산술 시프트 레지스터

박창수*, 손창우*, 조경연*
*부경대학교 전자컴퓨터정보통신공학부

Arithmetic Shift Register

Chang-Soo Park*, Chang-Woo Son*, Gyeong-Yeon Cho*
*Dept. of Electric, Computer, Telecommunication, Pukyong National University

요 약

본 논문에서는 의사난수발생기로 사용할 수 있는 산술 시프트 레지스터(ASR, Arithmetic Shift Register)를 제안한다. 산술 시프트 레지스터는 $GF(2^n)$상에서 0이 아닌 초기 값에 0 또는 1이 아닌 임의의 수를 곱하는 수열로 정의한다. 산술 시프트 레지스터의 주기는 2^n-1로 최대 주기를 가진다. 또한 소프트웨어 및 하드웨어로 구현이 용이하다.

제안한 산술 시프트 레지스터는 종래의 선형귀환 시프트 레지스터와 같이 암호, 오류수정부호, 몬테카를로 적분, 데이터통신 등 여러 분야에서 폭 넓게 사용될 수 있다.

1. 서론

1)

의사난수 발생기는 암호, 오류수정부호, 몬테카를로 적분, 데이터통신 등 여러 분야에서 폭 넓게 사용되고 있다. 이러한 의사난수발생기로는 선형 귀환 시프트 레지스터(LFSR, Linear Feedback Shift Register)가 간단하고, 동작속도가 빠르며, 수학적으로 잘 정의되어 있는 장점을 가지므로 많이 사용되고 있다. 또한 선형 귀환 시프트 레지스터를 변형시킨 캐리 귀환 시프트 레지스터(FCSR, Feedback with Carry Shift Register)에 대한 연구도 진행되고 있다[1-5].

선형 귀환 시프트 레지스터는 구성방식에 따라서 피보나치 구성과 갈로이 구성 방식이 있다. 피보나치 선형 귀환 시프트 레지스터를 그림 1에 보인다.

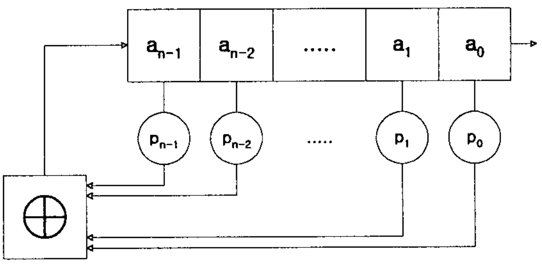

그림 1 피보나치 선형 귀환 시프트 레지스터

그림 1에서 a_0, a_1, ⋯, a_{n-1}은 초기 값이 저장되어 있으며 새로운 값 a_n은 식(1)로 주어진다.

$$a_n = \sum_{i=0}^{n-1} p_i a_i (\bmod 2) \qquad (1)$$

이러한 피보나치 선형 귀환 시프트 레지스터는 소프트웨어 구현이 곤란하므로 이를 그림 2와 같이 구성한 것이 갈로이 선형 귀환 시프트 레지스터이다.

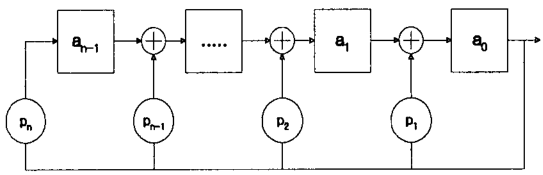

그림 2 갈로이 선형 귀환 시프트 레지스터

그림 2에서 순환 방정식은 식(2)가 된다.

$$a_i' = a_{i+1} + p_{i+1} a_0 \qquad \text{for } 0 \le i \le n-2 \qquad (2)$$
$$a_{n-1}' = p_n a_0$$

본 논문에서는 선형 귀환 레지스터처럼 의사난수발생기로 사용할 수 있는 새로운 구조의 산술 시프트 레지스터(ASR, Arithmetic Shift Register)를 제안한다. 산술 시프트 레지스터는 $GF(2^n)$에서 일정한 상수 D를

이 논문은 2002년도 두뇌한국21사업에 의하여 지원되었음.

연속적으로 곱하는 구조이며, 이를 본 논문에서는 ASR-D로 기술한다. ASR-2는 갈로이 선형 귀환 시프트 레지스터와 수학적으로 동일한 형태를 가진다.

본 논문에서 제안하는 산술 시프트 레지스터는 소프트웨어 및 하드웨어 구현이 용이하며, 상수 D를 변경시켜서 다양한 종류의 난수를 얻을 수 있는 장점을 가진다.

2. 산술 시프트 레지스터

Definition 1

$GF(2^n)$상에서 0이 아닌 초기 값 S_0에 0 또는 1이 아닌 임의 수 D를 곱하는 수열을 산술 시프트 레지스터(ASR-D: Arithmetic Shift Register-D)로 정의한다. ASR-D의 i번째 상태 S_i는 S_0D^i가 된다.

Lemma 1

$GF(2^n)$상에서 0 또는 1이 아닌 임의 수 D에 대하여 '$D^k = 1$'이 되는 t가 '$t = 2^n-1$'로 유일하면 0을 제외한 모든 수 $R\in\{1, 2, \cdots, 2^n-1\}$는 $D^u\in\{1, 2, \cdots, 2^n-1\}$로 표현할 수 있다.

증명 : $D^u\in\{1, 2, \cdots, 2^n-1\}$로 표현할 수 없는 수 R_{NO}가 존재한다면 '$\#(R - R_{NO}) < 2^n-1$'이 된다. 이를 만족하기 위해서는 식(3)이 성립되어야 한다.

$$(\exists p), (\exists q), D^p = D^q \qquad (3)$$

식(3)의 양변을 D^q로 나누면 '$D^{p-q} = 1$'이 된다. 정의에 의하면 '$p-q=2^n-1$'이 되며, '$p=2^n-1+q$'가 된다. $p, q\in\{1, 2, \cdots, 2^n-1\}$로 정의 하였으므로 이 식을 만족하는 p, q는 존재하지 않는다. □

Lemma 2

$GF(2^n)$상에서 0 또는 1이 아닌 임의 수 D가 있고, D에 대하여 '$D^k = 1$'이 되는 t가 '$t = 2^n-1$'로 유일하면 0을 제외한 모든 수 S는 $S = S_0D^u\in\{1, 2, \cdots, 2^n-1\}$로 표현할 수 있다. S_0는 0이 아닌 임의의 수이다.

증명 : *Lemma* 1로부터 D^u는 0을 제외한 모든 수 $R\in\{1, 2, \cdots, 2^n-1\}$을 생성할 수 있다. 따라서 $RS_0\in\{1, 2, \cdots, 2^n-1\}$이다. □

Definition 2

비복원 다항식(irreducible polynomial) $P(x)$로 표현되는 $GF(2^n)$상에서 0 또는 1이 아닌 임의 수 D에 대하여 '$D^k = 1$'이 되는 t가 '$t = 2^n-1$'로 유일하면 $P(x)$를 ASR-D의 특성 다항식(characteristic polynomial)이라 한다.

Theorem

$GF(2^n)$상에서 특성 다항식(characteristic polynomial)으로 표현되는 ASR-D의 주기는 '2^n-1'이다.

증명 : *Lemma* 1, *Lemma* 2로부터 증명할 수 있다. □

Lemma 3

$GF(2^n)$상에서 '$2^n-1 = U\times V$'인 합성수이고 '$A^U=D$'인 A가 존재하는 비복원 다항식은 ASR-D의 특성 다항식이 아니다.

증명 : '$D^V = (A^U)^V = A^{UV} = 1$'이다. 따라서 '$D^t = 1$'이되는 t가 '$t = 2^n-1$'로 유일하지 않다. □

Example

'$2^{32}-1 = 3\times 5\times 17\times 257\times 65537$'이다. $GF(2^{32})$상의 비복원 다항식 '$Pa(X)$= 0x197943fc9'에서 '$(\text{0x32389d6f})^3 = 2$'이다. 따라서 $Pa(X)$는 ASR-2의 특성 다항식이 아니다. 비복원 다항식 '$Pb(X)$= 0x19fa0ff27'에서는 *Lemma* 3을 만족하는 A가 존재하지 않으므로 $Pb(X)$는 ASR-2의 특성 다항식이다.

Lemma 4

$GF(2^n)$상에서 '2^n-1'이 소수이면 모든 비복원 다항식은 ASR-D의 특성 다항식이다.

증명 : Fermat의 little theorem에 의하여 '$t = 2^n-1$, $D^k = 1$'이 된다. t가 소수이므로 '$D^k = 1$'이 되는 t는 '$t = 2^n-1$'로 유일하다. □

'2^i-1' 형태의 소수를 Mersenne 소수라고 하며, $i = \{\cdots, 13, 17, 19, 31, 61, 89, 107, 127, 521, \cdots\}$이 알려져 있다[9].

ASR-2에서 특성 다항식 $P(X)=X^n+\sum P_i\times X^i$, $i\in\{0, 1, 2, \cdots, 2^n-1\}$이고, 상태 S에서 레지스터의

값을 $\sum S_i \times X^i$, $i \in \{0, 1, 2, \cdots, 2^n-1\}$이라 하면 다음 상태 S'의 레지스터 값은 식(4)와 같이 된다.

$$S'_i = S_{i-1} + P_i S_{n-1} \quad \text{for } 1 \le i \le n-1 \qquad (4)$$
$$S'_0 = S_{n-1}$$

식(4)의 산술 시프트 레지스터는 왼쪽으로 시프트되며 식(2)의 갈로이 선형 귀환 시프트 레지스터는 오른쪽으로 시프트되는 점을 감안하면 식(4)는 식(2)와 수학적으로 동일한 형태를 가진다.

3. 구 현

ASR-D에서 D가 작은 수이면 소프트웨어로 구현이 용이하다. 32 비트 컴퓨터에서 GF(2^{32})상의 ASR-2를 C로 프로그램하면 표 1과 같다.

표 1 $GF(2^{32})$상의 ASR-2

```
#define POLY    0x9fa0ff27
unsigned int asr_2;
asr_2 = (asr_2<<1) ^
        ( -(asr_2>>31) & POLY );
```

또 다른 예로 ASR-6은 표 2와 같이 구현할 수 있다.

표 2 $GF(2^{32})$상의 ASR-6

```
int asr_6;
asr_6 ^= (asr_6<<1) ^
         ( (asr_6>>31) & POLY );
asr_6 = (asr_6<<1) ^
        ( (asr_6>>31) & POLY );
```

ASR-D의 하드웨어 구현은 상수 D를 $GF(2)$상에서의 행렬식으로 표현하여 구현할 수 있다[6-8]. 이를 정리하면 다음과 같다.

Lemma 5

$GF(2^n)$상의 곱셈 '$C=S\times D$'은 D가 상수라면 $GF(2^n)$ 상에서의 행렬식 곱셈 $|C|^T = |M| \times |S|^T$가 된다.

증명 : $GF(2^n)$상의 다항식 S와 D는 각각 $S=\sum_{i=0}^{n-1} s_i x^i$, $D=\sum_{i=0}^{n-1} d_i x^i$로 표현할 수 있다. 또한 특성다항식 P는 $P=\sum_{i=0}^{n} p_i x^i$로 표현할 수 있다. 단위 함수 $u(\ )$를 다음과 같이 정의하면,

$$u(i, j, m) = 1 \text{ if } m = i + j$$
$$= 0 \text{ if } m \neq i + j$$

다항식 곱셈 '$C=S\times D$'는 다음과 같이 된다.

$$C = S\times D = \sum_{i=0}^{2n-2} c_i x^i$$
$$c_m = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} u(i,j,m) s_i d^j, \quad while\ m=(0,1,\cdots,2n-2)$$

C 다항식의 계수는 다음과 같은 과정으로 계산할 수 있다.

```
for (i=2n-2 ; i > n-1 ; i--)
    for (j=0 ; j < n+1 ; j++)
        ci-j = ci  · pn-j ⊕ ci-j
```

따라서 $c_i \in \{c_{n-1}, c_{n-2}, \cdots, c_0\}$은

$$c_i = \sum_{j=0}^{n-1} f_j(d_{n-1}, d_{n-2}, \cdots, d_0, p_{n-1}, \cdots, p_0)\cdot s_j,$$
$$where \quad d_i, p_i, f_j(\cdots) \in GF(2)$$

이 된다. □

예로써 $GF(2^8)$상에서 특성 다항식이 '$P(x)$ = 0x11b'인 ARS-6의 순환 행렬식 $S \rightarrow S'$는 *Lemma* 5에 의하여 다음과 같이 구해준다.

$$\begin{vmatrix} S_7' \\ S_6' \\ S_5' \\ S_4' \\ S_3' \\ S_2' \\ S_1' \\ S_0' \end{vmatrix} = \begin{vmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix} \times \begin{vmatrix} S_7 \\ S_6 \\ S_5 \\ S_4 \\ S_3 \\ S_2 \\ S_1 \\ S_0 \end{vmatrix}$$

4. 결 론

본 논문에서는 선형 귀환 시프트 레지스터(LFSR, Linear Feedback Shift Register)와 같이 의사난수발생기로 사용이 가능한 새로운 구조의 산술 시프트 레지스터(ASR, Arithmetic Shift Register)를 제안하였다. 산술 시프트 레지스터는 $GF(2^n)$에서 일정한 상수 D를 연속적으로 곱하는 구조이며, 이를 ASR-D로 표현하였다.

$GF(2^n)$상에서 0 또는 1이 아닌 임의 수 D에 대하여 '$D^k = 1$'이 되는 t가 '$t = 2^n - 1$'로 유일하게 되는 비복원 다항식이 ASR-D의 특성 다항식이며, ASR-D의 주기는 '$2^n - 1$'로 최대주기를 가진다. '$2^n - 1$'이 Mersenne 소수이면 모든 비복원 다항식이 ASR-D의 특성 다항식이다.

제안한 산술 시프트 레지스터는 소프트웨어 및 하드웨어 구현이 용이하므로 암호, 오류수정부호, 몬테카를로 적분, 데이터통신 등 여러 분야에서 의사난수 발생기로 폭 넓게 사용될 수 있다.

[참고문헌]

1] M. Goresky, and M. Klapper, "Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers," IEEE Transaction on Information Theory, Vol. 48, No. 11, pp. 2826-2836, Nov. 2002

[2] J. Noras, "Fast pseudorandom sequence generators: Linear feedback shift registers, cellular automata, and carry feedback shift registers," Univ. Bradford Elec. Eng. Dept., Rep. 94, 1997

[3] M. Goresky, M. Klapper, and L. Washington, "Fourier transforms and the 2-ardic span of periodic binary sequencs," IEEE Transaction on Information Theory, Vol. 46, pp. 687-691, Mar. 2000

[4] B. Schneier, *Applied Cryptography*, 2nd ed. NewYork, Wile, 1996

[5] P. LEcuyer, and F. Panneton, "A New Class of Linear Feedback Shift Register Generators," Proceedings of the 2000 Winter Simulation Conference, pp. 690-696, 2000

[6] E.D. Mastrovito, "VLSI Designs for Multiplication over Finite Fields $GF(2^m)$," Proc. Sixth Int'l Conf. Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes(AAECC-6), pp. 297-309, Jul. 1988

[7] T. Zhang, and K. Parhi, "Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polynomilas," IEEE Transactions on Computer, Vol. 50, No. 7, pp. 734-749, Jul. 2001

[8] C. Paar, P. Fleischmann, and P. Roelse, "Efficient Multiplier Architectures for Galois Fields," IEEE Transactions on Computers, Vol. 47, No. 2, pp. 162-170, Feb. 1998

[9] *Mersenne Primes: History, Theorems and Lists* http://www.utm.edu/research/primes/mersenne/