通信情報保護學會論文誌
第 7 卷 第 4 號, 1997. 12

혼합형 이진 수열 발생기

이 훈 재*, 문 상 재**

On A Hybrid Binary Sequence Generator

Hoon Jae Lee, Sang Jae Moon

요 약

키 수열 발생기는 함수 조합 형태에 따라 여러 가지로 분류될 수 있으며, 비도 기본 요소(랜덤 특성, 주기, 선형 복잡도, 상관 면역도, 키 수열의 수 등)는 비선형 함수에 따라 달라진다. 모든 기본 요소를 잘 만족하는 키 수열 발생기는 설계가 어렵지만, 각 요소별로 특성이 뛰어난 발생기를 잘 조합하면 고비도 시스템을 설계할 수 있다. 본 논문에서는 선형 복잡도와 상관 면역도 측면에서 강한 개선된 합산 수열 발생기와 키 수열 수가 많은 일반화된 메모리 다수열 발생기를 조합하여 혼합형 수열 발생기를 제안하고, 비도 수준을 분석하였다.

Abstract

Keystream sequence generator has many types of combining function and its basic factors of crypto-degree(randomness, period, linear complexity, correlation immunity, the number of output sequences) depend on nonlinear function. It is hard to design a high crypto-degree keystream generator with strong criterian, but is possible by combining two strong generators for different factor. In this paper, we combined an improved summation generator(ISUM-BSG) which has a large linear complexity and a high order of correlation immunity with a generalized memory sequence generator(GMEM-BSG) which has a number of output sequences. We called it a hybrid binary sequence generator(HYB-BSG) and analyzed it.

I. 서 론

스트림 암호는 키 수열 발생기와 평문을 XOR시킴으로서 구현이 용이할 뿐 아니라 비도 수준에 대한 객관화(비도의 수치화)가 가능하기 때문에 블록 암호와 더불어 일반적으로

* 국방과학연구소
* * 경북대학교 전기전자공학부

고속 데이터 암호에 많이 사용된다. 스트림 암호의 비도 수준에 대한 평가의 기본 요소는 키 수열 발생기의 랜덤 특성[1-2], 주기[1-4], 선형 복잡도[3,4], 상관 면역도[5]및 출력 키 수열의 수[6-7]등을 들 수 있는데, 이러한 기본요소를 모두 잘 만족하는 발생기는 현재까지 알려진 바 없다.

일반적으로 키 수열 출력에 대한 랜덤 특성(randomness)은 여러 가지 알려진 검증 기술[1-2]로서 측정이 가능하며, 최대 주기(maximal period)는 설계 조건에 제약을 가함으로서 얻을 수 있다. 그러나 선형 복잡도(linear complexity), 상관 면역도(correlation immunity) 및 출력 키 수열의 수(number of output sequences)등은 각 발생 알고리듬 형태에 따라 크게 차이가 난다. 선형 복잡도는 비선형 출력을 동등한 선형 LFSR 모델로 나타낼 때 가장 짧은 LFSR의 단수이며, 비선형 필터형[8-9], 클럭조절형[10] 및 메모리형[11-12]등에서 크게 된다. 상관 면역도는 함수의 단일 입력 또는 다수의 입력과 조합된 최종 출력간에 상관 면역(상호 정보=0)의 정도를 수치화한 것으로서 메모리형 발생기와 다단계 XOR 조합형 발생기[5]등에서 강한 면을 보이고 있다. 그리고 출력 키 수열의 수는 비밀 키의 교체에 따라 나타날 수 있는 모든 키 수열 사이클의 수로서 Golic의 메모리 수열 발생기(memory sequence generator, MEM-BSG)[6-7], switched-tap LFSR(STLFSR)을 이용한 switched-tap 다수열 발생기(switched-tap sequence generator, ST-BSG)[13] 및 일반화된 메모리 다수열 발생기(generalized memory sequence generator, GMEM-BSG)[13]등에서 크게 나타난다. 본 제안에서는 선형 복잡도와 상관 면역도 측면에서 강한 2비트 메모리를 갖는 개선된 합산 수열 발생기(improved summation generator, ISUM-BSG)[14]와 다수열 발생기로 알려진 GMEM-BSG를 혼합하여 최종적으로 비도 요소를 골고루 잘 만족하는 혼합형 키 수열 발생기(hybrid sequence generator, HYB-BSG)를 제안, 분석한다. 이들 두 발생기를 최종 조합하는 방법은 여러 가지 있겠지만 본 논문에서는 랜덤 특성과 선형 복잡도, 상관 면역도의 계산이 용이한 XOR 함수를 사용한다.

II. 혼합형 이진 수열 발생기

키 수열 발생기에서 선형 복잡도를 강화시키기 위하여 일반적으로 비선형 함수를 이용하는데, 그 구성방법상 LFSR의 임의 탭을 비선형 필터형태로 조합하는 비선형 필터형(nonlinear filter type)과 여러개의 LFSR 출력을 비선형 함수로 조합시키는 비선형 조합형(nonlear combiner type)으로 나누어진다. 비선형 조합형은 조합 함수에 메모리 비트를 사용하는 메모리형(combiner with memory), 메모리를 사용하지 않는 비메모리형(memoryless combiner), 그리고 LFSR 클럭 위상을 가변시키는 클럭 조절형(clock-controlled generator)으로 세분된다.

1. 개선된 합산 수열 발생기

메모리형의 일종인 개선된 합산 수열 발생기[14]는 그림 2-1과 같이 2개의 LFSR로 부터 얻은 수열 a_j와 b_j, 과거 carry c_{j-1} 및 과거 메모리 d_{j-1}을 XOR하여 비선형 함수 출력 y_j를 다음과 같이 얻는다.

$$y_j=x_j\oplus d_{j-1}=(a_j\oplus b_j\oplus c_{j-1})\oplus d_{j-1}$$
$$c_j=f(a_j,b_j,c_{j-1})=a_jb_j\oplus(a_j\oplus b_j)c_{j-1}$$
$$d_j=f(a_j,b_j,d_{j-1})=b_j\oplus(a_j\oplus b_j)d_{j-1}$$

여기서, x_j는 j 순간의 합산 수열 발생기 출력, (a)는 LFSR1 의 출력 수열, (b)는 LFSR2 의 출력 수열, (c)는 carry 수열, $c_{-1}=0$(carry 초기값), (d)는 memory 수열, $d_{-1}=0$(메모리 초기값), $j=0, 1, 2 \ldots$ 이다.

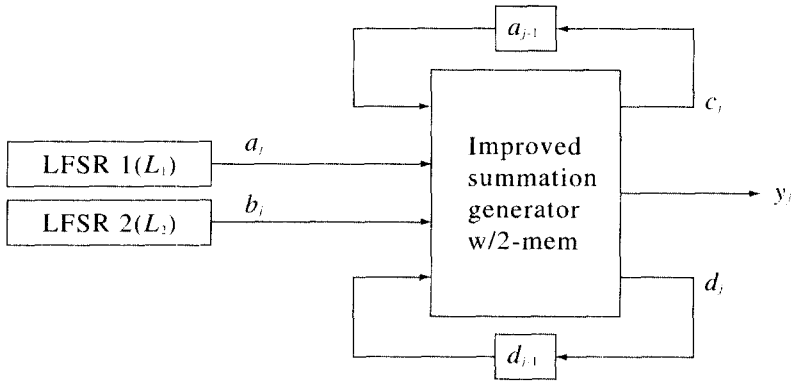


그림 2-1. 2 비트 메모리를 갖는 개선된 합산 수열 발생기

Fig. 2-1. Improved summation generator with 2-bit memory.

합산 수열 발생기[11]는 carry-출력간 상관확률이 1/4로 매우 큰 상관성을 갖기 때문에 출력에 연속된 "0" 또는 "1"이 나타날 때 상관성 공격[12]에 의하여 해독될 수 있지만, ISUM-BSG는 상관성 확률이 1/2인 비선형 함수 출력 d_{j-1}을 추가함으로서 출력으로부터 carry 뿐만 아니라 메모리를 유추할 수 없도록 보완된 것이다.

[정리 2.1] LFSR$_1$과 LFSR$_2$의 초기치가 nonnull이고, gcd(L_1, L_2)=1일 때 ISUM-BSG의 주기, 선형 복잡도 및 상관 면역도는 다음과 같다[14].

(ⅰ) 주기 $P_{ISUM\text{-}BSG}=(2^{L_1}-1)(2^{L_2}-1)$

(ⅱ) 선형 복잡도 $LC_{ISUM\text{-}BSG}\approx P_{ISUM\text{-}BSG}$

(ⅲ) 상관 면역도 $CI_{ISUM\text{-}BSG}=1$(최고 차수 상관 면역도)

2. 일반화된 메모리 다수열 발생기

상용 메모리의 대용량화 추세에 맞추어 Golic 발생기[16-17]를 일반화시킨 것이 그림 2-2의 일반화된 모델(GMEM-BSG)[13]이다. Golic 발생기에서 LFSR$_1$ 대신에 그림 2-2의 점선 블록과 같이 여러개의 LFSR을 비선형 조합하면 수열 (u)의 선형 복잡도를 키울 수 있기 때문에 대형 메모리를 사용할 수 있게 된다. GMEM-BSG 발생기는 LFSR$_2$가 지정한 랜덤 번지에서 랜덤 수열 (v)를 1-비트 읽어(read) 낸 후 비선형 함수 $F_M(u_1, u_2, \ldots, u_M)$의 출력 수열 ($u$)를 LFSR$_3$가 지정한 랜덤 번지에 쓰는(write) 메모리형 발생기이다.

GMEM-BSG 설계 조건:

G1: $1\le k<\min(m_2, m_3)$

G2: $2^{m_3}-1<LC_u$

G3: $m_{1_1}, m_{1_2}, \ldots, m_{1_M}, m_2, m_3$는 쌍마다 서로 소이다(pairwise prime in pairs).

G4: $3\le k\le m_2-2$라면, LFSR$_2$의 k개 비트들은 등간격으로 출력되어야 한다.

[정리 2.2] (GMEM-BSG의 주기, 선형 복잡도, 키 수열의 수)[13]

만일 GMEM-BSG가 설계 조건 G1-G4를 모두 만족하고, 모든 LFSR의 초기치가 nonnull일 때 출력 수열 (v)에 대한 주기 P_v와 선형 복잡도 LC_v는 다음과 같다.

$$P_u P_2 \mid P_v \mid P_u P_2 P_3 \tag{2-1}$$

$$LC_u \sum_{i=0}^{k}\binom{m_2}{i} \le LC_v \le (2^{m_3}-1)LC_u \sum_{i=0}^{k}\binom{m_2}{i} \tag{2-2}$$

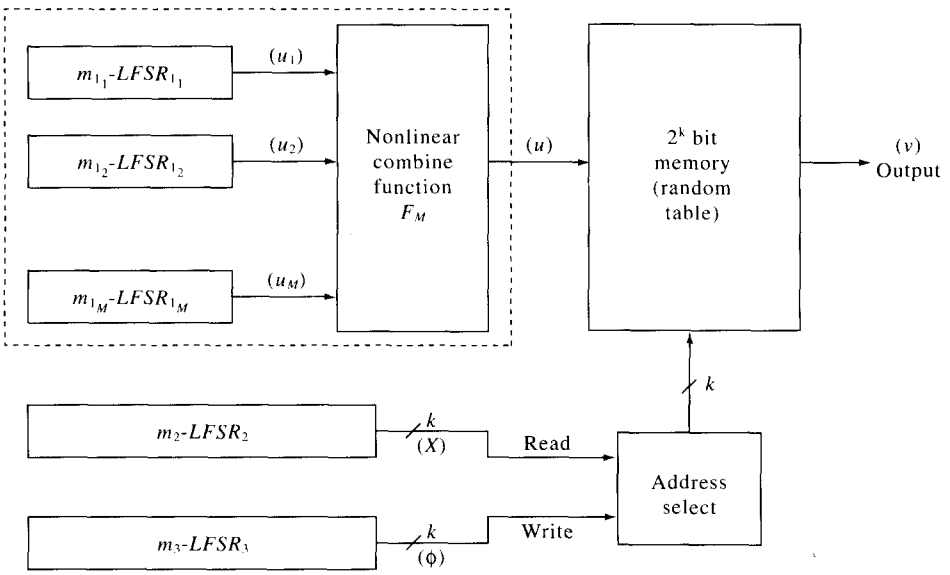


그림 2-2. 일반화된 메모리 다수열 발생기

Fig. 2-2. Generalized memory sequence generator.

여기서 P_u은 수열 (u)의 주기, P_2와 P_3는 $LFSR_2$와 $LFSR_3$의 주기를 말하며, LC_u은 수열 (u)의 선형 복잡도를 말한다. 그리고 만일 GMEM-BSG가 아래의 조건들

$$\gcd(LC_u, m_2)\neq LC_u \tag{2-3}$$

$$\gcd(P_2, \frac{P_u}{\gcd(P_u, P_2)})=1 \tag{2-4}$$

$$\gcd(P_3, P_u P_2)=1 \tag{2-5}$$

를 모두 만족할 때 출력 키 수열의 수는 $P_u P_2 P_3$가 된다.

3. 혼합형 이진 수열 발생기 제안

그림 2-3은 메모리형 발생기의 일종인 ISUM-BSG와 다수열 발생기인 GMEM-BSG를 XOR 조합한 HYB-BSG를 나타낸 것이다. 여기서 두 발생기를 XOR 조합하는 이유는 XOR 함수의 랜덤 특성이 우수할 뿐 아니라 최종 비도 계산이 용이해지기 때문이다. ISUM-BSG는 선형 복잡도와 상관 면역도 측면에서 강하고, 다수열 발생기인 GMEM-BSG는 키 수열 수가 많기 때문에 이들을 조합하면 종합적인 비도수준이 증가될 수 있다.

(설계 조건)

H1: 사용된 모든 LFSR은 각각 최대 주기 탭을 갖으며, 각각의 단수는 서로 소일 것.

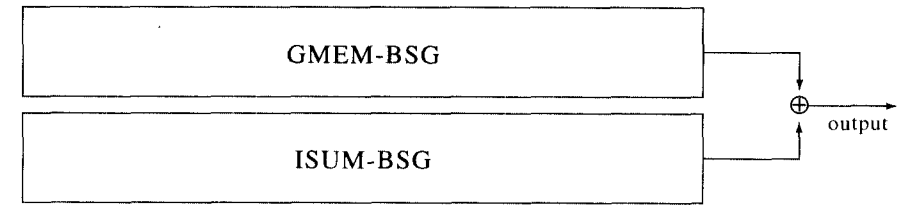
H2: GMEM-BSG의 설계 조건(G1-G4)을 모두 만족할 것.

한편, F_M함수를 구체화시켜 M=4인 F_4 함수를 랜덤 특성과 선형 복잡도 계산이 용이한 조건으로다음과 같이 선택하였다.

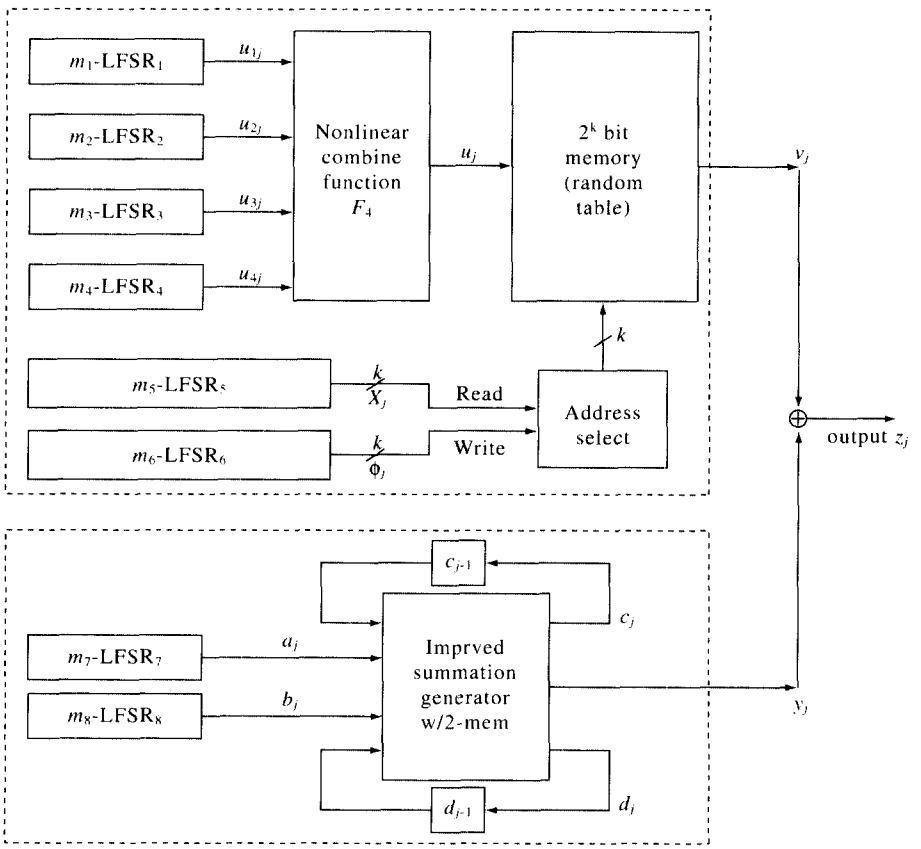
$$F_4(x_1, x_2, x_3, x_4)=x_1x_2x_3\oplus x_1x_3x_4\oplus x_2x_3x_4\oplus x_1x_2\oplus x_1x_3\oplus x_1x_4\oplus x_2x_4\oplus x_2\oplus x_4\oplus 1$$

F_4를 갖는 혼합형 발생기(HYB-BSG):

M=4개의 LFSR이 만들어낸 선형 수열



a) Hybrid binary sequence generator



b) HYB-BSG with F_4

그림 2-3. 혼합형 이진 수열 발생기

Fig. 2-3. Hybrid binary sequence generator.

u_{1j}~u_{4j}는 비선형 함수 F_4를 통하여 u_j로 생성되어 write 번지 수열 Φ_j가 지정한 번지에 저장되고, 다시 read 번지 수열 X_j가 지정한 번지 데이타가 읽혀져서 v_j수열이 생성된다. 그리고 LFSR7, 8 선형 출력은 과거 carry c_{j-1}과 새로 추가된 d_{j-1}에 의해 합산되어 비선형 출력 y_j가 생성된다. 이들 두 수열 v_j와 y_j가 XOR되어 최종 수열 z_j가 생성된다.

[정리 2.3] (F_4를 갖는 HYB-BSG의 주기. 선형

복잡도, 상관 면역도)

만일 제안된 발생기가 설계 조건을 만족하고, 모든 LFSR의 초기치가 nonnull일 때 F_4를 갖는 HYB-BSG의 출력 수열 z_j에 대한 주기 $P_{HYB\text{-}BSG}$, 선형 복잡도 $LC_{HYB\text{-}BSG}$ 및 상관 면역도 $CI_{HYB\text{-}BSG}$는 다음과 같다.

$$\begin{cases} P_{HYB\text{-}BSG}=P_{GMEM\text{-}BSG}\cdot P_{ISUM\text{-}BSG}, \\ (P_1P_2P_3P_4P_5)\cdot(P_7P_8)\,|\,P_{HYB\text{-}BSG}\,|\,(P_1P_2P_3P_4P_5P_6)\cdot(P_7P_8) \end{cases} \tag{2-6}$$

$$\begin{cases} LC_{HYB\text{-}BSG}=LC_{GMEM\text{-}BSG}+LC_{ISUM\text{-}BSG}, \\ LC_u\sum_{i=0}^{k}\binom{m_5}{i}+LC_{ISUM\text{-}BSG}\le LC_{HYB\text{-}BSG}\le(2^{m_6}-1)LC_u\sum_{i=0}^{k}\binom{m_5}{i}+LC_{ISUM\text{-}BSG} \end{cases} \tag{2-7}$$

$$\begin{cases} CI_{HYB\text{-}BSG}=CI_{GMEM\text{-}BSG}+CI_{ISUM\text{-}BSG}, \\ 1\le CI_{HYB\text{-}BSG} \end{cases} \tag{2-8}$$

여기서 $P_i(i=1, 2, \ldots, 8)$는 $LFSR_i$ 출력 수열의 주기, $P_{GMEM\text{-}BSG}$는 GMEM-BSG 출력 v_j의 주기, $P_{ISUM\text{-}BSG}$는 ISUM-BSG 출력 y_j의 주기, LC_u는 u_j 수열의 선형 복잡도, $LC_{GMEM\text{-}BSG}$는 GMEM-BSG 출력 v_j의 선형 복잡도, $LC_{ISUM\text{-}BSG}$는 ISUM-BSG 출력 y_j의 선형 복잡도, $CI_{GMEM\text{-}BSG}$는 GMEM-BSG 출력 v_j의 상관 면역도, $CI_{ISUM\text{-}BSG}$는 ISUM-BSG 출력 y_j의 상관 면역도이다.

(증명)

(i) $(P_1\cdot P_2\cdot P_3\cdot P_4\cdot P_5)\,|\,P_{GMEM\text{-}BSG}\,|\,(P_1\cdot P_2\cdot P_3\cdot P_4\cdot P_5\cdot P_6)$ 이고,

$P_{ISUM\text{-}BSG}=(P_7\cdot P_8)$이므로 식 (2-6)이 성립 된다.

(ii) 참고문헌[13]에 의하여 XOR 함수 출력에 대한 선형 복잡도는 결합되기 전의 각 각의 선형 복잡도의 합이 된다. 그리고 $LC_{GMEM\text{-}BSG}$는 정리 2.2에 의하여 $LC_u\sum_{i=0}^{k}\binom{m_5}{i}\le LC_{GMEM\text{-}BSG}\le(2^{m_6}-1)LC_u\sum_{i=0}^{k}\binom{m_5}{i}$이므로 식 (2-7)이 성립한다.

(iii) 참고문헌[15]에 의하여 상관 면역도가 1인 수열과 다른 수열이 XOR될 경우 전체 수열의 상관 면역도는 최소한 1 이상이 된다. 그리고 $CI_{ISUM\text{-}BSG}=1$이므로 식 (2-8)이 성립된다.

[정리 2.4] (F_4를 갖는 HYB-BSG의 키 수열 수)

만일 일반화 모델인 GMEM-BSG가 Golic의 조건 G1~G4를 만족하고, 또한 아래 조건들

$$\gcd(LC_u, m_5)\neq LC_u \tag{2-9}$$

$$\gcd(P_5, \frac{P_u}{\gcd(P_u, P_2)})=1 \tag{2-10}$$

$$\gcd(P_6, P_uP_5)=1 \tag{2-11}$$

를 만족할 때 F_4를 갖는 HYB-BSG의 출력수열 z_j에 대한 키 수열의 수는

$$N_{HYB\text{-}BSG}=P_1P_2P_3P_4P_5P_6 \tag{2-12}$$

가 된다. 단, $LFSR_i(i=1, 2, \ldots, 6)$는 nonnull 초기상태이다.

(증명) $N_{HYB\text{-}BSG}=N_{ISUM\text{-}BSG}\cdot N_{GMEM\text{-}BSG}=N_{GMEM\text{-}BSG}$
$=P_1P_2P_3P_4P_5P_6$

이다. 왜냐하면 ISUM-BSG는 단일 수열 발생기로서 출력 키 수열 수가 1이기 때문이다.

제안된 발생기는 ISUM-BSG와 GMEM-BSG를 혼합함으로써 기존 발생기보다 훨씬 강한 비도(주기, 선형 복잡도, 상관 면역도 및 키 수열의 수)를 얻을 수 있다.

III. 설계 예제 및 분석

F_4를 갖는 HYB-BSG에 대하여 설계 예제를 제시한 다음 랜덤 특성 검증, 주기, 선형 복잡도, 상관 면역도 및 키 수열의 수 등을 분석한다.

1. 설계 예제

(설계조건)

① $m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8$: 쌍마다 서로 소

② $1 \le k < \min(m_5, m_6)$

③ $2^{m_6}-1 < LC_u$

④ $LFSR_s$에서 읽기번지를 위한 탭출력들은 등간격일 것

그림 2-3의 키 수열 발생기에 대해서 $LFSR_i(1 \le i \le 8)$의 원시다항식은 모든 $i, j(i \ne j)$에 대하여 $\gcd(m_i, m_j)=1$ 즉, 각각 서로 소인 최대주기 탭을 갖는 $LFSR_i(m_i=\deg[g_i(x)])$를 설계조건 ①에 따라 선택하여야 한다. 우선, $k=14$를 택하여 ②에 따라 $m_5=16$, $m_6=15$를 선택하였고, ③에서 $2^{15}-1=32,767 < LC_u = m_1m_2m_3 + m_1m_3m_4 + m_2m_3m_4 + m_1m_2 + m_1m_3 + m_1m_4 + m_3m_4 + m_2 + m_4 + 1 = 33,248$

을 만족하도록 $m_1=17$, $m_2=19$, $m_3=23$, $m_4=29$를 택하였다. 그리고 전체적인 주기와 선형 복잡도를 크게하기 위하여 설계조건 ①을 고려하여 $m_7=31$, $m_8=37$을 선택하였다. 이렇게 결정된 8개의 최대 주기 탭을 갖는 LFSR의 원시 다항식을 생성하면[15] 다음과 같다.

$g_1(x)=x^{17}+x^7+x^5+x^3+x^2+x+1$

$g_2(x)=x^{19}+x^9+x^6+x^3+x^2+x+1$

$g_3(x)=x^{23}+x^{12}+x^6+x^3+x^2+x+1$

$g_4(x)=x^{29}+x^{11}+x^7+x^3+x^2+x+1$

$g_5(x)=x^{16}+x^{10}+x^7+x+1$

$g_6(x)=x^{15}+x^{13}+x^5+x+1$

$g_7(x)=x^{31}+x^3+1$

$g_8(x)=x^{37}+x^{18}+x^2+x+1$

2. 랜덤 특성 검증

제안 발생기의 키 수열 전 주기에 대한 랜덤 특성 검증은 불가능하므로 적당한 길이로 표본 추출(sampling)한 키 수열의 국부적 랜덤 특성(local randomness)[11]을 검증하였으며, 그 결과를 다음 표 3-1에 나타내었다. 검증 방법으로는 몇가지 항목에 대한 이상적인 경우의 키 수열에 대한 적합도를 검증하였으며, 여기에는 널리 알려진 chi-square test를 사용하였다. 그리고 판정 치를 결정하는 유의 수준(significance level)은 일반적 값인 0.05 를 택하였다. Chi-square 분포는 참고 문헌[11]에서 취하였고, 검증 항목은 frequency test, serial test, generalized serial test, Poker test 및 autocorrelation test를 적용하였다. 실제로 임의의 키 수열 출력을 약 16만 비트 표본 데이터로 3가지를 추출하여 국부적인 랜덤검증(χ^2-test, 유의 수준 0.05)을 실시한 결과(표 3-1 및 그림 3-1) 모든 검증 항목을 무난히 통과함으로서 랜덤 특성이 우수하다고 판단된다.

3. 비도요소 분석

HYB-BSG 키 수열 발생기에 대한 비도요소는 정리 2.3에 의해서 다음과 같이 계산된다.

- 주기 $P_{HYB\text{-}BSG} \ge (2^{17}-1)(2^{19}-1)(2^{23}-1)(2^{29}-1)(2^{16}-1)(2^{31}-1)(2^{37}-1) \simeq 10^{51}$
- 선형 복잡도 $LC_{HYB\text{-}BSG} = LC_u \sum_{i=0}^{14} \binom{16}{i} + LC_{ISUM\text{-}BSG} \simeq LC_{ISUM\text{-}BSG} \simeq P_{ISUM\text{-}BSG} = (2^{31}-1)(2^{37}-1) \simeq 10^{20}$

  $(\because LC_u \sum_{i=0}^{14} \binom{16}{i} \ll LC_{ISUM\text{-}BSG})$
- 상관 면역도 $CI_{HYB\text{-}BSG} \ge CI_{ISUM\text{-}BSG} = 1$
- 키 수열 수 $N_{HYB\text{-}BSG} = (2^{17}-1)(2^{19}-1)(2^{23}-1)(2^{29}-1)(2^{16}-1)(2^{15}-1) \simeq 10^{36}$

제시된 F_4 함수 형태의 HYB-BSG는 기존의 ISUM-BSG의 약점인 키 수열의 수를 크게 개선시켰고, GMEM-BSG보다 선형 복잡도와 상관 면역도가 개선되었기 때문에 종합적인 안전성(비도)이 크게 강화된 키 수열 발생기임을 알 수 있다.

표 3-1. 혼합형 발생기의 랜덤 특성 검증 결과

Table 3-1. The results of randomress for HYB-BSG.

Test items	Threshold	Test results		
		Sample 1	Sample 2	Sample 3
1) Frequency test	3.84	0.103	0.025	1.550
2) Serial test	5.99	0.550	2.043	2.087
3) Generalized t-serial test				
t=3	9.48	2.902	5.650	4.211
t=4	15.50	5.086	11.477	6.598
t=5	26.29	10.954	22.709	10.540
4) Poker test				
m=3	14.067	2.300	5.535	3.430
m=4	24.996	12.080	19.450	20.337
m=5	44.654	25.192	26.304	28.654
5) Autocorrelation test	max.≤0.05	max=0.0063	max=0.0064	max=0.0086

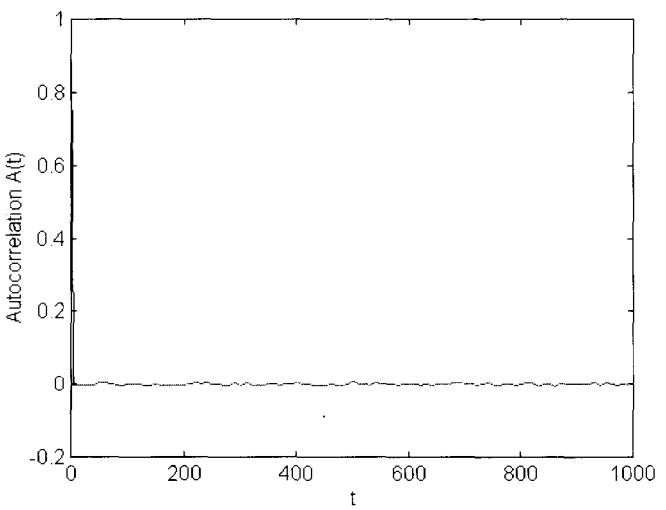


그림 3-1. 자기상관성 검증 결과

Fig. 3-1. The results of autocorrelation test.

IV. 결 론

본 논문에서는 선형 복잡도 및 상관 면역도가 강한 ISUM-BSG와 다수열 출력 수열로 알려진 GMEM-BSG를 조합한 혼합형 HYB-BSG를 제안하였다. 이들 두 발생기를 최종 조합하는 방법은 랜덤 특성과 선형 복잡도, 상관 면역도의 계산이 용이한 XOR 함수를 사용하였다. 제안된 HYB-BSG 발생기의 랜덤 특성, 주기, 선형 복잡도, 상관 면역도 및 키 수열의 수등

비도요소를 분석하였고, 이를 쉽게하기 위하여 간단한 예제를 제시하였다. 제시된 F_4 함수 형태의 HYB-BSG는 기존의 ISUM-BSG의 약점인 키 수열의 수를 크게 개선시켰고, GMEM-BSG보다 선형 복잡도와 상관 면역도가 개선되었기 때문에 종합적인 안전성(비도)이 크게 강화된 키 수열 발생기임을 알 수 있다.

참 고 문 헌

[1] Henry J. Beker and Fred C. Piper, *Cipher systems: The Protection of Communications*, Northwood Books, London, 1982.

[2] Henk C.A. van Tilborg, *An Introduction to Cryptology*, KLUWER ACADEMIC PUBLISHERS, Boston, etc., 1988.

[3] R. A. Rueppel and O. J. Staffiebach, "Products of Linear Recurring Sequences with Maximum Complexity," IEEE Trans. on Infor. Theo., Vol. IT-33, No. 1, pp. 124-131, Jan. 1987.

[4] J. Dj. Golic, "On the Linear Complexity of Functions of Periodic GF(q)" Sequences,"IEEE Trans. on Infor. Theo., Vol. 35, No. 1, pp.69-75, Jan. 1989.

[5] T. Siegenthaler, "Correlation-Immunity of Nonlonear Combining Functions for Cryptographic Applications," IEEE Trans. on Infor. Theo., Vol.IT-30, No. 5, pp. 776-780, Sep. 1984.

[6] J. Dj. Golic, M. M. Mihaljevic, "Minimal Linear Equivalent Analysis of a Variable-Memory Binary Sequence Generator," IEEE Trans. on Infor. Theo., Vol.IT-36, pp.190-192, Jan. 1990.

[7] J. Dj. Golic, "The Number of Output Sequences of a Binary Sequence Generator," LNCS 547, Advances in Cryptology-EUROCRYPT' 91, pp.160-167, 1991.

[8] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

[9] E. J. Groth, "Generation of Binary Sequences with Controllable Complexity," IEEE Trans. on Infor. Theo., Vol. IT-17, No. 3, pp. 288-296, May 1971.

[10] D. Gollmann, "Clock-Controlled Shift Registers : A Review," IEEE Journal on Selected Area in Comm., Vol.7, No.4, pp.525-533, May 1989.

[11] Rainer A. Rueppel, "Correlation Immunity and the Summation Generator," Advances in Cryptology, Proceedings of CRYPTO'85, pp. 260-272, 1985.

[12] E. Dawson, "Cryptanalysis of Summation Generator," Advances in Cryptology-AUSCRYPT'92, Lecture Notes in Computer Science, Springer-Verlag, pp.209-215, 1993.

[13] 이훈재, 문상재, "다수열 출력 이진 수열 발생기," 정보보호학회 논문지 제7권, 제3호, pp. 11-22, 1997년 9월.

[14] 이훈재, 문상재, "2비트 메모리를 갖는 개선된 합산 수열 발생기," 정보보호학회 논문지 제7권, 제2호, pp.93-106, 1997년 6월.

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

□ 著者紹介

이 훈 재

1985년 2월 경북대학교 공과대학 전자공학과(전자공학, 공학사)
1987년 2월 경북대학교 대학원 전자공학과(통신공학, 공학석사)
1987년 2월 - 현재 국방과학연구소 선임연구원
1993년 3월 - 현재 경북대학교 정보통신 박사과정

※ 주관심분야 : 정보보호기술, 디지털 통신, 정보통신망

문 상 재

1972년 2월 서울대학교 공과대학 공업교육과(전자공학, 공학사)
1974년 2월 서울대학교 대학원 전자공학과(통신공학, 공학석사)
1984년 6월 미국 UCLA(통신공학, 공학박사)
1984년 6월 - 85년 6월 UCLA Postdoctor 근무
1984년 6월 - 85년 6월 미국 OMNET 컨설턴트
1974년 ~ 현재 경북대학교 공과대학 전기전자공학부 교수

※ 주관심분야 : 정보보호, 디지털 통신, 정보통신망