JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 5 : 1104~1109 May. 2015

클럭 조절 방식의 임계 클럭 조절형 LM-128 이진 수열 발생기 제안

조정복*

A proposal of binary sequence generator, Threshold Clock-Controlled LM-128

Jung-bok Jo*

Division of Computer Engineering, Dongseo University, Pusan 617-716, Korea

요 약

디지털 콘텐츠의 급속한 발전으로 미래의 요구에 부합할 수 있는 고속의 보안 암호 알고리즘 설계는 중요하다. 본 논문에서는 기존의 수열 발생기 보다 더 높은 처리율을 갖는 자체 수축형 LM-128 합산 수열 발생기를 제안한다. 임계 클럭 조절형 LM-128의 설계하고 구현하여 더 낮은 클럭 사이클을 가져서 더 높은 키 수열 발생 속도를 증명한다. 제안된 임계 클럭 조절형 발생기는 128비트 비밀 키와 초기 벡터를 갖는 내부 상태 256비트로 구성되어진다. 128-비트의 보안 수준의 암호는 고화질 및 고품질의 디지털 콘텐츠 보안에 적합하다.

ABSTRACT

Due to the rapid growth in digital contents, it is important for us to design a high speed and secure encryption algorithm which is able to comply with the existing and future needs. This paper proposes an alternative approach for self-decimated LM-128 summation sequence generator, which will generate a higher throughput if compared to the conventional generator. We design and implement a threshold clock-controlled LM-128 and prove that it has a lower clock cycle and hence giving a higher key stream generation speed. The proposed threshold clock-control LM-128 generator consists of 256 bits inner state with 128 bits secret key and initialization vector. The cipher achieves a security level of 128 bits to be adapted to the digital contents security with high definition and high quality.

키워드 : 키수열, 이진수열, 클럭 조절, LM-128

Key word : keystream, binary sequence, clock-control, LM-128

Received 27 April 2015, **Revised** 30 April 2015, **Accepted** 08 May 2015

* **Corresponding Author** Jung-bok Jo(E-mail:jobok@gdsu.dongseo.ac.kr, Tel:+82-51-320-1720)
Division of Computer Engineering, Dongseo University, Pusan 617-716, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.5.1104 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 통신망의 급격한 발전과 더불어 디지털 콘텐츠 데이터가 고화질/고용량의 멀티미디어 자료 형태로 변모해가고 있으며, 이에 따라 암호 알고리즘도 고비도, 고속화 및 고신뢰도 설계가 요구된다.

선형 귀환 이동 레지스터(Linear Feedback Shift Registers:LFSR)는 하드웨어와 소프트웨어에 적합하며 빠른 암호율과 복호율이 허용되어 일반적으로 스트림 암호에 사용된다. 또한, LFSR에 의해 주 귀환 다항식은 큰 주기 및 우수한 통계적 특성을 가지며 연속적으로 생성된다[1].

일반적으로 선형성은 취약점 회피와 LFSR에 계산된 수열 특성을 이용하기 위해 수열 발생기의 구성 요소로 LFSR을 사용하고, 비선형성은 조합함수, 필터링 함수로 비선형 부울 함수를 사용하여 양쪽 모두 불규칙한 주기 LFSRs를 사용한다[2,3]. 또한 클럭 조절형을 사용하여 비선형성을 높일 수 있다[4,5].

자체 수축형(Self_Decimation) LM-128[6]은 LFSR에 자기 클럭 조절형 구조(Self_Decimated clock control Structure)가 추가 되었으며, 2개의 비트 메모리를 가지고 있는 합산 수열 발생기[7]를 기초로 한 발생기이다.

본 논문에서 제안된 임계 클럭 조절형(Threshold clock-controlled) LM-128은 클럭 조절형 알고리즘인 자체 수축형 LM-128에서 클럭의 최대 주기를 최소화시켜 키의 발생 속도를 향상 시켰으며 출력되는 키 수열에 비선형성을 증가시켜 상관 공격[8] 등의 암호 해독을 어렵게 하였으며, 소프트웨어적으로 키 수열의 생성시간을 단축시키는데 목적이 있다.

Ⅱ. 키 수열 발생기

2.1. 합산 수열 발생기

일반적으로 지칭하는 합산 수열 발생기(r=2)는 그림 1과 같이 2개의 LFSR과 1개 비트의 메모리에 기초를 두는 합산 수열 발생기이다. 그림 2의 LM 합산 수열 발생기[9]는 2개의 비트 메모리를 가지고 있으며 여기서 두 개의 LFSR을 L_a와 L_b로 표시하고 각각의 메모리 비트는 C, D로 시간을 j라 할 때 A_j와 B_j는 각각 L_a와 L_b의 출력이며 캐리(carry) C_j는 f_c에 의해 결정되고, D_j는 f_d에 의해 결정 된다. 출력 함수 f_z는 키 수열 비트와 z_j로 나타내어지며 출력 함수를 f_c, f_d, f_z로 정의하면 다음과 같다.

$$f_c = C_j = A_jB_j \oplus (A_j \oplus B_j)C_{j-1} \quad (1)$$

$$f_d = D_j = B_j \oplus (A_j \oplus B_j)C_{j-1} \quad (2)$$

$$f_z = Z_j = A_j \oplus B_j \oplus C_{j-1} \oplus D_{j-1} \quad (3)$$

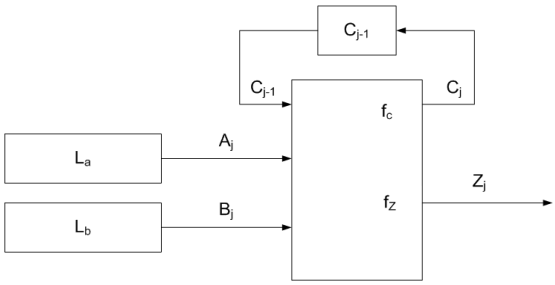


그림 1. 합산 수열 발생기(r=2)
Fig. 1 Summation generator (r=2)

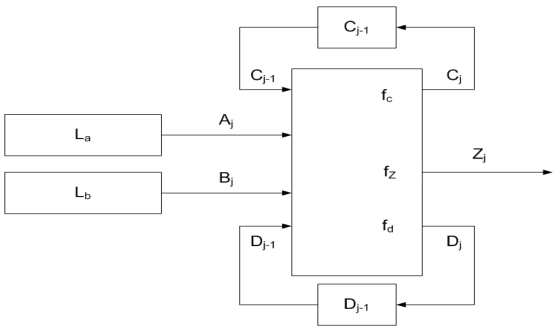


그림 2. LM 합산 수열 발생기
Fig. 2 LM summation generator

2.2. 자체 수축형 LM-128 합산 수열 발생기

자체 수축형 LM-128 합산 수열 발생기는 자기 클럭 조절 구조가 추가된 합산 수열 발생기 계열이며, 그림 3과 같다. 그림에서 키 수열 발생기는 두 개의 LFSR로 구성되며, 다음 메모리 상태와 키 수열 비트를 생성하기 LFSR의 출력 비트는 결합 함수 f_z, 캐리 함수 f_c 및 메모리 함수 f_d에 각각 입력된다. LFSR 에는 불규칙한 클럭이 공급되며, 하나의 LFSR에 공급되는 불규칙한 클럭수는 자신의 LFSR에서 생성된 비선형 필터함수(f_a 또는 f_b)로부터 얻어진다.

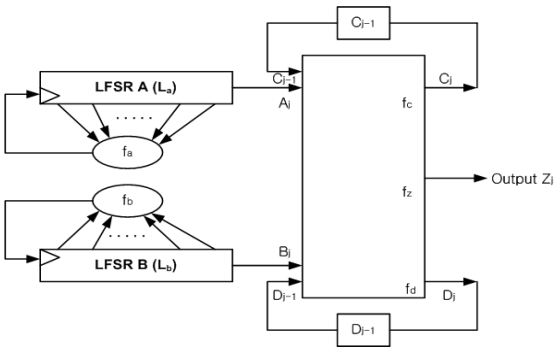


그림 3. 자체 수축형 LM 수열 발생기
Fig. 3 Self_Decimated LM generator

캐리 상태 C_j는 f_c에 의해, 메모리 상태 D_j는 f_d에 의해 정의된다. 클럭 조절 함수 f_a와 f_b는 두 LFSR의 현 상태에 의해 얻어지며, LFSR은 랜덤하게 클럭 조절된 후 캐리, 메모리 및 키 수열 출력을 생성한다. 자체 수축형 LM-128은 처음 초기화 과정에서 키(k)와 초기값(iv)로부터 내부 상태가 채워지며, 내부 상태 길이가 키 길이보다 더 길기 때문에 내부 상태를 채우기 위한 키 확장 과정이 요구된다.

2.2.1. 키 수열 발생

자체 수축형 LM-128 합산 수열 발생기는 두개의 클럭 조절형 LFSR과 캐리 및 메모리 비트를 가지며, LFSR의 길이는 각각 127비트와 129비트 이다. 모든 메모리 비트들은 자체 수축형 LM-128에게 256비트의 내부 상태 비트를 제공하며, 128비트 키와 128비트 초기화 벡터에 의하여 내부 상태가 채워진다.

자체 수축형 LM-128 합산 수열 발생기의 출력 키 수열은 LFSR 수열과 캐리 및 메모리 수열이 합쳐져서 생성된다. 자체 수축형 LM-128의 LFSR은 모든 비트가 "0"인 상태로 초기화되는 것을 허용하지 않는다.

출력 키 수열 비트 Z_j, 캐리비트 C_j, 메모리 비트 D_j는 구조상 LM 합산 수열 발생기와 동일한 형태(식 (1)~(3))를 취하지만, 출력 수열의 비도 수준이 크게 개선된다.

2.2.2. 클럭제어

자체 수축형 LM-128은 자신의 LFSR의 주기를 제어하여 각각의 레지스터에 불규칙한 주기 LFSR을 발생하는데 두 단의 범위{1...4}값을 계산하기 위하여 L_a로부터 두 단의 값을 받아서 f_a의 계산에 의해 L_a의 주기[1-4]를 선택하는 값을 가지게 된다. 유사하게 L_b의 두 단 값을 받아서 L_b의 주기를 준다. 주기는 제어함수 f_a와 f_b에 의해 얻는다.

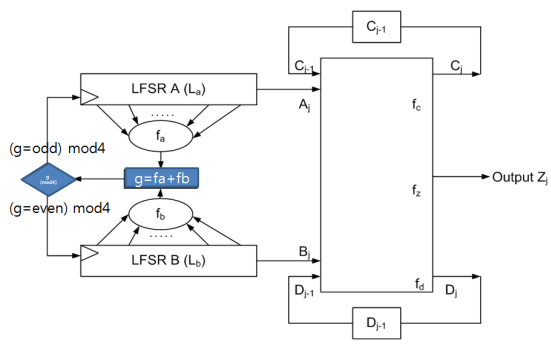
$$f_a(L_a) = 2L_{a.42}(t) + L_{a.85}(t) + 1 \quad (4)$$

$$f_b(L_b) = 2L_{b.43}(t) + L_{b.86}(t) + 1 \quad (5)$$

이 설계는 클럭 조절형 LM 계열에 적용되며, 키 수열 발생기는 일반형에서 LFSR의 개수 n=2를 선택하여 LFSR에 L_i의 주기는 L_{i+1} 또는 L_1부터 L_n까지의 주기가 사용된다.

2.3. 임계 클럭 조절형 LM-128

임계 클럭 조절형 LM-128 발생기는 클럭 조절 구조가 추가된 합산 수열 발생기 계열이며, 최대 클럭 주기를 최소화 시킨 합산 수열 발생기이며 그림 4와 같다.



(a)

f_a	f_b	g	g_a	g_b
1	1	2	1	2
1	2	3	3	1
1	3	4	1	4
1	4	5	1	1
..	..	..	..	..
4	1	5	1	1
4	2	6	1	2
4	3	7	3	1
4	4	8	1	4

(b)

그림 4. Threshold clock-controlled LM-128 (a) Sequence generator (b) Clock-Controller
Fig. 4 Threshold clock-controlled LM-128 (a) Sequence generator (b) Clock-Controller

그림에서 키 수열 발생기는 두 개의 LFSR로 구성되며, 다음 메모리 상태와 키 비트 수열을 생성하기 LFSR의출력 비트는 결합 함수 f_z, 캐리 함수 f_c 및 메모리 함수 f_d에 각각 입력된다. LFSR에는 불규칙한 클럭이 공급되며, 하나의 LFSR에 공급되는 불규칙한 클럭수는 두개의 LFSR에서 생성된 비선형 필터함수(g)로부터 얻어진다. 이 때 클럭 조절의 방법은 $g=(f_a+f_b)$mod4로 발생된 클럭 수만큼 홀수(odd)일 때는 위쪽 L_a 레지스터를 작동하고, 짝수(even)일 때는 아래쪽 L_b 레지스터를 작동하게 된다.

캐리 상태 C_j는 f_c에 의해, 메모리 상태 D_j는 f_d에 의해 정의된다. 클럭 조절 함수 g는 두 LFSR의 현 상태에 의해 얻어지며, LFSR은 랜덤하게 클럭 조절된 후 캐리, 메모리 및 키 수열 출력을 생성한다. 임계 클럭 조절형 LM-128은 처음 초기화 과정에서 키(k)와 초기값(iv)로부터 내부 상태가 채워지며, 내부 상태 길이가 키 길이보다 더 길기 때문에 내부 상태를 채우기 위한 키 확장 과정이 요구된다.

2.3.1. 키 수열 발생

임계 클럭 조절형 LM-128 합산 수열 발생기는 두 개의 클럭 조절형 LFSR과 캐리 및 메모리 비트를 가지며, LFSR의 길이는 각각 127비트와 129비트 이다. 모든 메모리 비트들은 임계 클럭 조절형 LM-128에게 256비트의 내부 상태 비트를 제공하며, 128비트 키와 128비트 초기화 벡터에 의하여 내부 상태가 채워진다. 임계 클럭 조절형 LM-128 합산 수열 발생기의 출력 키 수열은 LFSR 수열과 캐리 및 메모리 수열이 합쳐져서 생성된다. 임계 클럭 조절형 LM-128의 LFSR은 모든 비트가 “0”인 상태(all zero state)로 초기화되는 것을 허용하지 않는다. 출력 키 수열 비트 Z_j, 캐리비트 C_j, 메모리 비트 D_j는 구조상 LM 합산 수열 발생기와 동일한 형태(식 (1)~(3))를 취하지만, 출력 수열의 비도 수준이 크게 개선된다.

2.3.2. 클럭 제어

임계 클럭 조절형 LM-128은 각 탭 L_a와 L_b의 값으로부터 g값을 구한 후 g값이 5이상이면 g값에서 4만큼의 수를 차감한 값의 수만큼 LFSR A의 클럭을 1~4회 귀환이동하고, 4미만이면 g값만큼 LFSR B를 1~4의 클럭 수만큼 귀환 이동하며, 나머지 선택에서 제외된 LFSR은 1회 클럭 이동하게 된다. 주기는 제어함수 f_a, f_b, g 그리고 g_a 및 g_b를 다음 수식과 같이 얻는다. f_a 와 f_b는 수식(4)~(5)와 같은 함수를 사용한다.

$$\begin{aligned} g &= f_a + f_b \\ g_a &= g \bmod 4 \quad (\text{if } g:\text{odd}) \\ g_b &= g \bmod 4 \quad (\text{if } g:\text{even}) \end{aligned} \tag{6}$$

이 설계는 클럭 조절형 LM 계열에 적용되며, 키 수열 발생기는 일반형에서 LFSR의 개수 n=2를 선택하여 LFSR에 L_i의 주기는 L_{i+1} 또는 L_1부터 L_n까지의 주기가 사용된다.

Ⅲ. 시뮬레이션 및 결과

임계 클럭 조절형 LM-128 키 수열 발생기를 이용하여 연속되는 출력 데이터 16만 비트씩 샘플 값을 출력한 후 빈도 검증(Frequency test), 계열 검증(Serial test), 일반화 계열검증(Generalized serial test), 포커 검증(Poker test) 및 자기상관성 검증(Autocorrelation test) [10]등의 랜덤 검증 및 선형 복잡도(Linear Complexity: LC), 주기 (Period: P) 등의 시험검증을 실시하였다.

각각의 선택된 검증 항목을 시험하여 모든 항목 검증 결과가 기준 이내에서 표 1 및 표2와 같이 양호한 출력을 얻을 수 있음을 확인하였다. (표에서 시험 결과 값은 판정치의 범위 이내에 포함되면 각 항목별 랜덤성이 양호함)

표 1. 자체 수축형 LM-128 랜덤성 검증 결과
Table. 1 Rendomness test for Self_Decimated LM-128

Test Item	Criterion	Result 1	Result 2
Frequency test	3.841	0.692	0.117
Serial test	5.991	0.803	0.547
Generalized serial test			
t=3	9.488	4.927	0.688
t=4	15.507	9.876	4.427
t=5	26.296	16.294	10.519
Poker test			
m=3	14.067	3.680	2.070
m=4	24.996	20.633	10.833
m=5	44.654	18.087	28.742
Autocorrelation test	max ≤0.05	0.007	0.007

표 2. 임계 클럭 조절형 LM-128 랜덤 테스트 결과
Table. 2 Randomness test for Threshold clock-controlled LM-128

Test Item	Criterion	Result 1	Result 2
Frequency test	3.841	0.482	0.245
Serial test	5.991	2.634	0.258
Generalized serial test			
t=3	9.488	2.949	5.848
t=4	15.507	6.278	13.263
t=5	26.296	18.137	16.311
Poker test			
m=3	14.067	3.800	9.554
m=4	24.996	7.937	14.885
m=5	44.654	42.692	28.596
Autocorrelation test	max ≤0.05	0.004	0.003

정리 1. 선형 복잡도 LC와 주기 P는 아래와 같다.

$$LC \geq 2^{4.6} \times 2^{\lceil (m-11)/2 \rceil} \quad (7)$$

$$P \geq 2^{4.6} \times 2^{\lceil (m-11)/2 \rceil} \quad (8)$$

보조정리 1. 자체 수축형 LM-128과 임계 클럭 조절형 LM-128의 선형 복잡도 LC 및 주기 P는 다음과 같다.

$$LC \geq 2^{4.6} \times 2^{\lceil (256-11)/2 \rceil} = 2^{4.6} \times 2^{123} \approx 2^{128} \quad (9)$$

$$P \geq 2^{4.6} \times 2^{\lceil (256-11)/2 \rceil} = 2^{4.6} \times 2^{123} \approx 2^{128} \quad (10)$$

자체 수축형 LM-128과 임계 클럭 조절형 LM-128 알고리즘에 대해 5회씩 156,000개의 키수열을 생성시켰으며, 각각의 시간에 대해 평균값을 표 3과 같이 생성됨을 알 수 있었다.

표 3. 키 수열 생성 시간 분석
Table. 3 Keystream generation performances in second

Keystream generator	Generated time
Self_Decimated LM-128	0.73375sec
Threshold_clock-controlled LM-128	0.49180sec

[주] 테스트환경 : CPU = 셀러론 2.4Ghz, RAM = 512MB

자체 수축형 LM-128과 임계 클럭 조절형 LM-128 알고리즘은 랜덤성이 양호할 뿐만 아니라 주기, 선형 복잡도 등 암호 안정성이 좋다는 것을 확인 할 수 있었다. 임계 클럭 조절형 LM-128의 경우에는 클럭주기의 향상으로 인해 자체 수축형 LM-128 보다 소프트웨어적으로 30%가량 생성시간이 향상되었음을 확인할 수 있었다.

Ⅳ. 결 론

본 논문에서는 LM-128 발생기를 개선하여 콘텐츠 보호에 적합한 구조로 기존의 클럭 조절 구조의 효율성을 높이는 임계 클럭 조절형 LM-128을 제시하였고, 기존의 자체 수축형 LM-128과 비교하기 위하여 랜덤성 시험, 주기 및 LC와 같은 비도(안전성) 요소에 대한 안전성 검증을 실시하였다. 검증 결과 임계 클럭 조절형 LM-128은 랜덤성이 양호 할뿐 아니라 암호 안정성 요소인 주기와 LC 값이 2^{128}(현재 수준의 최소 기준인 2^{80}을 크게 초과)으로 크게 개선된 알고리즘이며, 고화질/고용량의 콘텐츠 보호에 많은 응용이 예상될 수 있다.

REFERENCES

[1] J. Massey. "Shift-Register Synthesis and BCH Decoding," I*EEE Transactions on Information Theory*, IT-15, no. 1, pp. 122-127, Jan. 1969.

[2] C. Paar, J. Pelzl, “Stream Ciphers”, Chapter 2 of *Understanding Cryptography, A Textbook for Students and Practitioners*.(companion web site contains online cryptography course that covers stream ciphers and LFSR), Springer, 2009.

[3] P. Kitsos, N. Sklavos, K. Papadomanolakis and O. Koufopavlou, “Hardware Implementation of Bluetooth Security”, *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 21-29, Jan.-Mar. 2003.

[4] V. S. Pendluri, P. Gupta, R. Majumdar, “Design and Implementation of Keystream Generator with Improved Security,” in *ICACT2011*, Gangwon-Do, pp. 1626-1631, 2011.

[5] P. Chandra, *Bulletproof Wireless Security - GSM, UTMS, 802.11 and Ad Hoc Security*, Elsevier, 2005.

[6] J. Kim, S. Cho, T. Kim and Hoonjae Lee, "A proposal of the Self_Decimated LM-128 Keystream Generator," in *Proceeding of the 21th KIPS Spring Conference*, Seoul, pp.

1011-1014, 2004.

[7] R. Rueppel, “Correlation Immunity and the Summation Generator,” *Advance in Cryptology -CRYPTO '85,* Lecture Notes in Computer Science, Vol. s18, pp. 260-272, Springer-Verlag, 1985.

[8] W. Meier and O. Staffelbach. "Correlation Properties of combiners with Memory in Stream Ciphers," *Advance in Cryptology -EUROCRYPT '90*, Lecture Notes in Computer Science, Vol. 473, pp. 204-312, Springer-Varlag, 1990.

[9] Hoonjae Lee, Sangjae Moon, “On an Improved Summation Generator with 2-Bit Memory,” *Signal Processing*, Vol. 80, no. 1. pp. 211-217, Jan. 2000.

[10] A. Menezes, *HandBook of Applied Cryptography*, CRC Press, 2001.

조정복(Jung-bok Jo)

1978년 경북대학교 전자계산기공학과 졸업
1986년 영남대학교 대학원 전자계산기전공 공학석사
1996년 동경도립과학기술대학 대학원 공학시스템전공 공학박사
현재 동서대학교 컴퓨터공학부 교수
※관심분야 : 퍼지시스템, 유전알고리즘 (본문과 같이)