새로운 자기 수축 발생기

최 세 아, 양 경 철

포항공과대학교 전자전기공학과

A New Class of Self-Shrinking Generators

Sea Che, Kyeongcheol Yang

Depart. of Electronic and Electrical Engineering, POSTECH

sea78@postech.ac.kr, kcyang@postech.ac.kr

요 약

자기 수축 발생기(self-shrinking generator)는 Meier와 Staffelbach에 의해 제안되었으며[4], 구조가 간단하고 키수열을 생성하는 속도가 빠르기 때문에 스트림 암호시스템으로 각광받고 있다 [5]. 본 논문에서는 자기 수축 발생기의 새로운 구성방법을 제안한다. 제안된 자기 수축 발생기는 하나의 선형귀환회로와 주어진 짝수 m에 의하여 정의되며 일반적으로 선형귀환회로의 귀환다항식으로 원시다항식을 사용한다. 이 경우 키수열은 균형성을 만족하며, 선형귀환회로의 귀환다항식의 차수를 d_Y라고 하면 주기는 $m2^{d_Y-2}$ 이다. m을 $2^{\eta}\zeta$로 표현하면 선형복잡도 L_Z는 $2^{d_Y+\eta-3} \le L_Z \le \frac{m}{2}(2^{d_Y-1}-(d_Y-2))$이다. 따라서 제안된 자기 수축 발생기는 기존의 자기 수축 발생기에 비하여 암호학적으로 우수한 성질을 갖는다.

I. 서론

스트림 암호시스템(stream cipher system)은 비밀키 암호시스템(secret-key cryptosystem)의 일종으로 많은 양의 데이터를 빠르게 암호화 할 수 있으며, 일반적으로 선형귀환회로(LFSR, linear feedback shift register)를 이용하여 키수열을 생성한다 [5], [6]. 스트림 암호시스템이 안전하기 위해서는 키수열의 주기가 길어야 하고, 선형복잡도(linear complexity)가 커야한다.

$A=\{a_i\}_{i=0}^{\infty}$를 이진수열(binary sequence)이라 정의하고, 임의의 정수 i에 대하여 $a_{i+P_A}=a_i$를 만족하는 최소의 양의 정수를 P_A라 한다면, P_A를 A의 주기라 한다. 한 주기 동안의 0의 수와 1의 수의 차이가 1 또는 그 이하이면 그 수열은 균

형성을 만족한다(balanced)고 한다.

쉬프트 연산자 x를 $xa_i \triangleq a_{i+1}$이라 정의하면, 이진 다항식 $f(x)=x^m+f_{m-1}x^{m-1}+\cdots+f_0$에 대해 다음과 같이 확장할 수 있다:

$$f(x)a_i \triangleq a_{i+m}+f_{m-1}a_{i+m-1}+\cdots+f_0a_i.$$

본 논문은 정보통신부의 경북대 ITRC가 지원하는 연구과제의 결과입니다.

A의 특성다항식(characteristic polynomial) $f_A(x)$는 임의의 i에 대해서 $f(x)a_i=0$ 를 만족하는 최소 차수의 다항식이고, $f_A(x)$의 차수(degree)를 수열 A의 선형복잡도(linear complexity 혹은 lin- ear span)라 한다.

임의의 수열 A에 대하여 $f_A(x)$의 차수를 d_A라 할 경우 $P_A=2^{d_A}-1$ 을 만족한다면, 수열 A를 최장주기 수열(maximal-length sequence or m- sequence)이라 한다. 최장주기 수열의 특성다항식이 원시다항식(primitive polynomial)이라는 것은 잘 알려진 사실이다 [3].

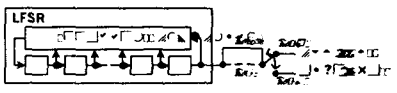

그림 1: 자기 수축 발생기

Meier와 Staffelbach에 의해 제안된 자기 수축 발생기는 Coppersmith 등이 제안한 수축발생기의 구조를 변형한 클럭제어발생기(clock-controlled generator)의 일종이다 [2], [4].

그림 1에서 보는 바와 같이 자기 수축 발생기의 키수열은 LFSR의 수열의 홀수 번째 비트가 1인 경우 그 다음 비트들로 구성된다. 즉,

$\hat{Y}=\{\hat{y}_i\}_{i=0}^{\infty}$을 LFSR의 수열이라 하고, w_j를 수열 $\{\hat{y}_{2i}\}_{i=0}^{\infty}$의 j번째 1의 위치라 할 경우 키수열 $\hat{Z}=\{\hat{z}_j\}_{i=0}^{\infty}$는 $\hat{z}_j=\hat{y}_{2w_j+1}$로 정의된다 [4].

자기 수축 발생기는 한 비트의 키수열을 생성하기 위해서 평균적으로 네게의 클록 펄스를 필요로 한다. 일반적으로 자기 수축 발생기에서 LFSR의 수열로 최장주기 수열을 사용하는데, 이 경우에 키수열은 균형성을 만족한다. $d_{\hat{Y}}$를 LFSR의 귀환다항식의 차수라 할 때, 키수열 $\hat{Z}$의 주기 $P_{\hat{Z}}$는 $2^{\cdot d_{\hat{Y}}/2\cdot}\le P_{\hat{Z}}\le 2^{d_{\hat{Y}}-1}$이다. 또한 키수열의 선형복잡도 $L_{\hat{Z}}$는 $2^{\cdot d_{\hat{Y}}/2\cdot}\le L_{\hat{Z}}\le 2^{d_{\hat{Y}}-1}-(d_{\hat{Y}}-2)$이다 [4].

본 논문에서는 기존의 자기 수축 발생기의 구조를 변형시킨 새로운 자기 수축 발생기를 제안한다. 새로운 자기 수축 발생기는 키수열의 선택방법을 제외하면 기존의 자기 수축 발생기와 같은 구조를 갖는다. 일반적으로 키수열은 균형성을 만족하며, 기존의 자기 수축 발생기의 키수열에 비하여 더 큰 주기와 더 큰 선형복잡도를 갖는다.

본 논문의 구조는 다음과 같다. II장에서는 새로운 자기 수축 발생기의 구성방법과 키수열의 균형성 및 주기를 보인다. III장에서는 키수열의 선형복잡도와 그에 따른 전산실험 결과를 나타낸다. IV장에서는 결론을 도출한다.

II. 새로운 자기 수축 발생기

새로운 자기 수축 발생기는 기존의 자기 수축 발생기와 마찬가지로 한 개의 LFSR만을 사용한다. LFSR의 수열을 $Y=\{y_i\}_{i=0}^{\infty}$라하고 키수열을 $Z=\{z_i\}_{i=0}^{\infty}$라 하자. 임의의 짝수 m과 $0\le k<m/2$에 대하여, w_j를 수열 $\{y_{mi}\}_{i=0}^{\infty}$의 j번째 1의 위치라 하면 $z_{\frac{m}{2}j+k}=y_{mw_j+2k+1}+y_{mw_j+2k+2}$로 표현된다.

$Y=\{y_i\}_{i=0}^{\infty}$를 차수가 d_Y인 최장주기 수열이라 하고, P_Y를 Y의 주기라고 한다. Y의 $(m+1)$개의 연속적인 비트들로 구성된 벡터 $(y_0,y_1,\cdots,y_m)$, $(y_m,y_{m+1},\cdots,y_{2m})$, …들을 고려한다면, 주어진 짝수 m과 모든 $i\ge 0$에 대하여 벡터 $(y_{mi},y_{mi+1},\cdots,y_{m(i+1)})$는 $m(2^{d_Y}-1)$후에 반드시 반복된다. 따라서 키수열은 주기적인 수열임을 쉽게 알 수 있다.

정리 1 Y를 제안된 자기 수축 발생기의 LFSR의 수열로서 차수가 d_Y인 최장주기 수열이라 하자. 만약 m이 짝수로서 $m<d_Y$이고 $(m,2^{d_Y}-1)=1$이면, 키수열 Z는 균형성을 만족한다.

증명) 최장주기 수열의 특성에 의하여, 한 주기 동안 길이가 $(m+1)(\le d_Y)$인 모두 0이 아닌 모든 벡터는 정확하게 2^{d_Y-m-1}번씩 나타난다. 함수 $\Phi: F_2^m\to F_2^{\frac{m}{2}}$를

$$\Phi(y_{mi+1},y_{mi+2},\cdots,y_{m(i+1)})=(y_{mi+1}+y_{mi+2},\cdots,y_{m(i+1)-1}+y_{m(i+1)})$$

로 정의하면, 함수 Φ는 전사함수이고, $2^{\frac{m}{2}}$개의 F_2^m의 원소를 하나의 $F_2^{\frac{m}{2}}$의 원소에 대응시킨다. 키수열의 생성규칙에 의하여 $y_{mi}=1$일 때에만 키수열이 생성되므로, w_j를 수열 $\{y_{mi}\}_{i=0}^{\infty}$의 j번째 1의 위치라고 하면, 키수열

$$\begin{aligned}Z&=\{z_{\frac{m}{2}j},z_{\frac{m}{2}j+1},\cdots,z_{\frac{m}{2}(j+1)-1}\}_{j=0}^{\infty}\\&=\{y_{mw_j+1}+y_{mw_j+2},\cdots,y_{m(w_j+1)-1}+y_{m(w_j+1)}\}_{j=0}^{\infty}\\&=\{\Phi(y_{mw_j+1},y_{mw_j+2},\cdots,y_{m(w_j+1)})\}_{j=0}^{\infty}\end{aligned}$$

로 나타낼 수 있다. 따라서 Y의 m주기 동안 키수열에는 $F_2^{\frac{m}{2}}$이 모든 원소가 정확하게 $2^{d_Y-\frac{m}{2}-1}$번씩 나타난다. □

제안된 자기 수축 발생기의 키수열의 주기는 수축발생기에서의 주기의 증명방법과 비슷한 방법으로 증명할 수 있다.

정리 2 $Y=\{y_i\}_{i=0}^{\infty}$를 제안된 자기 수축 발생기의 LFSR의 수열로서 차수가 d_Y인 최장주기 수열이라 하자. 만약 m이 짝수로서 $(m,2^{d_Y}-1)=1$이면, 키수열 Z의 주기 P_Z는 $m2^{d_Y-2}$이다.

증명) $B=\{y_{2i+1}+y_{2i+2}\}_{i=0}^{\infty}$와 $C=(y_0,\cdots,y_0,y_m,\cdots,y_m,y_{2m}\cdots)$라 정의하자. 여기서 수열 C는 y_{mi}를 $\frac{m}{2}$번씩 반복하여 얻는다. 그러면 B의 주기 P_B는 $2^{d_Y}-1$이고, C의 주기 P_C는 $\frac{m}{2}(2^{d_Y}-1)$이다. [2]의 정리 1에 의하여, 키수열의 주기는 $\mathrm{lcm}\,(2^{d_Y-1},m2^{d_Y-2})$임을 알 수 있다. □

III. 새로운 자기 수축 발생기의 선형복잡도

스트림 암호시스템이 안정적이기 위해서는 키수열의 선형복잡도가 커야한다. 키수열의 선형복잡도를 증명하기 위하여 다음의 보조정리가 필요

하다.

보조정리 3 ([1]) d_V를 임의의 양의 정수, $\alpha \in F_{2^{d_V}}$를 원시원(primitive element), $T: F_{2^{d_V}} \rightarrow F_2$를 F_2-선형사상이라 하자. 수열 $\{a^i\}_{i=0}^{\infty}$에서 $T(x)=1$을 만족하는 $(i+1)$번째 원소를 v_i라 하자. 그러면 수열 $V=\{v_i\}_{i=0}^{\infty}$는 $F_{2^{d_V}}$상의 수열로서 주기가 2^{d_V-1}이며, 선형복잡도는 기껏해야 $2^{d_V-1}-(d_V-2)$ 이하이다. 특히,

$$\sum_{i=0}^{2^{d_V-1}-(d_V-2)} \binom{2^{d_V-1}-(d_V-2)}{i} v_{i+e}=0$$

을 만족한다.

정리 4 $Y=\{y_i\}_{i=0}^{\infty}$를 제안된 자기 수축 발생기의 LFSR의 수열로서 차수가 d_Y인 최장주기 수열이라 하자. 만약 임의의 정수 η와 임의의 홀수 ζ에 대하여 $m=2^{\eta}\zeta$이고, $(m, 2^{d_Y}-1)=1$이라면, 키수열의 선형복잡도 L_Z는

$$2^{d_Y+\eta-3} < L_Z \leq \frac{m}{2}(2^{d_Y-1}-(d_Y-2))$$

이다.

증명) 정리 2에 의하여 키수열 Z의 주기 $P_Z = m2^{d_Y-2}$이고, 특성다항식을 $f_Z(x)$라 했을 때, $f_Z(x) \mid x^{P_Z}-1$ 이다.

(하한) F_2상에서 $f_Z(x) \mid (x^{\zeta}+1)^{2^{d_Y+\eta-2}}$이다. 임의의 기약다항식 $p_i(x)$ $(1 \leq i \leq q,\ p_1(x)=x+1)$에 대하여 $(x^{\zeta}+1)=p_1(x)p_2(x)\cdots p_q(x)$라 하면, $0 \leq l_i \leq 2^{d_Y+\eta-2}$ $(0 \leq i \leq q)$에 대하여

$$f_Z(x)=\prod_{i=1}^{q} p_i(x)^{l_i}$$

로 나타낼 수 있다. $l \triangleq \max_{0 \leq i \leq q} l_i$라 정의한다. 만약 $l \leq 2^{d_Y+\eta-3}$이면 키수열의 주기는 $m2^{d_Y-2}$보다 작은 값을 갖게 되므로 모순이다. 따라서 키수열의 선형복잡도 L_Z는 $L_Z > 2^{d_Y+\eta-3}$이다.

(상한) α를 $F_{2^{d_V}}$의 원시원이라 하고, $\gamma \in F_{2^{d_V}}$를 $x_i=\mathrm{Tr}(\gamma\alpha^i)$를 만족하는 원소로 두자. $T(x)=\mathrm{Tr}(\gamma(\alpha+\alpha^2)x)$라 정의하면 보조정리 3에 의하여 상한을 증명 할 수 있다. □

표 1에 기존의 자기 수축 발생기의 주기와 선형복잡도를 나타내었으며, 제안된 자기 수축 발생기의 m에 따른 주기와 선형복잡도를 표 2~5에 나타내었다. 제안된 자기 수축 발생기는 $m=2$인 경우에 기존의 자기 수축 발생기와 같은 범위의 주기와 선형복잡도를 가지며, $m>2$인 경우에는 기존의 자기 수축 발생기에 비하여 더욱 좋은 암호학적 성질을 만족함을 확인 할 수 있다. 또한, 전산 실험 결과 선형복잡도의 하한은 정리 4에서 구한 값보다 더욱 큰 값을 가짐을 알 수 있다. 따라서 하한 경계를 개선하기 위하여 더욱 연구할 필요가 있다.

LFSR의 차수	주기	선형복잡도
2	2	2
3	2~4	2~3
4	8	5
5	16	10~13
6	32	25~28
7	64	54~59
8	128	118~122
9	256	243~249
10	512	498~504
11	1024	1009~1015
12	2048	2031~2038
13	4096	4072~4085
14	8192	8170~8180

표 1: 기존의 자기 수축 발생기의 주기 및 선형복잡도

LFSR의 차수	주기	선형복잡도
2	1	1
3	2~4	2~3
4	8	6
5	16	11~13
6	32	27~28
7	64	58~59
8	128	117~122
9	256	240~249
10	512	498~504
11	1024	1009~1015
12	2048	2030~2038
13	4096	4076~4085
14	8192	8169~8180

표 2: $m=2$일 때 제안된 자기 수축 발생기의 주기 및 선형복잡도

LFSR의 차수	주기	선형복잡도
2	4	4
3	8	6
4	16	10~11
5	32	25~26
6	64	55~56
7	128	113~118
8	256	234~244
9	512	494~498
10	1024	1008
11	2048	2020~2030
12	4096	4069~4076
13	8192	8164~8170
14	16384	16349~16360

표 3: $m=4$일 때 제안된 자기 수축 발생기의 주기 및 선형복잡도

LFSR의 차수	주기	선형복잡도
2	3	2
3	12	8
4	3~12	3~12
5	48	37~79
6	36	31~33
7	192	171~177
8	120~144	108~138
9	768	738~747
10	480~528	461~516
11	3072	3027~3045
12	2016~2112	1987~2100
13	12288	12243~12255

표 4: $m=6$일 때 제안된 자기 수축 발생기의 주기 및 선형복잡도

LFSR의 차수	주기	선형복잡도
2	8	8
3	16	11~12
4	32	23~24
5	64	50~52
6	128	108~112
7	256	226~236
8	120~144	108~138
9	1024	992~996
10	2048	2011~2016
11	4096	4055~4060
12	8191	8146~8152
13	16384	16329~16340

표 5: $m=8$일 때 제안된 자기 수축 발생기의 주기 및 선형복잡도

IV. 결론

자기 수축 발생기의 새로운 구성방법을 제안하고, 기존의 자기 수축 발생기보다 더욱 좋은 암호학적 성질을 가짐을 보였다. 모든 경우에 대하여, 제안된 자기 수축 발생기의 키수열은 기존의 자기 수축 발생기의 키수열보다 더 큰 주기와 더 큰 선형복잡도를 가진다.

참고문헌

[1] S. R. Blackburn, "The linear complexity of the self-shrinking genrator," *IEEE Trans. on Inform. Theory*, IT-45, no. 6, pp. 2073-2077, Sep. 1999.

[2] D. Coppersmith, H, Krawczk, and Y. Mansour, "The shrinknig genrator," *Advanced in Cryptology-CRYPTO'93*, LNCS, vol.773, pp. 22-39, 1993.

[3] S. W. Golomb, *Shift Resister Sequences*, Aegean Park Press, 1982.

[4] W. Meier and O. Staffelbach, *"The self-shrinking generator,"* Advanced in Cryptology-EURPCRYPT'94, LNCS, vol. 950, pp. 205-214, 1995.

[5] A. J. Menezes, P. C. Oorshot, S. A. Vanstone, *Handbok of Applied Cryptography*, CRC Press, 1997.

[6] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.