論文
3-9-20

GSM에 사용될 A5 스트림 암호의 개선에 관한 연구 (A Study on the Advanced A5 Stream Cipher in GSM Mobile System)

이 훈 재* 류 명 춘**
(Hoon-Jae Lee) (Myung-Chun Ryoo)

요 약

본 논문에서는 GSM 암호 시스템에 적용되고 있는 A5 스트림 암호의 취약점을 보완하는 확장형 A5 알고리즘을 제안한다. 또한 제안된 알고리즘에 대하여 주기와 선형복잡도, 랜덤 특성 등 안전성 요소를 분석한 후 기존의 알고리즘과 비교한다.

ABSTRACT

In this paper, we propose an extended version of A5 stream cipher, which have been used in GSM mobile system. And we analyze the proposed algorithm in parameters with period, linear complexity and randomness, and compare to the original parameters.

1. 서론

최근 암호학계에는 미국의 AES [1]와 NESSIE (New European Schemes for Signature, Integrity and Encryption) [2]라는 차세대 유럽 암호 표준화 프로젝트 그리고 일본의 CRYPTREC[3] 과제가 큰 흐름을 주도하고 있다. AES는 DES를 개선시키기 위한 미국의 대형 프로젝트로서 Rijndael [4]이 이미 표준으로 확정된 바 있으며, NESSIE 프로젝트에는 2002년 12월을 목표로 블록 암호, 스트림 암호, message authentication codes (MAC), collision-resistant and one-way hash functions, 비대칭 암호, 비대칭 디지털 서명, 비대칭 신분확인 등 10개 분야에 대하여 각각의 표준을 결정하는 대규모 과제라고 볼 수 있다. 이 중 동기식 스트림 암호 분야에는 현재 호주의 Simpson과 Dawson이 제안한 LILI-128 암호 [5]를 포함하여 SOBER-t16, SOBER-t32 [6] 등 6개의 후보가 제안되었다. 일본에서도 IPA(Information Promotion Association)가 주축이 되어 2002년말을 개발 목표로 CRYPTREC(Cryptography Research and Evaluation Committee) 과제를 진행 중이다. 이 과제에는 7개 분야에 대한 암호/인증 알고리즘의 공모가 이루어지고 있으며, 이 중의 한 분야가 스트림 암호이다. 우리나라에서도 이와 유사한 대형 프로젝

* 정회원 : 동서대학교 인터넷공학부 정보네트워크공학전공 조교수
논문접수 : 2002. 10. 10.
** 정회원 : 경운대학교 컴퓨터전자정보공학부 컴퓨터공학전공 조교수
심사완료 : 2002. 12. 12.
※ 이 논문은 2001년도 학술진흥재단의 지원에 의하여 연구되었음(KRF-2001-003-E00198)

트가 구상되고 있으며, 블록암호, 스트림 암호, 해쉬 함수 등에 대한 암호 알고리즘 공모과정이 예비 진행 중이다[7].

디지털 이동 통신 시스템의 대표적인 표준안으로는 IS-95, GSM (global system for moblie communication) 그리고 PACS 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. 따라서 보안 측면에서 GSM으로의 로밍 서비스를 제공하기 위한 메시지 암호화를 위하여 A5 알고리즘을 개선이 필요하다고 본다.

본 논문에서는 GSM 암호 시스템에 적용되는 메시지 암호 등 스트림 암호를 개선한다. 기존의 64비트 키 길이의 GSM 암호의 취약점[9]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 랜덤성 테스트를 사용하는데[8], 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 안정성 분석을 통하여 제안된 시스템의 안전성을 검증한다.

2. A5 개선 알고리즘

2.1 스트림 암호

스트림 암호 알고리즘은 키의 길이와 평문의 길이가 같으면 정보이론 관점에서 완벽하다고 증명된 one-time pad를 현실적인 관점에서 구현하고자 하는 시도로 개발되었다. 개념적으로는 평문을 이진 수열로 부호화하여 이진 수열 발생기에서 생성된 이진 수열과 비트별 XOR하여 이진 수열로 된 암호문을 발생하는 방식이 스트림 암호 알고리즘이라 할 수 있다. 스트림 암호는 꼭 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 등)에 대하여 이론적인 값을 계산할 수 있다는 장점이 있다. 또한 데이터에 대한 에러 전파현상이 발생하지 않으며, 하드웨어로 알고리즘을 구현하는 것이 비교적 용이하다.

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 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[8, 11], Netscape에 들어 있는 RC4[8, 11]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 발생시키느냐에 달려 있으며, 아래의 기준을 따른다[8, 11].

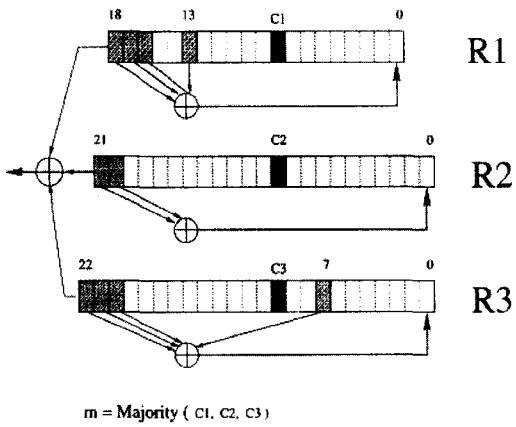
1) 주기(period): 출력 키 수열은 주기에 대한 최소값이 보장되어야 한다.
2) 랜덤 특성(randomness): 출력 키 수열은 좋은 랜덤 특성을 갖어야 한다.
3) 선형복잡도(liner complexity): 출력 키 수열은 큰 선형 복잡도를 갖어야 한다.

2.2 기존 A5 알고리즘

기존의 A5 스트림 암호 알고리즘[11]은 [그림 1]과 같이 3개의 LFSR (linear feedback shift registers)로 구성되어 있으며, 레지스트의 길이는 19비트, 22비트, 23비트들로 구성되어 있다. 그들 각각을 R1, R2, R3라고 한다. 각 레지스터의 오른쪽 비트부터 '0'으로 표시한다. R1의 귀환 탭(feedback taps) 위치는 13, 16, 17, 18이고, R2의 귀환 탭은 20, 21이며, 마지막 R3의 귀환 탭은 7, 20, 21, 22이다. 각 LFSR(linear feedback shift registrer)에서는 귀환 탭의 비트를 함께 XOR한 후 그 결과를 모아 맨 오른쪽 비트 자리에 입력하고, 나머지 비트들은 한 비트씩 왼쪽으로 이동되는 선형 귀환 이동 레지스터이다.

각 LFSR의 연결 다항식은 최대 주기의 수열을 생성하기 위하여 원시 다항식(primitive polynomial)이 사용되며, 19단 R1 LFSR에 사용되는 연결 다항식 P1(X), 22단 R2 LFSR에 사용되는 연결 다항식 P2(X), 그리고 23단 R3 LFSR에 사용되는 연결 다항식 P3(X)는 다음과 같다.

$$P_1(X) = X^{19} \oplus X^{18} \oplus X^{17} \oplus X^{16} \oplus X^{13} \oplus 1$$
$$P_2(X) = X^{22} \oplus X^{21} \oplus X^{20} \oplus 1$$
$$P_3(X) = X^{23} \oplus X^{22} \oplus X^{21} \oplus X^{20} \oplus X^{7} \oplus 1$$



[그림 1] A5 스트림 암호
[Fig. 1] A5 stream cipher.

그들은 다음의 다중 논리(majority function)를 사용하여 stop/go방법으로 클럭을 제어한다. 각 레지스터의 클럭을 조절하는 다중 논리신호는 자신의 중간 비트 값 (R1-8번째 비트, R2-10번째 비트, R3-10번째 비트)을 각각 취한 다음 세 개의 비트의 모음에서 "0" 또는 "1" 중 다수결이 높은 레지스터가 클럭을 받아서 움직이는 원리이다. 예를 들면, 세 개의 비트가 (1,0,0)일 경우의 다수결 출력은 "0"이 되며, "0"을 출력하게 된 R2 레지스터와 R3 레지스터는 클럭을 받아서 움직이게 되고(go), 나머지 R1 레지스터는 소수 출력을 발생하였기 때문에 정지하여 있다(stop). 다음 번 클럭에서는 바뀐 상태를 갖고 다시 다수결 원리를 적용하게 된다. 이 때 각 스텝은 어느 쪽의 두 개의 레지스터나 세 개의 레지스터가 클럭되며, 각 레지스터는 확률적으로 3/4는 움직이게(go) 되고 1/4의 경우에는 정지(stop)한다.

<표 1> $g(s_1, s_2, s_3)$ 함수
<Table 1> $g(s_1, s_2, s_3)$ function.

S1 S2 S3	g의 값	g(s1,s2,s3)
0 0 0	0	{1,2,3}
0 0 1	1	{1,2}
0 1 0	1	{1,3}
0 1 1	2	{2,3}
1 0 0	1	{2,3}
1 0 1	2	{1,3}
1 1 0	2	{1,2}
1 1 1	3	{1,2,3}

A5 스트림 암호에서 생성되는 키 스트림 발생기는 다음과 같이 정리된다. 각 레지스터는 Majority 함수를 사용하여 3개의 클럭이 조절된다. $S_i(t)=(S_{ij}(t))$ 은 $t \geq 0$일 경우에 $LFSR_i$의 상태를 나타내며, stop/go 클럭을 조절하기 위해 $LFSR_i$의 중간 비트를 T_i로 나타낸다.

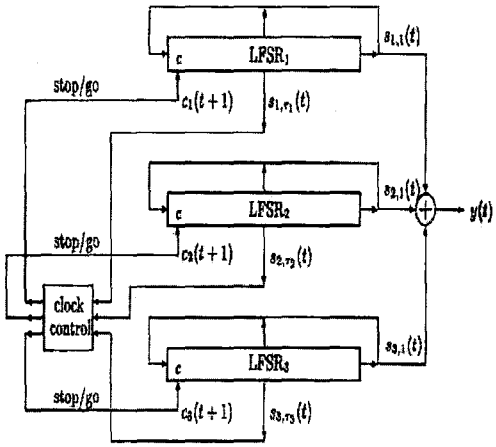
즉 $T_1=8$, $T_2=10$, $T_3=10$을 제공하게 된다. 클럭 조절 결과, $C=(C(t))_{\infty_{t=1}}$인 경우 $C(t)=g(S_{1,T1(t-1)}, S_{2,T2(t-1)}, S_{3,T3(t-1)})$가 된다. g는 <표 1>과 같이 3개의

majority 변수를 받아서 4개의 출력 값을 만들어 낸다.

$g(s_1, s_2, s_3) = \{i, j\}$, if $s_i=s_j\neq s_k$ for $i<j$

이고, $k\neq i, j$ 클럭 컨트롤 값에 의해서 LFSR들의 연산을 실행한 후 최종 키수열 출력 y(t)를 다음과 같이 발생하게 된다.

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



[그림 2] A5 키 수열 발생기

[Fig. 2] A5 Keystream generator.

A5 알고리즘에서의 안전성 분석은 참고 문헌 [9]에 의하여 다음과 같이 요약할 수 있다.

[특성 1] A5 알고리즘의 안전성 요소는 다음과 같다.[9]

1) 주기 : $P = (2^{19}-1)(2^{22}-1)(2^{23}-1) \approx 2^{64}$
2) 선형복잡도 : $LC \approx 2^{19} * 2^{21} = 2^{40}$
3) 랜덤특성 : 양호함

하지만 A5 알고리즘은 사용된 세 개의 LFSR 각각에 대한 단수가 짧았기 때문에 선형 복잡도가 낮게 나타났으며, 결국 Golic[9]에 의하여 암호 해독되었다.

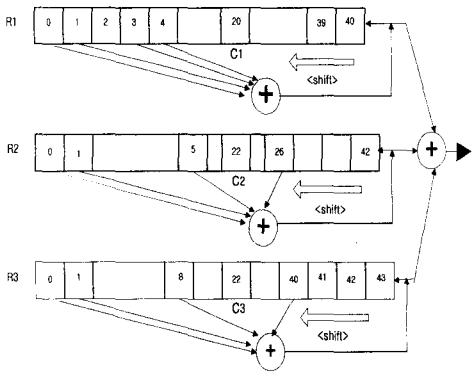
2.3 개선 A5 알고리즘

기존의 A5 알고리즘은 각 레지스터의 크기가 현재 수준에서의 합리성이 떨어지는 64-비트 키를 갖도록 설계되었기 때문에 암호학적 안전성의 문제를 갖게 되었다. 이에 따라서 본 논문에서는 A5 알고리즘을 확장하여 개선하였다. 개선 알고리즘에서는 기존의 키 비트의 크기를 현재 수준에서의 안전성 기준으로 인정되는 Lenstra[13] 키 크기 기준을 만족할 수 있도록 키 크기를 2배(64비트에서 128비트로)로 확장하였다. 참고로 Lenstra[13]에 의한 대칭키 암호에 대한 연도별 키 크기는 2000년 기준 70비트, 2005년 기준 74비트, 그리고 2010년 기준 78비트이며, 이 때 키 크기는 최소 키 비트를 말한다.

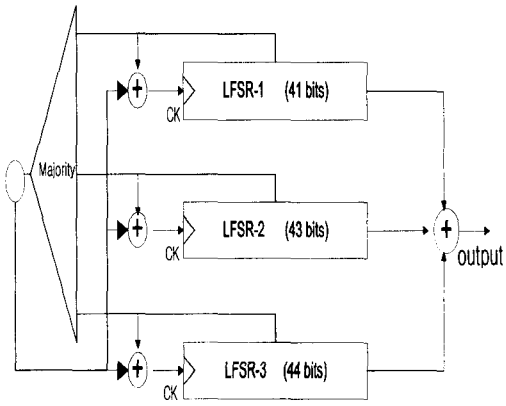
개선된 A5 알고리즘은 [그림 3] 및 [그림 4]와 같이 L_1=41, L^2=43, L^3=44단으로 증가시켰다. 각 레지스터의 연결 다항식은 최대 주기의 수열을 생성하기 위해 원시 다항식 발생기준[12]에 따라서 생성되었다. 사용된 세 개의 LFSR에 대한 원시 다항식은 41단(비트) 레지스터 R1, 43단 레지스터 R2 및 44단 레지스터 R3에 대한 특성 다항식(characteristic polynomial)으로 다음과 같다. 이 때 각각의 레지스터는 2^{41}-1, 2^{43}-1, 2^{44}-1의 출력 수열 주기를 갖게 된다.

$g_1(X) = X^{41} \oplus X^4 \oplus X^3 \oplus X^1 \oplus 1$
$g_2(X) = X^{43} \oplus X^{26} \oplus X^5 \oplus X^1 \oplus 1$
$g_3(X) = X^{44} \oplus X^{40} \oplus X^8 \oplus X^1 \oplus 1$

각 레지스터들의 탭들을 XOR로 연산한 값을 최상위 비트에 넣고 majority함수에 의해 각 레지스터들의 최상위 비트 값을 연산하여 출력한다. majority 함수의 인수는 각 레지스터의 중간 비트 값으로 결정한다. 각 레지스터의 중간 값은 20, 22, 22로 설정한다.



[그림 3] 다수 논리(C1,C2,C3)
[Fig. 3] Majority(C1,C2,C3).



[그림 4] 개선된 A5 키 수열 발생기
[Fig. 4] Improved A5 Keystream Generator.

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

1) 주기 : $P=(2^{41}-1)(2^{43}-1)(2^{44}-1) \approx 2^{128}$
2) 선형복잡도 : $LC \approx 2^{41}*2^{43} = 2^{84}$
3) 랜덤특성 : 양호함(<표 1> 참조)

3. 시뮬레이션 및 분석

3.1 랜덤성 검증[8]

수학적으로 완전한 난수열 (truly random sequence)의 확률 변수열 $\{X_n\}$이 독립(independent)이고 같은 분포를 가질 때 $X_n = x_n$인 실현치의 수열 $\{x_n\}$을 의미한다.

주어진 수열에 대한 randomness의 정의를 i.i.d(independent and identically distributed)의 관점에서 볼 때 여러 가지의 통계적 검정의 주된 원리는 그 수열이 가지고 있는 각 항들 사이의 독립성을 보장할 수 없는 상호관련성 (correlation)이나 같은 분포를 따르지 않는 빈도의 편향성 (bias)등과 같은 통계적 약점을 찾아내는데 있다. 통계적 검정의 원리로부터 한 수열이 어떤 통계적 검정을 통과하였다 함은 random하지 않다고는 할 수 없다는 소극적인 긍정이며, 그 수열이 random하다고 단정하는 적극적인 긍정은 아니다.

확률 및 통계의 이론은 우리에게 randomness에 대한 수치적 척도를 제시하며 많은 검정방법들이 알려져 있으나 그 중에서 이진수열의 randomness검정에 유용하고 다루기에 편리한 방법들만을 소개한다. 도수-m 검정은 전체 수열의 "0"과 "1"에 대한 balanced 특성을 평가하며, 계열 검정은 연속적인 두 비트간의 연속변화(0→1, 1→0) 확률이 랜덤한지를 검증한다. 일반 계열검정은 연속적인 3 비트 (또는 그 이상)에서의 연속변화(예, 00→0, 00→1 등) 확률이 랜덤한지를 검증하고, 포커 검정은 3 비트(또는 그 이상) 블록으로 나눈 후 각 블록단위로 랜덤한지를 검증하며, 자기상관성 검정은 랜덤 수열의 자기상관 특성 만족 여부를 검증한다.

1) 도수-m 검정 (Frequency-m Test)

N비트 이진수열 $u_N=(u_0, u_2, \cdots, u_{N-1})$을 m비트 단위로 나누었을 때 $n=\lfloor \frac{N}{m} \rfloor$개의 bloc- ks(u_{km}, $u_{km+1}, \cdots, u_{km+m-1}$), k=0,1,2, ⋯,n-1들이 m차원에서 균등하게 분포되어 있는가를 검정하는 방법이다. 이때 n개의 m비트 blocks들은 아래 2^m개중의 하나가 된다. 여기서 $\lfloor x \rfloor$는 x보다 작지 않은 최소의 정

수를 의미한다. 이들에서 (0,0, ···,0)인 block의 개수를 n(0), (0,0, ···,0,1)인 block의 개수를 n(1), ···, (1,1, ···,1)인 block의 개수를 $n(2^m-1)$이라 하자. 위의 2^m가지 형태 block의 각각의 확률은 $\frac{1}{2^m}$ 이므로 n개중에서 위의 형태가 나올 평균 개수는 $\frac{n}{2^m}$ 이다. 그러므로 통계량

$$T=\sum_{i=0}^{2^m-1}\frac{(n(i)-\frac{n}{2^m})^2}{\frac{n}{2^m}}=\frac{2^m}{n}\sum_{i=0}^{2^m-1}n(i)^2-n$$

은 근사적으로 자유도가 2^m-1인 χ^2-분포를 따른다. 이진수열이 random하다면 T의 값이 작은 값으로 될 것이고 random하지 않다면 T의 값이 큰 것으로 나타날 것이므로 $P(\chi^2 \geq x_{0.01})=0.01$일 때 기각영역은 $T> x_{0.01}$이다. 즉 유의수준 1%로 T의 값이 $x_{0.01}$보다 클 경우에는 random하지 않다고 할 수 있고, T의 값이 $x_{0.01}$보다 작을 경우에는 random하지 않다고는 할 수 없으므로 이 test로는 random하지 않다는 것을 판정할 수 없다는 것이다. 좀더 일반적으로 말하면 $P(\chi^2 \geq x_a)= a,(0< a<1)$를 만족하는 실수 x_a를 χ^2-분포표에서 구하면 유의수준 a에 대한 기각역은 $\{T \geq x_a\}$이다.

2) 계열검정 (Serial Test)

계열 검정은 이진수열 $u_N=(u_0,\cdots,u_{N-1})$에서 "0"이 "0"이나 "1"로 전이되어 가는 과정이 random한가를 조사하는 방법이며, 수열이 이 검정을 통과하면 각 비트가 그 앞의 비트에 독립임을 제시하여 준다. 수열 u_N을 연속된 2비트 $u_0u_1, u_1u_2, u_2u_3,\cdots, u_{n-2}u_{n-1}$ 로 나누었을 때 '00'의 개수를 n_{00}, '01'의 개수를 n_{01}, '10'의 개수를 n_{10}, '11'의 개수를 n_{11}이라 하고 전체 N비트 중 '0'의 개수를 n_0, '1'의 개수를 n_1이라 하자. 이 때 다음 등식이 성립한다.

$n_{00}+n_{01}=n_0$ 혹은 n_0-1

$n_{10}+n_{11}=n_1$ 혹은 n_1-1

$n_{00}+n_{01}+n_{10}+n_{11}=n-1$

n_0+n_1=N

n_{ij}의 기대치는 $\frac{N-1}{4}$ 이다.

통계량

$$T=\sum_{i,j=0}^{1}\frac{(n_{ij}-\frac{N-1}{4})^2}{\frac{N-1}{4}}-\sum_{i=0}^{1}\frac{(n_i-\frac{N}{2})^2}{\frac{N}{2}}$$

는 근사적으로 자유도가 2인 χ^2-분포를 따른다. 이것을 다른 식으로 표현하면

$$T=\frac{4}{N-1}(n_{00}^2+n_{01}^2+n_{10}^2+n_{11}^2)-\frac{2}{N}(n_0^2+n_1^2)+1$$

식으로 나타난다. 이 통계량을 이용하여 randomness를 검정하는 방법을 계열검정 (Serial Test)라고 한다.

여기서, χ^2-분포에서 유의 수준 5%, 자유도 2의 한계 값은 5.99이다. 따라서 T의 통계량의 값이 5.99보다 큰 경우에, 계열검정에 대하여 유의 수준 5%로 이 이진수열은 난수성이 없다고 판단되어 기각한다.

3) 일반계열검정 (Generalized Serial Test)

Serial test를 일반화시킨 것으로 키 수열 중에서 규칙적인 패턴이나 상호 의존성을 검출하는데 있어서는 Poker test보다 우수하다. n비트의 키 수열을 $a_0, a_1, \cdots, a_{n-1}$이라 할 때 t비트 열 $\vec{r}=r_0r_1\cdots r_{t-1}$이 j($0\leq j\leq$n-1)번째 위치에서 발생되는 빈도를 $f_0, f_1, \cdots, f_{2^t-1}$, 그리고 t-1비트 열이 j번째 위치에서 발생되는 빈도를 $g_1, g_2, \cdots, g_{2^{t-1}}-1$라 하면, 이상적인 경우 각각의 t비트 열은 n/2t만큼 발생될 것이다. 시험 통계량은 다음 식으로 구해지며, 이 때 자유도는 2^{t-1}이다. t=3, 4, 5일 때 자유도는 각각 4, 8, 16이며, χ^2판단치는 각각 9.48, 15.50, 26.29이다. 단, 여기서 t는 $2\leq t\leq$(n+1)/2 및 n/2t $\geq$5인 범위의 정수로 선택된다.

$$\chi^2 = \frac{2^t}{n}\sum_{i=0}^{2^t-1}(f_i - \frac{n}{2^t})^2 - \frac{2^{t-1}}{n}\sum_{i=0}^{2^{t-1}-1}(g_i - \frac{n}{2^{t-1}})^2$$

4) 포커검정 (Porker Test)

N비트 이진수열 u_N=($u_0, u_1, \cdots, u_{N-1}$)을 m비트 단위로 분할하여 $n = \lfloor \frac{N}{m} \rfloor$ 개의 블록들(u_{km}, $u_{km+1}, \cdots, u_{km+m-1}$)이 m차원에서 균등하게 분포되어 있는가를 검정하는 방법이다.

이 블록 중에서 i개의 1과 m-i개의 0으로 이루어진 블록의 개수를 n(i)라 하면, 이때 N비트의 이진수열이 Random하다면 각 i(1<i<m)에 대하여 n(i)의 평균값은

$$\overline{n(i)} = \binom{m}{i}\frac{n}{2^m}, 0 \le i \le m$$

이 된다. 그러므로 통계량

$$T = \sum_{i=0}^{m}\frac{(n(i) - \binom{m}{i}\frac{n}{2^m})^2}{\binom{m}{i}\frac{n}{2^m}} = \frac{2^m}{n}\sum_{i=0}^{m}\frac{(n(i))^2}{\binom{m}{i}} - n$$

는 근사적으로 자유도가 m인 χ^2-분포를 따른다.

이와 같은 randomness를 검정하는 방법을 포커 검정법 (Poker Test)이라고 한다. 이 검정방법은 도수-m 검정에서 사용되는 통계량보다 단순하므로 이용하기에는 쉬우나 정밀성은 떨어진다.

χ^2-판단치는 (자유도가 m=3일 때 14.067 , m=4일 때 24.996 , m=5일 때 44.654)이다.

5) 자기상관성검정 (Autocorrelation Test)

계열검정은 바로 뒤에 있는 비트로 전이되어 가는 과정을 조사한 것이다. 이와 같은 과정을 d비트 떨어진 비트간의 전이를 생각한 것이 자동상관검정이다.

자동상관검정에는 다음과 같은 통계량들이 사용된다.

① (u_1, u_{d+1})(u_2, u_{d+2}) $\cdots$(u_{n-d}, u_n)에 관하여 계열 검정을 하는 일반적인 경우로 확장하는 것이 한 방법이다.

② 이진수열 N비트 $u_1, u_2, \cdots, u_n$로 부터 ($u_1, u_2, \cdots, u_{n-d}$) 와 ($u_{d+1}, u_{d+2}, \cdots, u_n$)와의 상관관계를 조사하는 통계량으로 다음을 생각하여 보자.

$$A(d) = \sum_{i=1}^{N-d}(1-2u_i)(1-2u_{d+i})$$

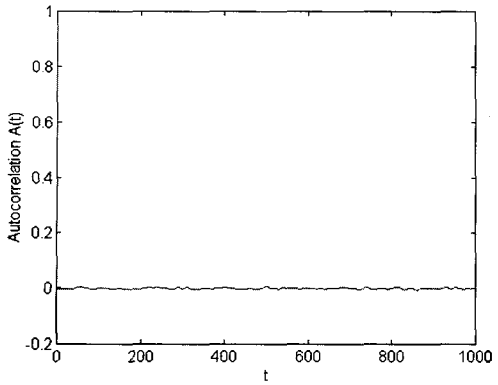
이진수열이 random하다면, 즉 독립이고 같은 분포를 갖으면, 통계량 A(d)의 평균은 0이고 분산은 N-d이다. N-d가 충분히 클 경우 (N-d $\ge$30)에는 중심극한 정리에 의하여 Z= $\frac{A(d)}{\sqrt{N-d}}$ 는 근사적으로 표준 정규분포 N(0, 1)을 따른다.

3.2 안전성 요소 분석

<표 2> 랜덤 테스트 판정 결과

<Table 2> Test results for randomness.

	검증항목	판정치	검정 결과1	검정 결과2	검정 결과3
1	Frequency test	3.841	0.027	1.366	0.000
2	Serial test	5.991	1.386	2.542	2.675
3	Gen-t serial test t = 3 t = 4 t = 5	 9.488 15.507 26.296	 6.916 12.459 23.057	 3.970 8.262 18.490	 2.818 3.138 5.657
4	Poker test m = 3 m = 4 m = 5	 14.067 24.996 44.654	 6.138 17.288 37.310	 5.241 9.919 37.419	 8.197 8.926 25.167
5	Autocorrelation test	max $\le$ 0.05	max=0.0029	max=0.006	max=0.007



[그림 5] 자기상관성 검증 결과

[Fig, 5] Test results for autocorrelation.

<표 3> 개선전과 개선후의 비교분석

<Table 3> Comparisons for the impreved algorithm.

항목	개선 전	개선 후
주기	$\approx 2^{64}$ if gcd(19, 21, 23)=1	$\approx 2^{128}$ if gcd(41, 43, 44)=1
랜덤 테스트	양호함	양호함
선형 복잡도	$2^{19}*2^{21}= 2^{40}$	$2^{41}*2^{43}=2^{84}$

[그림 4]의 개선된 키 수열 발생기를 이용하여 연속되는 출력 데이터를 얻은 후 frequency test, serial test, generalized serial test, poker test 및 autocorrelation test 등의 랜덤성[8]을 시험하였다. 시뮬레이션을 위한 랜덤 테스트용 데이터인 키 수열은 각각 16만 비트씩 3개의 샘플로 취하였으며, 각각 선택된 검증 항목을 테스트하여, 모든 항목 검증 결과가 기준 이내에서 <표 2>와 같이 양호한 출력을 얻을 수 있음을 확인하였다.

개선된 A5 알고리즘은 <표 3>에서 기존의 방식과 비교 할 때 랜덤성이 양호할 뿐만 아니라 주기, 선형복잡도 등 암호 안전성이 크게 개선됨을 확인할 수 있었다.

결론적으로 본 제안 알고리즘은 최근 각광을 받고 있는 IMT-2000 등 무선통신망 정보보호에 적용될 수 있으리라고 판단된다.

4. 결론

본 논문에서는 A5 알고리즘의 키 길이에 따른 문제점을 해결하기 위하여 A5 개선 알 고리즘을 제안하였다. 개선된 A5 알고리즘에 대한 안전성을 분석하기 위하여 랜덤 검증 시뮬레이션을 실시하였으며, 5가지의 랜덤테스트 항목을 모두 통과하였기 때문에 랜덤 특성이 양호함을 확인하였다. 또 다른 안전성에서 주기는 2^{128}이고, 선형복잡도는 2^{84}로 기존의 방식에 비하여, 각각 2^{64}배 및 2^{44}배 향상되었음을 분석하였다.

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

※ 참고 문헌

[1] AES site in http://csrc.nist.gov/encryption/aes/.

[2] NESSIE site in http://www.cosic.esat.kuleuven.ac.be/nessie/.

[3] CRYPTREC site in http://www.ipa.go.jp/security/.

[4] J. Daemen, V. Rijmen, "The Block Cipher Rijndael," Smart Card Research and Applications, LNCS 1820, J.-J. Quisquater and B. Schneier, Eds., Springer-Verlag, 2000, pp. 288-296.

[5] L. Simpson, E. Dawson, J. Dj. Golic and W. Millan, "LILI Keystream Generator," Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptology SAC'2000, LNCS, 2000.

[6] Sober-t16 in https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submission.html.

[7] 류희수, 정교일, "차세대 암호 알고리듬 동향," 한국전자통신연구원 주간기술동향 1052권, 2002년 6월 25일.

[8]. A.J. Menezes, et al., "Handbook of Applied Cryptography(2nd Ed.)," CRC Press, 1997.

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

[10] Hoonjae Lee, Sangjae Moon, "On An Improved Summation Generator with 2-Bit Memory," Signal Processing, Vol.80, No1, pp.211-217, Jan. 2000.

[11] R.Schineier, Applied Cryptography(2nd Ed), Jolm-Wiley & Son, 1996.

[12] B.Park, H.Choi, T.Chang and K.Kang, "Period of Sequences of Primitive Polynomials," Electronics Letters, Vol.29, No.4, pp.390-391, Feb.1993.

[13] A.K. Lenstra & E.R. Verheul, "Selecting Cryptographic Key Sizes," PKC2000, Jan, 2000. (http://security.ece.orst.edu/koc/ece575/papers/cryptosizes.pdf)

이 훈 재

1985년 2월 : 경북대학교 전자공학과 졸업(학사)
1987년 2월 : 경북대학교 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 전자공학과 졸업(박사)
1987년 2월~1998년 1월 : 국방과학연구소 선임연구원
1998년 2월~2002년 2월 : 경운대학교 컴퓨터전자정보공학부 조교수
2002년 3월~현재 : 동서대학교 인터넷공학부 정보네트워크공학전공 조교수
<주관심 분야> 정보보호, 네트워크보안, 정보통신

류 명 춘

1989년 2월 : 영남대학교 전산공학과 졸업(학사)
1991년 2월 : 영남대학교 전산공학과 졸업(석사)
1995년 8월 : 영남대학교 전산공학과 박사과정 수료
1993년 8월~1997년 2월 : 영남대 학교 전산공학과 시간강사
1997년 3월~1999년 2월 : 경운대학교 컴퓨터공학과 전임강사
1999년 3월~현재 : 경운대학교 컴퓨터전자정보공학부 컴퓨터공학전공 조교수
<주관심 분야> 지능정보시스템, 침입탐지, 데이터마이닝