제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

무선 이동 통신에 적합한 A5 스트림 암호의 개선

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

An Improved A5 Stream Cipher for a mobile Communications

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

요 약

본 논문에서는 GSM 암호 시스템에 적용되는 메시지 암호 등을 위한 A5 스트림 암호를 개선하였다. 기존의 64비트 키 길이의 GSM 암호의 취약점을 보완하기 위해 키 길이를 두 배로 늘림으로서 키 수열을 복잡하게 하였고, 랜덤성, 주기 그리고 선형 복잡도 측면에서 분석하였다. 사용된 알고리즘은 C언어로 시뮬레이션 하였으며, 통계적 분석 기법을 통하여 개발 알고리즘의 출력 특성을 분석하였다.

1. 서론

디지털 이동 통신 시스템의 대표적인 표준안으로는 IS-95[1], GSM (global system for moblie communication)[2] 그리고 PACS[3] 등이 있으며, ETSI (european telecommuication stand ard institute)에 의해 제안된 유럽의 TDMA (time division multiple access)이동 통신망 표준이 GSM이다.

GSM에서 제공하는 보안을 위한 알고리즘들의 수출 제한으로 인해 로밍 서비스를 제공하기 위해서는 보안 알고리즘들이 서비스 제공자에 의해 개발, 제공되어져야 한다. 우리나라 역시 IMT-2000으로의 진화과정에서 GSM시스템에 대한 연구가 필요하며, 고유의 암호 알고리즘들이 개발되어져야 할 것이다. 따라서 본 논문에서는 보안 측면에서 GSM으로의 로밍 서비스를 제공하기 위한 메시지 암호화를 위하여 A5 알고리즘을 개선하고자 한다.

본 논문에서는 GSM 암호 시스템에 적용되는 메시지 암호 등 스트림 암호를 개선한다. 기존의 64비트 키 길이의 GSM 암호의 취약점[6]을 보완하기 위하여 키 길이를 두 배로 늘림으로서 키 수열을 복잡하게 하고, 분석결과 좋은 랜덤성 뿐만 아니라 기존의 알고리즘 보다 주기와 선형복잡도를 크게 증가시키는지 확인하고자 한다. 사용된 알고리즘은 C언어로 구현하여, 통계적 분석 기법을 통해서 개발될 알고리즘의 출력 특성을 분석한다. 통계분석 방법은 Menezes등[4]의 기본랜덤 특성평가방법을 이용하였다. 세부항목은 빈도 테스트(frequency test), 시리얼 테스트(serial test), 일반 시리얼 테스트(generalized serial test), 포카 테스트(poker test), 자기상관성 테스트(autocorrelation test) 등을 수행하였으며, 그 결과 제시된 모든 테스트를 통과하고자 한다. 마지막으로 주기, 선형복잡도 등 암호학적 안전성 분석을 통하여 제안된 시스템의 안전성을 검증한다.

2. A5 개선 알고리즘

2.1 스트림 암호 알고리즘

스트림 암호 알고리즘은 키의 길이와 평문의 길이가 같으면 정보 이론 관점에서 완벽하다고 증명된 one-time pad를 현실적인 관점에서 구현하고자 하는 시도로 개발되었다. 개념적으로는 평문을 이진 수열로 부호화하여 이진 수열 발생기에서 생성된 이

진 수열과 비트별 XOR하여 이진 수열로된 암호문을 발생하는 방식이 스트림 암호 알고리즘이라 할 수 있다. 스트림 암호는 이진 수열 발생기만 사용되는 것은 아니고 적당한 범위의 문자열을 발생시키는 난수 발생기만 있으면 언제든지 구성될 수 있다.

스트림 암호 알고리즘은 블록 암호 알고리즘과는 달리 비교적 수학적 분석이 가능하여 여러 가지 중요한 수치 (주기, 선형복잡도, 랜덤 특성, 상관 면역도, 키 수열 사이클 수)에 대하여 이론적인 값을 계산할 수 있다는 장점이 있다. 또한 데이터에 대한 에러 전파현상이 발생하지 않으며, 하드웨어로 알고리즘을 구현하는 것이 비교적 용이하다.

현재 발표된 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 알고리즘과 Rueppel계열의 합산 수열 발생기[7] Netscape에 들어 있는 RC4[8]가 대표적이며, 이진 난수열 발생기 형태로 제안되어 있으나 실제로 사용되는 것이 알려진 예는 별로 없다.

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

(1) 주기(period): 출력 키 수열은 주기에 대한 최소값이 보장되어야 한다.
(2) 랜덤 특성(randomness): 출력 키 수열은 좋은 랜덤 특성을 갖어야 한다.
(3) 선형복잡도(liner complexity): 출력 키 수열은 큰 선형 복잡도를 갖어야 한다.
(4) 상관 면역도(correlation immunity): 출력 키 수열은 높은 상관 면역도를 갖는다.
(5) 키 수열 사이클 수 (keystream cycle): 출력 키 수열은 1개 이상의 키 수열 사이클에서 발생되어야 한다.

2.2 기존 A5 알고리즘

기존의 A5 스트림 암호 알고리즘[2]은 3개의 LFSR (linear feedback shift registers)로 구성되어 있으며, 레지스터의 길이는 R1에서 19비트, R2에서 22비트, R3에서 23비트들로 구성되어 있다. 각 레지스터의 오른쪽 비트부터 '0'으로 표시한다.

R1의 taps 위치는 13, 16, 17, 18, R2의 taps 위치는 20, 21 및 R3의 taps 위치는 7, 20, 21, 22이다. 각 레지스터의 taps 비트를 함께 XOR하여, 그 결과를 모아 왼쪽으로 쉬트프 된 레지스터의 '0' 비트 안에 넣는다.

각 LFSR의 연결 다항식은 최대 주기의 수열을 생성하기 위하여 원시 다항식(primitive polynomial)이 사용되는데, 19단 LFSR에 사용되는 연결 다항식은 $P_1(X) = X^{19} \oplus X^{18} \oplus X^{17} \oplus X^{16} \oplus X^{13} \oplus 1$, 22단 LFSR에 사용되는 연결 다항식은 $P_2(X) = X^{22} \oplus X^{21} \oplus X^{20} \oplus 1$, 23단 LFSR에 사용되는 연결 다항식은 $P_3(X) = X^{23} \oplus X^{22} \oplus X^{21} \oplus X^{20} \oplus X^7 \oplus 1$이다. 그들은 다음의 majority function을 사용하여 stop/go방법의 클럭을 사용한다. 각 레지스터의 클럭 신호인 majority function는 자신의 중간 비트 값 (R1-8bit, R2-10bit ,R3-10 bit)을 취한다. 각 clock cycle은 산출된 클럭신호인 majority function과 각 레지스터 클럭신호 동의에 의해서 클럭이 움직인다. 각 스텝은 어느쪽의 두 개의 레지스터나 세 개의 레지스터가 클럭되며, 각 레지스터는 3/4은 움직임이 가능하고 1/4는 정지하는 것이 가능하다.

A5 스트림 암호에서 생성되는 키 스트림 발생기의 각 레지스터는 Majority()함수를 사용하여 3개의 clock이 컨트롤 된다. $S_i(t)=(S_{ij}(t))$ 은 $t \geq 0$일 경우에 $LFSR_i$의 상태를 나타내며, stop/go 클럭을 컨트롤하기 위해 $LFSR_i$의 중간비트를 T_i로 나타낸다. 즉 $T_1=8$, $T_2=10$, $T_3=10$을 제공하게 된다. 클럭 컨트롤 결과 $C=(C(t))^{\infty}_{t-1}$인 경우 $C(t)=g(s_1,T_1(t-1), s_2,T_2(t-1), s_3,T_3(t-1))$이 된다. g는 majority의 3개의 변수(인자)를 받아 4개의 출력 값을 만들어 낸다.

$$g(s_i, s_j, s_k) = \{i, j\}, \text{ if } s_i=s_j \neq s_k \text{ for } i < j \text{ and } k \neq i, j$$

클럭 컨트롤 값에 의해서 LFSR들의 연산 결과 후 output y(t)를 출력하게 된다.

$$y(t)=S_{1,1}(t)+S_{2,1}(t)+S_{3,1}(t),\ t \geq 1$$

[특성 1] A5 알고리즘의 안전성 분석 결과는 다음과 같다[5-6].

-주기 : $P=(2^{19}-1)(2^{21}-1)(2^{23}-1) \approx 2^{64}$
-선형복잡도 : $LC \approx 2^{19}*2^{21}=2^{40}$
-랜덤특성 : 양호함

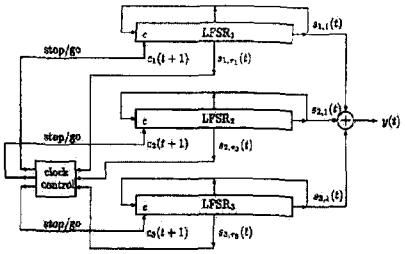

그림 1. A5 키 수열 발생기

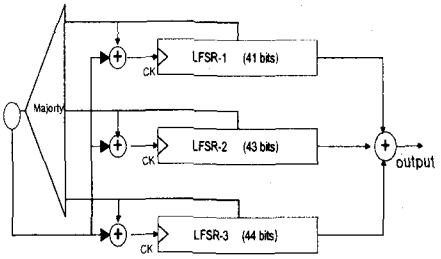

그림 3. 개선된 A5 키 수열 발생기

2-3. 개선된 A5 알고리즘

개선 알고리즘은 기존의 A5 알고리즘의 각 레지스터의 크기를 L_1=41, L_2=43, L_3=44단으로 증가(그림 2)시켰으며, 이렇게 되면 비트 크기는 64비트에서 128비트로 늘어난다. 각 레지스터의 연결 다항식은 최대 주기의 수열을 생성하기 위해 원시 다항식이 사용되는데 41단(비트) 레지스터 R1에 사용되는 다항식 $g_1(X) = X^{41} \oplus X^4 \oplus X^3 \oplus X^1 \oplus 1$, 43단 레지스터 R2에 사용되어진 다항식 $g_2(X) = X^{43} \oplus X^{26} \oplus X^5 \oplus X^1 \oplus 1$ 및 44단 레지스터 R3에 사용되어진 다항식 $g_3(X) = X^{44} \oplus X^{40} \oplus X^8 \oplus X^1 \oplus 1$를 참고문헌 [9]에 따라 발생 시켰다. 따라서 각 레지스터는 2^{41}-1, 2^{43}-1, 2^{44}-1의 주기를 지게 된다. 각 레지스터들의 tap들을 XOR로 연산한 값을 최상위 비트에 넣고 majority함수에 의해 각 레지스터들의 최상위비트 값을 연산하여 출력한다.

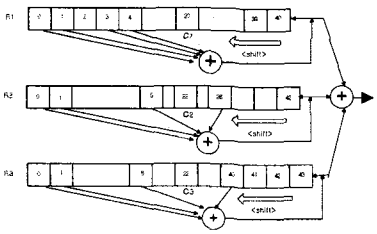

그림 2. Majorty(C1,C2,C3)

Majority함수의 인수는 각 레지스터의 중간 비트 값으로 결정한다. 각 레지스터의 중간 값은 20, 22, 22로 설정한다.

그림3은 개선된 A5 키 수열 발생기를 나타내고 있다.

[특성 2] gcd(L1, L2 L3)=1이고, 모든 LFSR의 초기값이 nonnull이라고 가정하면 A5 알고리즘의 안전성은 분석 결과는 다음과 같다.

-주기 : $P=(2^{41}-1)(2^{43}-1)(2^{44}-1) \approx 2^{128}$

-선형복잡도 : $LC \approx 2^{41} * 2^{43} = 2^{84}$

-랜덤특성 : 양호함

3. 시뮬레이션 및 결과

개선된 A5 알고리즘을 이용하여 랜덤 데이터를 만들었으며, frequency test, serial test, generalized serial test, poker test 및 autocorrelation tes등의 랜덤 테스트[4]를 실시하였다.

시뮬레이션을 위한 랜덤 테스트용 데이터인 키 수열 각각 16만 비트씩 3개의 샘플로 취하였으며, 각각 선택된 검증 항목을 테스트하여, 모든 항목 검증 결과가 기준 이내에서 [표1]와 같이 양호한 출력을 얻을 수 있었다.

개선된 알고리즘에서 비트 수(단수)가 커지면 검증이 어렵기 때문에 작은 크기의 축소 모델에 대한 시뮬레이션을 실시하였으며, 그 결과는 [특성 2]와 유사하였다. 개선방식은 [표2]에서 기존의 방식과 비교 할 때 랜덤성이 양호 할 뿐만 아니라 주기, 선형복잡도등 암호 안전성이 크게 개선됨을 확인 할 수 있었다.

결과적으로 본 제안 알고리즘은 IMT-2000 등 무선통신망 정보보호에 적용될 수 있으리라고 판단된다.

표 1. 랜덤 테스트 판정 기준치

	검증항목	판정치	검정 결과1	검정 결과2	검정결과3
[1]	Frequency test	3.841	0.014	1.366	0.000
[2]	Serial test	5.991	0.643	2.542	2.675
[3]	Gen-t serial test				
	t = 3	9.488	0.953	3.970	2.818
	t = 4	15.507	5.915	8.262	3.138
	t = 5	26.296	14.254	18.490	5.657
[4]	Poker test				
	m = 3	14.067	1.027	5.241	8.197
	m = 4	24.996	16.976	9.919	8.926
	m = 5	44.654	24.946	37.419	25.167
[5]	Autocorrelation test	max ≤ 0.05	max=0.005	max=0.006	max=0.007

표 2. 개선전과 개선후의 비교분석

비교항목	개선전	개선후
주기	$\approx 2^{64}$ if gcd(19, 21, 23)=1	$\approx 2^{128}$ if gcd(41, 43, 44)=1
랜덤테스트	양호함	양호함
선형복잡도	$2^{19}*2^{21}= 2^{40}$	$2^{41}*2^{43}=2^{84}$

4. 결 론

본 논문에서는 A5 알고리즘의 키 길이에 따른 문제점을 개선하기 위하여 A5 개선 알고리즘을 제안하였다. 개선된 A5 알고리즘의 안전성을 분석하기 위하여 랜덤 검증 시뮬레이션을 실시 하였으며, 5가지의 랜덤테스트 항목을 모두 통과하였기 때문에 랜덤 특성이 양호함을 확인하였다. 또 다른 안전성에서 주기는 2^{128}이고, 선형복잡도는 2^{84}으로 기존의 방식에 비하여, 각각 2^{64}배 및 2^{44}배 향상되었음을 확인하였다.

결론적으로 기존 방식과 비교 할 때 제안 방식은 랜덤성이 양호 할 뿐만 아니라 암호 안전성이 크게 개선된 알고리즘이며. GSM 정보보호뿐만 아니라 IMT-2000등 무선 통신망 정보보호에 적용될 수 있다.

참고문헌

[1] TIA/EIA IS-95A "Mobile-Base Station Compatibility Standard for Dual-Mode Wideband Spread Specturm Cellular System", July. 1993.

[2] ETSI, "European Digital Cellular Telecommunucation System(phase 02)-Security Related Network Functions", July. 1993.

[3] JTC, "personal Communications Services PACS Air Interface Specification", Jan. 1995.

[4] A. Menezes, et al. *Handbook of Applied Cryptography(2nd edition)*, CRC press 1997.

[5] 김범식, 신인철 "해쉬함수와 스트림 암호기의 개발 및 GSM 보안 시스템에의 적용". 한국정보처리학회 논문지 제 7권 제 8호, PP211-217, Jan. 2000.

[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, No1, PP211-217, Jan. 2000.

[8] B.schineier, *Applied Cryptography(2nd edition)*, John-Wiley & Son,1996.

[9] B.Park, H.Choi T.Chang and K.Kang, "Perod of Sequence of Primitive Polynomials" Electronics Letters, Vol.29, No.4, PP390-391, Feb. 1993.