情報保護學會論文誌
第12券 第3號, 2002. 6

두개의 특성 다항식으로 구성된 이진 난수열 발생기에 관한 연구

김 대 엽*, 주 학 수**, 임 종 인***

A Study on a Binary Random Sequence Generator with Two Characteristic Polynomials

Dae-Youb Kim*, Hak-Soo Ju***, Jong-In Lim***

요 약

선형 쉬프트 레지스터를 이용한 이진 난수 발생기의 연구는 1970년대부터 연구되어져 왔으며, 이러한 이진 난수열 발생기는 스트림 암호 기법에 이용되어졌다. 일반적으로, 이진 난수열 발생기는 최대 주기의 선형 쉬프트 레지스터와 선형 복잡도가 높은 난수를 발생시키기 위하여 비선형 여과함수 또는 비선형 결합함수로 구성된다. 그러므로, 높은 선형 복잡도 뿐만 아니라, 긴 주기를 갖는 이진 난수열의 생성은 스트림 암호 기법의 안전성을 평가하는데 중요한 요소가 된다. 일반적으로 L개의 레지스터와 1개의 궤환 함수 또는 특성 다항식으로 구성된 선형 쉬프트 레지스터의 최대 주기는 2^L-1을 넘을 수 없다. 본 논문에서는 L개의 레지스터와 2개의 부분 특성 다항식으로 구성된 새로운 이진 난수열 발생기를 제안한다. 제안된 이진 난수열 발생기는 초기 상태 값에 따라 기존의 선형 쉬프트 레지스터에서 생성한 수열의 주기와 같거나 긴 주기를 갖는 이진 난수열을 생성하며, 생성 수열의 선형복잡도 역시 증가된다.

ABSTRACT

A Research of binary random sequence generator that uses a linear shift register had been studied since the 1970s. These generators were used in stream cipher. In general, the binary random sequence generator consists of linear shift registers that generate sequences of maximum period and a nonlinear filter function or a nonlinear combination function to generate a sequence of high linear complexity. Therefore, To generate a sequence that have long period as well as high linear complexity becomes an important factor to estimate safety of stream cipher. Usually, the maximum period of the sequence generated by a linear feedback shift register with L registers is less than or equal to 2^L-1. In this paper, we propose new binary random sequence generator that consist of L registers and 2 sub-characteristic polynomials. According to an initial state vector, the least period of the sequence generated by the proposed generator is equal to or long than it of the sequence created by the general linear feedback shift register, and its linear complexity is increased too.

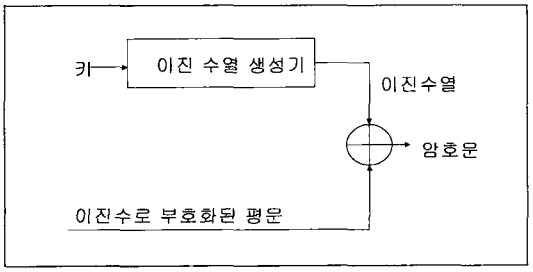
Keyword : *Random Number, LFSR, 최소주기, 선형복잡도*

* 시큐아이닷컴(주), 정보보호연구소(david_kdy@hanmail.net)
** 한국정보보호진흥원(hsju@kisa.or.kr)
*** 고려대학교 정보보호 대학원(jilim@tiger.korea.ac.kr)

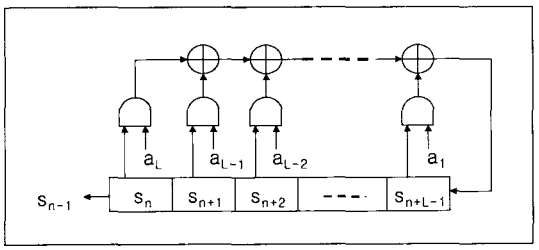
Ⅰ. 서 론

1970년대 초부터 유럽을 중심으로 연구 발전된 선형 쉬프트 레지스터(Linear Feedback Shift Register, LFSR)는 이진 난수열 발생기를 사용한 스트림(stream) 암호 시스템에 활용되어 왔다. 일반적으로, 스트림 암호 시스템은 〔그림 1〕에서와 같이 이진 수열과 부호화된 평문을 이진 난수열 발생기에서 생성된 수열과 비트 XOR하여 암호문을 생성한다. 그러므로, 스트림 암호 시스템에서 사용되는 이진 난수열 발생기는 긴 주기를 갖는 수열을 발생해야 하며, 이를 보장할 수 있어야 한다. 선형 쉬프트 레지스터는 최소 주기(least period), 선형 복잡도(linear complexity) 등과 같은 수학적으로 분석 가능한 수치에 대하여 이론적인 값을 정확하게 계산할 수 있다는 장점이 있다. 긴 주기와 높은 선형 복잡도를 갖는 이진 수열을 생성하기 위하여, 최대 주기를 갖는 선형 쉬프트 레지스터의 출력 수열들을 비선형 결합 함수(non-linear combination function)에 입력시켜 그 결과 값을 사용하거나, 비선형 필터 함수(non-linear filter function)를 사용하여 선형 복잡도를 높이는 방법이 일반적으로 연구되어졌다.[3,4,5,6,8]

선형 쉬프트 레지스터를 이용한 이진 수열 발생기의 경우 〔그림 2〕에서와 같이 L개의 레지스터와 1개의 궤환 함수(feedback function)



〔그림 1〕 스트림 암호



〔그림 2〕 선형 쉬프트 레지스터

$$f(s_n, s_{n+1}, \cdots, s_{n+L-1}) = a_L s_n + a_{L-1} s_{n+1} + \cdots + a_1 s_{n+L-1} \quad (1)$$

로 구성된다. $a_1, \cdots, a_{L-1}$은 0과 1값을 취하며, a_L은 항상 1값을 취한다. a_i는 i번째 레지스터의 연결 상태를 나타내는데, 이를 궤환 상수(feedback constant)라고 정의한다. 또한 $a_1, \cdots, a_L$을 궤환 상수로 갖는 L개의 레지스터로 구성된 선형 쉬프트 레지스터의 특성 다항식(characteristic polynomial)을 다음과 같이 정의한다:

$$c(x) = \sum_{n=0}^{L} a_n x^n, \quad a_i \in \{0,1\}, a_0 = 1 \quad (2)$$

이진 수열 $\tilde{s}$를 L개의 레지스터로 구성된 선형 쉬프트 레지스터의 출력 수열이라 할 때, 수열 $\tilde{s}$의 $t-1$번째 항을 s_{t-1}로 표시한다. 또한, 시각 t에서 각 레지스터의 값 $s_t, s_{t+1}, \cdots, s_{t+L-1}$을 레지스터의 상태 벡터(state vector)로 정의하고, $(s_t, s_{t+1}, \cdots, s_{t+L-1})$로 나타낸다. 특히, $(s_0, s_1, \cdots, s_{L-1})$을 선형 쉬프트 레지스터의 초기 상태 벡터 또는 초기 값이라 부르며, 선형 쉬프트 레지스터를 운영하기 위해 각 레지스터에 설정된 초기 값을 의미한다. $(s_0, s_1, \cdots, s_{L-1})$을 초기 상태 벡터로 갖는 선형 쉬프트 레지스터에서 생성된 이진 수열 $\tilde{s}$은 다음과 같다:

$$s_0, s_1, s_2, \cdots, s_{L-1}, s_n = \sum_{i=1}^{L} a_i s_{n-i},$$
모든 $n \geq L$에 대하여 (3)

특히, $s_n = \sum_{i=1}^{L} a_i s_{n-i}$을 L차 선형 순환 관계($L-th$ order linear recurrence relation)라 정의하고, 모든 덧셈 연산의 결과는 법(modulus) 2 아래에서의 결과로 간주한다. 위의 수식에서 알 수 있듯이, 출력 수열 $\tilde{s}$의 t번째 항 s_t의 생성에 영향을 주는 것은 레지스터의 상태 벡터 $(s_{t-L}, s_{t+1}, \cdots, s_{t-1})$ 뿐이고, 0이 아닌 상태 벡터의 가지 수가 2^L-1개이므로, 출력 수열 $\tilde{s}$의 최소 주기는 2^L-1을 넘을 수 없다.

본 논문에서는, L개의 레지스터와 2개의 서로 다른 부분 특성 다항식(sub-characteristic polynomial)으로 구성된 새로운 이진 난수열 발생기를 제안한다. 제안하는 발생기는 0이 아닌 초기 상태 벡터에서

주기 2^L-1 또는 $2(2^L-1)$을 갖는 이진 난수열을 발생한다. 그러므로, 일반 선형 쉬프트 레지스터를 사용해 생성한 수열의 주기보다 긴 수열을 생성할 수 있다. 일반적인 선형 쉬프트 레지스터와 제안하는 이진 수열을 구분하기 위하여, 이후로 $L-LFSR$ (Linear Feedback Shift Register with L Registers)은 L개의 레지스터로 구성된 최대 주기를 보장하는 기존의 선형 쉬프트 레지스터를 의미하고, $L-BRG$(Binary Random Sequence Generator with L Registers)는 본 논문에서 제안하는 L개의 레지스터로 구성 된 이진 수열 발생기를 의미한다.

본 논문은 다음과 같이 구성된다. 2.1절은 최소 주기를 계산하기 위한 기본 이론을 소개한다. 2.2절에서 우리는 새로운 이진 난수열 발생기 $L-BRG$를 제안하고, 그 성질에 대하여 논한다. 2.3절에서는 실제 $L-BRG$를 구성하는 방법을 제시한다.

Ⅱ. 이진 난수열 발생기

2.1 기본 이론

이 절에서는 선형 쉬프트 레지스터로 구성된 이진 난수열 발생기의 출력 수열 성질을 파악하기 위한 기본적인 정의와 이론을 소개한다. 우리는 선형 쉬프트 레지스터의 이와 같은 성질을 이용하여 제안하는 이진 난수열 발생기 $L-BRG$의 최소 주기를 계산할 수 있다.

[정의 1]

다항식 $f(x)$를 $GF(2)[x]$에 속하는 0이 아닌 다항식이라 하자. $f(0)\neq 0$이라 가정하면, $f(x)|x^e-1$을 만족하는 가장 작은 양의 정수 e를 다항식 $f(x)$의 위수(order)라 정의한다.

[정의 2]

순환 그룹 $GF(2^m)^*$의 생성원소(generator) α를 $GF(2^m)^*$의 원시 원소(primitive element)라 정의한다.

[정의 3]

$GF(2)[x]$에 속하는 다항식 $f(x)$를 $GF(2)$ 상의 m차 기약 다항식(irreducible polynomial)이라 하자. 만약 $f(x)$의 위수가 2^m-1이면, $f(x)$를 원시 다항식(primitive polynomial)이라 정의한다.

$\tilde{s}$를 $L-LFSR$의 출력 수열이라 하자. 일반적으로, $L-LFSR$에 의해서 구현된 L차 선형 순환 관계 (L-th order linear recurrence relation)가 $\tilde{s}$을 생성하는 최소 차의 선형 순환 관계일 필요는 없다. 선형 순환 수열 $\tilde{s}$는 하나의 최소 다항식(minimum polynomial) $m_{\tilde{s}}(x)\in GF(2)[x]$와 대응되며, 이 최소 다항식 $m_{\tilde{s}}(x)$는 $\tilde{s}$를 생성하는 최소 차의 선형 순환 관계의 특성 다항식을 의미한다. 주어진 선형 순환 수열 $\tilde{s}$에 대하여 최소 다항식은 유일하게 존재하며, $\tilde{s}$의 모든 특성 다항식은 $m_{\tilde{s}}(x)$를 약수로 갖는다. 이 최소 다항식은 Berlekamp-Massay LFSR Synthesis Algorithm을 사용해서 쉽게 찾을 수 있다.[1,2,3]

[정리 4][1]

0이 아닌 초기 상태를 갖는 선형 쉬프트 레지스터의 출력 수열을 $\tilde{s}$라 하자. 특성 다항식 $c(x)$가 $GF(2)$ 상에서 기약 다항식이라 가정하면, $\tilde{s}$의 최소 주기는 $c(x)$의 위수와 같다.

그러므로, $L-LFSR$을 구성하는 특성 다항식이 원시 다항식이면, 0이 아닌 초기 상태 벡터에 의해서 생성된 이진 수열 $\tilde{s}$의 최소 주기는 2^L-1이 된다. 또한 이 주기는 L개의 레지스터로 구성된 선형 쉬프트 레지스터가 생성할 수 있는 최대 주기가 된다. 이와 같이 최대 주기를 갖는 수열을 최대 길이 수열(maximal length sequence)이라 부르고, 이 수열을 생성하는 선형 쉬프트 레지스터를 최대 길이 선형 쉬프트 레지스터(maximal length LFSR)라 부른다.

2.2 이진 난수열 발생기

이 절에서 우리는 L개의 레지스터로 구성된 새로운 이진 난수열 발생기 $L-BRG$를 제안한다. 제안하는 $L-BRG$는 L개의 레지스터와 $GF(2)$ 위에서 정의된 2개의 다항식

$$f(x)=a_Lx^L+a_{L-1}x^{L-1}+\cdots+a_1x+a_0$$
$$g(x)=b_Lx^L+b_{L-1}x^{L-1}+\cdots+b_1x+b_0 \qquad (4)$$

로 구성되며, 다항식 $f(x)$와 $g(x)$는 다음과 같은 조건을 만족한다.

(조건 1) 두 다항식의 계수 a_0, a_L, b_0, b_L은 모두 0이 아닌 $GF(2)$의 원소들이다.
(조건 2) 두 다항식 $f(x)$와 $g(x)$의 곱을

$$f(x)g(x)=c_{2L}x^{2L}+\cdots+c_1x+c_0 \tag{5}$$

라 할 때, 짝수 차 항의 합으로 구성된 다항식

$$c(x)=c_{2L}x^{2L}+c_{2L-2}x^{2L-2}+\cdots+c_2x^2+c_0 \tag{6}$$

는 L차 기약 다항식의 제곱 형태로 표현된다.

우리는 (조건 2)에서 정의한 다항식 $c(x)$를 $L-BRG$의 특성 다항식이라 정의하고, $f(x)$와 $g(x)$를 부분 특성 다항식(sub-characteristic polynomial)이라 부른다. 위에서 정의된 $L-BRG$의 초기 상태 벡터를 $(s_0, s_1, \cdots, s_{L-1})$라 하고, 이진 난수열 $\tilde{s}=s_0, s_1, \cdots$을 $L-BRG$가 생성한 수열이라 하면, L 보다 크거나 같은 모든 n에 대하여, s_n을 다음과 같은 규칙에 따라 생성한다: $n-L$이 0 또는 짝수일 때

$$s_n=a_Ls_{n-L}+a_{L-1}s_{n-(L-1)}+\cdots+a_1s_{n-1} \tag{7}$$

이고, $n-L$이 홀수일 때

$$s_n=b_Ls_{n-L}+b_{L-1}s_{n-(L-1)}+\cdots+b_1s_{n-1} \tag{8}$$

이다.

[정리 5]

수열 $\tilde{s}$를 L차 부분 특성 다항식 $f(x)=\sum_{i=0}^{L}a_ix^i$와 $g(x)=\sum_{j=0}^{L}b_jx^j$로 구성된 $L-BRG$에서 생성된 이진 수열이라 하고, $c(x)=\sum_{i=0}c_{2i}x^{2i}$, $c_n=\sum_{\substack{i+j=n\\0\le i,\ j\le L}}a_ib_j$를 $L-BRG$의 특성 다항식이라 하자. 또한, 수열 $\tilde{s}'$를 $2L$개의 레지스터와 특성 다항식 $c(x)$로 구성된 선형 쉬프트 레지스터 $2L-LFSR$에서 생성된 이진 수열이라 하자. 수열 $\tilde{s}'$를 생성하기 위해 사용된 $2L-LFSR$의 초기 상태 벡터 $(s'_0, s'_1, \cdots, s'_{2L-1})$가 수열 $\tilde{s}$의 초기 $2L$개의 항 $\{s_0, s_1, \cdots, s_{2L-1}\}$과 같다면, 두 수열 $\tilde{s}$와 $\tilde{s}'$는 같다.

(증명)

이진 수열 $\tilde{s}$의 연속된 $2L$개의 항 $(s_0, s_1, \cdots, s_{2L-1})$을 $c(x)$를 특성 다항식으로 갖는 선형 쉬프트 레지스터 $2L-LFSR$의 초기 상태 값이라 하자. 증명을 위하여 수학적 귀납법을 사용한다. $n\ge 2L$을 만족하는 모든 정수 n에 대하여 $2L-LFSR$이 생성한 이진 수열 $\{s'_0, s'_1, \cdots, s'_{n-1}\}$과 $L-BRG$이 생성한 이진 수열 $\{s_0, s_1, \cdots, s_{n-1}\}$이 같다고 가정하자. 이제, $2L-LFSR$의 s'_n과 $L-BRG$의 s_n이 같음을 증명하자. 먼저, $n-L$이 짝수인 경우를 고려하면, 식 (7)에 의하여 s_n은 다음과 같이 표현된다:

$$\begin{aligned}s_n&=a_Ls_{n-L}+a_{L-1}s_{n-(L-1)}+\cdots+a_1s_{n-1}\\&=\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}a_{2i}s_{n-2i}+\sum_{i=1}^{\lceil\frac{L}{2}\rceil}a_{2i-1}s_{n-(2i-1)}\end{aligned} \tag{9}$$

가정에 의하여 $n-L$이 짝수이므로 $(n-2i)-L$은 짝수이고, $(n-(2i-1))-L$은 홀수이다. 그러므로 식 (9)는 다음과 같이 다시 표현될 수 있다:

$$\begin{aligned}s_n&=\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}a_{2i}\sum_{j=1}^{L}a_js_{n-2i-j}\\&\quad+\sum_{i=1}^{\lceil\frac{L}{2}\rceil}a_{2i-1}\sum_{j=1}^{L}b_js_{n-(2i-1)-j}\\&=\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}\sum_{j=1}^{L}a_{2i}a_js_{n-2i-j}\\&\quad+\sum_{i=1}^{\lceil\frac{L}{2}\rceil}\sum_{j=1}^{L}a_{2i-1}b_js_{n-(2i-1)-j}\end{aligned} \tag{10}$$

위에서 a_{2i}은 $GF(2)$ 상에서 $b_{2i}+(a_{2i}+b_{2i})$과 같으므로

$$\begin{aligned}s_n&=\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}\sum_{j=1}^{L}b_{2i}a_js_{n-2i-j}\\&\quad+\sum_{i=1}^{\lceil\frac{L}{2}\rceil}\sum_{j=1}^{L}a_{2i-1}b_js_{n-(2i-1)-j}\\&\quad+\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}\sum_{j=1}^{L}(a_{2i}+b_{2i})a_js_{n-2i-j}\\&=\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}\sum_{j=1}^{L}b_{2i}a_js_{n-2i-j}\\&\quad+\sum_{i=1}^{\lceil\frac{L}{2}\rceil}\sum_{j=1}^{L}a_{2i-1}b_js_{n-(2i-1)-j}\\&\quad+\sum_{i=1}^{\lfloor\frac{L}{2}\rfloor}(a_{2i}+b_{2i})\sum_{j=1}^{L}a_js_{n-2i-j}\end{aligned} \tag{11}$$

이 된다. 가정에 의하여 $n-L$이 짝수이므로, $(n-2i)-L$도 짝수이다. 그러므로, s_{n-2i}은 $\sum_{j=1}^{L} a_j s_{n-2i-j}$과 같다. 또한, $L-BRG$의 정의에 의해서, a_0와 b_0는 $GF(2)$의 0이 아닌 원소이므로, s_n는 다음과 같이 쓸 수 있다:

$$\begin{aligned} s_n &= \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} \sum_{j=1}^{L} b_{2i} a_j s_{n-2i-j} \\ &\quad + \sum_{i=1}^{\lceil \frac{L}{2} \rceil} \sum_{j=1}^{L} a_{2i-1} b_j s_{n-(2i-1)-j} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} + b_{2i}) s_{n-2i} \\ &= \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} \sum_{j=1}^{L} b_{2i} a_j s_{n-2i-j} \\ &\quad + \sum_{i=1}^{\lceil \frac{L}{2} \rceil} \sum_{j=1}^{L} a_{2i-1} b_j s_{n-(2i-1)-j} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} b_0 + a_0 b_{2i}) s_{n-2i} \end{aligned} \tag{12}$$

이제 식 (12)에서 s_{n-m}의 계수를 고려하자. 각 부분합의 표현에서 s_{n-m}의 계수를 $a_r b_t$라고 할 때, $r+t=m$임을 쉽게 알 수 있다. m이 홀수인 경우를 먼저 고려하자. 식 (12)에서 r이 짝수이고, t가 홀수인 $a_r b_t$를 발견할 수 없다. 그러므로 r이 홀수이고, t가 짝수인 경우만을 고려하면 된다. 이제 식 (12)에서 r과 t가 각각 홀수와 짝수인 계수 $a_r b_t$를 찾아보면 앞의 두 합 $\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} \sum_{j=1}^{L} b_{2i} a_j s_{n-2i-j}$과 $\sum_{i=1}^{\lceil \frac{L}{2} \rceil} \sum_{j=1}^{L} a_{2i-1} b_j s_{n-(2i-1)-j}$에서 각각 한번씩 발견된다. 그러나 마지막 합 $\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} b_0 + a_0 b_{2i}) s_{n-2i}$에서는 발견할 수 없다. 그러므로 m이 홀수일 경우 s_{n-m}의 계수는 $GF(2)$ 상에서 0이 된다. 즉, 식 (12)에서 m이 짝수인 s_{n-m}만 존재한다. 이제, 위의 식은 다음과 같이 쓸 수 있다:

$$\begin{aligned} s_n &= \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} \sum_{j=1}^{\lfloor \frac{L}{2} \rfloor} b_{2i} a_{2j} s_{n-2i-2j} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} \sum_{j=1}^{\lceil \frac{L}{2} \rceil} a_{2i-1} b_{2j-1} s_{n-(2i-1)-(2j-1)} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} b_0 + a_0 b_{2i}) s_{n-2i} \\ &= \sum_{m=1}^{L} \Big(\sum_{i+j=2m, 0 \le i,\ j \le L} a_i b_j \Big) s_{n-2m} \\ &= \sum_{m=1}^{L} c_{2m} s_{n-2m} = s'_n \end{aligned} \tag{13}$$

그러므로, $n-L$이 짝수인 경우 s_n과 s'_n은 같다. $n-L$이 홀수인 경우도 유사한 방법으로 증명할 수 있다. $n-L$이 홀수라고 가정하면, $L-BRG$의 n번째 항 s_n은 식 (8)에 의하여 다음과 같이 표현된다:

$$\begin{aligned} s_n &= b_L s_{n-L} + b_{L-1} s_{n-(L-1)} + \cdots + b_1 s_{n-1} \\ &= \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} b_{2i} s_{n-2i} + \sum_{i=1}^{\lceil \frac{L}{2} \rceil} b_{2i-1} s_{n-(2i-1)} \end{aligned} \tag{14}$$

가정에 의하여, $n-L$이 홀수이므로 $(n-2i)-L$은 홀수이고, $(n-(2i-1))-L$은 짝수이다. 또한, b_{2i}는 $GF(2)$ 상에서 $a_{2i}+(b_{2i}+a_{2i})$와 같다. 그러므로 식 (15)는 다음과 같이 표현된다.

$$\begin{aligned} s_n &= \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} + (b_{2i} + a_{2i})) \sum_{j=1}^{L} b_j s_{n-2i-j} \\ &\quad + \sum_{i=1}^{\lceil \frac{L}{2} \rceil} b_{2i-1} \sum_{j=1}^{L} a_j s_{n-(2i-1)-j} \\ &= \sum_{j=1}^{L} \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} a_{2i} b_j s_{n-2i-j} \\ &\quad + \sum_{j=1}^{L} \sum_{i=1}^{\lceil \frac{L}{2} \rceil} b_{2i-1} a_j s_{n-(2i-1)-j} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} + b_{2i}) \sum_{j=1}^{L} b_j s_{n-2i-j} \end{aligned} \tag{15}$$

또한 $(n-2i)-L$의 값이 홀수이므로, $s_{n-2i} = \sum_{j=1}^{L} b_j s_{n-2i-j}$이 성립한다. 이를 이용하여, s_n은 다음과 같이 쓸 수 있다.

$$\begin{aligned} s_n &= \sum_{j=1}^{L} \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} a_{2i} b_j s_{n-2i-j} \\ &\quad + \sum_{j=1}^{L} \sum_{i=1}^{\lceil \frac{L}{2} \rceil} b_{2i-1} a_j s_{n-(2i-1)-j} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} + b_{2i}) s_{n-2i} \\ &= \sum_{j=1}^{L} \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} a_{2i} b_j s_{n-2i-j} \\ &\quad + \sum_{j=1}^{L} \sum_{i=1}^{\lceil \frac{L}{2} \rceil} b_{2i-1} a_j s_{n-(2i-1)-j} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} (a_{2i} b_0 + a_0 b_{2i}) s_{n-2i} \end{aligned} \tag{16}$$

$n-L$이 짝수인 경우와 같이, $n-L$이 홀수인 경

우도 s_{n-m}의 계수 $a_r b_t$는 $r+t=m$을 만족한다. m이 홀수인 경우를 먼저 고려하자. 이 경우, r과 t 중에서 하나는 짝수이고, 다른 하나는 홀수이다. 위의 식에서 s_{n-m}의 계수 $a_r b_t$를 관찰하면, 첫 번째 합 $\sum_{j=1}^{L}\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} a_{2i}b_j s_{n-2i-j}$에서 a_r의 색인 r은 항상 짝수이다. 그러므로 첫 번째 합에서 b_t의 색인 t는 항상 홀수이어야 한다. 그런데, b_t의 색인 t가 홀수인 항은 두 번째 합 $\sum_{j=1}^{L}\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} b_{2i-1}a_j s_{n-(2i-1)-j}$에서도 발견할 수 있다. 즉 m이 홀수인 경우, s_{n-m}의 계수 $a_r b_t$는 각 첨자 r과 t에 따라서 두 번씩 발견되거나, 아니면 발견되지 않는다. 그러므로, 식 (16)에서 m이 홀수인 s_{n-m}의 계수는 0이 된다. 따라서, 위의 식은 다음과 같이 바꿀 수 있다:

$$\begin{aligned} s_n &= \sum_{j=1}^{\lfloor \frac{L}{2} \rfloor}\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} a_{2i}b_{2j}s_{n-(2i+2j)} \\ &\quad + \sum_{j=1}^{\lfloor \frac{L}{2} \rfloor}\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} b_{2i-1}a_{2j-1}s_{n-(2i+2j-2)} \\ &\quad + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor}(a_{2i}b_0 + a_0 b_{2i})s_{n-2i} \\ &= \sum_{m=1}^{L}\Big(\sum_{\substack{i+j=2m \\ 0\le i,\ j\le L}} a_i b_j\Big)s_{n-2m} \\ &= \sum_{m=1}^{L} c_{2m}s_{n-2m} \end{aligned} \tag{17}$$

그러므로, $n-L$이 홀수인 경우, s_n과 s'_n은 같다. 즉, 특성 다항식 $c(x)$인 $2L-LFSR$가 $L-BRG$의 초기 $2L$개 항을 초기 상태 벡터로 취하여 생성한 수열 $\tilde{s}'$은 $\tilde{s}$과 같다. ■

위 정리 5에 의하여, $L-BRG$의 출력 수열 $\tilde{s}$는 일반 선형 쉬프트 레지스터의 출력 수열을 분석하는 방법으로 분석됨을 알 수 있다. 이제 $L-BRG$의 출력 수열 $\tilde{s}$의 최소 주기를 살펴보자.

[보조정리 6]

$h(x)$를 $GF(2)$ 상에서 정의된 위수가 e인 L차 기약 다항식이라 하자. $c(x)=h(x)^2$이라 가정하고, $S(c(x))$를 $c(x)$를 특성 다항식으로 갖는 선형 쉬프트 레지스터에서 생성한 모든 수열의 집합이라 하면, $S(c(x))$는 다음과 같은 수열들로 구성된다: 최소 주기가 1인 수열 1개, 최소 주기가 e인 수열 2^L-1개, 그리고 최소 주기가 $2e$인 수열 $2^{2L}-2^L$개.

(증명)

[1]의 정리 6.63에 의하여 명백하다. ■

[정리 7]

$c(x)=h(x)^2$을 특성 다항식으로 갖는 $L-BRG$에서 0이 아닌 초기 상태 벡터에 의해 생성된 이진 난수열을 $\tilde{s}$라 정의하자. 다항식 $h(x)$이 위수를 e라 하면, $\tilde{s}$의 최소 주기는 e 또는 $2e$이다.

(증명)

정리 5에 의하여, $\tilde{s}$는 $S(c(x))$의 원소이다. 가정에 의하여 $L-BRG$의 초기 상태 벡터가 0이 아니므로, 보조정리 6에 의하여 $\tilde{s}$의 주기는 e 또는 $2e$이 된다. ■

위 정리 7에 의하여, $L-BRG$의 특성 다항식 $c(x)=h(x)^2$에서 $h(x)$가 원시 다항식인 경우, 생성된 수열 $\tilde{s}$의 주기는 0이 아닌 초기 상태에 따라서 2^L-1 또는 $2(2^L-1)$이 된다. 또한 $\tilde{s}$의 최소 다항식 $m_{\tilde{s}}(x)$은 $c(x)$의 약수이므로, $m_{\tilde{s}}(x)=h(x)$ 또는 $m_{\tilde{s}}(x)=h(x)^2$임을 알 수 있다. 그러므로 (x)=h(x)^2 $L-BRG$에서 생성된 이진 난수열의 선형 복잡도는 초기 상태에 따라 L 또는 $2L$의 값을 갖는다.

[표 1]은 L개의 레지스터로 구성된 일반 선형 쉬프트 레지스터의 출력수열과 $L-BRG$의 출력수열의 최대 주기와 선형 복잡도의 크기를 비교한 결과를 설명한다.

[표 1] 출력 수열의 특성

	L-LFSR	L-BRG
최대 주기	2^L-1	$2(2^L-1)$
최대 선형복잡도	L	$2L$

[표 1]에서 설명하는 것처럼, 동일한 레지스터로 구성된 $L-LFSR$과 $L-BRG$의 주기와 선형 복잡도는 최대 두 배의 차이를 보이고 있다.

2.3 부분 특성 다항식

이 절에서는 원시 다항식 $h(x)$가 주어졌을 때,

$c(x)=h(x)^2$을 특성 다항식으로 갖는 $L-BRG$를 구성하는 방법을 제안한다. $L-BRG$를 실제 구성하기 위해서는 부분 특성 다항식 $f(x)$와 $g(x)$를 생성해야 되며, 구현의 용이성을 위하여 계수 0인 항을 많이 갖는 다항식을 사용하는 것이 좋다. 이와 같은 부분 특성 다항식을 찾는 한가지 방법을 제시한다. $c(x)=\sum_i^{2L} c_i x^i = \sum_{i=0}^{L} c_{2i} x^{2i}$라 할 때, 먼저 L이 짝수인 경우 $f(x)$와 $g(x)$를 다음과 같이 구성한다:

$$\begin{aligned} f(x) &= x^L + x + 1 \\ g(x) &= x^L + \sum_{i=1}^{L-1} c_{2i} x^{2i-1} + 1 \end{aligned} \tag{18}$$

두 다항식 $f(x)$와 $g(x)$의 곱에서 짝수 차 항만을 취한 결과는 다음과 같다:

$$a(x)=x^L(x^L+1)+x\left(\sum_{i=1}^{L-1} c_{2i} x^{2i-1}\right)+(x^L+1) \tag{19}$$

이 결과 값이 $c(x)$와 같은가를 확인하면 된다.

$$\begin{aligned} a(x) &= x^{2L} + \sum_{i=1}^{L-1} c_{2i} x^{2i} + 1 \\ &= \sum_{i=0}^{L} c_{2i} x^{2i} \end{aligned} \tag{20}$$

이므로, $a(x)=c(x)$가 성립한다. 그러므로 제안된 $f(x)$와 $g(x)$를 부분 특성 다항식으로 갖는 $L-BRG$의 특성 다항식은 $c(x)$가 된다.

(예 8)

특성 다항식 $c(x)=x^{16}+x^8+x^6+x^4+1$을 갖는 $8-BGR$를 고려하자. 제시한 방법에 의하여, $f(x)$와 $g(x)$를 다음과 같이 정의하자:

$$\begin{aligned} f(x) &= x^8+x+1, \\ g(x) &= x^8+x^7+x^5+x^3+1 \end{aligned} \tag{21}$$

두 다항식 $f(x)$와 $g(x)$의 곱은 $c(x)$가 됨을 쉽게 알 수 있다.

이제, L이 홀수인 경우를 고려하자. L이 홀수인 경우 $f(x)$와 $g(x)$를 다음과 같이 정의하자:

$$\begin{aligned} f(x) &= x^L + 1 \\ g(x) &= x^L + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} c_{2i} x^{2i} + \sum_{\lceil \frac{L}{2} \rceil}^{L-1} c_{2i} x^{2i-L} + 1 \end{aligned} \tag{22}$$

이제 두 다항식의 곱 $f(x)\,g(x)$에서 짝수 차 항만을 고려하자.

$$\begin{aligned} &(x^L)\left(x^L + \sum_{\lceil \frac{L}{2} \rceil}^{L-1} c_{2i} x^{2i-L}\right) + \left(\sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} c_{2i} x^{2i} + 1\right) \\ &= x^{2L} + \sum_{\lceil \frac{L}{2} \rceil}^{L-1} c_{2i} x^{2i} + \sum_{i=1}^{\lfloor \frac{L}{2} \rfloor} c_{2i} x^{2i} + 1 \\ &= \sum_{i=0}^{L} c_{2i} x^{2i} \end{aligned} \tag{23}$$

위 식 (25)의 결과는 $c(x)$와 같음을 알 수 있다.

(예제 9)

특성 다항식 $c(x)=x^{18}+x^8+1$을 갖는 $8-BGR$를 고려하자. 제시한 방법에 의하여, $f(x)$와 $g(x)$를 다음과 같이 정의하자:

$$f(x)=x^9+1, \quad g(x)=x^9+x^8+1 \tag{24}$$

이 두 다항식을 부분 특성 다항식으로 갖는 $8-BGR$에서 초기 상태 벡터 (1,1,1,1,1,1,1,1)로 생성한 수열은 다음과 같다:

11111111101010101101010100111111110001
01011000101001001111001011011011111110011
10101000110101000011111000001011000000010
01000001100100011101100110111101110010 11
10100100110101100011111100001010100000 10
10100011111100110101101110100111011 1000
11001100001000100000100010001100110011 10
11101101110111100110010100010010100 0101
11100111101101101100111100100010100 1000
10101100111111101101010111101010010 1111
10010010110110010011110110001011110 0010
01010011001010111011111110111010110 01101
00100011100100001101100000111100000 0101
00000010100000011110000110110001110 01001
10100101110101111011111101100101100 10010

0100101100101111101111010111011010011001
1110001000110001000010011000010111000111
1101001101101011100111110100010110100010
0011100110001101110000111010000011010000
0001110000000110000000010000000010000000
0110000001110000011010000111010001101110
0011100110110100011110100001011100001000
1100011000100111000101101001111101011010
0111111010010101110010100110111100011100
1100001100100000100100000101100001111100
0011010100111010101101111111100101010100
0101010101.

위 수열의 최소 주기는 $1022=2(2^9-1)$ 이다.

다음과 같은 순서에 의하여, 새로운 이진 난수열 발생기를 쉽게 구성할 수 있다. 또한 특성 다항식 $h(x)$를 사용하는 기존의 선형 쉬프트 레지스터를 쉽게 교체할 수 있다.

(단계1) L차 원시 다항식 $h(x)$를 선택한다.
(단계2) $c(x)=h(x)^2$을 계산한다.
(단계3) 앞에서 제시한 방법을 사용하여, 두 부분 특성 다항식 $f(x)$와 $g(x)$를 계산한다.
(단계4) 부분 특성 다항식 $f(x)$와 $g(x)$를 사용하여 이진 난수열 발생기를 구성한다.

Ⅲ. 결 론

일반적인 스트림 암호 시스템의 안전도는 이진 난수열 발생기의 안전도에 근거를 두고 있다. 그러므로 스트림 암호 시스템에 사용되는 이진 난수열 발생기는 긴 주기와 높은 선형 복잡도, 그리고 다양한 난수성질을 충족시킬 수 있어야 한다. 일반적으로 최대 길이 선형 쉬프트 레지스터를 사용하기 때문에, 이진 난수열 발생기의 주기에 대한 연구는 거의 찾아 볼 수 없다. 본 논문에서는 일반적인 선형 쉬프트 레지스터와 동일한 레지스터의 개수를 가지고, 선형 쉬프트 레지스터에서 생성한 수열 보다 긴 주기를 갖는 수열을 생성할 수 있는 새로운 이진 난수열 발생기를 제안했다. 제안된 이진 난수열 발생기는 L개의 레지스터와 원시 다항식의 제곱 형태의 특성 다항식을 택할 경우, 최소 주기의 상한이 $2(2^L-1)$이 된다. 이는 L개의 레지스터로 구성된 최대 주기 선형 쉬프트 레지스터에서 생성할 수 있는 수열의 주기의 두 배가된다. 또한 제안된 이진 난수열 발생기에서 생성된 수열의 성질을 파악하기 위해 기존의 선형 쉬프트 레지스터에서 생성된 수열의 성질을 파악할 때 사용한 정리들을 그대로 사용할 수 있다.

$L-BRG$의 경우 초기 값에 따라 생성 수열의 주기에 차이가 있을 수 있으므로, 이에 대한 연구와 비선형함수를 $L-BRG$에 적용하는 방법에 대한 연구가 수행되어야 한다. 또한 $L-BRG$의 생성 수열의 난수성질에 대한 연구도 향후 계속 연구되어야 한다.

참 고 문 헌

[1] Rudolf Lidl, Harald Niederreiter, "Chapter6. Linear Recurring Sequences", Introduction to Finite Fields and Their Application, Cambridge University, 1986.

[2] James L. Massey, "Shieft-Register Synthesis and BCH Decoding", IEEE Trans. on Info. Theory, Vol. IT-15, January 1969.

[3] Rainer A Ruppel, "Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators", IEEE Trans.

[4] E. L. Key, "An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators", IEEE Trans. on Info. Theory, Vol. IT-22, Nov. 1976.

[5] Rainer A. Ruppel, Othmar J. Staffelbach, "Products of Linear Recurring Sequences with Maximum COmplexity", IEEE. Trans. on Info. Theory, Vol. IT-33, No.1, January, 1987.

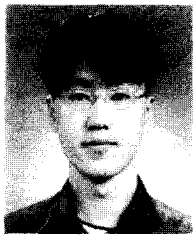
[6] Gorth, "Generation of Binary Sequence with Controllable Complexity", IEEE Trans. on Info, Theory, Vol IT-17, May 1971.

[7] Kenneth H. Rosen, "Elementary Number Theory and Its Applications", ADDISON WeSELEy, 1988.

[8] 한국전자통신 연구소편, "제4장. Stream 암호 시스템", 현대 암호학, 한국전자통신연구소, 1991.

〈著者紹介〉

김 대 엽 (Dae-Youb Kim) 정회원
1994년 2월 : 고려대학교 수학과 졸업
1996년 8월 : 고려대학교 수학과 석사(대수학 전공)
2000년 2월 : 고려대학교 수학과 박사(대수학 전공)
1997년 8월~2001년 3월 : (주)텔리맨, 위성통신 연구소 선임연구원
2001년 4월~현재 : (주)시큐아이닷컴 정보보호 연구소 선임연구원
〈관심분야〉 CAS, Smart Card, PKI, 유/무선 보안프로토콜



주 학 수 (Hak-Soo Ju)
1997년 8월 : 고려대학교 수학과 졸업
1999년 8월 : 고려대학교 수학과 이학석사(대수학 전공)
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원 연구원
〈관심분야 〉 ECC, 워터마킹, PKI

임 종 인 (Jong-In Lim) 정회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사(대수학 전공)
1986년 2월 : 고려대학교 수학과 박사(대수학 전공)
1986년 2월~현재 : 고려대학교 수학과 정교수
2000년10월~현재 : 고려대학교 정보보호 대학원 원장
〈관심분야〉 블록암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘의 분석