Self_Decimated LM-128 키 수열 발생기 제안

김정주*, 조상일*, 김태훈* 이훈재**
*동서대학교 소프트웨어전문대학원
**동서대학교 인터넷 공학부
e-mail:puhasupercd@hotmail.com,

A proposal of the Self_Decimated LM-128 Keystream Generator

Jung-Ju Kim*, Sang-Il Cho*, Tae-Hoon Kim*, Hoon-Jae Lee**
*Graduate School of software, Dong-Seo University
**School of Internet Engineering, Dong-Seo University

요 약

본 논문에서 제안된 Self_Decimated LM-128 키 수열 발생기(Keystream generator)는 2개의 비트 메모리 합산 수열발생기(summation generator)를 갖는 자체 클럭 조절형 키 수열 발생기(stream cipher)이다. Self_Decimated LM-128은 LM 계열에서 제시된 특수한 암호로 128비트 키와 128비트 초기 벡터 그리고 257 비트의 내부 상태를 가지며 128 비트의 보안 레벨을 유지한다. 알려진 보안 분석의 공격에 대비해서 2-비트 메모리를 이용한 합산 수열발생기와 자체 클럭 조절형 키 수열 발생기를 포함한다.

1. 서론

LFSR(Linear Feedback Shift Register)은 일반적으로 CRC(Cyclic Redundancy Codes), 확산대역 통신(spread spectrum communication), 통신 동기회로, 스크램블러(scrambler)등에 많이 이용되었다. 또한, 하드웨어와 소프트웨어로 구현이 용이하여 고속 암·복호가 요구되는 스트림 암호에서 많이 적용되고 있다. 하지만, LFSR은 그들의 선형성 때문에 출력 수열로부터 쉽게 예측(암호해독)이 가능하며, 길이 L인 LFSR은 2L 비트 출력으로부터 초기 값을 쉽게 유추할 수 있다[3].

일반적으로 스트림 암호에서는 LFSR이 지니는 선형성을 없애기 위해 합산 수열 발생기[5]를 키 수열 발생기로 사용하며, 1985년에 Rueppel에 의해 제시되었다. 합산 수열 발생기의 최하위 특정 비트(LBS, Least significant bit)는 키 수열을 형성하고 다른 비트들은 캐리(carry)비트들이며 메모리에 저장된다. 키 수열은 다음 비트 생성을 위해 결합함수(combining function)의 입력으로 사용되어진다.

본 논문에서 제안된 Self_Decimated LM-128은 자체 클럭 조절형 구조(Self_Decimated clock control Structure)가 추가되었으며, 2-비트 메모리로 출력 수열의 예측이 어렵게 되며, 자체 클럭 조절형 구조는 출력되는 키 수열의 비선형을 크게 증가시킨다.

2. Self_Decimated LM 발생기

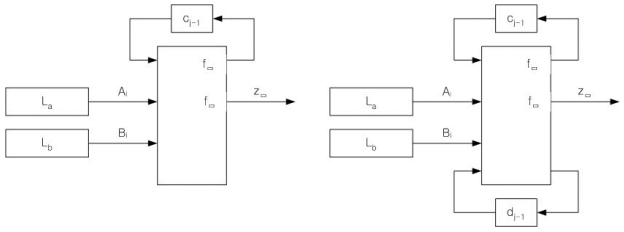
일반화된 합산 수열발생기는 그림 1과 같이 (n=2) 메모리 2개의 LFSR과 1개 비트의 메모리에 기초를 두는 합산 수열발생기이다. 여기서 두개의 LFSR을 L_a와 L_b로 표시하고 각각의 메모리 비트는 c로 시간을 j라 할 때 A_j와 B_j는 각각 L_a와 L_b의 출력이며 캐리(carry) c_j는 f_c에 의해 결정된다. 출력함수 f_z는 키 수열 비트 z_j로 나타내어지며, 출력함수를 f_c, f_d, f_z로 정의하면 다음과 같다.

$$c_j = f_c(A_j, B_j, c_j) = A_j B_j \oplus (A_j \oplus B_j) c_{j-1}$$

$$d_j = f_d(A_j, B_j, d_j) = B_j \oplus (A_j \oplus B_j) d_{j-1}$$

$$z_j = f_z(A_j, B_j, c_j, d_j) = A_j \oplus B_j \oplus c_{j-1} \oplus d_{j-1}$$

합산 수열발생기는 divide-and-conquer-attack에서 해독되며, 이는 Cryptanalysis of Summation Generator[1]에 기술되어있다. 그리고 고속상관공격은 Correlation Properties of Combiners with Memory in Stream Ciphers[4]와 Fast Correlation Attacks on the summation Generator[2]에 각각 설명되어 있다.



a) Summation Generator b) LM Generator

그림 1. 합산 수열 발생기(r=2) 및 LM 발생기

2.1 Self_Decimated LM 발생기의 구성

Self_Decimated LM의 클럭 조절 구조는 추가된 합산 수열발생기[5]를 바탕으로 하는 키 수열발생기 계열이다. Self_Decimated LM계열에서 (그림 2) 키 수열 발생기는 두개의 LFSR에 기초를 두고 다음 메모리 상태와 키 수열 비트를 생성하기 위해 LFSR의 결과 비트는 결합함수 f_c, f_d, f_z에 각각 입력된다. LFSRs의 불규칙한 클럭은 자신의 LFSR 두 단 내용에 의해 결정된다.

두 개의 LFSR 상태는 자기 LFSR의 메모리 상태의 내용을 위해 정의되고 시간 j에서 출력 z_j는 f_z에 의해 생성된다. 다음 메모리상태 c_j는 f_i에 의해 구하고, d_j는 f_d에 의해 구한다. 클럭함수 f_a와 f_b는 현 상태에 의해 얻어지며, 각 LFSR은 클럭 함수의 출력에 따라 각각의 메모리 상태와 키 수열 비트를 생성한다. 또한, 각 LFSR의 불규칙 클럭은 자신의 LFSR 두 단의 내용에 따라 주기가 결정된다. 메모리 c_j는 f_c에 의해 계산되며, d_j는 f_d에 의해 계산된다. 클럭함수 f_a와 f_b는 현 상태 데이터에 의해 결정되고, 각 LFSR은 클럭함수의 결과에 따라 주기 값과 메모리 상태 c_{j-1}을 c_j로, d_{j-1}을 d_j에 갱신한다.

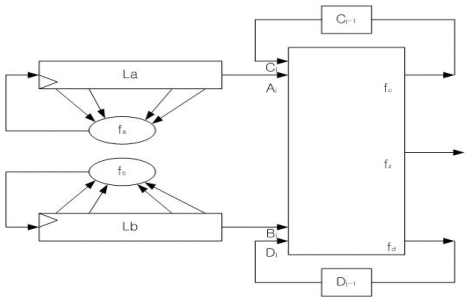


그림 2 Self_Decimated LM 발생기

Self_Decimated LM은 처음 초기화 과정에서 키(k)와 초기화 벡터(i = initial key)을 가지고 내부 상태를 채우며, 내부 상태는 키의 길이가 더 중요하여 필요시 키 확장 과정이 요구된다.

2.2 Self_Decimated LM-128

본절에서는 Self_Decimated LM-128, 스트림 암호의 키 수열 발생, 클럭제어, 키 로딩과 재입력을 상세히 기술한다.

1) 키 수열 발생

Self_Decimated LM-128은 2개의 자체 클럭 조절형 LFSR과 2개의 메모리 비트를 가지며, 각 LFSR 길이는 127비트 및 129비트이다. 모든 메모리 비의 트들은 Self_Decimated LM-128에게 257비트의 의 내부 상태 비트를 주며, 128비트 키와 127비트 초기화벡터를 내부 상태로 가진다.

Self_Decimated LM 발생기의 출력 키스트림은 LFSR 수열과 메모리수열이 합쳐져서 생성되며, Self_Decimated LM-128의 두 의존 클럭 LFSR은 L_a와 L_b 그리고 메모리 c, d의 한 비트 신호를 가진다. L_a와 L_b의 귀환다항식은 원시다항식으로 선택되고 LFSR의 모든 비트가 0으로 초기화되는 것을 허용하지 않는다.

$$L_a = x^{127} \oplus x^{107} \oplus x^{10} \oplus x^9 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$$

$$L_b = x^{129} \oplus x^{117} \oplus x^{14} \oplus x^{11} \oplus x^{10} \oplus x^9 \oplus x^8 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$$

출력 키 수열 비트 z_j와 시간 j 그리고 메모리 비트 c_j, d_j는 합산 수열 발생기와 동일하기 위해 아래와 같이 정의된다.

$$c_j = A_jB_j \oplus (A_j \oplus B_j)c_{j-1}$$
$$d_j = B_j \oplus (A_j \oplus B_j)d_{j-1}$$
$$z_j = A_j \oplus B_j \oplus c_{j-1} \oplus d_{j-1}$$

2) 클럭제어

Self_Decimated LM-128은 자신의 LFSR의 클럭을 제어하여 각각의 레지스터에 불규칙한 클럭 LFSR을 발생하는데 두 단의 범위1....4 값을 계산하기 위하여 L_a로부터 두 단의 값을 받아서 f_a의 계산에 의해 L_a의 클럭 [1~4]를 선택하는 값을 가지게 된다. 유사하게 L_b의 두 단 값을 받아서 L_b에 클럭을 준다. 주기는 제어함수 f_a와 f_b에 의해 얻는다.

$$f_a(L_a) = 2 * L_{a42}(t) + L_{a85}(t) + 1$$
$$f_b(L_b) = 2 * L_{b43}(t) + L_{b86}(t) + 1$$

이 설계는 Self_Decimated LM계열에 적용되며, 키 수열 발생기는 n을 기초로 하는 LFSR에 L_i의 주기가 L_{i+1} 또는, L_1로 부터 L_n까지의 주기가 사용된다.

3) 키 로딩과 키 재 입력

몇몇의 통신망들에서 전체 메시지를 요청하는 오류가 발생하는데 동기스트림 암호(synchronous stream cipher)가 사용되면 안전을 위해 다른 키 수열이 사용되는 것을 요구한다. 그리고, 이것을 위해서 키 재 입력은 비밀키와 클리어가 보내진 추가적인 초기화 백터(iv)를 사용하는 방법을 제공하거나 다른 방법으로 공개되어야 한다.

여기서 Self_Decimated LM-128의 초기 키 로딩과 키 재 입력 방법은 다음과 같다. Self_Decimated LM-128를 위해 키(k) 및 초기벡터(iv)는 모두 128비트 길이를 가지며 키와 벡터는 내부상태 257비트를 채운다. 또한, 초기설정 과정은 재 입력을 위해 사용될 수 있으며 키 수열 발생기를 위해 초기상태를 생성하는 과정은 발생기 자체를 두 번 사용하고 L_a의 시작 상태는 XORing에 의해 간단하게 $L_a = (k \oplus iv) \bmod 2^{127}$ 같이 나타난다. 키(k), 초기화 벡터(iv)는 2개의 128이진 비트를 얻는다. L_b를 위해 129비트들의 초기상태는 128비트 키에 의하여 얻고 내부의 129비트워드를 포함하면서 왼쪽으로 1비트 이동한다. 그리고 초기벡터가 먼저 0과 내부 129비트 워드를 포함한 XORing, 다시 말해서 $L_b = (k \ll 1) \oplus (0 | iv)$이다.

길이 257비트인 하나의 출력 문자열을 생성하기 위하여 암호가 실행되면 암호의 두 번 되풀이로부터 L_a는 초기상태를 위해 출력 문자열의 첫 번째 128비트가 사용되고 L_b는 잔여 129비트가 사용된다. 암호는 두 번째 실행 257비트의 출력 문자열로 시작되며 키 수열발생을 시작할 때 두 번째의 출력은 키 수열 발생기의 초기상태 구성을 위해 사용된다. 이전같이 처음 128개의 정보는 L_a의 초기상태를 형성하고 그리고 잔여 129비트들은 L_b의 초기상태를 이루며 어느 한쪽의 LFSR이 0으로 초기화되는 것은 있을 수 없다. 이것은 Self_Decimated LM 알고리즘 그 자체에 사용되는 것으로 알고리즘의 알려진 안전성과 빠른 수행 양쪽 모두를 이용한다. Self_Decimated LM의 높은 보안 때문에 우리는 키 재 입력 과정에서 최상의 공격이 철저한 키 검색이라고 결론을 내린다.

3. 시뮬레이션 및 결과

Self_Decimated LM-128 키 수열 발생기를 이용하여 연속되는 출력 데이터 16만 비트씩 3회의 샘플 값을 출력한 후 Frequency test, Serial test, Generalized serial test, Poker test 및 Autocorrelation test[6]등의 랜덤 테스트와 Linear Complexity, Period등의 테스트를 실시하였다.

[표 1] Self_Decimated LM 키 수열 특성

Register Lengths	Linear Complexity	Period
5, 6	168	189
5, 7	209	3,937
6, 7	293	8,001
7, 8	967	32,385
7, 9	1,089	64,897
8, 9	2,251	130,305
9, 10	9,465	522,753
9, 11	9,354	1,046,017
10, 11	14,164	2,094,081
11, 13	58,209	16,766,977
13, 15	76,801	268,394,497

검증 항목 테스트하여 [표 1]와 같이 균등하게 계산된 Linear Complexity 와 Period를 이끌어 낼 수 있었고, 검증 항목은 기준은 [표 2]와 같다.

특성 1. Linear Complexity LC와 Period P는 아래와 같이 정의된다.

[표 2] 랜덤 테스트 판정 결과

	검증항목	판정치	결과치-1	결과치-2	결과치-3
1	Frequency test	3.841	0.692	1.550	0.117
2	Serial test	5.991	0.803	3.337	0.547
3	Generalized serial test t = 3 t = 4 t = 5	 9.488 15.507 26.296	 4.927 9.876 16.294	 5.779 7.629 12.606	 0.688 4.427 10.519
4	Poker test m = 3 m = 4 m = 5	 14.067 24.996 44.654	 3.680 20.633 18.087	 8.845 17.373 22.642	 2.070 10.833 28.742
5	Autocorrelation test	max ≤ 0.05	max = 0.007	max = 0.005	max = 0.007

$$LC \geq 25*2^{\lceil \frac{(n-11)}{2} \rceil} = 2^{4.6}*2^{\frac{(n-11)}{2}}$$

$$P \leq 25*2^{\lceil \frac{(n-11)}{2} \rceil} = 2^{4.6}*2^{\frac{(n-11)}{2}}$$

특성 1에 의하여 Self_Decimated LM-128의 LC 및 P는 다음과 같다.

$$LC \geq 2^{4.6}*2^{\lceil \frac{(256-11)}{2} \rceil} = 2^{4.6}*2^{123} \approx 2^{128}$$

$$P \geq 2^{4.6}*2^{\lceil \frac{(256-11)}{2} \rceil} = 2^{4.6}*2^{123} \approx 2^{128}$$

Self_Decimated LM-128 알고리즘은 랜덤특성이 양호 할 뿐만 아니라 주기, 선형 복잡도, Linear Complexity 등 암호 안정성이 좋다는 것을 확인 할 수 있었다.

4. 결론

본 논문에서는 자체 클럭 조절 구조 및 2개의 비트 메모리 합산 수열 발생기를 기본 발생기로 갖는 Self_Decimated LM-128을 제시하였다.

Self_Decimated LM-128은 랜덤성이 양호 할 뿐 아니라 암호 안전성이 크게 개선된 알고리즘이며, 차세대 무선 통신망 정보보호에 적용될 수 있다. 안전성 분석결과, 주기는 2^{128}이고, 선형 복잡도 역시 2^{128}이기 때문에 보안특성이 우수하다고 할 수 있다.

참고문헌

[1] E.Dawson, "Cryptanalysis of Summation generator,"Advances in Cryptology - ASIACRYPT '92, Lecture Notes in Computer Science, Vol. 718, pp. 209-215, Springer-Verlag, 1993.

[2] J. Golic, M. Salmasizadeh, and E. Dawson, "Fast Correlation Attacks on the summation Generator," Journal of cryptology, Vol. 13, No.2, pp. 245-262, 2000.

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

[4] W. Meier and O. Staffelbach, "Correlation Properties of combiners with Memory in Stream Ciphers,"Advances in Cryptology-EUROCRYPT' 90, Lecture Notes in Computer Science, Vol. 473, pp. 204-213, Springer-Verlag, 1990.

[5] R.Rueppel, "Correlation Immunity and the Summation Generator,"Advances in Cryptology - CRYPTO '85," Lecture Notes in Computer Science, Vol. 218, pp. 260-272, Springer-Verlag, 1985.

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