PingPong-128 키수열 발생기

정회원 이 훈 재*, 문 상 재**, 박 종 욱***

PingPong-128 Keystream Generator

Hoon-jae Lee*, Sang-jae Moon**, Jong-Wook Park*** ***Reguler Members***

요 약

본 논문에서는 합산 수열 발생기에 기초한 새로운 PingPong-128(PP-128) 키수열 발생기를 제안한다. 제안된 PingPong-128은 PingPong 계열로 제시된 특수한 암호이며, 128비트 키와 128비트 초기 벡터 그리고 258 비트의 내부 상태를 갖으며, 128 비트의 비도 수준을 유지한다. PingPong-128에 대하여 합산 수열발생기와 클럭 조절형 키 수열 발생기에 대한 알려진 공격에 대한 암호 분석을 실시하였다.

Key Words : Keystream, 스트림 암호(Stream Cipher), 합산 수열 발생기, 주기, 선형 복잡도

ABSTRACT

In this paper, we propose the PingPong-128(PP-128) keystream generator, based on summation generator. Proposed PingPong-128, a specific cipher of the PingPong Family, takes 128 bits key and 128 bit initial vector, has 258 bit internal state, and achieves a security level of 128 bits. The security analysis of PingPong-128 is presented, including the resistence to known attacks against the summation generator and other clock-controlled generators.

Ⅰ. 서 론

선형 귀환 이동 레지스터(LFSR, linear feedback shift registers)는 하드웨어와 소프트웨어에 적합하며, 빠른 암호속도 및 복호속도가 지원되어 스트림 암호에 많이 사용된다. 또한 원시다항식을 갖는 선형 귀환 이동 레지스터에 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 완전한 주기는 귀환 다항식이 알려져 있다면 수열의 연속 L항으로부터 구해지고, 알려져 있지 않다면 $2L$항으로부터 알 수 있다[1]. 선형성을 갖는 취약점을 회피할 뿐 아니라 LFSR의 좋은 통계 특성을 이용하기 위한 키 수열 발생기의 구성 요소로서 일반적으로 LFSR을 사용하며, 조합 함수 또는 필터 함수를 이용한 비선형 부울 함수를 사용하거나 불규칙한 클럭 제어 LFSR을 사용하는 방법으로 스트림 암호의 비선형성을 증대시킨다.

합산 수열 발생기는 스트림 암호를 위한 키 수열 발생기로 1985년 Rueppel[5]에 의해 제안되었다. 합산 수열 발생기는 일정한 클럭을 갖는 r개의 이진 LFSRs(입력) 및 $\lceil \log_2 r \rceil$ 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 사

※본 연구는 정보통신부지원 대학 IT 연구센터 육성지원사업에 의하여 수행되었습니다.
* 동서대학교 컴퓨터정보공학부 (hjlee@dongaeo.ac.kr), ** 경북대학교 전자전기컴퓨터공학부 (sjmoon@knu.ac.kr)
*** 국가보안기술연구소 (khspjw@etri.re.kr)
논문번호 : KICS2004-12-307, 접수일자 : 2004년 12월 xx일

용되어진다.

합산 수열 발생기는 Dawson의 divide-and-conquer-attack[1]에 의하여 해독되었으며, 또한 Golic의 상관 공격[2] 및 Meier 등의 고속 상관 공격[4]에 의하여 취약점을 보였다. 한편, 그림 b)에 나타낸 LM 발생기[8,10]의 d_j 메모리 비트는 Meier 공격 및 Dawson 공격에 대응하기 위하여 추가되었으며, Golic의 고속 상관 공격에는 취약점을 보일 수 있다.

본 논문에서 제안된 PingPong-128은 기존의 LM 합산 수열 발생기에서 상호 클럭 조절형 구조(Mutual clock-control Structure)를 추가하여 합산 수열발생기를 기초로 하는 새로운 발생기이며, 상호 클럭 조절형 구조의 목적은 출력되는 키 수열에 비선형성을 증가시켜 상관 공격 등의 암호해독을 어렵게 하는 것이다.

Ⅱ. PingPong-128 제안

본 절에서는 PingPong 계열 및 PingPong-128 키 수열 발생기를 제안한다.

2.1 PingPong 계열 제안

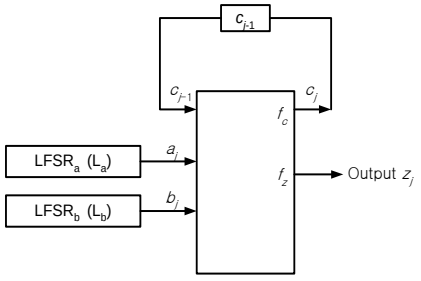
$r=2$인 합산 수열 발생기[5, 9-10]는 그림 1 a)와 같이 2개의 LFSR과 1-비트 메모리에 기초를 두는 합산 수열 발생기이며, $r=2$인 LM 합산 수열 발생기[8]는 그림 1 b)와 같이 d_{j-1} 메모리를 갖는다. 여기서 두개의 LFSR을 L_a와 L_b로 표시하고, 캐리는 c로 표시한다. j 시점에서 a_j와 b_j는 각각 LFSR L_a와 L_b의 출력이며(j 시점 에서 L_a의 1-비트 출력은 a_j로 표기하고, L_b의 1-비트 출력은 b_j로 표기함), 캐리 c_j는 f_c에 의하여, 메모리 d_j는 f_d에 의하여 결정된다. 출력 함수 f_z는 키 수열 비트 z_j를 출력하며, 함수 f_c, f_z, f_d는 다음과 같이 정의된다.

$$z_j = f_z(a_j, b_j, c_{j-1}, d_{j-1}) = a_j \oplus b_j \oplus c_{j-1} \oplus d_{j-1} \quad (1)$$

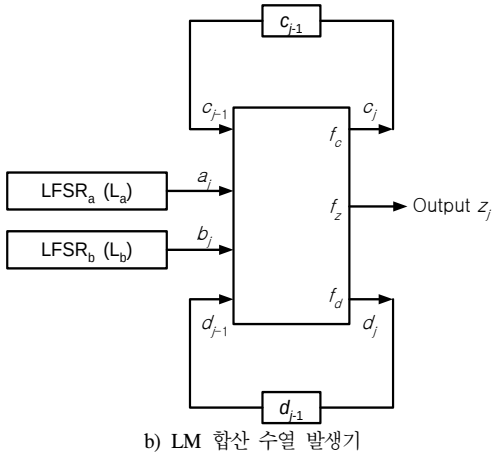
$$c_j = f_c(a_j, b_j, c_{j-1}) = a_j b_j \oplus (a_j \oplus b_j) c_{j-1} \quad (2)$$

$$d_j = f_d(a_j, b_j, d_{j-1}) = b_j \oplus (a_j \oplus b_j) d_{j-1} \quad (3)$$

PingPong-128 발생기는 상호 클럭 조절 구조가 추가된 합산 수열발생기 계열이며, 그림 2와 같다.



a) 합산 수열 발생기



b) LM 합산 수열 발생기

그림 1. 합산 수열 발생기와 LM 합산 수열 발생기 (r=2)

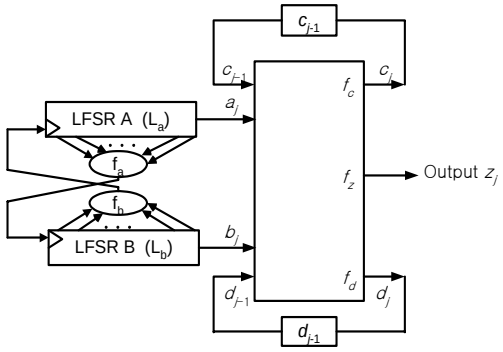


그림 2. PingPong-128 발생기

그림에서 키 수열 발생기는 두개의 LFSR로 구성되며, 다음 메모리 상태와 키 수열 비트를 생성하기 위해 LFSR의 출력 비트는 결합 함수 f_z, 캐리 함수 f_c 및 메모리 함수 f_d에 각각 입력된다. LFSR은 불규칙한 클럭이 공급되며, 하나의 LFSR에 공급되는 불규칙 클럭수는 나머지 LFSR에서 생성된 비선형 필터함수(f_a 또는 f_b)로부터 얻어진다. 두 개의 LFSR 상태는 두 LFSR의 기억상태의 내용을 위해 정의되고, 시점 j에서 출력 z_j는 f_z에 의해 생

성된다. 캐리 상태 c_j는 f_c에 의해, 메모리 상태 d_j는 f_d에 의해 정의된다. 클럭 조절 함수 f_a와 f_b는 두 LFSR의 현 상태에 의해 얻어지며, LFSR은 랜덤하게 클럭 조절된 후 캐리, 메모리 및 키 수열 출력을 생성한다. 또한, LFSR의 불규칙 클럭은 나머지 LFSR의 특정한 두 탭의 내용에 따라 클럭 수가 랜덤하게 결정된다. PingPong-128은 처음 초기화 과정에서 키(k)와 초기화 벡터(i, initial key)로부터 내부 상태가 채워지며, 내부 상태 길이가 키 길이보다 더 길기 때문에 내부 상태를 채우기 위한 키 확장 과정이 요구된다.

2.2 PingPong-128 발생기

본 절에서는 PingPong 계열의 PingPong-128 키 수열 발생기, 주기 제어, 키 로딩과 재 입력, 성능 및 공격 분석을 다룬다. 여기서 "PingPong"은 클럭을 주고 받는 과정이 핑퐁 게임을 닮았다는 의미를 갖는다.

2.2.1 키 수열 발생

PingPong-128은 두개의 상호 클럭 조절형 LFSR과 캐리 및 메모리 비트를 가지며, LFSR의 길이는 각 각 127비트, 129비트이다. 모든 메모리 비트들은 PingPong-128에게 258비트의 내부 상태 비트를 제공하며, 128비트 키와 128비트 초기화벡터에 의하여 내부상태가 채워진다. PingPong-128 발생기의 출력 키 수열은 LFSR 수열과 캐리 및 메모리수열이 합쳐져서 생성된다. L_a와 L_b의 귀환다항식은 각각 다음과 같은 원시다항식 $p_a(x)$, $p_b(x)$로 부터 선택되며, LFSR의 모든 비트가 0 상태(all zero state)로 초기화되는 것을 허용하지 않는다.

$$p_a(x)=x^{127}\oplus x^{109}\oplus x^{91}\oplus x^{84}\oplus x^{73}\oplus x^{67}\oplus x^{66}\oplus x^{63}\oplus x^{56}\oplus x^{55}\oplus x^{52}\oplus x^{48}\oplus x^{45}\oplus x^{42}\oplus x^{41}\oplus x^{37}\oplus x^{34}\oplus x^{30}\oplus x^{27}\oplus x^{23}\oplus x^{21}\oplus x^{20}\oplus x^{19}\oplus x^{16}\oplus x^{13}\oplus x^{12}\oplus x^{7}\oplus x^{6}\oplus x^{2}\oplus x^{1}\oplus 1 \quad (4)$$

$$p_b(x)=x^{129}\oplus x^{125}\oplus x^{121}\oplus x^{117}\oplus x^{113}\oplus x^{109}\oplus x^{105}\oplus x^{101}\oplus x^{97}\oplus x^{93}\oplus x^{89}\oplus x^{85}\oplus x^{81}\oplus x^{77}\oplus x^{73}\oplus x^{69}\oplus x^{65}\oplus x^{61}\oplus x^{57}\oplus x^{53}\oplus x^{49}\oplus x^{45}\oplus x^{41}\oplus x^{37}\oplus x^{33}\oplus x^{29}\oplus x^{25}\oplus x^{21}\oplus x^{17}\oplus x^{13}\oplus x^{9}\oplus x^{5}\oplus 1 \quad (5)$$

출력 키 수열 비트 z_j, 캐리 비트 c_j, 메모리 비트 d_j는 구조상 LM 합산 수열 발생기와 동일한 형태(수식 (1)~(3))를 취하지만, 출력 수열 및 비도 수준은 크게 개선된다.

2.2.2 클럭 제어

PingPong-128에서 두 개의 LFSR은 각각 다른 LFSR의 클럭을 랜덤하게 제어하여 각각의 레지스터에 불규칙한 클럭을 발생시키며, 두 탭이 1~4 범위 값을 계산하기 위하여 L_a로부터 얻어지고, L_b는 랜덤한 1~4개의 클럭 수만큼 귀환 이동한다. 비슷하게 L_b의 두 탭 값으로부터 1~4 범위의 랜덤 값을 얻은 후 L_a의 클럭을 제어한다. 제어함수 f_a와 f_b는 다음과 같이 정의된다.

$$f_a(L_a)=2L_{a42}(t)+L_{a85}(t)+1 \quad (6)$$

$$f_b(L_b)=2L_{b43}(t)+L_{b86}(t)+1 \quad (7)$$

2.2.3 키 로딩과 키 갱신

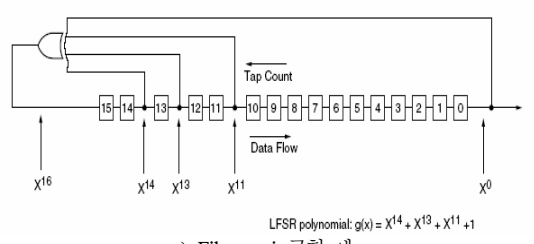
통신시스템에서 동기 에러는 전체 메시지(또는 남은 메시지)의 재전송을 요구하며, 이 때 동기식 스트림 암호(synchronous stream cipher)의 경우에는 안전성을 위해 다른 키 수열이 사용되어야 한다. 이를 위해서 키 갱신(rekeying)은 비밀키(k)와 평문 상태로 전송될 초기벡터(iv)를 재동기 시키는 방법이나 또는 다른 공개된 방법이 적용되어야 한다.

본 논문에서는 PingPong-128에서 초기 키 로딩과 키 갱신을 다음과 같이 제안한다. PingPong-128에서 키(k) 및 초기벡터(iv)는 모두 128비트 길이를 가지며, 키와 벡터는 내부상태 256비트(초기에 캐리 및 메모리는 '0'로 초기화)를 채운다. 또한, 초기설정 과정은 키 갱신을 위해 사용될 수 있으며, 키 수열발생기의 초기상태를 생성하는 과정은 발생기 자체를 두 번 사용하고 L_a의 시작상태는 XORing에 의해 간단하게 $L_a=(k\oplus iv) \bmod 2^{127}$ 같이 나타낸다. 키(k), 초기화벡터(iv)는 2개의 128비트를 얻는다. L_b에 대한 129 비트 초기상태는 128 비트 키로부터 얻고, 내부의 129비트워드를 포함하면서 왼쪽으로 1비트 이동한다. 그리고 초기벡터가 먼저 0과 내부 129비트 워드를 포함한 XORing, 다시 말해서 $L_b=(k\ll 1)\oplus(0\,|\,iv)$이다. 일단 키와 초기벡터가 설정된 후, PingPong-128 키 수열 발생기를 작동시켜 258비트 길이의 키 수열을 2회 생성한 다음, 나중 258비트를 이용하여 다음과 같이 두 LFSR 및 캐리 비트들을 재초기화 한다. 즉, 처음 127 비트는 L_a의 초기상태를 설정하고, 다음 129 비트는 L_b의 초기상태를, 그리고 나머지 2 비트로 캐리비트(c0, d0)를 설정한다. 이 때, 어느

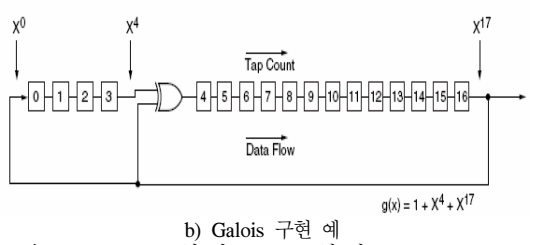
하나의 LFSR이라도 0-벡터로 초기화되어서는 안된다. 이렇게 재초기화하게 되면 PingPong-128의 높은 보안성 때문에 키 갱신 과정에 대한 최상의 공격은 키 전수 검사(exhaustive key-search attack)임을 알 수 있다.

2.2.4 구현

일반적으로 LFSR의 구현 시에는 그림 3과 같이 Fibonacci 구현과 Galois 구현 방법이 적용될 수 있다. PingPong-128은 양쪽의 LFSR이 Fibonacci구현보다 오히려 Galois구현이 용이하며, 이것은 구현의 소프트웨어 성능에 근거된 설계 결정이다. 두 방법이 구현상 하드웨어에 효율적이지만 Galois구현은 Fibonacci보다 소프트웨어에 조금 더 효율적인 것으로 관찰되며, 이들 두 가지 구현 방법이 처음 LFSR 상태와 다른 출력을 생성한다.



a) Fibonacci 구현 예



b) Galois 구현 예

그림 3. Fibonacci 구현 및 Galois 구현 예

Ⅲ. 분 석

본 절에서는 실험적인 결과에 기초를 두는 PingPong-128발생기의 키 수열특성을 제공하며, PingPong-128발생기가 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 선형복잡도는 Berlekamp-Massey 알고리즘[3]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.

PingPong-128 키 수열 특성을 관측하기 위한 실험은 표 1과 같다. 짧은 길이에 대한 예제는 서로 다른 길이의 두 LFSR을 가지며, 각각의 쌍에 대해서 서로 다른 귀환 다항식을 선택하였다. 실험에서 귀환 다항식 탭 위치 선택은 키 수열 특성에 큰 영향이 없었으며, LFSR 길이는 각각의 쌍에 대하여 짧은 길이에 대해서 모든 초기 상태(예, 5,6의 경우 2^{11})로 시뮬레이션 하였다. 예를 들면, 레지스터 길이 5, 6을 선택할 경우 결과에 따른 선형복잡도는 23 이상 값을 갖는 다양한 형태로 나타났으며, 이때 최소 선형복잡도를 선택하였다. 주기와 최소 선형복잡도를 시뮬레이션한 결과는 표 1과 같다. 표에서 얻어진 값들로부터 최소 선형복잡도와 주기의 방정식을 다음과 같이 구하였다. 레지스터 길이 n은 두 레지스터 길이의 합으로 표시할 때, 선형복잡도 LC의 하한경계 값은 $LC \geq 25 * 2^{\lceil (n-11)/2 \rceil} = 2^{4.6 * 2^{(n-11)/2}}$가 되며, 비슷한 방법으로 주기 P는 $P \geq 25 * 2^{\lceil (n-11)/2 \rceil} = 2^{4.6} * 2^{(n-11)/2}$로 표현된다.

표 1. 작은 사이즈에 대한 키 수열 특성

레지스터 길이	선형 복잡성	주기
5,6	23	25
5,7	50	50
6,7	43	51
7,8	93	101
7,9	200	206

따라서 PingPong-128에 대한($n = 256$) 선형복잡도의 하한경계 값과 주기는 아래 식과 같다.

$$LC \geq 2^{4.6} * 2^{\lceil (256-11)/2 \rceil} = 2^{4.6} * 2^{4.6} * 2^{123} \approx 2^{128} \quad (7)$$

$$P \geq 2^{4.6} * 2^{\lceil (256-11)/2 \rceil} = 2^{4.6} * 2^{4.6} * 2^{123} \approx 2^{128} \quad (8)$$

PingPong-128의 설계 기준강도는 2^{128}이며, 여러 가지 공격에 대하여 기본적인 키 수열특성은 큰 선형복잡도 및 긴 주기 때문에 안전하게 된다.

3.2 공격 분석

본 절에서는 PingPong-128의 각개 공격(divide-

and-conquer attack), 고속 상관공격(fast correlation attack), Time/Memory/Data Tradeoff 공격, 대수적 공격에 대하여 분석한다.

3.2.1 divide-and-conquer attack

합산 수열 발생기에 대하여 L_a와 L_b의 길이들이 각각 m과 n이며, 연속적인 키 수열 k비트, 즉 $(Z_j)_{j=0}^{k}$ 값을 사전에 알고 있다고 가정한다. 이 때 L_a와 L_b의 초기 상태는 다음 알고리즘[1]를 이용하여 찾을 수 있다.

① L_a의 초기상태와 메모리 비트 c_{-1}을 추측한다.
② $j=0$로 설정한다.
③ 수식 (1)과 알려진 키 수열 비트 z_j를 사용하여 R_b의 j번째 비트인 b_j를 계산한다.
④ 수식 (2)와 계산된 b_j를 사용하여 c_j를 계산한다.
⑤ j를 증가시킨 후 $j<n$이면 ③단계로 간다.
⑥ 추측한 L_a의 초기상태와 계산된 L_b의 초기상태, 그리고 c_{n-1}을 사용하여 합산 수열 발생기를 초기화시킨다.
⑦ 후보 키 수열 $(z')_{j=n}^{k}$을 생성한 후에 관찰된 키 수열 $(z)_{j=n}^{k}$과 비교한다.
⑧ 만일 $(z')_{j=n}^{k}$과 $(z)_{j=n}^{k}$이 동일하다면, L_a와 L_b의 진짜 초기상태의 검색에 성공하였으며, 그렇지 않다면 ①단계로 간다.

이 공격법은 $m+1$ 비트의 키 전수검사(exhaustive search)를 요구하며, 즉, $m+n$ 비트인 두 레지스터의 초기 값을 찾기 위하여 L_a의 길이 m과 메모리 비트 c에 해당하는 $m+1$ 비트가 필요로 한다. 결과적으로 공격 복잡도는 2^{m+1}이 되며, 필요한 기지 평문의 양은 대략 $m+n+1$이 된다.

한편, PingPong-128의 클럭 제어 메커니즘은 클럭 마다 1~4의 값을 랜덤하게 가지며, 정확 클럭 정보가 암호공격자에게는 알려지지 않는다. 그러나 이 divide-and-conquer attack은 클럭을 정확히 알고 있어야만 공격이 가능하기 때문에 PingPong-128 발생기는 이 공격에 안전하다.

3.2.2 고속 상관공격

합산 수열 발생기는 메모리 비트 c_j와 키 수열 비트 z_j가 표 2와 같이 큰 상관성을 갖는다. 즉, $p(c_j=z_j)=0.25$이다. $z_j=a_j\oplus b_j\oplus c_{j-1}$이고, $z_{j+1}=a_{j+1}\oplus b_{j+1}\oplus c_j$이다. $c_j=z_j\oplus 1$이 확률 0.75로 유지되기 때문에, $z_{j+1}=a_{j+1}\oplus b_{j+1}\oplus z_j\oplus 1$이 확률 0.75를 유지한다.

표 2. 합산 수열발생기 c_j 및 z_j 상관특성

a_j	b_j	c_{j-1}	c_j	z_j
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

z_j'을 키 수열의 이진 시차 비트라고 두면, 임의 시점에서 $z'_j=z_{j+1}\oplus z_j$이 되고, 이 때 $z'_j=a_{j+1}\oplus b_{j+1}\oplus 1$이 된다. 합산수열발생기의 이진 시차 수열 z_j'은 그림 4와 같이 두 개 LFSR 출력 합과 이진 잡음 e_j를 더한 것으로 나타내며 이 모형의 잡음 확률은 0.25이다. 이는 0.5보다 작은 표준편차를 갖기 때문에 상관성 공격[2]이 가능해진다.

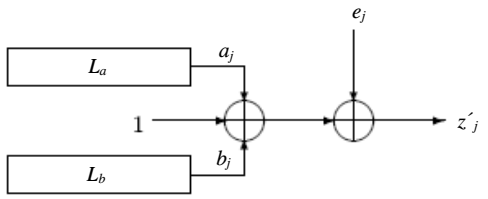


그림 4. 합산수열발생기의 고속 상관성공격 모델

합산 수열발생기에 대한 고속 상관 공격 알고리즘은 LFSR 수열에 기반한 잡음 모델로 생각할 수 있다. 패리티 검사에 기초한 반복 확률 알고리즘이 관측된 수열에 대한 이진 시차 수열로부터 LFSR 수열을 재구성할 목적으로 에러 정정 과정을 수행할 수 있도록 한다.

고속 상관 공격 알고리즘[2]은 다음과 같이 나타내어진다.

① 관찰된 키 수열로부터 이진시차수열을 계산한다.

② 각각의 이진시차수열 z_j', $j=1,..,k$에 대하여 패리티 검사 값을 계산한다.

③ 각 z_j'에 대한 패리티 검사 값들을 이용하여 오차의 확률 p_j를 계산한다.

④ 만일 $p_j>0.5$이면, $j=1,..,k$에서의 $z'_j=z'_j \oplus 1$과 $p_j=1-p_j$를 설정한다.

⑤ 모든 패리티 검사들이 만족할 때까지 되풀이 한다.

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

한편, 고속상관공격은 관찰된 키 수열에 대한 반복 에러 정정 알고리즘 모델이 적용되고 있다. 그러나 반복 에러 정정 알고리즘은 LFSR의 규칙적인 클럭을 요구한다. 반복 에러 정정 알고리즘에 바탕을 두지 않는 고속상관공격들도 있다. 이것의 예로, LILI-128에 Jonsson와 Johansson의 고속상관공격이다[7]. 공격법은 LILI-128 클럭 제어 레지스터 상태를 예측하고, 그때 데이터 생성레지스터에 불규칙하게 출력되는 수열에 대해서 고속상관공격을 한다. PingPong-128계열의 키 수열발생기는 LFSR의 상호 불규칙 클럭을 기초로 하여 클럭과 데이터발생을 쉽게 분리될 수 없기 때문에 상기에 소개된 고속상관공격[7]들은 PingPong-128발생기에 적용될 수 없다.

3.2.3 Time/Memory/Data Tradeoff 공격

시간/메모리 거래 공격[6]의 목적은 주어진 시간 내에 내부 상태를 찾아내는데 있으며, 공격은 두 단계로 처리된다. 선처리 단계 동안에 암호 해독가는 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, ($\log_2 S$와 같은 이진 워크 크기에서의) 메모리 용량, (검사 테이블에 대한) 계산 시간, (검사 테이블에 대한) 사전 계산 시간, 그리고 (키 갱신이 없는) 데이터 길이(즉, 알려진 데이터의 길이)를 표시한다. 시간/메모리 거래 공격[6]은 $T.M=s$, $P=M$, 그리고, $D=T$를 만족한다. 257 비트의 내부 상태를 갖는 PingPong-128에 대하여, T나 M이 2^{128}보다 더 크게 나타나며, 이는 키 전수 공격보다 더 어렵다.

Ⅳ. 결 론

본 논문에서는 차세대 이동 통신들과 같은 무선 통신에 적합한 PingPong-128을 제안하였다. 제안된 키 수열 발생기는 LM 발생기를 클럭 통제함으로서 비선형성을 높였다. $n=256$으로 주어진 제안 발생기에 대한 분석결과 주기는 2^{128}이상, 선형 복잡도는 2^{128}이상이 조사되었으며, 기본 랜덤 테스트 항목을 잘 만족함을 알 수 있었다. 이 알고리즘은 고속화를 요구하는 이동 통신, 위성 통신 또는 다양한 네트워크로 많은 응용이 예상된다.

참 고 문 헌

[1] E.Dawson, “Cryptanalysis of Summation generator,” *Advances in Cryptology - ASIACRYPT ’92*, Lecture Notes in Computer Science, Vol. 718, pp. 209-215, Springer-Verlag, 1993.

[2] 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.

[3] J. Massey, “Shift-Register Synthesis and BCH Decoding,” *IEEE Transcations on Information Theroy*, IT-15, No.1, pp.122-127, January 1969.

[4] W. Meier and O. Staffelbach, “Correlation Properties of combiners with Memory in Stream Ciphers,” *Advances in Cryptology-EUROCRYPT’ 90*, Lecture Notes in Computer Science, Vol. 473, pp. 204-213, Springer-Verlag, 1990.

[5] R.Rueppel, “Correlation Immunity and the Summation Generator,” *Advances in Cryptology-CRYPTO ’85*, Lecture Notes in Computer Science, Vol. 218, pp. 260-272, Springer-Verlag, 1985.

[6] S. Babbage, “Improved exhaustive search attacks on stream cipher,” *European Convention on Security and Detection*, IEEE Conference Publication, vol 408, pp.161-166, 1995.

[7] F. Jonsson and T. Johansson, “A fast corre-

lation attack on LILI-128," *Information Processing Letters*, Vol. 80, No. 3, pp. 122-127, Jan. 1969.

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

[9] 이상진, 지성택, 김용대, 고승철, "상관관계 공격에 안전한 합산 키 수열 발생기," *정보보호학회논문지*, 1995.

[10] Daewan Han, Moonsik Lee, "An Algebraic Attack on the Improved Summation Generator with 2-bit Memory," *Information Processing Letters*, Aug. 2004.

이 훈 재 (Hoon-jae Lee) 정회원

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 3월~2002년 2월 경운대학교 컴퓨터전자정보공학부 조교수
2002년 3월~현재 동서대학교 인터넷공학부 부교수
<관심분야> 암호이론, 네트워크보안, 디지털 통신

문 상 재 (Sang-jae Moon) 정회원

1972년 2월 서울대학교 공업교육과 졸업(전자공학 학사)
1974년 2월 서울대학교 대학원 전자공학과 졸업(전자공학 석사)
1984년 6월 미국 UCLA 통신공학과 졸업(통신공학 박사)
1984년 7월~1985년 6월 UCLA Postdoctor 근무
1974년 12월~현재 경북대학교 공과대학 전자전기공학부 교수
2001년 2월~2002년 1월 한국정보보호학회 회장
1999년 8월~현재 경북대학교 ITRC 연구센터장
<관심분야> 정보보호, 이동 네트워크

박 종 욱 (Jong-Wook Park) 정회원

1986년 경북대학교 전자공학과 졸업(공학사)
1988년 경북대학교 대학원 전자공학과 졸업(공학석사)
2002년 경북대학교 대학원 전자공학과 졸업(공학박사)
1988년 2월~2000년 1월 국방과학연구소 선임연구원,
2000년 2월~현재 국가보안기술연구소 책임연구원
<관심분야> 정보통신보안, 정보보호시스템
E-mail : khspjw@etri.re.kr