디지털 콘텐츠 보호에 적합한 암호알고리즘 제안

조상일*, 이훈재**
*동서대학교 디자인&IT전문대학원
**동서대학교 컴퓨터정보학부
e-mail:i3011@hotmail.com

A proposal of the Encrytption algorithm for Digital Contents Security

Sang-Il Cho*, Hoon-Jae Lee**
*Graduate School of Design & IT, Dongseo University
**Div. of Computer & Information Eng., Dongseo University

요 약

최근의 통신망의 급격한 발전으로 디지털 콘텐츠 분야에서도 고화질/고용량으로 변모하고 있으며, 이러한 환경속에서 콘텐츠의 안전한 보호를 위한 고비도, 고속화 및 고신뢰도 암호 알고리즘의 설계가 요구되고 있다. 본 논문에서 제안된 Threshold clock-controlled LM은 클럭 조절형 암호 알고리즘의 클럭 최대 주기를 최소화시켜 키 수열의 발생 속도를 향상 시켰으며 128비트 키, 128 초기화 백터, 그리고 257 비트의 내부 상태를 가지며, 128-비트의 보안 레벨을 유지함으로써 안전성이 보장되어 고화질/고용량의 디지털 콘텐츠 보호에 적합함을 알 수 있다.

1. 서론

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 암호률과 복호률이 허용되어 일반적으로 스트림 암호에 사용된다. 또한, LFSR에 의해 주 귀환 다항식은 큰 주기 및 좋은 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.

Self_Decimated LM_128[3]은 LFSR에 자기 클럭 조절형 구조(Self_Decimated clock control Structure)가 추가 되었으며, 2개의 비트 메모리를 가지고 있는 합산 수열 발생기[2]를 기초로 한 발생기이다.

본 논문에서 제안된 Threshold clock-controlled LM type I은 클럭 조절형 알고리즘인 Self_Decimation LM_128에서 클럭의 최대 주기를 최소화시켜 키의 발생 속도를 향상 시켰으며 출력되는 키 수열에 비선형성을 증가시켜 상관 공격 등의 암호 해독을 어렵게 하였으며, 소프트웨어적으로 키 수열의 생성시간을 단축 시키는데 목적이 있다.

2. 키 수열 발생기

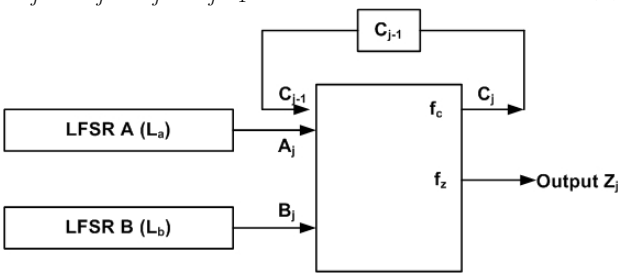
2.1 합산 수열 발생기

일반적으로 지칭하는 합산 수열 발생기(r=2)는 그림 1과 같이 2개의 LFSR과 1개 비트의 메모리에 기초를 두는 합산 수열 발생기이다. LM 합산 수열 발생기[4]는 2개의 비트 메모리를 가지고 있으며 여기서 두 개의 LFSR을 L_a와 L_b로 표시하고 각각의 메모리 비트는 C, D로 시간을 j라 할 때 Aj와 Bj는 각각 L_a와 Lb의 출력이며 캐리(carry) Cj는 fc에 의해 결정되고, Dj는 fd에 의해 결정 된다. 출력 함수

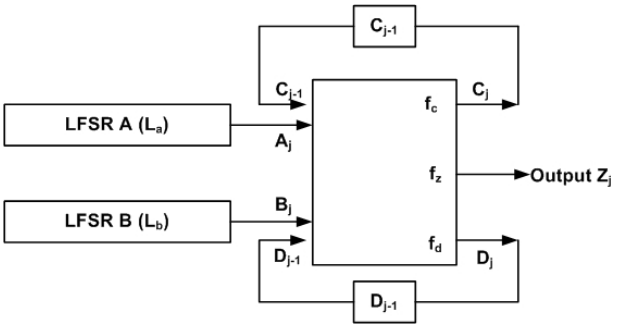
※본 연구는 정보통신부지원 대학 IT 연구센터 육성지원사업에 의하여 수행되었습니다.

fz는 키 수열 비트와 zj로 나타내어지며 출력 함수를 fc, fd, fz로 정의하면 다음과 같다.

$$C_j = A_j B_j \oplus (A_j \oplus B_j) C_{j-1} \quad (1)$$
$$D_j = B_j \oplus (A_j \oplus B_j) C_{j-1} \quad (2)$$
$$Z_j = A_j \oplus B_j \oplus C_{j-1} \quad (3)$$



(그림 1) 합산 수열 발생기(r=2)



(그림 2) LM 합산 수열 발생기

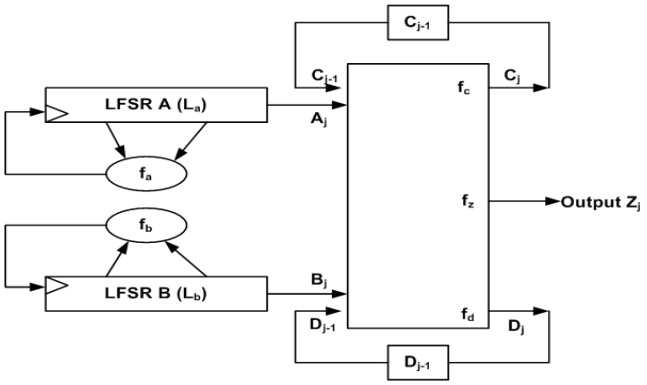
2.2 Self_Decimated LM_128 합산 수열 발생기

Self_Decimated 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.

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.

2.2.1 키 수열 발생

Self_Decimated LM_128 합산 수열 발생기는 두 개의 클럭 조절형 LFSR과 캐리 및 메모리 비트를 가지며, LFSR의 길이는 각각 127비트와 129비트 이다. 모든 메모리 비트들은 Self_Decimated LM_128에게 256비트의 내부 상태 비트를 제공하며, 128비트 키와 128비트 초기화 벡터에 의하여 내부 상태가 채워진다.



(그림 3) Self_Decimated LM_128 합산 수열 발생기

Self_Decimated LM_128 합산 수열 발생기의 출력 키 수열은 LFSR 수열과 캐리 및 메모리 수열이 합쳐져서 생성된다. Self_Decimated 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.

2.2.2 클럭제어

Self_Decimated 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.

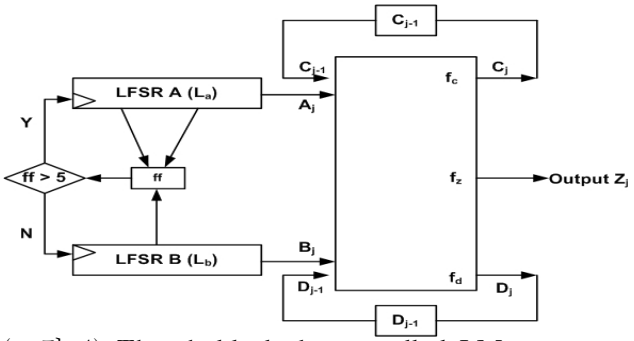
$$f_a(L_a) = 2L_a \cdot_{42}(t) + L_a \cdot_{85}(t) + 1 \quad (4)$$
$$f_b(L_b) = 2L_b \cdot_{43}(t) + L_b \cdot_{86}(t) + 1 \quad (5)$$

이 설계는 clock-controlled LM 계열에 적용되며, 키 수열 발생기는 n을 기초로 하는 LFSR에 L_i의 주기가 L_{i+1} 또는, L_1부터 L_n까지의 주기가 사용된다.

2.3 Threshold clock-controlled LM type I

Threshold clock-controlled LM type I 발생기는 클럭 조절 구조가 추가된 합산 수열 발생기 계열이며, 최대 클럭 주기를 최소화 시킨 합산 수열 발생

기이며 그림 4와 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. LFSR에는 불규칙한 클럭이 공급되며, 하나의 LFSR에 공급되는 불규칙한 클럭수는 두개의 LFSR에서 생성된 비선형 필터함수(ff)로부터 얻어진다.



(그림 4) Threshold clock-controlled LM

캐리 상태 C_j는 f_c에 의해, 메모리 상태 D_j는 f_d에 의해 정의된다. 클럭 조절 함수 ff는 두 LFSR의 현 상태에 의해 얻어지며, LFSR은 랜덤하게 클럭 조절된 후 캐리, 메모리 및 키 수열 출력을 생성한다.

2.3.1 키 수열 발생

Threshold clock-controlled LM 합산 수열 발생기는 두 개의 클럭 조절형 LFSR과 캐리 및 메모리 비트를 가지며, LFSR의 길이는 각각 127비트와 129비트 이다. 모든 메모리 비트들은 Threshold clock-controlled LM에게 256비트의 내부 상태 비트를 제공하며, 128비트 키와 128비트 초기화 벡터에 의하여 내부 상태가 채워진다. Threshold clock-controlled LM 합산 수열 발생기의 출력 키 수열은 LFSR 수열과 캐리 및 메모리 수열이 합쳐져서 생성된다. Threshold clock-controlled LM의 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 클럭제어

Threshold clock-controlled LM은 각 탭 L_a와 L_b의 값으로부터 ff값을 구한 후 ff값이 5이상이면 ff값에서 4만큼의 수를 차감한 값의 수만큼 LFSRa의 클럭을 1~4회 귀환이동하고, 4미만이면 ff값만큼 LFSRb를 1~4의 클럭 수 만큼 귀환 이동하며, 나머지 선택에서 제외된 LFSR은 1회 클럭 이동하게 된다. 주기는 ff는 식(6)에 의해 얻는다.

$$ff = 4L_b \cdot_{64}(t) + 2L_a \cdot_{42}(t) + L_a \cdot_{85}(t) + 1 \qquad (6)$$

이 설계는 clock-controlled LM 계열에 적용되며, 키 수열 발생기는 n을 기초로 하는 LFSR에 L_i의 주기가 L_{i+1} 또는, L_1부터 L_n까지의 주기가 사용된다.

3. 시뮬레이션 및 결과

Self_Decimated LM-128과 Threshold clock-controlled LM 키 수열 발생기를 이용하여 연속되는 출력 데이터 16만 비트씩 샘플 값을 출력한 후 Frequency test, Serial test, Generalized serial test, Poker test 및 Autocorrelation test[5]등의 랜덤 테스트와 Linear Complexity(LC), Period(P) 등의 테스트를 실시하였다.

<표 1> Self_Decimated LM_128 랜덤 테스트 결과

검증항목	판정치	결과1	결과2
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> Threshold clock-controlled LM 랜덤 테스트 결과

검증항목	판정치	결과1	결과2
Frequency test	3.841	1.774	0.309
Serial test	5.991	2.190	1.440
Generalized serial test			
t=3	9.488	2.995	2.995
t=4	15.507	8.484	5.186
t=5	26.296	17.153	13.329
Poker test			
m=3	14.067	1.285	9.110
m=4	24.996	19.647	10.280
m=5	44.654	35.287	41.525
Autocorrelation test	max≤0.05	0.007	0.006

각각의 선택된 검증 항목을 테스트하여 모든 항목

검증 결과가 기준 이내에서 표 1, 2와 같이 양호한 출력을 얻을 수 있음을 확인 하였다.

clock-controlled LM 계열의 키 수열 특성을 관측하기 위한 실험은 표 3과 같다. 짧은 길이에 대한 예제 각각은 서로 다른 길이의 두 LFSR을 가지며, 각각의 쌍에 대해서 서로 다른 귀환 다항식을 선택하였다. 실험에서 귀환 다항식 탭 위치 선택은 키 수열 특성에 큰 영향이 없었으며, LFSR 길이는 각각의 쌍에 대하여 50가지 랜덤 초기 상태로 시뮬레이션 하였다. 예를 들면, 레지스터 길이 9, 10을 선택할 경우 결과에 따른 선형복잡도는 400~822 사이로 다양하게 나타났으며, 최소 선형복잡도를 선택하였다. 표에서 얻어진 값들로부터 최소 선형복잡도와 주기의 방정식을 다음과 같이 구하였다.

<표 3> 키 수열의 특성

레지스터 길이	선형 복잡도	주기
5, 6	23	25
5, 7	50	50
6, 7	43	51
7, 8	93	101
7, 9	200	206
8, 9	200	200
9, 10	400	401
9, 11	804	810

레지스터 길이 n은 두 레지스터 길이의 합으로 표시할 때, 선형 복잡도(LC)의 하한경계 값은 $LC \geq 2^{4\times 6}\times 2^{(n-11)/2}$가 되며, 비슷한 방법으로 주기(P)는 $P \geq 2^{4\times 6}\times 2^{(n-11)/2}$로 표현된다.

따라서 clock-controlled LM 형태에 대한 (n-256) 선형 복잡도의 하한경계 값과 주기는 아래 식과 같다.

$$LC \geq 2^{4\times 6}\times 2^{\lceil (256\times 11)/2 \rceil} = 2^{4\times 6}\times 2^{123} \approx 2^{128} \quad (9)$$

$$P \geq 2^{4\times 6}\times 2^{\lceil (256\times 11)/2 \rceil} = 2^{4\times 6}\times 2^{123} \approx 2^{128} \quad (10)$$

clock-controlled LM 형태의 설계 기준강도는 2^{128}이며, 여러 가지 공격에 대하여 기본적인 키 수열 특성은 큰 선형복잡도 및 긴 주기 때문에 안전하게 된다.

clock-controlled LM 계열인 Self_Decimated LM-128과 Threshold clock-controlled LM 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

테스트환경 = CPU:셀러론 2.4Ghz, RAM : 512MB

키 수열 발생기	생성시간
Self_Decimated LM_128	0.73375sec
Threshold_clock-controlled LM type I	0.51380sec

Self_Decimated LM-128과 Threshold clock-controlled LM 알고리즘은 랜덤성이 양호할 뿐만 아니라 주기, 선형 복잡도, Linear Complexity 등 암호 안정성이 좋다는 것을 확인 할 수 있었다.

Threshold clock-controlled LM type I의 경우에는 클럭주기의 향상으로 인해 Self_Decimated LM_128 보다 소프트웨어적으로 30%가량 생성시간이 향상되었음을 확인할 수 있었다.

4. 결론

본 논문에서 우리는 클럭 조절 구조 및 2개의 비트 메모리 합산 수열 발생기를 기본 발생기로 하는 Threshold clock-controlled LM type I을 제시하였다.

Threshold clock-controlled type I은 랜덤성이 양호 할뿐 아니라 암호 안정성이 크게 개선된 알고리즘이며, 고화질/고용량의 콘텐츠 보호에 많은 응용이 예상될 수 있다.

참고문헌

[1] J. Massey. "Shift-Register Synthesis and BCH Decoding," IEEE Transactions on Information Theroy, IT-15, No. 1, pp 122-127, Jan. 1969.

[2] 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.

[3] 김정주, 조상일, 김태훈, 이훈재, "Self_Decimated LM_128 키 수열 발생기 제안," 제21회 한국정보처리학회 춘계학술발표대회, 제 11권, 제1호, pp. 1011-1014, 2004.

[4] Hoonjae Lee, Sangjae Moon, "On an Improved Summation Generator with 2-Bit Memory," Signal Processing, Vol. 80, No. 1. pp. 211-217, January 2000.

[5] A. Menezes, "HandBook of Applied Cryptography," CRC Press, 1997.