LILI-256 키수열 발생기 제안

조상일*, 최성훈* 이훈재**
*동서대학교 소프트웨어전문대학원
**동서대학교 정보네트워크공학과
e-mail:i3011@orgio.net

A proposal of the LILI-256 Keystream Generator

Sang-Il Cho*, Sung-Hoon Choi*, Hoon-Jae Lee**
*Graduate School of software, Dong-Seo University
**Information Network Engineering, Dong-Seo University

요 약

차세대 Mobil 무선 통신에 적용 가능한 LILI-128 암호의 개선에 대해서 논의한다. 이동통신 단말기처럼 음성 신호를 고속으로 변환하여 전달할 때는 스트림 암호와 블록 암호가 주로 적용되는데, 특히 고속 무선 통신에서는 스트림 암호가 유리하다. 본 논문에서는 유럽 지역 NESSIE 차세대 암호 후보로 제안된 바 있는 LILI-128의 약점을 보완하여 LILI-256 키수열 발생기로 개선하였다.

1. 서론

LILI-128[1]스트림 암호는 유럽 GSM 표준암호인 A5에 이어 유럽지역 IMT-2000 표준암호 후보로 제안되고 있는 동기식 스트림 암호 알고리즘이다.

스트림 암호의 안전성은 여러 종류의 암호 공격에 대하여 얼마나 강한 키수열을 발생시키느냐에 달려 있다. LILI-128 암호는 몇가지 측면에서 취약한 단점을 가지고 있다.[10]

본 논문에서는 LILI-128보다 더 강한 키 수열을 발생시키기 위해 128비트를 256비트로 늘려 기존의 알고리즘 보다 주기와 선형복잡도를 크게 증가시킨 LILI-256 키수열 발생기를 설계 제안한다.

제안된 알고리즘의 출력 특성을 분석하기 위하여 통계분석기법을 적용한다. 통계분석 방법은 랜덤성 테스트를 사용하는데, 세부항목은 빈도 테스트(frequency test), 시리얼 테스트(serial test), 일반 시리얼 테스트(generalized serial test), 포카 테스트(poker test), 자기상관성 테스트(autocorrelation test) 등[2]을 수행하였으며, 제안 방식의 출력수열이 이러한 테스트를 통과하는지 시뮬레이션한다.

2. LILI-128 알고리즘 개선

2.1 스트림 암호 알고리즘

스트림 암호 알고리즘이란 이진화된 평문과 이진 키 수열의 배타적 논리합(XOR)연산을 실행하여 암호문을 생성하는 알고리즘을 말하며, 이 때 출력키 수열에 대한 특성과 발생 방법이 안전도에 직접적인 영향을 미친다. 스트림 암호 알고리즘은 블록 암호 알고리즘과는 달리 비교적 수학적 분석이 가능하여 여러 가지 중요한 수치(주기, 선형복잡도, 랜덤 특성, 상관 면역도, 키 수열 사이클 수등)에 대하여 이론적인 값을 계산할 수 있다는 장점이 있다.[2-7] 또한 스트림 암호는 에러확산이 없고, 하드웨어 구현이 용이하고, 통신지연이 없으며, 고속 통신이 가능한 것 등의 잇점으로 인해서 이동·무선통신 전송로 구간의 링크 암호 또는 군사·외교용으로 많이 사용되고 있다. 종래에는 선형 귀환 쉬프트 레지스터를 비선형적인 방법으로 결합하거나 시간을 제어하는 방식으로 개발되었고, 주기 및 선형복잡도를 정확하게 계산할 수 있는 알고리즘이 제안되었으나, 최근에 이러한 경향이 많이 퇴색되고 있다. 현재 발

표된 스트림 암호 알고리즘은 상당히 많은 종류가 있으나, 블록 암호 알고리즘처럼 개별적인 체계로 존재하기보다는 비공개된 상태로 사용되고 있으며, 암호화 이외의 분야에 이용되는 것은 드문 편이다. 스트림 암호의 예로는 유럽에서 이동 통신용으로 사용 중인 GSM 장비에 내장되어 있는 A5 알고리즘[8], Rueppel 합산 수열 발생기[7], Netscape에 들어 있는 RC4[7]가 대표적이다.

스트림 암호의 안전성은 여러 종류의 암호 공격에 대하여 얼마나 강한 키 수열을 발생시키느냐에 달려 있으며, 아래의 기준을 따른다[7. 2].

C1) 주기(Period) : 출력 키 수열은 주기에 대한 최소값이 보장되어야 한다.

C2) 랜덤 특성(Randomness) : 출력 키 수열은 좋은 랜덤 특성을 갖어야 한다.

C3) 선형복잡도(Liner complexity) : 출력 키 수열은 큰 선형 복잡도를 갖어야 한다.

C4) 상관 면역도(Correlation immunity) : 출력 키 수열은 높은 상관 면역도를 갖는다.

C5) 키 수열 사이클 수(Keystream cycle) : 출력 키 수열은 1개 이상의 키 수열 사이클에서 발생되어야 한다.

2.2 LILI-128 암호 알고리즘

2개의 레지스터를 사용하고 있는 LILI-128 암호의 구조는 그림 1과 같으며, 사용된 선형 귀환 이동 레지스트 (LFSR, linear feedback shift register)는 39단 $LFSR_c$과 89단 $LFSR_d$으로 구성되어 있는데, 이 중에서 $LFSR_d$는 $LFSR_c$의 출력에 의하여 클럭 통제를 받게 된다. 통제되는 클럭 수는 통상적인 경우 랜덤하게 설정된 f_c함수에 의하여 생성된 정수값(1~4범위)만큼 $LFSR_d$의 클럭을 이동시키며, 그 후 $LFSR_d$의 내부 값으로부터 f_d 필터 함수를 통하여 필터 수열(filtered sequence)을 발생하게 된다.

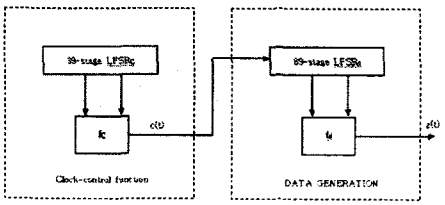


그림 1. LILI-128 스트림 암호

LILI-128 암호에서 39단 $LFSR_c$, 89단 $LFSR_d$의 원시다항식(primitive polynomial)은 다음과 같이 정의된다.

$g_c(x) = x^{39} \oplus x^{35} \oplus x^{33} \oplus x^{31} \oplus x^{17} \oplus x^{15} \oplus x^{14} \oplus x^2 \oplus 1$

$g_d(x) = x^{89} \oplus x^{83} \oplus x^{80} \oplus x^{55} \oplus x^{53} \oplus x^{43} \oplus x^{39} \oplus x \oplus 1$

여기서 $\oplus$는 배타 논리합인 XOR(exclusive-or)연산을 의미한다. $LFSR_c$는 일반적인 39단 이동 레지스터 및 귀환비트 조합으로 구현이 가능하다. 그리고 출력 f_c회로는 $LFSR_d$의 좌측 이동 클럭 수를 결정하는 것이다. LILI-128의 최종 출력 수열은 비선형 여과 함수(nonlinear filter function) f_d로부터 얻어지는 비트 수열이 된다.

[특성1] LILI-128 알고리즘의 안전성 특성은 다음과 같이 요약된다[1].

- 주기 : $P = (2^{38}-1)(2^{89}-1) \approx 2^{128}$
- 선형복잡도 : $(\frac{L_d}{r}) \cdot Pc = (\frac{89}{6}) \cdot (2^{39}-1) \approx 2^{68}$
- 랜덤특성 : 양호함

2.3 개선된 LILI-256 알고리즘

개선 알고리즘은 2.1절의 스트림 암호 설계 기준을 잘 만족하도록 설계하였다. 기존의 LILI-128 알고리즘의 각 레지스터 크기를 127단 $LFSR_c$[그림 3] 및 129단 $LFSR_d$[그림 4]로 증가 시켰으며, 키 비트 크기를 128비트에서 256비트로 늘렸다.

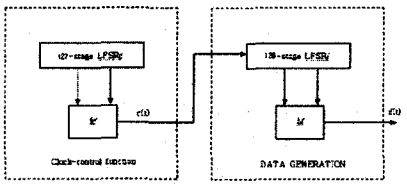


그림 2. 개선된 LILI-256 스트림 암호

각 레지스터의 연결 다항식은 최대 주기의 수열을 생성하기 위해 원시 다항식이 사용되는데, 참고문헌[9]의 방법에 따라 생성한 결과는 다음과 같다.

127단 레지스트에 사용되는 다항식은

$g_c(x) = x^{127} \oplus x^{20} \oplus x^7 \oplus x^3 \oplus x^2 \oplus x \oplus 1$,

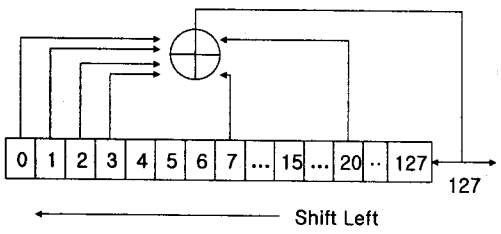
129단 레지스트에 사용되는 다항식은

$g_d(x) = x^{129} \oplus x^{125} \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1$ 이다

또한 Clock Control Function (f_c)는

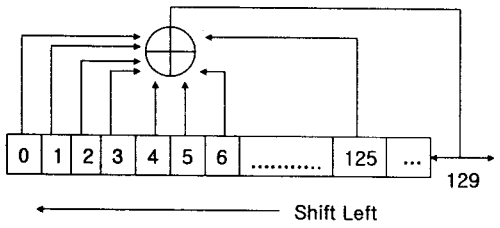
$f_c = 2*C[64] + C[40] + 1$ 이다.

여기서 C[i]는 $LFSR_c$의 i번째 탭값이다.



$g_c(x) = x^{127} \oplus x^{20} \oplus x^7 \oplus x^3 \oplus x^2 \oplus x \oplus 1$

그림 3. 확장된 127단 $LFSR_c$



$g_d(x) = x^{129} \oplus x^{127} \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x \oplus 1$

그림 4. 확장된 129단 $LFSR_d$

[특성2] gcd(127,129)=1이고, 모든 LFSR의 초기값이 nonnull이라고 가정하면 개선된 LILI-256알고리즘의 안전성 분석 결과는 다음과 같다.

- 주기 : $P = (2^{127}-1)(2^{129}-1) \approx 2^{256}$
- 선형복잡도 : $(\frac{L_d}{r}) \cdot Pc = (\frac{129}{6}) \cdot (2^{127}-1) \approx 2^{132}$
- 랜덤특성 : 양호함

[표 1] 개선전과 개선후의 비교분석

비교항목	개선전	개선후
주 기	$\approx 2^{128}$ if gcd(39,38) =1	$\approx 2^{256}$ if gcd(127,129)=1
랜덤테스트	양호함	양호함
선형복잡도	$(\frac{L_d}{r}) \cdot Pc$ $=(\frac{89}{6}) \cdot (2^{39}-1) \approx 2^{98}$	$(\frac{L_d}{r}) \cdot Pc$ $=(\frac{129}{6}) \cdot (2^{127}-1) \approx 2^{132}$

3. 시뮬레이션 및 결과

개선된 키 수열 발생기를 이용하여 연속되는 출력 데이터를 16만 비트씩 3회의 샘플값을 출력한 후 frequency test, serial test, generalized serial test, poker test 및 autocorrelation test[2]등의 랜덤 테스트를 실시하였다.

[표 2] 랜덤 테스트 판정 결과

	검증 항목	판정치	검정 결과1	검정 결과2	검정 결과3
1	Frequency test	3.841	0.211	0.578	0.394
2	Serial test	5.991	1.947	2.687	1.513
3	Generalized serial test				
	t = 3	9.488	3.756	8.360	3.241
	t = 4	15.507	4.559	13.325	3.823
	t = 5	26.296	9.631	21.548	14.126
4	Poker test				
	m = 3	14.067	4.630	3.950	2.690
	m = 4	24.996	13.853	18.417	8.813
	m = 5	44.654	21.021	40.842	25.075
5	Autocorrelation test	max $\leq$ 0.05	max=0.0033	max=0.0037	max=0.0027

각각의 선택된 검증 항목을 테스트하여 모든 항목 검증 결과가 기준 이내에서 [표 2]와 같이 양호한 출력을 얻을 수 있음을 확인하였다.

개선된 LILI-256 알고리즘은 기존의 방식과 비교할 때 랜덤성이 양호 할 뿐만 아니라 주기, 선형복잡도 등 암호 안정성이 크게 개선됨을 확인 할 수 있었다.

4. 결론

LILI-128 스트림 암호 알고리즘은 IMT-2000에 적용될 암호화 알고리즘으로서 (LC가 2^{80}이하로서) 공격에 취약한 단점을 가지고 있다.

본 논문에서는 이러한 단점을 개선하기 위해 키 비트크기를 128비트에서 256비트로 증가시켰으며 주기, 랜덤테스트, 선형복잡도 등의 안정성을 분석하였다. 그 결과 5가지 랜덤테스트 항목을 모두 통과하였으며, 랜덤 특성이 양호함을 확인하였다. 또 다른 안전성에서 주기는 2^{256}, 선형복잡도는 2^{132}으로 기존 방식에 비하여 각각 2^{64}배 및 2^{44}배의 향상이 되었음을 확인하였다.

결론적으로 기존 방식과 비교 할 때 제안 방식은 랜덤성이 양호할 뿐 아니라 암호 안전성이 크게 개선된 알고리즘이며, IMT-2000 등 무선 통신망 정보보호에 적용될 수 있다.

참고문헌

[1] E. Dawson, A. Clark, J. Golic, W. Millan, L. Penna, L. Simpson, "The LILI-128 Keystream Generator," 1st NESSIE Workshop, Nov. 2000.

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

[3] D. Stinson, *Cryptography Theory and Practice(2nd ED)*, CRC Press, 2002.

[4] Van Tilborg, *Fundamentals of Cryptography*, KAP Press, 2000.

[5] 이훈재, 문상재, "FPGA/VHDL을 이용한 LILI-128 암호의 고속화 구현에 관한 연구," 정보보호학회논문지, 제 11권 제 3호, pp.23-32, 2001년 6월호.

[6] Jovan Dj.Golic, "Cryptanalysis of Alleged A5 Stream Cipher," Springer-Verlag, 1998.

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

[8] R.Schineier, *Applied Cryptography(2nd Ed)*, Joln-Wiley & Son, 1996.

[9] B.Park, H.Choi, T.Chang and K.Kang, "Period of Sequences of Primitive Polynomials," Electronics Letters, Vol.29, No.4, pp390-391, Feb. 1993.

[10] S. Babbage, "Cryptoanalysis of LILI-128," 2nd NESSIE Workshop, Sep. 2001.