논문 2006-43CI-1-1

갈로이 선형 궤환 레지스터의 일반화

(Generalization of Galois Linear Feedback Register)

박 창 수*, 조 경 언*

(Chang-Soo Park and Gyeong-Yeon Cho)

요 약

본 논문은 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 수 D를 곱하는 수열로 정의한다. 그리고 이를 본 논문에서는 ASR-D로 표현한다.

$GF(2^n)$상에서 '$D^k=1$'이 되는 t가 '$t=2^n-1$'로 유일하게 되는 비복원다항식이 ASR-D의 특성다항식이며, ASR-D의 주기는 '2^n-1'로 최대주기를 가진다. 갈로이 선형 궤환 시프트 레지스터는 ASR-2^{-1}에 해당한다. 그러므로 제안하는 산술 시프트 레지스터는 갈로이 선형 궤환 시프트 레지스터를 일반화한 것이다. $GF(2^n)$상의 ASR-D의 선형복잡도는 '$n \le LC \le \frac{n^2+n}{2}$'으로 종래의 선형 궤환 시프트 레지스터와 비교하여 안정도가 높다. 제안한 산술 시프트 레지스터의 소프트웨어 구현은 종래의 선형 궤환 시프트 레지스터에 비하여 효율적이며, 하드웨어 복잡도는 동일하다.

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

Abstract

This thesis proposes Arithmetic Shift Register(ASR) which can be used as pseudo random number generator. Arithmetic Shift Register is defined as progression that multiplies random number D, not 0 or 1 at initial value which is not 0, and it is represented as ASR-D in this thesis.

Irreducible polynomial that t which makes '$D^k=1$' satisfies uniquely as '$t=2^n-1$' over $GF(2^n)$ is the characteristic polynomial of ASR-D, and the cycle of Arithmetic Shift Register has maximum cycle as '2^n-1'. Galois Linear Feedback Shift Register corresponds to ASR-2-1. Therefore, Arithmetic Shift Register proposed in this thesis generalizes Galois Linear Feedback Shift Register. Linear complexity of ASR-D over $GF(2^n)$ is '$n \le LC \le \frac{n^2+n}{2}$' and in comparison with existing Linear Feedback Shift Register stability is high. The Software embodiment of arithmetic shift register proposed in this thesis is efficient than that of existing Linear Shift Register and hardware complexity is equal.

Arithmetic shift register proposed in this thesis can be used widely in various fields such as cipher, error correcting codes, Monte Carlo integral, and data communication etc along with existing linear shift register.

Keywords: 갈로이, 선형 궤환 레지스터, Galois, Feedback Register, Shift Register

I. 서 론

최근에 정보통신 분야의 비약적인 발전으로 인해 거의 모든 정보를 인터넷을 통해 공유할 수 있게 되었다. 그로인해 보안이 중요한 이슈가 되었고, 암호학 연구가

* 정회원, 부경대학교 대학원 컴퓨터공학과
(Department of Computer Engineering, Graduate School, Pukyong National University)

※ 이 논문은 2004년도 두뇌한국21사업에 의하여 지원되었음

접수일자 : 2005년9월17일 수정완료일 : 2006년1월3일

많이 진행되었다. 또한 컴퓨터의 처리능력이 상당히 발달하여 암호 해독 시간이 단축 되어 수학적으로도 더욱 더 복잡성을 요구하게 되었다.

암호는 블록 암호와 스트림 암호로 나뉘는데, 그 가운데 스트림 암호는 비트 단위로 암호화를 수행하므로 에러 전파가 없고 블록 암호보다 속도가 빠르다는 장점이 있다. 스트림 암호에서 암호화를 위해서 사용하는 것이 의사난수발생기이다. 의사난수발생기는 암호뿐만 아니라 오류수정부호, 몬테칼로 적분, 데이터통신 등 여러 분야에서 폭 넓게 사용되고 있다. 이러한 의사난수발생기로는 선형 궤환 시프트 레지스터(LFSR, Linear Feedback Shift Register)가 간단하고, 동작속도가 빠르며, 수학적으로 잘 정의되어 있는 장점을 가지므로 많이 사용되고 있다. 또한 선형 궤환 시프트 레지스터를 변형시킨 캐리 궤환 시프트레지스터(FCSR, Feedback with Carry Shift Register)에 대한 연구도 진행되고 있다[1][5].

선형 궤환 시프트 레지스터는 구성방식에 따라서 피보나치 구성과 갈로이 구성 방식이 있다. 피보나치 선형 궤환 시프트 레지스터는 소프트웨어로 구현이 곤란하다는 단점이 있어 이를 변형한 것이 갈로이 선형 궤환 시프트 레지스터로 널리 사용되고 있다.

본 논문에서는 선형 궤환 시프트 레지스터처럼 의사난수발생기로 사용할 수 있는 새로운 구조의 산술 시프트 레지스터(ASR, Arithmetic Shift Register)를 제안한다. 산술 시프트레지스터는 갈로이 선형 궤환 시프트레지스터를 일반화한 것으로 $GF(2^n)$에서 일정한 상수 D를 연속적으로 곱하는 구조이며, 이를 본 논문에서는 ASR-D로 기술한다.

ASR-2^{-1}은 갈로이 선형 궤환 시프트 레지스터에 해당한다. 따라서 본 논문에서 제안하는 산술 시프트 레지스터는 갈로이 선형 궤한 레지스터를 일반화한 것이다.

본 논문에서 제안하는 산술 시프트 레지스터는 소프트웨어 및 하드웨어 구현이 용이하며, 상수 D를 변경시켜서 갈로이 선형 궤환 시프트레지스터와 동등 이상의 선형복잡도를 가지는 다양한 종류의 난수를 얻을 수 있는 장점을 가진다. 따라서 암호, 오류수정부호, 몬테카를로 적분, 데이터 통신 등 여러 분야에서 활용될 수 있다.

본 논문은 Ⅱ장에서 선형 궤환 시프트레지스터에 대해서 설명하고, Ⅲ장에서 산술 시프트 레지스터를 보이고 Ⅳ장에서 소프트웨어와 하드웨어로 구현하며, Ⅴ장에서 선형복잡도를 구하고, Ⅵ장에서 결론을 맺는다.

Ⅱ. 선형 궤환 시프트 레지스터

선형 궤환 시프트 레지스터는 시프트 레지스터를 구성하는 방식에 따라서 피보나치 선형 궤환 시프트 레지스터와 갈로이 선형 궤환 시프트레지스터로 나눌 수 있다. 이 장에서는 두 선형 궤환 시프트 레지스터에 대해서 알아보겠다.

1. 피보나치 선형 궤환 시프트 레지스터

피보나치 선형 궤환 시프트 레지스터를 그림 1에 나타내었다. 피보나치 선형 궤환 시프트 레지스터에서 $a_0, a_1, \cdots, a_{n-1}$은 초기값이 저장되어 있으며 새로 입력되는 값 a_n은 식 1로 주어진다.

$$a_n = \bigoplus_{i=0}^{n-1} p_i a_i \tag{1}$$

이러한 피보나치 선형 궤환 시프트 레지스터는 소프트웨어 구현이 곤란한 단점이 있다(4장 구현 및 비교 참조).

2. 갈로이 선형 궤환 시프트 레지스터

피보나치 선형 궤환 시프트 레지스터는 소프트웨어로 구현이 곤란한 단점이 있다. 이 단점을 보완하기 위해서 구성한 것이 갈로이 선형 궤환 시프트 레지스터이다. 갈로이 선형 궤환 시프트 레지스터를 그림 2에 나타내었다.

갈로이 선형 궤환 시프트 레지스터는 마지막 단의 출력이 동시에 궤환함수를 통과한 후 앞단의 출력과 모듈로 2 덧셈을 하여 다음 단으로 입력되며, 순환 방정식은 식 2가 된다.

$$\begin{aligned} a_i' &= a_{i+1} \oplus p_{i+1} a_0 \quad \text{for } 0 \le i \le n-2 \\ a_{n-1}' &= p_n a_0 \end{aligned} \tag{2}$$

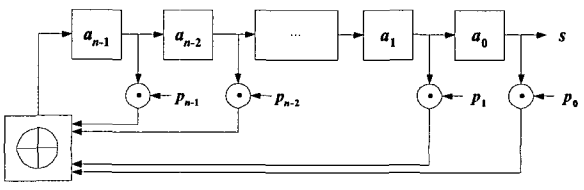

그림 1. 피보나치 선형 궤환 시프트 레지스터
Fig. 1. Fibonacci Linear Feedback Shift Register.

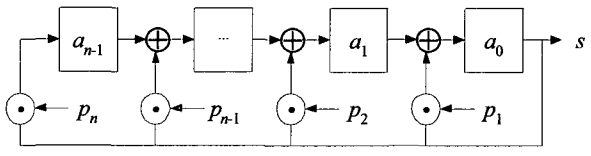

그림 2. 갈로이 선형 궤환 시프트레지스터
Fig. 2. Galois Linear Feedback Shift Register.

Ⅲ. 산술 시프트 레지스터

정의 3.1 $GF(2^n)$상에서 0이 아닌 초기 값 A_0에 0 또는 1이 아닌 임의의 수 D를 곱하는 수열을 산술 시프트 레지스터(ASR-D : Arithmetic Shift Register-D)로 정의한다. ASR-D의 i 번째 값(상태) A_i는 A_0D^i가 된다.

Lemma 3.1 갈로이 선형 궤환 시프트 레지스터는 '$D=2^{-1}$'인 산술 시프트 레지스터이다. 즉, 산술 시프트 레지스터는 갈로이 선형 궤환 시프트 레지스터의 일반형이다.

Proof 갈로이 선형 궤한 시프트 레지스터의 순환 방정식인 식 (2)는 $GF(2^n)$상에서 비복원다항식(irreducible polynomial)이 $P(x)$인 경우에 '$A_{i+1}=\frac{A_i}{2}$'를 나타낸다. 따라서 정의 3.1에 의하여 갈로이 선형 궤환 시프트 레지스터는 ARS-2^{-1}이다. □

Lemma 3.2 $GF(2^n)$상에서 0 또는 1이 아닌 임의의 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.

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

$$(\exists p),(\exists q),D^p=D^q \tag{3}$$

식 3의 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 되어야 한다. 그러나 $p,q\in\{1,2,\cdots,2^n-1\}$로 정의하였으므로 이 식을 만족하는 p,q는 존재하지 않는다. □

Lemma 3.3 $GF(2^n)$상에서 0 또는 1이 아닌 임의의 수 D가 있고, D에 대하여 '$D^k=1$'이 되는 t가 '$t=2^n-1$'로 유일하면 0을 제외한 모든 수 A는 $A=A_0D^u\in\{1,2,\ldots,2^n-1\}$로 표현할 수 있다. A_0는 0이 아닌 임의 수이다.

Proof Lemma 3.1로부터 D^u는 0을 제외한 모든 수 $R\in\{1,2,\cdots,2^n-1\}$을 생성할 수 있다. 따라서 $RA_0\in\{1,2,\cdots,2^n-1\}$이다. □

정의 3.2 비복원 다항식 $P(x)$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 특성다항식(characteristic polynomial)이라 한다.

정리 $GF(2^n)$상에서 특성다항식(characteristic polynomial)으로 표현되는 ASR-D의 주기는 '2^n-1'이다

Proof Lemma 3.1과 Lemma 3.2로부터 증명할 수 있다. □

Lemma 3.4 $GF(2^n)$상에서 '2^n-1'의 모든 소수 인수 p에 대하여 '$U=\frac{2^n-1}{p}$, $D^U\neq 1$'인 비복원다항식이 ASR-D의 특성다항식이다.

Proof '$2^n-1=pU$'이고 '$C^p=D$'인 C가 존재하면, '$D^U=C^{pU}=1$'이 된다. 따라서 '$D^k=1$'이 되는 t가 '$t=2^n-1$'로 유일하기 위해서는 '2^n-1'의 모든 소수 인수 p에 대하여 '$U=\frac{2^n-1}{p}$, $D^U\neq 1$'이 되어야 한다. □

예 1 '$2^{32}-1=3\times5\times17\times257\times65537$'이다. $GF(2^{32})$상의 비복원다항식 '$Pa(X)=0\times197943fc9$'에서 $D=2$인 경우에 '$2^{5\times17\times257\times65537}=1$'이다. 따라서 $Pa(X)$는 ASR-2의 특성다항식이 아니다. 비복원다항식 '$Pb(X)=0\times19fa0ff27$'에서는 $D=2$인 경우에 Lemma 3.3을 만족하므로 $Pb(X)$는 ASR-2의 특성다항식이다.

Lemma 3.5 $GF(2^n)$상에서 '2^n-1'이 소수이면 모든 비복원다항식은 ASR-D의 특성다항식이다.

Proof 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. □

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

Ⅳ. 구현 및 비교

1. 소프트웨어 구현

32 비트 컴퓨터에서 $GF(2^{32})$상의 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터를 C언어로 프로그램화하면 표 1과 같다.

표 1에서 32 비트 산술 시프트 레지스터는 & 연산 1회, xor 연산 1회, 시프트 연산 2회만을 수행하므로 총 4번의 연산이 필요하다. (int) 형변환 연산자는 해당하는 기계어를 선정하는 기능만을 수행하는 것으로 연산 시간을 소요하지 않는다.

이와 비교하여 갈로이 선형 궤환 시프트 레지스터는 & 연산 2회, or 연산 1회, xor 연산 1회, 시프트 연산 2회를 수행하므로 총 6번 연산이 필요하다. 그리고 피보나치 선형 궤환 시프트 레지스터는 xor 연산 6회, or 연산 1회, 시프트 연산 7회 수행해서 총 14회 연산을 필요로 한다.

32 비트 컴퓨터에서 $GF(2^{64})$상의 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터를 C언어로 프로그램한 것을 표 2에 보인다.

32 비트 컴퓨터에서 $GF(2^{32})$상과 $GF(2^{64})$상에서 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터를 C언어로 프로그램하는 경우에 각각 수행되는 동작을 비교하여 표 3에 보인다.

표 3으로부터 ASR-2가 종래의 갈로이 선형 궤환 시프트 레지스터보다 소프트웨어 구현시에 $GF(2^{32})$상에서는 필요한 연산 수가 갈로이 선형 궤환 시프트 레지스터보다 33%, 피보나치 선형 궤환 시프트 레지스터보다 71% 적게 필요함을 알 수 있다. 또한 $GF(2^{64})$상에서는 각각 18%와 53%가 적게 필요하다.

따라서 ASR-2는 종래의 갈로이 및 피보나치 선형 궤환 시프트 레지스터보다 동작속도가 빠르므로 효율적임을 알 수 있다.

표 1. $GF(2^{32})$상의 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터의 C프로그램

Table 1. C program of ASR-2, Galois and Fibonacci Linear Feedback Shift Register over $GF(2^{32})$.

```
unsigned int P ; /* Characteristic polynomial */
unsigned int A, B ;

/* ASR-2 */
A = (A << 1) ^ ((int)A >> 31) & P) ;

/* Galois-LFSR */
A = ((A ^ (-(A & 1) & P)) >> 1) | ( A<< 31) ;

/* Fibonacci-LFSR */
B = A ^ P ;
B ^= B >> 16 ;
B ^= B >> 8 ;
B ^= B >> 4 ;
B ^= B >> 2 ;
B ^= B >> 1 ;
A = (A >> 1) | (B << 31) ;
```

표 2. $GF(2^{64})$상의 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터의 C프로그램

Table 2. C program of ASR-2, Galois and Fibonacci Linear Feedback Shift Register over $GF(2^{64})$.

```
unsigned int P[2] ; /* Characteristic polynomial */
unsigned int A[2], B, C ;

/* ASR-2 */
B = (int)A[1] >> 31 ;
A[1] = ((A[1] << 1) | (A[0] >> 31)) ^ (B & P[1]) ;
A[0] = (A[0] << 1) ^ (B & P[0]) ;

/* Galois-LFSR */
B = -(A[0] & 1) ;
C = A[1] ^ (B & P[1]) ;
A[0] = ((A[0] ^ (B & P[0])) >> 1) | (C << 31) ;
A[1] = (C >> 1) | (B << 31) ;

/* Fibonacci-LFSR */
B = A[1] ^ P[1] ^ A[0] ^ P[0] ;
B ^= B >> 16 ;
B ^= B >> 8 ;
B ^= B >> 4 ;
B ^= B >> 2 ;
B ^= B >> 1 ;
A[0] = (A[0] >> 1) | (A[1] << 31) ;
A[1] = (A[1] >> 1) | (B << 31) ;
```

표 3. $GF(2^{32})$상과 $GF(2^{64})$상에서 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터의 동작속도 비교

Table 3. Compare operation speed of ASR-2, Galois and Fibonacci Linear Feedback Shift Register over $GF(2^{32})$ and $GF(2^{64})$.

	ASR-2				
	&	or	xor	shift	total
$GF(2^{32})$	1		1	2	4
$GF(2^{64})$	2	1	2	4	9
	Galois-LFSR				
	&	or	xor	shift	total
$GF(2^{32})$	2	1	1	2	6
$GF(2^{64})$	3	2	2	4	11
	Fibonacci-LFSR				
	&	or	xor	shift	total
$GF(2^{32})$		1	6	7	14
$GF(2^{64})$		2	8	9	19

표 4. $GF(2^{32})$상의 ASR-6의 C프로그램
Table 4. C program of ASR-6 over $GF(2^{32})$.

```
unsigned int P ; /* Characteristic polynomial */
unsigned int A ;
A ^= (A << 1) ^ ((int)A >> 31) & P) ;
A = (A << 1) ^ ((int)A >> 31) & P) ;
```

표 5. $GF(2^{32})$상의 ASR-D의 C프로그램
Table 5. C program of ASR-D over $GF(2^{32})$.

```
unsigned int P ; /* Characteristic polynomial */
unsigned int A, D ;
unsigned int B ;
for (B=0 ; D ; D >>= 1)
  { if (D&1) B ^= A ;
    A = (A<<1)^((int)A>>31)&P) ; }
```

ASR-D에서 D가 작은 값이면 소프트웨어 구현이 용이하다. $GF(2^{32})$상에서 ASR-6를 C 언어로 프로그램 한 것을 표 4에 보인다.

$GF(2^{32})$상에서 임의 값 D에 대한 ASR-D를 C 언어로 프로그램 한 것을 표 5에 보인다.

2. 하드웨어 구현

ASR-2를 하드웨어로 구현한 것을 그림 3에 보인다.

그림 3과 그림 2를 비교하면 시프트되는 방향만 다른 것을 제외하고는 동일한 것을 알 수 있다. 따라서 ASR-2와 갈로이 및 피보나치 선형 궤환 시프트 레지스터의 하드웨어 복잡도는 동일하다.

D가 일반적인 값인 경우에 ASR-D의 하드웨어 구현은 상수 D를 $GF(2)$상에서의 행렬식으로 표현하여 구성할 수 있다[6][8].

Lemma 4.1 $GF(2^n)$상의 곱셈 $'C = D \times S'$은 D가 상수라면 $GF(2)$상에서의 행렬식 곱셈 $C^T = M \times S^T$ 가 된다.

Proof $GF(2^n)$상의 다항식 S와 D는 각각

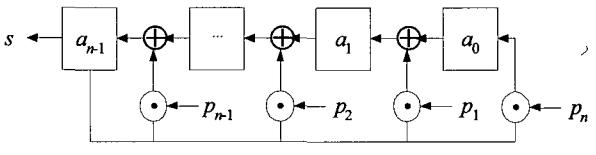

그림 3. ASR-2의 회로도
Fig. 3. Circuit of ASR-2.

$S = \sum_{i=0}^{n-1} s_i x^i$, $D = \sum_{i=0}^{n-1} d_i x^i$ 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,

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

다항식 곱셈 $'C = D \times S'$는 다음과 같이 된다.

$$C = S \times D = \sum_{i=0}^{2n-2} c_i x^i$$

$$c_m = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} u(i,j,m) \cdot s_i \cdot d_i$$
$$while \quad m = (0, 1, \cdots, 2n-2)$$

C 다항식의 계수는 다음과 같은 과정으로 계산할 수 있다.

$$\text{for} \quad (i = 2n-2; i > n-1; i--)$$
$$\text{for} \quad (j = 0; j < n+1; j++)$$
$$c_{i-j} = c_i \cdot p_{n-1} \oplus c_{i-j}$$

따라서 $c_i \in \{c_{n-1}, c_{n-2}, \cdots, 0\}$은 $c_i = \sum_{j=0}^{n-1} f_i($ $d_{n-1}, d_{n-2}, \cdots, d_0, p_{n-1}, p_{n-2}, \cdots, p_0) \cdot s_j$, 여기서 $d_i, p_i, f_i(\cdots) \in GF(2)$이 된다.

한편 행렬 M의 원소를 m_{ij}라고 하면 $c_i = \sum_{j=0}^{n-1} m_{ij} \cdot s_j$ 이다.

예로써 $GF(2^8)$상에서 특성다항식이 $'P(x) = 0 \times 11b'$인 ARS-6의 순환행렬식 $S \rightarrow S'$는 Lemma 4.1에 의하여 다음과 같이 구해준다.

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

V. 선형 복잡도

이 장에서는 산술 시프트 레지스터의 안전성을 검증하기 위해 선형복잡도를 구하고, 갈로이 및 피보나치 선형 궤환 시프트 레지스터와 비교한다.

$GF(2^n)$상에서 ASR-D의 초기값 $A_0(x)$와 i번째의 값 $A_i(x)$ 및 특성방정식 $P(x)$는 식 4와 같이 표현할 수 있다.

$$A_0(x)=\sum_{k=0}^{n-1}a_{0,k}x^k,\ A_i(x)=\sum_{k=0}^{n-1}a_{i,k}x^k,$$
$$P(x)=x^n\oplus\sum_{k=0}^{n-1}p_kx^k \tag{4}$$

ASR-2에서 출력 s_i와 $A_{i+1}(x)$의 계수는 다음과 같이 된다.

$$s_i=a_{i,n-1}$$
$$a_{i+1,j}=a_{i,j-1}\oplus(s_i\cdot p_j)$$
$$\text{for } j\in\{1,2,\cdots,n-1\}$$
$$a_{i+1,0}=s_i\cdot p_0$$

위 식은 $2n$원 1차 연립 방정식이므로 $2n$개 출력 s를 알면 $A_0(x)$와 $P(x)$의 모든 계수를 풀이할 수 있다. 즉, ASR-2의 선형 복잡도는 n으로 갈로이 선형 궤환 시프트 레지스터 및 선형 궤환 시프트 레지스터와 동일하다.

ASR-D에서 출력 s_j와 $A_{j+1}(x)$의 계수는 Lemma 4.1의 순환행렬식에 의하여 다음과 같이 된다.

$$s_i=a_{i,n-1}$$
$$a_{i+1,j}=\sum_{k=0}^{n-1}m_{jk}\cdot a_{i,k}\quad \text{for } j\in\{0,1,2,\cdots,n-1\}$$

위 식은 미지수가 $m_{i,j}$와 $a_{0,i}$인 'n^2+n'원 1차 연립 방정식이다.

그러므로 $GF(2^n)$상의 ASR-D의 선형 복잡도 LC는 식 5와 같이 된다.

$$n\le LC\le\frac{n^2+n}{2} \tag{5}$$

VI. 결 론

본 논문에서는 의사난수발생기로 사용이 가능한 새로운 구조의 산술 시프트 레지스터(ASR, Arithmetic Shift Register)를 제안하였다. 산술 시프트 레지스터는 $GF(2^n)$상에서 0이 아닌 초기 값 A_0에 0 또는 1이 아닌 임의의 수 D를 연속적으로 곱하는 구조이며, 본 논문에서는 이를 ASR-D로 표현하였다.

갈로이 선형 궤환 시프트 레지스터는 ASR-2^{-1}로 표현할 수 있다. 그러므로 본 논문에서 제안한 산술 시프트 레지스터는 갈로이 선형 궤환 시프트 레지스터를 일반화한 것이다.

$GF(2^n)$상에서 0 또는 1이 아닌 임의 수 D에 대하여 '$D^k=1$'이 되는 t가 '$t=2^n-1$'로 유일하게 되는 비복원다항식이 ASR-D의 특성다항식이며, ASR-D의 주기는 '2^n-1'로 최대주기를 가진다.

$GF(2^{32})$상의 ASR-2를 32 비트 C 언어로 프로그램화하면 필요한 연산 수가 갈로이 선형 궤환 시프트 레지스터보다 33%, 피보나치 선형 궤환 시프트 레지스터보다 71% 적게 필요하므로 종래의 궤환 시프트 레지스터보다 효율적임을 알 수 있다.

한편 ASR-2를 하드웨어의 복잡도는 종래의 궤환 시프트 레지스터와 동일하다.

$GF(2^n)$상의 ASR-2의 선형복잡도는 n으로 종래의 궤환 시프트 레지스터와 동일하며, ASR-D의 선형복잡도는 '$n\le LC\le\frac{n^2+n}{2}$'으로 종래의 궤환 시프트 레지스터보다 높아서 안전도가 높다.

제안한 산술 시프트레지스터는 소프트웨어 및 하드웨어 구현이 용이하므로 암호, 오류수정부호, 몬테카를로 적분, 데이터통신 등 여러 분야에서 의사난수발생기로 폭 넓게 사용될 수 있다.

참 고 문 헌

[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(2m)," 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 Polynomials," 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/.

저 자 소 개

박 창 수 (정회원)

1995년 인제대학교 전자공학과 학사

2001년 부경대학교 컴퓨터공학과 석사

2004년 부경대학교 컴퓨터공학과 박사 수료

<주관심분야 : 반도체 회로설계, 암호 알고리즘, 컴퓨터 구조>

조 경 연 (정회원)

1990년 인하대학교 전자공학과 박사

1983년~1991년 삼보컴퓨터 기술연구소 책임연구원

1991년~2000년 삼보컴퓨터 기술연구소 기술고문

1998년~2003년 에이디칩스 기술고문

1991년~현재 부경대학교 공과대학 전자컴퓨터정보통신공학부 교수

<주관심분야 : 전산기구조, 반도체 회로설계, 암호 알고리즘>