선형복잡도 측면에서 FCSR의 이론적인 특성 및 분석 연구

(On the Characteristic and Analysis of FCSR Sequences for Linear Complexity)

서 창 호 †, 1 (Chang-Ho Seo) 김 석 우 ††, 2 (Seok-Woo Kim)

요 약 유한체 $GF(p)$에서 $r=2p+1$이 2-솟수이고, p에 대한 2의 위수 m을 가질 때, $q=r^e, (e \geq 2)$를 연결정수로 갖는 FCSR의 생성된 출력 수열에 대한 선형복잡도를 구한다. 또한, 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, 선형복잡도 측면에서 출력된 수열의 암호학적 특성을 살펴본다.

키워드 : FCSR, 선형 복잡도

Abstract We have derived the linear complexity of a binary sequence generated by a Feedback with Carry Shift Regiater(FCSR) under the following condition: q is a power of a prime such that $q=r^e, (e \geq 2)$ and $r=2p+1$, where both r and p are 2-prime. Also, 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 in view of the linear complexity.

Key words : FCSR, Linear Complexity

1. 서 론

정보보호 서비스 중 암호화 서비스를 제공하기 위해서 무선통신(IS-95, GSM,CDMA, IMT-2000) 및 전산보안 분야에서 가장 널리 사용되는 암호 기법의 하나로 이진 난수열(Binary Random Sequence)을 이용한 방법이 있다. 일반적으로 난수란 십진난수가 보편적인데, 정보보호 측면에서는 이진 난수가 일반적으로 사용되며, 이들은 암호학적으로 안전하고 또한 고속으로 난수 발생이 가능하여야 한다.

임의의 주기가 있는 이진 수열을 하나의 멱급수로 보면 그에 대응되는 유리 다항식 $\frac{p(x)}{q(x)}$가 존재하며, 이 유리 다항식이 기약으로 표시되었다면, $q(x)$에 대응하는 LFSR로 그 수열을 생성할 수 있다. 이때 $q(x)$의 차수를 선형복잡도(Linear Complexity)라 한다.

키 수열 발생기의 안전성을 검증하는 대표적인 방법으로 선형 복잡도[1]와 상관관계[2]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 방법이라기보다는 안전성을 평가하는 측도로 고려되는 경우가 많다. 따라서 키 수열 발생기를 설계할 때 상관 관계 공격을 피하기 위한 방법으로 무상관 함수와 무상관도에 대한 개념이 도출하였다[2]. 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 무상관

1. 본 연구는 한국학술진흥재단 신진교수연구과제지원사업 2003-003-D00345 연구 결과로 수행하였음
2. 본 연구는 2004년도 한세대학교 교내학술연구비에 의하여 연구되었음
† 정 회 원 : 공주대학교 응용수학과 교수
chseo@kongju.ac.kr
†† 종신회원 : 한세대학교 정보보호학과 교수
swkim@hansei.ac.kr
논문접수 : 2005년 3월 4일
심사완료 : 2005년 6월 10일

도를 동시에 증가시킬 수 있다.

기존의 스트림 암호는 대부분 LFSR(Linear Feedback Shift Register)를 비선형 결합하여 비트열을 발생한다[3]. 그런데 비선형 결합함수를 사용하면 입력과 출력사이에 상관관계가 존재하여 시스템에 약점이 존재한다[2]. 이러한 문제점을 해결하기 위하여 LFSR의 출력수열을 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 run이나 gap 이 발생하면 케리(carry) 수열을 예측할 수 있고 이로부터 LFSR의 출력을 예측할 수 있어 해독되었다[2].

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[4]. LFSR이 유한체 위의 다항식에 근거하여 설계되었다면, FCSR는 2-adic 수에 근거하여 설계되었다고 할 수 있다. 마찬가지 개념으로 주기가 있는 이진 수열을 2-adic 수[5]로 고려하면, 그에 대응하여 하나의 유리수 $\frac{p}{q}$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 유한체 $GF(p)$에서 $r=2p+1$이 2-숏 수이고, p에 대한 2의 위수 m을 가질 때, $q=r^e, (e \geq 2)$를 연결정수로 갖는 FCSR의 생성된 출력 수열에 대한 선형복잡도 하한을 구한다. 또한 합산 난수 발생기와 유사하게 FCSR의 출력 수열을 상관관계에 안전한 비트별 논리합한 경우에 발생하는 수열의 선형복잡도 측면에서 암호학적 특성을 살펴본다.

본 논문의 구성은 다음과 같다. 2장에서는 FCSR의 개념, 동작에 대하여 살펴보고, 3에서는 선형복잡도 측면에서 FCSR의 특성에 대해서 설명한다. 4장에서는 효율적이며 안전한 키 수열 발생기 제안 및 암호학적인 특성에 대하여 기술한다. 5장에서는 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 1에서와 같이 레지스터의 초기치가 $(a_{t-1}, a_{t-2}, \cdots, a_1, a_0)$이고 메모리가 m이면 FCSR의 동작은 다음과 같다.

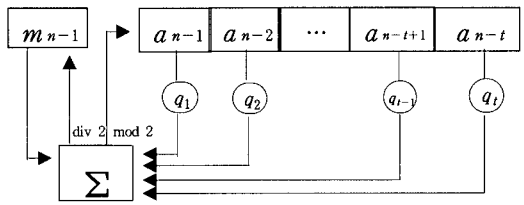

그림 1 FCSR의 동작도

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[5].

FCSR은 LFSR에 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.

3. FCSR의 선형 복잡도

다음은 FCSR의 선형 복잡도와 관련된 몇 가지 정리이다[3].

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.

본 장에서는 유한체 $GF(p)$에서 $r=2p+1$이 2-솟수이고, p에 대한 2의 위수 m을 가질 때, $q=r^e, (e \geq 2)$를 연결정수로 갖는 FCSR의 생성된 출력 수열에 대한 선형복잡도 하한에 대하여 살펴본다.

정리 1.[6] FCSR의 연결수 q가 2-prime이면 이러한 FCSR로부터 생성된 수열의 선형복잡도는 $\frac{q+1}{2}$ 보다 작거나 같다.

주의 1.[6] 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 원분 다항식(cyclotomic polynomial)[4]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 위수이면, $Q_p(x)$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 할 때, 정수 q을 strong 2-prime 연결수(strong 2-prime connection number)라고 한다.

정리 3. 만약 r=2p+1이고 p에 대한 2의 위수가 m일 경우 $(2^m \equiv 1 (\mathrm{mod} p))$에 $q=r^e$을 연결수로 사용한 FCSR로부터 생성된 수열의 선형 복잡도의 하한은 $lcm(m, \varphi(q)/r)+2$이다.

증명 : 정리 2와 마찬가지로, $Q_i(x)$가 i-th 원분 다항식(cyclotomic polynomial)일 때, 아래의 식은 다음과 같이 성립한다. 여기서, n은 $r^{e-1} \times p$이다.

$$\begin{aligned} x^n - 1 &= \prod_{d \mid n} Q_d(x) \\ &= \prod_{d \mid r^{e-1} \times p} Q_d(x) \\ &= Q_1(x) \times Q_r(x) \times \cdots \times Q_{r^{e-1}}(x) \\ &\quad \times Q_{rp}(x) \times \cdots \times Q_{r^{e-1} \times p}(x). \end{aligned}$$

$(2^m \equiv 1 (\mathrm{mod} p))$, $2^{r^{e-2} \times (r-1)} \equiv 1 (\mathrm{mod} r^{e-1})$이므로, $n=r^{e-1} \times p$에 대한 2의 위수는 $b=lcm(m, r^{e-2} \times (r-1))$이다.

$$Q_{r^{e-1} \times p}(x) = \prod_{i=1}^{\varphi(n)/b} r_i(x)$$

여기서 $r_i(x)$ 다항식은 b차 기약 다항식이며, 위수는 $r^{e-1} \times p$이다. 그런데 출력 수열의 주기가 $r^{e-1}(r-1)$이므로 FCSR의 최소 다항식은 적당한 i에 대해서 $(1+x^2) \times r_i(x)$를 약수로 갖는다. 그러므로 선형 복잡도의 하한은 $b+2$이다. □

따름정리 1. $r=2p+1$이고, $q=r^e$ ($e>2$인 정수)이면서 r이 strong 2-prime인 경우에 선형복잡도의 하한은 $r^{e-2} \times p \times (p-1)+2$이다.

증명 : 정리 3에 의해서, $2^{p-1} \equiv 1 (\mathrm{mod} p)$, $2^{r^{e-2} \times (r-1)} \equiv 1 (\mathrm{mod} r^{e-1})$이므로, 선형 복잡도의 하한은 $lcm(p-1, r^{e-2} \times (r-1))+2$이다.

한편, $lcm((p-1), r^{e-2} \times (r-1))$의 최소 공배수는 $r^{e-2} \times p \times (p-1)$이다.

그러므로 p와 $q=r^e$이 2-prime인 경우 선형복잡도의

하한은 $(r^{e-2}\times p\times(p-1))+2$이다. □

주의 3.[6] 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.

$$1+x+x^{p}+x^{p+1} = (1+x)^2(1+x+\cdots+x^{p-1})$$
$$= (1+x^2)(1+x+\cdots+x^{p-1})$$

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.

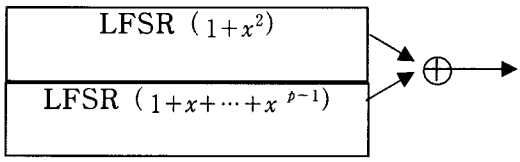

그림 2 FCSR의 동치 형태

FCSR의 연결 정수로 사용되는 2-prime의 정확한 밀도와 존재성에 대한 증명은 아직 없으나, 소수 중에서 2-prime인 소수는 약 1/3 정도 존재한다고 알려져 있다[7]. 컴퓨터 실험에 의해서, FCSR의 연결 정수로 사용할 만한 2-prime을 구하였고, 표 1에서와 같이 2 비트부터 비트를 증가하면 2-prime과 strong 2-prime의 갯수는 증가함을 알수 있다.

표 1 2-prime과 strong 2-prime의 개수

길이	2	3	4	5	6	7	8	9	10
2-prime	1	1	2	3	6	11	20	36	70
strong2-prime	0	0	1	1	0	1	2	1	1

길이	14	15	16	17	18	19	20
2-prime	814	1521	2861	5395	10179	19424	36912
strong2-prime	17	32	62	97	172	295	542

4. 난수 발생기 제안 및 특성

앞 장에서 살펴보았듯이 FCSR의 출력 수열의 선형 복잡도는 주기에 가깝다. 그러므로 그림 3과 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.

4.1 동작 설명

그림 3은 키 수열 발생기의 구성도이다. 최적 연 결수를 $q_1(=2p_1+1)$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.

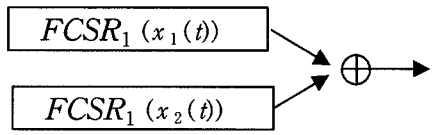

그림 3 키 수열 발생기

키 수열 발생기의 동작도

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.

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

4.2 특성

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.

- 주기 : $p_1\times p_2$
- 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 $(1,1,1,\cdots)$ 혹은 $(0,0,0,\cdots)$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 비

트별 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.

5. 결 론

FCSR는 LFSR보다 선형복잡도 관점에서 암호학적으로 우수한 스트림 암호의 구성 논리 소자이다. 본 논문에서는 Strong 2-prime을 연결수로 사용하면 적은 단으로 구성된 FCSR의 선형 복잡도는 주기의 반이라는 사실을 보였다. 그리고 p에 대한 2의 위수가 m이고 r=2p+1이 2-prime일 때 연결 정수 $q=r^e, (e \geq 2)$인 FCSR의 선형 복잡도를 구하였다. FCSR을 이용한 스트림 암호는 LFSR을 이용한 방법과 유사하게 개발할 수 있지만, 아직까지 그 효용성에 관한 연구는 거의 없다. 또한 두개의 FCSR을 비트별 논리합(bitwise exclusive-oring)으로 구성하면, 구현이 간단하면서도 암호학적인 특성이 우수한 스트림 암호 시스템을 설계할 수 있다. 특히 합산 난수 발생기가 봉착하였던 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] W.Meier and O.Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers," Journal of Cryptology, Vol.1, No.3, pp.159-176, 1989.

[3] D.E.Kunth, The art of computer Programming, Vol.2: Seminumberical Algorithms, Addison-Wesley, 1981.

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

[5] 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.

[6] 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, 2001.

[7] Hua Loo Keng, Introduction to Number Theory, Springer-Verlag, 1982.

[8] J. M. Massey, "Shift-Register Synthesis and BCH Decoding," IEEE Trans. Info. Theory, Vol.IT-15, pp.122-127, 1969.

[9] 서창호, 이상진, 김용대, 임종인, "FCSR의 선형복잡도 하한에 관하여", 통신정보보호학회 논문지, Vol.7, No.4, pp.127-132, 1997.

[10] 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, 2001.

서 창 호

1990년 고려대학교 수학과 졸업(학사) 1992년 고려대학교 일반대학원 수학과(이학석사). 1996년 고려대학교 일반대학원 수학과(이학박사). 1996년~1996년 국방과학연구소 선임연구원. 1996년~2000년 한국전자통신연구원 선임연구원, 팀장. 2000년~현재 공주대학교 응용수학과(정보보호전공) 부교수. 관심분야는 암호 알고리즘, PKI, 무선 인터넷 보안, 시스템 보안 등

김 석 우

1979년 항공대학교 통신정보공학과(공학사). 1989년 뉴저지공과대학교 전자계산학과(공학석사). 1987년~1989년 AT&T Bell Lab. 1995년 아주대학교 컴퓨터공학과(공학박사). 1980년~1997년 ETRI 부호기술부(현.국가보안기술연구소). 1997년~현재 한세대학교 IT학부/대학원 정보보호공학과 교수 관심분야는 정보보호평가, 무선랜 보안