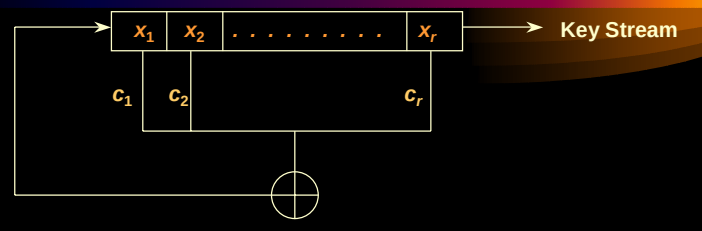
LFSR와 관련하여 연결 다항식(connection polynomial)이 정의되어 진다. 부울함수가 $f(x_1, x_2, x_3, \ldots, x_r) = c_1x_1 + c_2x_2 + c_3x_3 + \ldots + c_rx_r \bmod 2$인 경우에 해당 LFSR의 연결 다항식 $\delta(x)$는 아래와 같다. 앞으로의 논의에 있어서 $c_r = 1$인 LFSR만을 다루기로 한다.

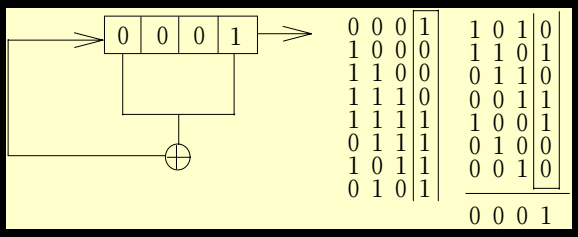
$$\delta(x) = 1 + c_1x + c_2x^2 + \cdots + c_rx^r$$

LFSR의 초기 상태(initial state)가 $[\, s_{r-1}, s_{r-2}, \ldots, s_1, s_0 \,]$이면 LFSR는 다음과 같은 선형 순환(linear recurrence)을 만족하는 수열 $s_0, s_1, s_2, \ldots$을 생성하게 된다.

$$s_i = c_1s_{i-1} + c_2s_{i-2} + \cdots + c_rs_{i-r} \bmod 2, \quad i \ge r$$

❑ Linear Feedback Shift Register





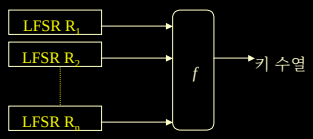
❑ Connection Polynomial

LFSR가 생성하는 수열의 주기는 연결 다항식의 유형과 밀접한 관계를 가지고 있다. 즉, 연결 다항식 $\delta(x)$가 차수(degree)가 r인 **원시 다항식(primitive polynomial)**이면 r개의 플립플롭으로 구성된 해당 LFSR는 최대 주기의 수열을 생성한다. 이에 대한 증명은 본 논의의 범위를 벗어나기 때문에 여기서는 생략하기로 한다. 차수가 r이고 계수(coefficient)가 2진수인 다항식 $\delta(x)$를 더 이상 인수분해가 되지 않는 **기약 다항식(irreducible polynomial)**이라고 할 때, 다항식 $x^{2^r-1}+1$이 $\delta(x)$에 의해서 나누어질 수 있는 가장 낮은 차수의 다항식이라면 즉, 2^r-1보다 작은 어떠한 k에 대해서도 $\delta(x)$가 x^k+1을 나눌 수 없다면 $\delta(x)$는 원시 다항식으로 정의된다.

[예] 차수가 $r = 4$인 2진 다항식 $f(x) = 1 + x + x^4$와 $g(x) = 1 + x + x^2 + x^3 + x^4$는 기약 다항식이다. 다항식 $f(x)$와 $g(x)$는 다항식 $x^{2^r-1} + 1 = x^{15} + 1$을 나누지만 $g(x)$는 다항식 $(x^5 + 1) = (1 + x)(1 + x + x^2 + x^3 + x^4)$도 나누기 때문에 $f(x)$만 원시 다항식이 된다.

❑ LFSR 기반의 스트림 암호

❑ 비선형 결합 생성기



LFSR이 지니는 **선형성**을 없애기 위한 가장 직접적인 방법은 그림에 나타나 있는 것처럼 여러 개의 LFSR를 병렬로 연결하여 각각의 LFSR에서 생성되는 키 수열에 **비선형 결합 함수(nonlinear combining function) *f***를 적용하는 것인데 이러한 유형의 키 수열 생성기를 **비선형 결합 생성기**(combining generator)라고 한다.

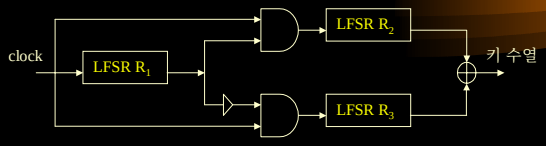
❑ Clock-controlled 생성기

Alternating Step Generator

Shrinking Generator

LFSR기반의 스트림 암호에 의해서 생성되는 키 수열에 비선형성을 내재 시키기 위한 또 하나의 시도는 **LFSR에 불규칙적인 클럭 신호**를 가하는 것이다. 일반적으로 LFSR에는 규칙적인 클럭 신호가 가해져서 LFSR의 플립플롭의 내용은 정기적으로 갱신되어진다. 하지만, 한 LFSR의 클럭 작동이 다른 LFSR에 의해서 제어된다면 보다 복잡한 수열이 생성될 수가 있을 것이다.

❑ Alternating Step Generator



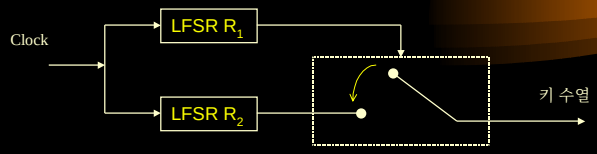
[예] LFSR R_1, R_2, R_3의 연결 다항식이 각각 $\delta_1(x) = 1 + x^2 + x^3$, $\delta_2(x) = 1 + x^3 + x^4$, $\delta_3(x) = 1 + x + x^3 + x^4 + x^5$이고 초기 상태가 각각 **[0, 0, 1], [1, 0, 1, 1], [0, 1, 0, 0, 1]** 이면 LFSR R_1, R_2, R_3의 출력은 다음과 같이 각각 주기가 7, 15, 31의 수열이 된다.

R_1 : 1 0 0 1 0 1 1
R_2 : 1 1 0 1 0 1 1 1 1 0 0 0 1 0 0
R_3 : 1 0 0 1 0 1 0 1 1 0 0 0 0 0 1 1 1 0 0 1 1 0 1 0 1 1 1 1 1 0 1 0 0 0

이때, 교체 단계 생성기에 의해서 생성되는 키 수열은 다음과 같다.

1 0 1 1 1 0 1 0 1 0 1 0 0 0 0 1 0 1 1 1 1 0 1 1 0 0 0 0 1 1 1 0 ...

❑ Shrinking Generator



[예] LFSR R_1, R_2의 연결 다항식이 각각 $\delta_1(x) = 1 + x + x^3$, $\delta_2(x) = 1 + x^3 + x^5$이고 초기 상태가 각각 **[1, 0, 0], [0, 0, 1, 0, 1]**이면 LFSR R_1, R_2의 출력은 다음과 같이 각각 주기가 7, 31의 수열이 된다.

R_1 : 0 0 1 1 1 0 1
R_2 : 1 0 1 0 0 0 0 1 0 0 1 0 1 1 0 0 1 1 1 1 1 0 0 0 1 1 0 1 1 1 0

이때, 수축 생성기에 의해서 생성되는 키 수열은 다음과 같다.

1 0 0 0 0 1 0 1 1 1 1 1 0 1 1 1 0 ....