DOI: 10.3745/KIPSTC.2009.16-C.3.357

NSG : 비선형 알고리즘을 이용한 블루투스 E_0 암호화시스템의 성능 개선

김 형 락[†] · 이 훈 재[††] · 문 상 재[†††]

요 약

합산수열 발생기는 간단한 하드웨어 또는 소프트웨어로 구현될 수 있고, 주기와 선형복잡도가 높은 특징이 있어 유비쿼터스 시대의 이동환경 보안장치에 적합하다. 하지만 Golic의 상관성공격과 Meier의 고속 상관성공격에 의해 취약성이 노출되었다. 본 논문에서는 합산 수열 발생기 형태의 E_0 알고리즘에서 LFSR과 비선형 귀환 이동 레지스터 NFSR(nonlinear feedback shift register) 를 조합한 형태로 개선하여 비선형성을 높이고, 상관성 공격 등의 암호해독이 어려운 새로운 알고리즘 NSG를 제안하고, 제안 알고리즘에 대하여 안전성 및 성능을 분석하였다.

키워드 : LFSR, NFSR, NSG, 합산수열발생기, 스트림암호화, E_0

NSG : A Security Enhancement of the E_0 Cipher Using Nonlinear Algorithm in Bluetooth System

Kim, HyeongRag[†] · Lee, HunJae[††] · Moon, SangJae[†††]

ABSTRACT

Summation generator can be easily made as a simple hardware or software and it's period and linear complexity are very high. So it is appropriate to mobile security system for ubiquitous environment. But it showed us the weakness by Golic's correlation attack and Meier's fast correlation attack. In this paper, we proposed a Nonlinear Summation Generator(NSG), which is improved by using LFSR and NFSR(nonlinear feedback shift register), is different from E_0 algorithm which use only LFSR in summation generator. It enhanced nonlinearity and is hard to decipher even though the correlation attack or fast correlation attack. We also analyzed the security aspects and the performances for the proposed algorithm.

Keywords : LFSR, NFSR, NSG, 합산수열발생기, 스트림암호화, E_0

1. 서 론

블루투스 기술은 1998년 스웨덴의 에릭슨이 주축이 되어 본격화된 기술로 사용자 정보 암호화를 위해서 E_0 알고리즘을 사용한다[5]. 이때 키 수열 발생을 위해 4개의 선형 귀환 이동 레지스터(linear feedback shift register, LFSR)를 갖는 합산수열발생기를 사용하고 있다.

합산 수열 발생기는 스트림 암호를 위한 키 수열 발생기로 1985년 Rueppel [1]에 의해 최초 제안되었다. 합산 수열 발생기는 일정한 클럭을 갖는 r개의 이진 LFSRs(입력) 및 $\lceil \log_2^r \rceil$ ($=ceiling(\log_2^r)$; $\lceil x \rceil = \infty\{n \in Z | x \le n\}$)비트의 메모리(입력)를 이용하며, 출력은 입력의 정수 합으로부터 얻는다. 합의 LSB(Least significant bit)비트는 키 수열을 생성하고, 나머지 비트들은 캐리(carry)비트들이며 메모리에 저장된다. 캐리 수열은 다음 비트 생성을 위해 결합함수(combining function)의 입력으로 사용되어진다.

LFSR은 하드웨어와 소프트웨어에 적합하며, 빠른 암호속도 및 복호속도가 지원되어 스트림 암호에 많이 사용된다. 또한 원시다항식을 갖는 LFSR에 의해 발생된 수열은 큰 주기 및 좋은 통계적 특성을 갖는다. 그러나 LFSR은 그들의 선형성 때문에 출력 수열로부터 쉽게 예측(암호해독)이 가능하며, 길이 L인 LFSR에 대하여 키 수열의 전체 주기는 귀환 다항식이 알려져 있다면 수열의 연속 L항으로부터 구해지고, 알려져 있지 않다면 $2L$항으로부터 알 수 있다[2].

합산수열 발생기는 간단한 하드웨어 또는 소프트웨어로 구현될 수 있고, 주기와 선형복잡도가 높은 특징이 있어 유비쿼터스시대의 이동환경 보안장치에 적합하다. 하지만 Golic

† 정 회 원 : 포항대학 컴퓨터응용과 부교수
†† 정 회 원 : 동서대학교 컴퓨터정보공학부 부교수
††† 정 회 원 : 경북대학교 전자전기컴퓨터학부 교수
논문접수 : 2009년 2월 24일
수 정 일 : 1차 2009년 5월 12일
심사완료 : 2009년 5월 25일

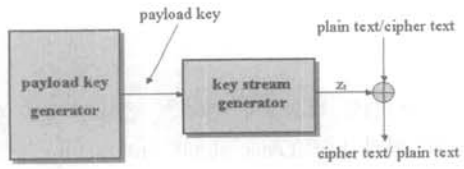
의 상관성공격[3]과 Meier의 고속 상관성공격 [4]에 의해 취약성이 노출되었다. 본 논문에서는 합산 수열 발생기 형태의 E_0 알고리즘 [5]에서 LFSR과 비선형 귀환 이동 레지스터 NFSR(nonlinear feedback shift register) 를 조합한 형태로 개선하여 비선형성을 높이고, 상관성 공격 등의 암호해독이 어려운 새로운 알고리즘 *NSG*를 제안하고, 제안 알고리즘에 대하여 안전성 및 성능을 분석한다.

2. *NSG*(Nonlinear Summation Generator) 제안

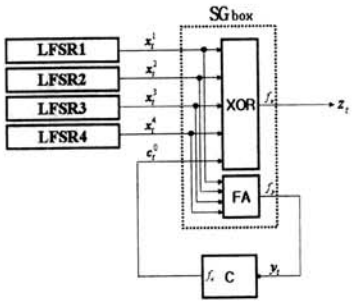
2.1 E_0 암호 알고리즘

짧은 거리에서 개체 간 통신을 제공하는 블루투스 기술에서 사용자의 정보는 패킷 페이로드를 암호화함으로써 보호된다. 이때 암호화는 E_0스트림 암호화기에 의해 수행된다. (그림 1) (a)는 E_0의 적용 범위를 보여주고, (그림 1) (b)는 4개의 LFSR에 기초를 둔 합산수열 발생기를 사용한 E_0 암호 알고리즘을 보여 준다[5].

(그림 1) (a)에서 스트림 암호 시스템 E_0는 세 가지 부분으로 구성된다. 첫 번째 부분은 초기화를 수행하고, 두 번째 부분은 키 스트림 비트를 생성하고, 그리고 세 번째 부분은 암호화와 복호화를 수행한다. 페이로드 키 발생기(payload key generator)는 적절한 순서로 입력 비트들을 조합한 후 키 수열 발생기에서 사용되는 4개의 LFSR에 이동한다. 암호시스템에서 주요한 부분은 두 번째이다. 키 수열 발생기는 Rueppel[1]이 제안한 합산 수열 암호화 발생기(summation stream cipher generator)를 사용한다.



(a) E_0 적용 범위



(b) E_0 알고리즘

(그림 1) E_0 스트림 암호화시스템

2.2 비선형 E_0 알고리즘 설계

본 절에서는 기존의 블루투스 암호 알고리즘에서 사용하고 있는 합산수열 발생기의 비선형성을 증가시키기 위하여 de Bruijn 수열 발생기로 구현된 NFSR을 사용한 *NSG*를 제안한다.

2.2.1 de Bruijn 수열[6,7]

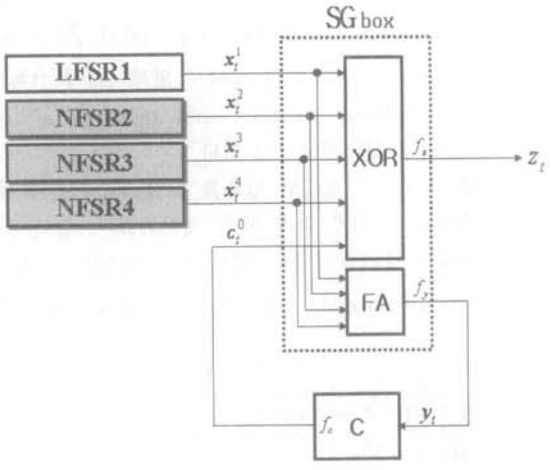
0과 1로 이루어진 주기 2^n인 수열 $\{a_i\}$에 대하여 연속으로 나타나는 2^n개의 벡터 $V_i = (a_i, a_{i+1}, a_{i+2}, \cdots, a_{i+n-1})$가 모두 다를 때 이 수열 $\{a_i\}$을 de Bruijn 수열이라고 한다. de Bruijn 수열은 예측이 불가능하면서 최대의 주기를 얻을 수 있고, 무작위성과 큰 선형 복잡도를 가진다. 또한 비선형성이 높으며 LFSR로부터 쉽게 생성할 수 있는 특성을 갖고 있다 [6,7].

Theorem 1 (Chang-Park, Chang-Song). 최대주기를 갖는 n단 LFSR의 귀환함수 f에 대하여 $h = f + x_1 x_2 \cdots x_{n-1} + 1$ 라 할 때 h를 귀환함수로 하는 이동레지스터에 의해 발생되는 수열을 de Bruijn 수열이라 하고, 이때 주기는 2^n이다 [6,7].

2.2.2 *NSG* 제안

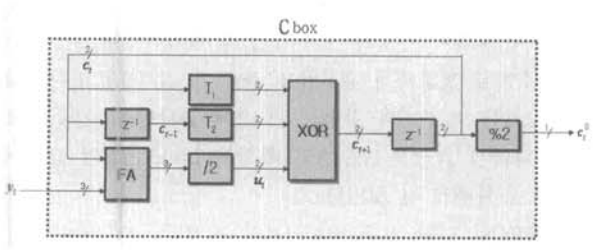
기존의 E_0 알고리즘에서 사용하는 합산수열발생기는 4개의 LFSR에 기초를 둔 합산수열 발생기를 사용하지만, 본 논문에서는 (그림 2)에서 보는 것처럼 1개의 LFSR과 3개의 NFSR을 사용한 합산수열 발생기인 *NSG*를 제안한다. 이때 LFSR은 출력 키 수열의 최소 주기를 보장해주고, 0-1 균형성을 제공해준다. 그리고 비선형 출력함수를 가지는 NFSR은 암호화 알고리즘에 비선형성을 높여준다 [8].

(그림 2)에서 살펴보면 x_t^1, x_t^2, x_t^3 및 x_t^4는 $LFSR_1$, $NFSR_2$, $NFSR_3$ 및 $NFSR_4$ 각각의 출력이고, SG box의 출력은 f_z함수에 의해 z_t가 된다. 캐리 c_t^0는 f_c함수에 의한



(그림2) 제안된 *NSG*

출력 y_t를 받은 c box의 출력으로 결정된다. (그림 3)에서는 y_t를 입력받아 캐리 c_t^0를 출력하는 c box를 보여준다.



(그림 3) c box

(그림 2)에서 x_t^i를 $LSFR_i$ 또는 $NSFR_i$의 t번째 심볼로 표시할 때, NSG의 출력은 아래의 식(1)과 식 (2)에 의해 주어진다.

$$z_t = f_z(x_t^1,x_t^2,x_t^3,x_t^4,c_t^0) = x_t^1 \oplus x_t^2 \oplus x_t^3 \oplus x_t^4 \oplus c_t^0 \in \{0,1\} \quad (1)$$

$$y_t = f_y(x_t^1,x_t^2,x_t^3,x_t^4) = \sum_{i=1}^{4} x_t^i \in \{0,1,2,3,4\} \quad (2)$$

그리고 (그림 3)에서 c box의 출력은 식 (3)과 식(4)에 의해 주어진다.

$$c_{t+1}^0 = f_c(x_t^1,x_t^2,x_t^3,x_t^4,c_t^0) = \{u_{t+1} \oplus T_1[c_t] \oplus T_2[c_{t-1}]\} \% 2 \in \{0,1\} \quad (3)$$

$$u_{t+1} = (u_{t+1}^1, u_{t+1}^0) = \lfloor \frac{y_t + c_t}{2} \rfloor \in \{0,1,2,3\} \quad (4)$$

여기에서 $T_1[\cdot]$, $T_2[\cdot]$는 GF(4)상에서 두 개의 다른 선형 전단사(bijection)이다. GF(4)가 최소다항식 x^2+x+1에 의해 생성된다고 가정하고, α를 GF(4)에서 이 다항식의 근으로 두었을 때, 사상 T_1과 T_2는 아래 식(5) 및 (6)과 같이 정의된다.

$$T_1 : GF(4) \rightarrow GF(4), \quad x \mapsto x \quad (5)$$

$$T_2 : GF(4) \rightarrow GF(4), \quad x \mapsto (\alpha+1)x \quad (6)$$

<표 1>에서 요약된 것처럼 GF(4)의 요소들은 이진 벡터로서 쓸 수 있다.

사상이 선형이기 때문에, XOR게이트를 사용해서 식 (7)과 (8)로 구현할 수 있다. 즉,

$$T_1 : \quad (x_1,x_0) \mapsto (x_1, x_0) \quad (7)$$

〈표 1〉 T_1 과 T_2 의 변환

x	$T_1[x]$	$T_2[x]$
00	00	00
01	01	11
10	10	01
11	11	10

$$T_2 : \quad (x_1,x_0) \mapsto (x_0, x_1 \oplus x_0) \quad (8)$$

NSG는 1개의 LFSR과 3개의 NFSR 그리고 1개의 캐리 비트를 가진다. 1개의 LFSR의 길이는 $L_1 = 129$이고, 3개의 NFSR 각각은 $N_2 = 23$, $N_3 = 37$, $N_4 = 67$이다. 모든 메모리 비트들은 NSG에게 256비트의 내부 상태 비트를 제공하며, 256비트 비밀키(key)와 256비트 초기화 벡터(iv)를 XOR한 결과 값 256비트를 내부 상태에 채운다. NSG의 출력 키 수열은 이동레지스터의 출력수열과 캐리 수열이 합쳐져서 생성된다.

$LFSR_1$, $NFSR_2$, $NFSR_3$ 및 $NFSR_4$의 귀환 다항식은 각각 다음과 같은 원시다항식 $p_1(x)$, $p_2(x)$, $p_3(x)$ 및 $p_4(x)$로부터 선택되며, $LFSR_1$의 모든 비트가 0 상태(all zero state)로 초기화 되는 것을 허용하지 않는다.

$$p_1(x) = x^{129} \oplus x^{117} \oplus x^9 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x^1 \oplus x^0 \quad (9)$$

$$p_2(x) = x^{22}x^{21}x^{20}x^{19}x^{18}x^{17}x^{16}x^{15}x^{14}x^{13}x^{12}x^{11}x^{10}x^9x^8x^7x^6x^5x^4x^3x^2x^1 \oplus x^{23} \oplus x^{19} \oplus x^8 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x^1 \oplus x^0 \oplus 1 \quad (10)$$

$$p_3(x) = x^{36}x^{35}x^{34}x^{33}x^{32}x^{31}x^{30}x^{29}x^{28}x^{27}x^{26}x^{25}x^{24}x^{23}x^{22}x^{21}x^{20}x^{19}x^{18}x^{17} x^{16}x^{15}x^{14}x^{13}x^{12}x^{11}x^{10}x^9x^8x^7x^6x^5x^4x^3x^2x^1 \oplus x^{37} \oplus x^{23} \oplus x^8 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x^1 \oplus x^0 \oplus 1 \quad (11)$$

$$p_4(x) = x^{66}x^{65}x^{64}x^{63}x^{62}x^{61}x^{60}x^{59}x^{58}x^{57}x^{56}x^{55}x^{54}x^{53}x^{52}x^{51}x^{50}x^{49}x^{48}x^{47} x^{46}x^{45}x^{44}x^{43}x^{42}x^{41}x^{40}x^{39}x^{38}x^{37}x^{36}x^{35}x^{34}x^{33}x^{32}x^{31}x^{30}x^{29}x^{28}x^{27} x^{26}x^{25}x^{24}x^{23}x^{22}x^{21}x^{20}x^{19}x^{18}x^{17}x^{16}x^{15}x^{14}x^{13}x^{12}x^{11}x^{10}x^9x^8x^7x^6 x^5x^4x^3x^2x^1 \oplus x^{67} \oplus x^{43} \oplus x^{10} \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus x^2 \oplus x^1 \oplus x^0 \oplus 1 \quad (12)$$

3. 분 석

본 절에서는 실험적인 결과에 기초를 두는 NSG의 키 수열 특성을 제공하며 NSG가 알려진 공격에 안전함을 보여준다.

3.1 키 수열의 특성

PN 이진 수열들을 위한 세 가지 기본 요구사항은 긴 주기, 높은 선형복잡도, 좋은 통계 특성이며, 긴 주기는 암호화된 긴 메시지를 사용할 때 동일한 키 수열의 재사용을 방지하고, 높은 선형 복잡도는 Berlekamp-Massey 알고리즘 [9]을 이용한 공격에 견딜 수 있도록 한다. 마지막으로 좋은 통계적인 특성은 키 수열이 "0"과 "1" 중 어느 한 방향으로 치우친 취약점을 이용한 공격에 견딜 수 있게 한다.

de Bruijn 수열을 포함한 제안된 알고리즘(키수열 발생기)에서 $\{x_t^1\}$, $\{x_t^2\}$, $\{x_t^3\}$ 및 $\{x_t^4\}$ 를 de Bruijn 수열을 포함한 원시다항식의 차수 L_1, N_2, N_3 및 N_4로 서로소인 4개의 이진 m-수열 이라 한다. 여기에서 $N2 \le N3 \le N4$ 라고 했을 때 제안된 알고리즘(키 수열 발생기)에서 주기 T는 다음과 같이 정의된다.

$$T = (2^{L_1} - 1) \cdot 2^{N_4} \tag{13}$$

짧은 단수에 대한 시뮬레이션 결과인 <표 2>에서는 시뮬레이션 주기값 T_{sim}이 주기 T와 정확하게 일치하여 $T_{sim} = T$을 만족함을 확인할 수 있었다. 또한 입력 $\{x_t^1\}$, $\{x_t^2\}$, $\{x_t^3\}$ 및 $\{x_t^4\}$에 대한 배타적 논리합인 출력 수열 $\{z_t\}$의 선형복잡도 LC는 그 주기 T와 근사함을 보여주었다.

$$T_{sim} = T \tag{14}$$

$$LC \approx T \tag{15}$$

위 <표 2>의 결과 값은 식(13)~(15)를 증명하는 대신 시뮬레이션을 통해 상한 경계가 잘 맞아 들어감을 보여주었다.

<표 2>에서 N열은 실수 상에서 더해지는 m-수열들의 합($N = L_1 + N_2 + N_3 + N_4$)이다. T 열은 식 (13)에 따른 합산 수열의 계산된 주기 값이다. T_{sim}열은 합산 수열의 시뮬레이션 된 주기의 결과 값을 나타내고, LC열은 언급된 차수의 다른 원시 최소다항식의 모든 가능한 모든 조합으로 얻어진 최소 선형복잡도 LC값을 보여준다. 짧은 단수에 대한 <표 2>의 시뮬레이션 결과에서 de Bruijn 수열의 주기 T는 시뮬레이션 결과 $T = T_{sim}$을 만족하였다. 즉, 식 (13)은 주기를 정확하게 표현함을 확인 할 수 있었고, 선형복잡도 LC는 식 (14)와 같이 주기 T에 근사함을 보여 주고 있다. 따라서 N값을 256 으로 확장하더라도 LC의 값은 주기 T에 근사하게 될 것이다.

〈표 2〉 *NSG*에서 시뮬레이션 된 주기 T_{sim}와 선형복잡도 LC

Taps of shift register	N	이론 추정치	시뮬레이션 값	
		T	T_{sim}	LC
(8,2,3,5)	18	8,160	8,160	8,156
(8,3,4,5)	19	8,160	8,160	8,157
(8,2,3,7)	20	32,640	32,640	32,641
(8,3,4,7)	22	32,640	32,640	32,640
(8,4,5,7)	24	32,640	32,640	32,638
(8,2,3,11)	24	522,240	522,240	522,241
(8,3,4,11)	26	522,240	522,240	522,239
(8,4,5,11)	28	522,240	522,240	522,239
• • • •	• • • •	• • • •	• • • •	• • • •
(129,23,37,67)	256	$(2^{129}-1)\cdot 2^{67}$	$((2^{129}-1)\cdot 2^{67})$	

*NSG*의 설계 기준 비도 (보안 레벨)은 2^{128}이며 여러 가지 공격에 대하여 기본적인 키 수열특성은 비선형성과 큰 선형복잡도 및 긴 주기 때문에 안전하게 된다.

3.2 공격 분석

본 절에서는 *NSG*의 고속 상관성 공격, Time/Memory/Data Tradeoff(시간/메모리/데이터 거래) 공격에 대하여 설명한다.

3.2.1 고속 상관공격

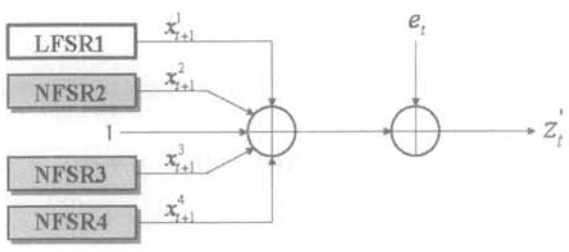
<표 3>은 *NSG*에서 메모리 비트 c_{t+1}^0(여기에서 $c_{t+1} = (c_{t+1}^1, c_{t+1}^0)$)와 키 출력 수열 비트 z_t간의 상관관계를 보여주는데, 이때 c_{t+1}^0와 z_t가 같아질 확률 $p(c_{t+1}^0 = z_t)$는 0.5 로 나타난다. $z_t = x_t^1 \oplus x_t^2 \oplus x_t^3 \oplus x_t^4 \oplus c_t^0$ 이고 $z_{t+1} = x_{t+1}^1 \oplus x_{t+1}^2 \oplus x_{t+1}^3 \oplus x_{t+1}^4 \oplus c_{t+1}^0$ 으로 표현할 때, $c_{t+1}^0 = z_t \oplus 1$ 이 확률 0.5 로 유지되기 때문에

$z_{t+1} = x_{t+1}^1 \oplus x_{t+1}^2 \oplus x_{t+1}^3 \oplus x_{t+1}^4 \oplus z_t \oplus 1$ 이 확률 0.5 를 유지한다.

z_t'을 키 수열의 이진 시차 비트라 두면, 임의 시점에서 $z_t' = z_{t+1} \oplus z_t$ 가 되고, 이때

$z_t' = x_{t+1}^1 \oplus x_{t+1}^2 \oplus x_{t+1}^3 \oplus x_{t+1}^4 \oplus 1$이 된다. *NSG*의 이진 시차 수열 z_t'은 (그림 4)와 같이 1개의 LFSR과 3개의 NFSR의 출력 합 그리고 이진잡음 e_t를 더한 것으로 형태로 나타낼 수 있으며, 이 모델에서 잡음 확률 e_t는 0.0 이다. 따라서 이 모델에서는 상관성 공격[3]이 어렵다고 할 수 있다.

*NSG*에 대한 고속 상관성 공격 알고리즘은 이동레지스터 수열에 기반한 잡음 모델로 생각 할 수 있다. 패리티 검사에 기초한 반복 확률 알고리즘이 관측된 수열에 대한 이진



(그림 4) *NSG*의 고속 상관성 공격 모델

〈표 3〉 *NSG*의 c_{t+1}^0 와 z_t 의 상관특성

x_t^1	x_t^2	x_t^3	x_t^4	c_t^0	c_t	c_{t+1}^0	c_{t+1}	Z_t
0	0	0	0	0	00	0	00	0
					10	0	10	
0	0	0	0	1	01	0	10	1
					11	0	00	
0	0	0	1	0	00	0	00	1
					10	0	10	
0	0	0	1	1	01	1	11	0
					11	1	11	
0	0	1	0	0	00	0	00	1
					10	0	10	
0	0	1	0	1	01	1	11	0
					11	1	11	
0	0	1	1	0	00	1	01	0
					10	1	01	
0	0	1	1	1	01	1	11	1
					11	1	11	
0	1	0	0	0	00	0	00	1
					10	0	10	
0	1	0	0	1	01	1	11	0
					11	1	11	
0	1	0	1	0	00	1	01	0
					10	1	01	
0	1	0	1	1	01	1	11	1
					11	1	11	
0	1	1	0	0	00	1	01	0
					10	1	01	
0	1	1	0	1	01	1	11	1
					11	1	11	
0	1	1	1	0	00	1	01	1
					10	1	01	
0	1	1	1	1	01	0	00	0
					11	0	10	
1	0	0	0	0	00	0	00	1
					10	0	10	
1	0	0	0	1	01	1	11	0
					11	1	11	
1	0	0	1	0	00	1	01	0
					10	1	01	
1	0	0	1	1	01	1	11	1
					11	1	11	
1	0	1	0	0	00	1	01	0
					10	1	01	
1	0	1	0	1	01	1	11	1
					11	1	11	
1	0	1	1	0	00	1	01	1
					10	1	01	
1	0	1	1	1	01	0	00	0
					11	0	10	
1	1	0	0	0	00	1	01	0
					10	1	01	
1	1	0	0	1	01	1	11	1
					11	1	11	
1	1	0	1	0	00	1	01	1
					10	1	01	
1	1	0	1	1	01	0	00	0
					11	0	10	
1	1	1	0	0	00	1	01	1
					10	1	01	
1	1	1	0	1	01	0	00	0
					11	0	10	
1	1	1	1	0	00	0	10	0
					10	0	00	
1	1	1	1	1	01	0	00	1
					11	0	10	

[Note] $c_t = (c_t^1, c_t^0)$, $c_{t+1} = (c_{t+1}^1, c_{t+1}^0)$

시차 수열로부터 이동레지스터 수열을 재구성할 목적으로 에러 정정 과정을 수행할 수 있도록 한다.

고속 상관성 공격 알고리즘 [3]은 다음과 같이 나타내어진다.

① 관찰된 키 수열로부터 이진 시차수열을 계산한다.
② 각각의 이진시차수열 z_t, $t=1,2,3,...,k$에 대하여 패리티 검사 값을 계산한다.
③ 각 z_t에 대한 패리티 검사 값들을 이용하여 오차의 확률 p_t를 계산한다.
④ 만일 $p_t > 0.5$ 이면, $t=1,2,3,...,k$에서의 $z_t' = z_t' \oplus 1$ 과 $p_j = 1-p_j$ 를 설정한다.
⑤ 모든 패리티 검사들이 만족할 때까지 되풀이 한다.

x를 개별 이동레지스터 피드백 다항식에 대한 전체 차수라고 할 때, 고속상관성 공격에 대한 복잡도 및 키 수열 요구량은 $O(2^{x/4})$ 이다[3].

3.2.2 시간/메모리/데이터 거래 공격

시간/메모리/데이터 거래 공격[10]의 목적은 주어진 시간 내에 내부 상태를 찾아내는데 있으며, 공격은 두 단계로 처리된다. 선 처리 단계 동안에 암호 해독기는 가능한 내부 상태를 출력 키 수열과 연관된 접두어에 검사테이블(look-up table)을 작성한다. 실제 공격 단계에서는, 검사테이블 검색을 통하여 알려진 키 수열 일부 비트를 가지고 유사한 내부 상태를 발견하려 한다.

S,M,T,P 그리고 D는 각각 내부 상태의 공간 크기, (log2S 와 같은 이진 워크 크기에서의)메모리 용량, (검사테이블에 대한)계산시간, (검사 테이블에 대한) 사전 계산시간, 그리고 (키 갱신이 없는) 데이터 길이(즉, 알려진 데이터의 길이)를 표시한다. 시간/메모리/데이터 거래 공격 [10]은 $T \cdot M = s$, $P = M$ 그리고, $D = T$ 를 만족한다. 256비트의 내부 상태를 갖는 *NSG*에 대하여, T나 M이 2^{128}보다 더 크게 나타나며, 이는 키 전수공격보다 더 어렵다.

3.3 성능비교

제안된 *NSG*알고리즘은 E_0에서 적용한 합산수열발생기의 취약점을 보강하였다. 즉, 취약점이 알려진 기존의 합산수열발생기에서 선형 입력 *LFSR*을 대체하고자 비선형 함수인 de Bruijn 수열을 적용하였다.

〈표 4〉 성능 요약표

구 분		E_0 합산수열발생기	제안된 *NSG*
보안요소	LFSR 갯수	4	1
	NFSR 갯수	0	3 (de Bruijn)
	LC	$\approx T_{E_0}$	$\approx T$
security analysis	고속상관성 공격	weak	secure
	TMTO 공격	weak	secure

[Note] $T_{E_0} = (2^{L_1}-1)(2^{L_2}-1)(2^{L_3}-1)(2^{L_4}-1)$, 여기서 L_1, L_2, L_3 및 L_4 는 4개 LFSR 각각의 길이

<표 4> 에서와 같이 제안된 *NSG*는 선형복잡도 *LC*가 주기에 근사하기 때문에 기존 합산수열발생기의 특성을 보유하고 있으며, 비선형 요소인 de Bruijn 발생기를 적용함으로서 기존의 공격방법에 안전함을 확인하였다.

4. 결 론

기존의 E_0블루투스 암호 알고리즘은 LFSR을 입력으로 하는 합산수열 발생기를 사용하였다. 본 논문에서는 기존의

합산수열 발생기에 비해 더 높은 비 선형성을 얻기 위해 LFSR 과 NFSR을 적절히 조합한 합산수열발생기인 *NSG*를 제안하였다. *NSG*의 설계 기준비도 (보안 레벨)는 2^{128}이며, 여러 가지 안전성 분석에 안전함을 보였다. 따라서 *NSG*는 근거리 무선통신 기술의 표준으로 자리 잡고 있는 블루투스 기술의 보안성을 크게 향상시킬 수 있다.

참 고 문 헌

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

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

[3] 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.

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

[5] "Specification on the Bluetooth System", version 1.1 February, 22, 2001.

[6] T. Chang, B. Park, Y. H. Kim, "An Efficient Inplementation of the D-Homomorphism for Generation of de Bruijn Sequences", IEEE Transactions on Information Theory, 45, 4, 1280-1283, 1999.

[7] T. Chang, I. Song, "Cross-Joins in de Bruijn Sequences and Maximum Length Linear Sequences", IEICE Transactions Fundamentals, Vol.E76-A, No.9, pp.1494-1501, September, 1993.

[8] Martin Hell, Thomas Johansson, Willi Meier, "Grain: A stream Cipher for constrained Environments, International Journal of Wireless and Mobile Computing", Vol.2, No.1 pp.86-93, 2007.

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

[10] S. Babbage, "Improved Exhaustive Search Attacks on Stream cipher", European Convention on Security and Detection, IEEE Conference Publication, Vol.408, pp.161-166, 1995

김 형 락

e-mail : hrkim@pohang.ac.kr

1992년 2월 경북대학교 전자공학과 졸업 (공학사)

1994년 2월 경북대학교 전자공학과(공학석사)

1999년 2월 경북대학교 전자공학과(박사수료)

1994년 1월~1995년 10월 LG 전자기술원 영상미디어연구소 연구원

1995년 11월~1996년 2월 (주)문화방송 기술연구소 연구원

1996년 3월~현 재 포항대학 컴퓨터응용과 부교수

관심분야 : 암호이론, 정보통신, 이동네트워크, u-네트워크 보안 등

이 훈 재

e-mail : hjlee@dongseo.ac.kr

1985년 2월 경북대학교 전자공학과 졸업 (공학사)

1987년 2월 경북대학교 전자공학과(공학석사)

1998년 2월 경북대학교 전자공학과(공학박사)

1987년 2월~1998년 1월 국방과학연구소 선임연구원(개발팀장)

1998년 3월~2002년 2월 경운대학교 컴퓨터공학과 조교수

2002년 3월~현 재 동서대학교 컴퓨터정보공학부 부교수

2007년 6월~현 재 동서대학교 유비쿼터스 IT전문인력양성사업단장(NURI)

관심분야 : 암호이론, 정보통신/네트워크, u-네트워크 보안, 부채널 공격 등

문 상 재

e-mail : sjmoon@ee.knu.ac.kr

1972년 2월 서울대학교 공업교육(전자)과 (공학사)

1974년 2월 서울대학교 전자공학과(공학석사)

1984년 6월 미국 UCLA 전자공학과(공학박사)

1984년 7월~1985년 6월 UCLA Postdoctoral 근무

1984년 7월~1985년 6월 미국 OMNET 컨설턴트

1974년12월~현 재 경북대학교 전자전기컴퓨터학부 교수

2000년 8월~현 재 경북대학교 이동네트워크 정보보호기술 연구센터 소장

2002년 2월~2008년 12월 한국정보보호학회 명예회장

관심분야 : 정보보호, 디지털 통신, 이동 네트워크 등