FCSR 난수열의 암호학적인 특성에 관한 연구

서 창 호[†]·김 정 녀[††]·조 현 숙[††]·김 석 우[†††]

요 약

합산 난수 발생기(Summation Generator)는 LFSR의 출력 수열을 정수 합산하여 키 수열을 발생한다. 이와 유사하게 두개의 FCSR의 출력 수열을 상관관계에 안전한 비트별 논리합(bitwise exclusive-oring)을 이용한 이진 난수열 발생기를 제안하고, 출력된 수열의 암호학적 특성을 살펴본다.

키워드 : 2-adic 복잡도, 캐리를 갖는 쉬프트레지스터, 선형복잡도

A Study on the Cryptographic Properties of FCSR Sequences

Chang-Ho Seo[†]·Jeong-Nyeo Kim[††]·Hyun-Sook Cho[††]·Seok-Woo Kim[†††]

ABSTRACT

A summation generator creates sequence from addition with carry of LFSR (Linear Feedback Shift Register) sequences. Similarly, it is possible to generate keystream by bitwise exclusive-oring on two FCSR sequences. In this paper, we described the cryptographic properties of a sequence generated by the FCSRs.

Key word : 2-adic span, Feedback with Carry Shift Register, linear complexity

1. 서 론

키 수열 발생기의 안전성을 검증하는 대표적인 방법으로 선형 복잡도[1]와 상관관계[3]에 의한 안전성 평가를 들 수 있다. 선형 복잡도가 작은 키 수열 발생기는 대수적 공격에 의하여 쉽게 해독되지만, 큰 선형 복잡도를 갖는 키 수열 발생기는 실질적으로 공격이 어렵다. 대수적인 공격은 실질적인 공격 방법이라기 보다는 안전성을 평가하는 측도로 고려되는 경우가 많다.

따라서 키 수열 발생기를 설계할 때 상관 관계 공격을 피하기 위한 방법으로 무상관 함수 와 무상관도에 대한 개념이 도출하였다[4]. 임의의 부울 함수는 상관 관계가 있는 선형 함수가 반드시 존재하며, 부울 함수의 대수적 차수와 무상관도에는 반비례 관계가 있다. 이것은 안전한 키 수열 발생기의 설계에 장애가 되는 요인으로 작용하는데 최적화 결합 논리를 사용한다면, 선형 복잡도와 무상관도를 동시에 증가시킬 수 있다.

기존의 스트림 암호는 대부분 LFSR(Linear Feedback Shift Register)를 비선형 결합하여 비트열을 발생한다[1]. 그런데 비선형 결합함수를 사용하면 입력과 출력사이에 상관관계가 존재하여 시스템에 약점이 존재한다[3]. 이러한 문제점을 해결하기 위하여 LFSR의 출력 수열을 정수로 고려하여 최종 출력수열을 이 정수의 합으로 생성하는 합산 난수 발생기(Summation Generator)가 제안되었다[4]. 그러나, 합산 난수 발생기는 최종 출력 수열과 LFSR의 출력 사이에는 상관관계가 존재하지 않으나 출력 수열이 연속해서 같은 값, 즉 run 이나 gap 이 발생하면 캐리(carry) 수열을 예측할 수 있고 이로부터 LFSR의 출력을 예측할 수 있어 해독되었다[5].

한편, 합산 난수 발생기에서 고려한 정수 합을 일반화시켜 LFSR에서 궤환되는 값을 비트별 논리합(bitwise exclusive-oring)으로 하지 않고 정수 덧셈 방식으로 동작되는 FCSR(Feedback with Carry Shift Register)이라는 난수발생기의 새로운 유형이 제안되었다[6]. LFSR이 유한체 위의 다항식에 근거하여 설계되었다면, FCSR는 2-adic 수에 근거하여 설계되었다고 할 수 있다. 마찬가지 개념으로 주기가 있는 이진 수열을 2-adic 수[7]로 고려하면, 그에 대응하여 하나의 유리수 $\frac{b}{q}$가 있고, 이 유리수가 기약이면 q에 대응되는 FCSR로 그 수열을 생성할 수 있다. 이 때 FCSR를 구성하는데 소요되는 단의 개수를 2-adic 복잡도(2-adic span)라 한다. 따라서 기존의 스트림 암호에서 LFSR를 FCSR로 대치하여도 암호학적인 문제점은 없을 것으로 예상된다.

본 논문에서는 합산 난수 발생기와 유사하게 FCSR의 출

※ 본 논문은 2000년도 2학기 공주대학교 교내 연구비에 의해 연구 되었음.
† 준 회 원 : 공주대학교 응용수학과 교수
†† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부
††† 종신회원 : 한세대학교 정보통신학과 교수
논문접수 : 2000년 8월 29일, 심사완료 : 2000년 11월 24일

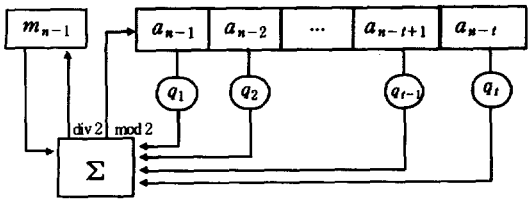
력 수열을 상관관계에 안전한 비트별 논리합한 경우에 발생하는 수열의 제반 암호학적 특성을 살펴본다.

본 논문의 구성은 다음과 같다. 2장에서는 FCSR의 개념, 동작 및 특성에 대하여 살펴보고, 3장에서는 효율적이며 안전한 키 수열 발생기 제안 및 암호학적인 특성에 대하여 기술한다. 4장에서는 결론을 제시하였다.

2. FCSR 소개

2가 아닌 소수 q에 대해서 $q+1=q_1 2+q_2 2^2+q_3 2^3+\cdots+q_t 2^t$, $q_i \in \{0, \pm 1\}$과 같은 이진 전개가 주어졌다고 하자. 이때 q를 연결수(connection number)로 하는 FCSR은 t개의 레지스터(register)와 메모리(memory) m으로 구성되어 있다.

(그림 1) 에서와 같이 레지스터의 초기치가 $(a_{t-1}, a_{t-2}, \cdots, a_1, a_0)$이고 메모리가 m이면 FCSR의 동작은 다음과 같다.



(그림 1) FCSR의 동작도

[단계 1] 정수합 $\sigma = \sum_{k=1}^{t} q_k a_{t-k} + m$을 구한다.

[단계 2] 최하위 비트 a_0를 출력하고, 레지스터의 content들을 오른쪽으로 한 칸씩 이동한다.

[단계 3] $a_t \equiv \sigma \pmod 2$를 쉬프트 레지스터의 최상위 셀(cell) 에 대치시킨다.

[단계 4] 메모리 m을 $(\sigma - a_t)/2$로 바꾼다.

정의 1. 소수 q가 2를 원시원(primitive element)으로 가질 때 q는 2-prime이라 한다.

2-prime인 소수 q를 FCSR의 연결 정수로 사용하면 FCSR의 동작에 필요한 단의 개수는 $t = \log_2 q$이고 주기는 $q-1$이다[7].

FCSR은 LFSR 에 없는 메모리가 동작에 필요하지만 구현하는데 큰 문제는 아니다. FCSR의 출력 수열은 LFSR의 출력 수열과 유사한 랜덤 특성을 갖고 있다. 한편 주기가 있는 임의의 이진 수열을 2-adic 수로 생각하면 하나의 기약 유리수 $\frac{p}{q}$를 대응시킬 수 있고, 이때 q를 연결수로 하는 FCSR을 이용하여 주어진 이진 주기 수열을 생성할 수 있다.

2.2 선형 복잡도

다음은 FCSR의 선형 복잡도와 관련된 몇 가지 정리이다[2].

보조정리 1. 각 $i = 1, 2, \cdots, h$에 대하여 수열 σ_i가 최소 다항식 $m_i(x)$에 의하여 생성되었다고 하고, 주기가 각각 r_i라 하자. 각 최소 다항식들이 각 쌍마다 서로소(pairwise relatively prime)이면 $\sigma_1 \oplus \sigma_2 \oplus \cdots \oplus \sigma_h$의 주기는 전체 주기의 최소 공배수와 같다.

보조정리 2. 각 $i = 1, 2, \cdots, h$에 대하여 수열 σ_i가 최소 다항식 $m_i(x)$에 의하여 생성되었다고 하고 주기가 각각 r_i라 하자. 각 최소 다항식들이 각 쌍마다 서로소(pairwise relatively prime)이면 $\sigma_1 \oplus \sigma_2 \oplus \cdots \sigma_h$의 최소 다항식은 $\prod_{i=1}^{h} m_i(x)$이다.

정의 2. $f \in GF(q)[x]$은 0이 아닌 다항식이고, $f(0) \neq 0$이라고 하자. $f(x) \mid x^e - 1$를 만족하는 최소 양의 정수 e를 다항식 $f(x)$의 위수(order) 라고 한다.

연결수 q에 대한 조건에 따라, FCSR 출력 수열의 선형 복잡도를 얻을 수 있다.

정리 1.[8] FCSR의 연결수 q가 2-prime이면 이러한 FCSR로부터 생성된 수열의 선형복잡도는 $\frac{q+1}{2}$ 보다 작거나 같다.

주의 1.[8] p와 $q = 2p+1$이 2-prime이라 하자. 그러면 q을 연결수로 사용한 FCSR의 선형복잡도는 $p+1$이다.

정리 2. 만약 p에 대하여 2의 위수로 m을 갖고 $(2^m \equiv 1 \pmod p)$, $q = 2p+1$이 2-prime이라 하자. 그러면 q을 연결수로 사용한 FCSR의 선형복잡도의 하한은 $m+2$ 이다.

(증명) : FCSR의 출력 수열의 특성 다항식

$$1 + x + x^p + x^{p+1} = (1+x)(1+x^p) \qquad (1)$$

이다.

그런데, $Q_i(x)$가 i-th cyclotomic 다항식(cyclotomic polynomial)[6]일 때, 아래의 식은 다음과 같이 성립한다.

$$\begin{aligned} x^p - 1 &= \prod_{d \mid p} Q_d(x) \\ &= Q_1(x) \times Q_p(x). \end{aligned}$$

$Q_p(x)$인 다항식은 가약이므로, m이 p에 대하여 2의 위

수이면, $Q_p(x)$는 차수가 m인 기약다항식 $r_i(x)$의 곱 형태로 표현된다.

$$Q_p(x) = \prod_{i=1}^{\varphi(p)/m} r_i(x)$$

여기서 $\varphi(p)=p-1$이고, $r_i(x)$ 는 차수 m를 갖는 기약 다항식이다. 따라서 식 (1)은

$$\begin{aligned} 1+x+x^p+x^{p+1} &= (1+x)(1+x^p) \\ &= (1+x)(1+x) \times \prod_{i=1}^{\varphi(p)/m} r_i(x) \\ &= (1+x^2) \times \prod_{i=1}^{\varphi(p)/m} r_i(x) \end{aligned}$$

이다.

그런데 출력 수열의 주기가 $2p$이므로 위수가 $2p$이면서, 식 (1)의 약수인 최소 다항식은 $(1+x^2)r_i(x)$이다. 그러므로 선형복잡도의 하한은 $m+2$ 이다. ■

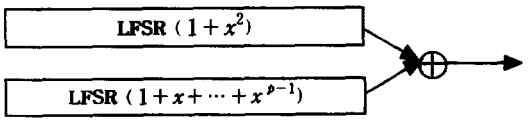
주의 2. $q=r^e$ ($e>2$ 인 정수)에 대하여 r이 2-prime이라 하면 q를 연결수로 사용한 FCSR의 출력 수열의 주기는 $\varphi(q)=r^{e-1}(r-1)$이다.

정의 3. 만약 p와 $q=2p+1$이 2-prime이라 할때, 정수 q을 strong 2-prime 연결수(strong 2-prime connection number)라고 한다.

주의 3.[8] p와 q가 2-prime이고 $q=2p+1$이라 하자. 그러면 q를 연결수로 사용한 FCSR의 주기는 $2p$이며, 선형 복잡도는 $p+1$이다. 이때 FCSR의 특성 다항식은 다음과 같다.

$$\begin{aligned} 1+x+x^p+x^{p+1} &= (1+x)^2(1+x+\ldots+x^{p-1}) \\ &= (1+x^2)(1+x+\ldots+x^{p-1}) \end{aligned}$$

여기서 p는 2-prime이므로 $1+x+\cdots+x^{p-1}$은 기약 다항식이다. 한편, FCSR 출력 수열의 특성 다항식은 $(1+x^2)(1+x+\cdots+x^{p-1})$이므로, 이 수열은 특성다항식을 $1+x^2$으로 갖는 LFSR(즉, 출력 수열이 101010… 혹은 010101…인 LFSR)과 특성 다항식을 기약인 $1+x+\cdots+x^{p-1}$으로 갖는 LFSR을 비트별 논리합한 수열과 같다.



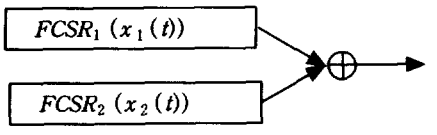
(그림 2) FCSR의 동치 형태

3. 난수 발생기 제안 및 특성

앞 절에서 살펴보았듯이 FCSR의 출력 수열의 선형 복잡도는 주기에 가깝다. 그러므로 (그림 3)과 같이 두개의 FCSR를 상관관계 공격에 강한 비트별 논리합 논리를 사용하여도 선형 복잡도는 클 것이다. 또한 비트별 논리합은 정수 덧셈에 대하여 비선형이므로 최종 출력 수열의 2-adic 복잡도도 클 것으로 예상된다. 그러므로 상관관계 공격에 안전한 키 수열 발생기를 제안하고, 암호학적인 특성 등을 살펴본다.

3.1 동작 설명

(그림 3)는 키 수열 발생기의 구성도이다. 최적 연결수를 $q_1(=2p_1+1)$인 $FCSR_1$과 $q_2(=2p_2+1)$인 $FCSR_2$인 2개의 FCSR 레지스터 값들은 비트별 논리합 논리에 의해 최종 출력 수열을 생성한다.



(그림 3) 키 수열 발생기

● <u>키 수열 발생기의 동작도</u>

[단계 1] $(x_1(t))$: $FCSR_1$의 출력 수열

[단계 2] $(x_2(t))$: $FCSR_2$의 출력 수열

[단계 3] $t=0,1,2,3,\cdots$에 대하여, 최종 출력 수열 $z(t)$는 다음과 같다.

$$z(t)=x_1(t) \oplus x_2(t).$$

3.2 특 성

정리 4. 최적 연결수가 $q_1(=2p_1+1)$인 $FCSR_1$과 $q_2(=2p_2+1)$인 $FCSR_2$가 2-prime인 비트별 논리합 수열의 주기 및 선형 복잡도는 다음과 같다.

- 주 기 : $p_1 \times p_2$
- 선형 복잡도 : p_1+p_2-1 혹은 p_1+p_2-2

(증명) : $FCSR_1(FCSR_2)$의 출력 수열은 특성 다항식이 $1+x^2$와 $1+x+\cdots+x^{p_1-1}$ $(1+x^2, 1+x+\cdots+x^{p_2-1})$인 LFSR를 비트별 논리합한 수열과 같다. 그러므로 최종 출력 수열 $z(t)$는 4개의 LFSR의 비트별 논리합 논리에 의해서 생성된 수열과 같다. 그런데, 특성 다항식 $1+x^2$을 가진 두개의 LFSR의 비트별 논리합에 의해서 생성된 수열은 (1, 1, 1, …) 혹은 (0, 0, 0, …)이다. 그러므로 FCSR의 비트별 논리합은 특성 다항식이 $1+x+\cdots+x^{p_1-1}$, $1+x+\cdots+x^{p_2-1}$인 두개의 LFSR를 비트별 논리합한 수열이거나, 이 수열의 보수(complement) 수열이다.

그런데 p_1, p_2는 2-prime이기 때문에 두개의 LFSR의 특성 다항식은 기약이다. 따라서 최종 출력 수열의 주기는 $p_1 \times p_2$이며, 선형 복잡도는 $(p_1-1)+(p_2-1)=p_1+p_2-2$ 이거나 $(p_1-1)+(p_2-1)+1=p_1+p_2-1$이다. ■

정수 덧셈 관점에서 비트별 논리합은 비선형이다. 따라서 합산 난수 발생기와 비슷하게 두개의 FCSR을 비트별 논리합하면 2-adic 복잡도가 매우 크다. 그리고, 두 수열의 비트별 논리합의 연산을 수행하면 상관관계 공격은 원천적으로 불가능하므로, FCSR의 비트별 논리합인 키 수열 발생기는 합산 난수 발생기와는 달리 상관관계 공격에 적용되지 않는다.

4. 결 론

FCSR을 이용한 스트림 암호는 LFSR을 이용한 방법과 유사하게 개발할 수 있지만, 아직까지 그 효용성에 관한 연구는 거의 없다. 본 논문에서와 같이 두개의 FCSR을 비트별 논리합(bitwise exclusive-oring)으로 구성하면, 구현이 간단하면서도 암호학적인 특성이 우수한 스트림 암호 시스템을 설계할 수 있다. 특히 합산 난수 발생기가 붕착하였던 상관관계 공격이 원천적으로 불가능하고 주기는 최대로 달성할 수 있는 $2\times p_1\times p_2$의 반이며, 선형 복잡도는 주기와 거의 같다. 또한 시뮬레이션 결과 2-adic 복잡도는 주기에 근접하다. 따라서 키 수열 발생기는 두개의 LFSR 사용하는 것보다는 FCSR 사용하는 것이 암호학적 특성이 우수하다.

참 고 문 헌

[1] R. A. Rueppel, 'Analysis and Design of Stream Ciphers', Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, In Communications and Control Engineering Series, 1986.

[2] R. A. Rueppel, 'Stream Ciphers, in Contemporary Cryptography : the Science of Information Integrity', Ch.2, pp.65-134, IEEE Press, 1992.

[3] W. Meier and O. Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers", Journal of Cryptology, Vol.1, No.3, pp.159-176, 1989.

[4] R. A. Rueppel, "Correlation Immunity and the Summation Generator," Advances in Cryptology- CRYPTO'85, LNCS 196, pp.260-272, 1986.

[5] Meier and O. Staffelbach, "Correlation Properties of combiners with memory in stream ciphers," Journal of Cryptology, Vol.5, No.1, pp.67-86, 1992.

[6] M. Goresky and A. Klapper, "Feedback Registers based on Ramified Extensions of the 2-Adic Numbers," Advances in Cryptology-CRYPTO'94, LNCS 950, pp.215-222, 1994.

[7] A. Klapper and M. Goresky, "Large Period nearly debruijn FCSR Sequences," Advances in Cryptology-CRYPTO'95, LNCS 921, pp.263-273, 1995.

[8] Changho Seo, Sangjin Lee, Yeoulouk Sung, Keunhee Han, Sangchoon Kim, "A lower bound on the linear span of an FCSR," IEEE Trans. on Information Theory, Vol.46, No.2, pp.691-693, 2000.

서 창 호

e-mail : chseo@kongju.ac.kr

1990년 고려대학교 수학과 졸업(학사)

1992년 고려대학교 일반대학원 수학과 (이학석사)

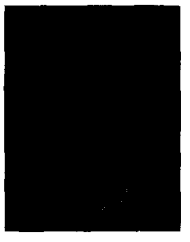
1996년 고려대학교 일반대학원 수학과 (이학박사)

1996년~1997년 국방과학연구소 선임연구원

1997년~2000년 한국전자통신연구원 선임연구원, 팀장

2000년~현재 공주대학교 응용수학과 조교수

관심분야 : 암호 알고리즘, PKI, 시스템 보안 등



김 정 녀

e-mail : jnkim@etri.re.kr

1987년 전남대학교 전산통계 학과 졸업 (학사)

1995년~1996년 Open Software Foundation Research Institute 공동연구 파견(미국)

2000년 충남대학교 대학원 컴퓨터공학과 (석사)

1988년~현재 한국전자통신연구원 보안운영체제연구팀장(선임연구원)

관심분야 : 운영체제, 분산 처리, 고장 감내, 시스템 보안

조 현 숙

e-mail : hscho@etri.ac.kr

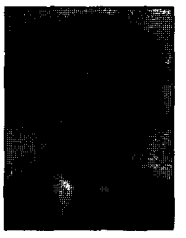
1979 전남대학교 수학과 졸업

1991 충북대학교 대학원 전자계산학과(석사)

2001 충북대학교 대학원 전자계산학과(박사)

1982년~현재 한국전자통신연구원 정보보호 기술연구 본부장

관심분야 : Network Security, Conditional Access, 인터넷 정보보호



김 석 우

e-mail : swkim@hansei.ac.kr

1979년 한국항공대학 통신정보공학과(학사)

1989년 뉴저지 공과대학 전자계산학과 (공학석사)

1995년 아주대학교 컴퓨터공학과 정보통신전공(공학박사)

1980년~1997년 한국전자통신연구원 책임연구원 실장

1997년~현재 한세대학교 정보통신학과 교수/전산소장/정보보호연구소장/군포창육보육센타 소장

관심분야 : 시스템 보안,네트워크 보안,시스템 평가 등