셀룰라 오토마타를 이용한 스트림 암호

이준석[†] · 장화식[††] · 이경현[†††]

요 약

본 논문에서는 셀룰라 오토마타를 이용한 스트림 암호 알고리즘를 제안한다. 제안 알고리즘의 안전성 평가를 위해 출력 수열에 대하여 FIPS PUB 140-2에서 제시하는 통계 검정을 수행하였으며, 부가적으로 스트림 암호 출력 수열에 대한 검정 방법으로 많이 사용되는 엔트로피 검정과 선형복잡도 검정 및 자기상관 검정을 수행함으로써 발생 수열의 랜덤성 결과를 보인다.

A Stream Cipher using A Cellular Automata

Jun-Seok Lee[†], Hwa-Sik Jang[††] and Kyung-Hyune Rhee[†††]

ABSTRACT

In this paper, we propose a stream cipher using a cellular automata. For the security evaluation, we use the statistical tests suggested on the report of FIPS PUB 140-2 and additionally, we apply entropy test, linear complexity test and auto-correlation test which are popular statistical tests for the output sequences of stream ciphers.

Key words: 셀룰라 오토마타(cellular automata), 스트림 암호(stream cipher)

1. 서 론

셀룰라 오토마타는 Von Neumann에 의해 스스로 조직화하고 재생산할 수 있는 모델로 소개된 국소적 상호작용에 의해 동시에 상태 갱신을 가지는 많은 셀들로 구성된 유한상태머신이다.

셀룰라 오토마타는 테스트패턴 생성기, 의사랜덤 비트 생성기, 암호학, 오류정정부호, 등의 많은 응용 분야에서 활용되고 있다[1]. 특히 셀룰라 오토마타는 인접한 이웃과의 결합 논리로 서로 연결되어 있고 그 형태가 규칙적인 배열로 구성되기 때문에 랜덤성이 좋은 랜덤 패턴을 효과적으로 생성할 수 있는 특성을 가지고 있다. 따라서 최근에 LFSR의 대안으로 셀룰라 오토마타가 암호 알고리즘에 대한 새로운 응용으로써 등장하고 있다.

[†] 준회원, 부경대학교 전자계산학과 박사수료
[††] 준회원, 대덕대학 인터넷정보기술계열 전임강사
[†††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부 전임, 조교수, 부교수

셀룰라 오토마타는 Wolfram에 의해 처음으로 암호학에 응용되었으며[2], Chaudhuri, Nandi 등에 의해서 $GF(2)$ 상의 선형 셀룰라 오토마타를 기반으로 한 키 스트림 생성기가 제안되고, 분석되었다[3,4]. 또한 Imai 등에 의해서는 $GF(q)$상의 선형 셀룰라 오토마타를 이용한 키 스트림 생성기가 제안되기도 하였다[5]. Kevin, Muzio 등에 의해서는 임의의 기약다항식에 대응하는 셀룰라 오토마타를 구성하는 방법에 대해서 연구되기도 하였다[6,7].

본 논문에서는 셀룰라 오토마타를 이용하여 스트림 암호 알고리즘을 제안하고, 알고리즘의 출력 비트 스트림에 대하여 FIPS(Federal Information Processing Standards)에서 제안하는 암호 모듈에 대한 요구사항에 만족하는가를 FIPS PUB 140-2를 기준으로 검정하였다[8]. 또한 스트림 암호 알고리즘에 대한 평가 방법으로 사용되는 엔트로피 검정과 선형복잡도 검정을 수행하였다. 검정 결과 FIPS PUB 140-2의 기준에 만족하는 통계 검정 결과를 얻을 수 있었으며 5% 유의수준의 엔트로피 검정에 대하여

만족하였고 선형복잡도 검정에서도 만족할 수 있는 결과를 얻었다.

본 논문의 구성은 셀룰라 오토마타에 대한 기본적인 소개를 2장에서 다루었으며, 3장에서 새로운 스트림 암호 알고리즘을 제안하고 4장에서 제안된 알고리즘의 평가를 수행하고 결과를 보인다. 마지막으로 5장에서 결론을 맺는다.

2. 셀룰라 오토마타

셀룰라 오토마타의 구조 중에서 가장 간단한 구조이면서 가장 폭 넓게 응용되고 있는 구조는 1차원 2상태 3이웃 셀룰라 오토마타이다. 각 셀의 상태는 0 또는 1의 상태를 가질 수 있다. 또한 각 셀의 상태천이는 자신의 현재 셀 상태와 인접한 두 이웃의 현재 셀 상태에 의존하여 갱신된다. 이를 식으로 표현하면 다음과 같다.

$$s_i^{t+1} = f(s_{i-1}^t,\ s_i^t,\ s_{i+1}^t)$$

여기서, s_i^t는 시간 t에서의 i번째 셀 상태를 의미한다. 또한 f는 셀 갱신 법칙이라고 불리는 차기상태함수이다. 그러므로 차기상태함수에 의하면 시간 t+1일 때의 i번째 셀의 상태(s_i^{t+1})는 시간 t에서의 이웃한 3개의 이웃, 왼쪽, 자신, 오른쪽 이웃의 상태(s_{i-1}^t, s_i^t, s_{i+1}^t)에 의존하여 결정되게 된다. 이 경우 차기상태함수가 3변수 함수이기 때문에 2^{2^3}, 즉 256개의 차기상태함수가 존재할 수 있다[4].

표 1. 셀룰라 오토마타의 셀 갱신 법칙(선형법칙)

이웃상태	111	110	101	100	011	010	001	000
법칙 60	0	0	1	1	1	1	0	0
법칙 90	0	1	0	1	1	0	1	0
법칙 102	0	1	1	0	0	1	1	0
법칙 150	1	0	0	1	0	1	1	0

여기에서 차기상태함수의 부울 표현식이 XOR 논리만으로 구성된다면 선형법칙(Linear Rule)이라 하고, 그렇지 않으면 비선형법칙(Non-linear Rule)이라고 한다. 법칙의 표현 방법은 가중치를 이용한 십진 표기법을 이용하여 나타낸다. 표 1은 선형법칙에 대한 예를 보여준다.

2.1 셀룰라 오토마타의 특성

n 개의 셀로 구성된 1차원 n 셀 선형 셀룰라 오토마타는 특성행렬(Characteristic Matrix)이라고 불리는 $n \times n$ T 행렬로 표현할 수 있다. 특성행렬의 각 원소들은 셀룰라 오토마타의 상태천이 시 이웃한 셀에 대한 의존도를 나타낸다. 특성행렬은 각 셀에 적용된 법칙에 따라 다음 식을 이용하여 쉽게 구할 수 있다.

$$T_{i,j} = \begin{cases} 1, & j\text{번째 셀이 } i\text{번째 셀에 영향을 미칠 경우} \\ 0, & \text{그 외의 경우} \end{cases}$$

셀 의존도를 3으로 제한된다면 특성행렬은 각 행마다 최대 3개의 원소가 상태 1 값을 가질 수 있는 대각행렬이 된다.

셀룰라 오토마타의 차기상태는 열벡터로 표현되는 현재 상태에 이 특성행렬을 적용함으로써 구할 수 있다. 이를 식으로 표현하면 다음과 같다.

$$s^{t+1} = T \cdot s^t$$

여기서, s^t 는 시간 t 에서의 셀룰라 오토마타의 상태를 나타내며, s^{t+1} 은 다음 시간 t+1 에서의 셀룰라 오토마타의 상태를 표현한다. 또한 T 는 각 셀에 적용된 상태천이법칙을 표현하는 특성행렬인 $n \times n$ 정방행렬이다.

2.2 그룹 셀룰라 오토마타

셀룰라 오토마타의 특성행렬 T 의 행렬식이 0이 아니면 그룹 셀룰라 오토마타(Group CA)라 한다.[4] 그룹 셀룰라 오토마타는 셀룰라 오토마타의 상태천이 그래프가 하나 이상의 사이클로 나타날 경우를 말한다.

그룹 셀룰라 오토마타의 특별한 형태로서 상태 0를 제외한 모든 상태가 사이클 길이 2^n-1인 하나의 사이클에 모두 존재할 경우를 최대길이 셀룰라 오토마타(Maximum Length CA)라고 한다. 여기서 n 은 셀룰라 오토마타의 크기이다. 또한 최대길이 셀룰라 오토마타의 특성행렬에 대한 특성다항식(Characteristic Polynomial)은 원시다항식(Primitive Polynomial)이 된다. 최대길이 셀룰라 오토마타는 우수한 의사랜덤 비트열을 만들어 낼 수 있는 중요한 특성을

가지고 있다[4].

그림 1은 1차원 선형 셀룰라 오토마타의 셀 구성에 대한 예를 보여준다. 이 셀룰라 오토마타의 특성 행렬, 특성다항식 그리고 행렬식의 값은 아래 식과 같다. 이 예가 최대길이 그룹 셀룰라 오토마타임을 그림 2의 상태 천이 그래프를 통하여 확인할 수 있다. 그림 2에서 10진 값은 셀룰라 오토마타의 셀 상태를 나타낸다.

$$T=\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$p(x)=x^4+x+1$$

$$det[T]=1$$

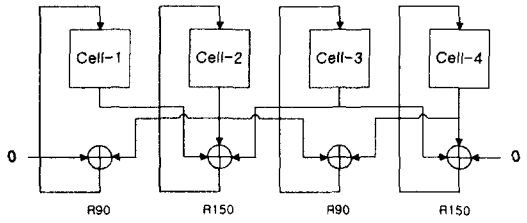


그림 1. 법칙〈90, 150, 90, 150〉을 갖는 CA의 구조

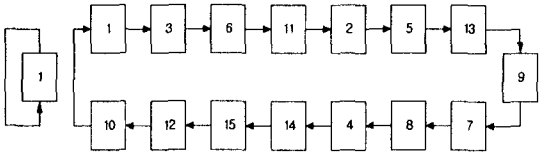


그림 2. 법칙〈90, 150, 90, 150〉 4-셀 셀룰라 오토마타의 상태천이 그래프

3. 새로운 스트림 암호 알고리즘

일반적인 스트림 암호 알고리즘의 기본 구성 요소는 LFSR을 근간으로 하고 있다. 본 논문에서 제안하는 방식은 셀룰라 오토마타를 기본 구성요소로 이용하여 새로운 암호 프리미티브를 제안하고 이를 이용한 스트림 암호 알고리즘을 제안한다. 이는 LFSR에 비해 셀룰라 오토마타가 구조적인 특성에 의해 보다 랜덤한 비트 스트림을 생성할 수 있는 특성을 가지고 있기 때문이다.

제안된 스트림 암호 알고리즘은 $GF(2)$상의 1차원 셀룰라 오토마타를 암호 알고리즘의 기본 구성요소로 사용한다. 이는 셀룰라 오토마타의 기본적인 특성인 단순성(Simple), 모듈러(Modulus), 규칙적인 구성(Regular Structure), 국부적인 상호작용(Local Interaction)에 기인한 하드웨어 구현의 용이함을 이용하여 고속의 알고리즘을 구현하기 위해서이다.

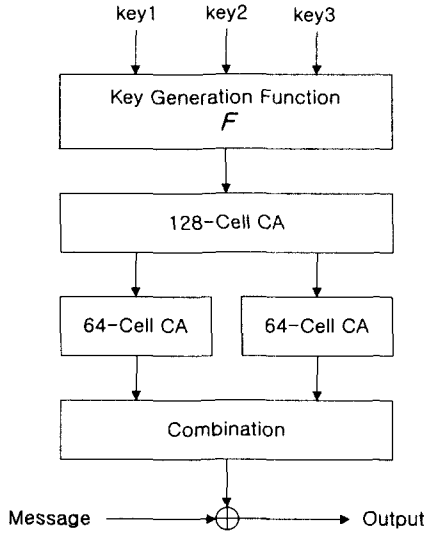


그림 3. 스트림 암호 알고리즘의 블럭도

제안된 스트림 암호 알고리즘의 블록도는 그림 3과 같이 전형적인 스트림 암호 구조를 따른다. 의사 랜덤 비트 생성기는 3개의 128비트 비밀키를 입력받아 키 생성 함수 F를 이용하여 128셀 셀룰라 오토마타의 초기 값으로 사용하게 될 128비트 키를 생성함으로써 키에 대한 안전성을 향상시켰다.

알고리즘에서 사용하는 셀룰라 오토마타의 구성은 최대 길이를 갖는 128차와 64차 원시다항식에 대응하는 하나의 128셀과 두 개의 64셀 1차원 선형 셀룰라 오토마타를 이용하여 구성하였다.

3.1 초기 상태값 생성

셀룰라 오토마타의 초기 상태값의 생성은 3개의 128 비트 비밀키 key1, key2, key3를 다음과 같은 초기 상태값 생성 함수의 입력으로 하여 생성한다. 초기 상태값 생성 함수 Fs는 비선형 함수(Non Linear Function)이면서 균형함수(Balanced Function)이다. 여기서 $\cdot$는 논리연산 AND, $'$은 논리연산

NOT, ⊕는 논리연산 XOR를 나타낸다.

$$F_s(k1, k2, k3) = (k1 \cdot (k2 \oplus k3)) \oplus k3$$
$$= k1 \cdot k2 + k1' \cdot k3$$

이렇게 생성된 128 비트 비밀키는 128-셀 셀룰라 오토마타의 초기 값으로 로드되어지고 셀룰라 오토마타의 천이법칙에 따라 새로운 상태로 천이 된다.

3.2 셀룰라 오토마타의 구성

셀룰라 오토마타의 구성은 셀의 개수가 $n = 128$인 하나의 1차원 선형 셀룰라 오토마타와 $n = 64$인 두 개의 1차원 선형 셀룰라 오토마타로 구성한다. 각각의 셀룰라 오토마타는 최대 길이를 보장하기 위해 다음과 같은 128차와 64차의 원시다항식을 이용하여 구성하였다.

$$p_{64}(x) = x^{64} + x^4 + x^3 + x + 1$$
$$p_{128}(x) = x^{128} + x^{29} + x^{27} + x^2 + 1$$

셀룰라 오토마타의 구성을 위해 사용한 법칙은 3-이웃으로 제한하였으며 법칙 90과 150만을 사용하였다. 또한 법칙 90과 150만을 이용하여 셀룰라 오토마타를 구성하기 때문에 항상 왼쪽과 오른쪽 이웃에 대하여 의존적이고 자신에 대한 의존도는 다음 식과 같이 구성되는 벡터 d에 따라서 달라진다.

$$d = [d_1, d_2, \cdots, d_i, \cdots, d_{n-1}, d_n]$$
$$d_i = \begin{cases} 1 & \text{법칙 150일 경우} \\ 0 & \text{법칙 90일 경우} \end{cases}$$

이는 그림 4와 같은 구조를 이용하여 동일한 구조에서 d_i 값을 제어함으로 구현할 수 있다. 벡터 d는 기약다항식(Irreducible Polynomial)을 상태천이법칙 90과 150만으로 구성된 셀룰라 오토마타의 특성다항식이 되도록 구성하는 알고리즘에 의해 구성된다[9,10].

그리고 가장 왼쪽과 오른쪽 셀의 왼쪽, 오른쪽 이웃의 입력이 존재하지 않기 때문에 이를 위한 입력으로 Null 값을 선택하였다. 이를 Null Boundary 셀룰라 오토마타라 한다.

제안된 키 스트림 생성기에 적용한 자신의 셀에 대한 의존도 벡터 d의 값을 128셀과 64셀 셀룰라 오토마타에 대하여 각각 16진 값으로 나타내었다.

셀룰라 오토마타에 대한 특성다항식은 특성행렬

$d_{64} = (9D4D\ ED99\ 39B7\ B2B9)$

$d_{128} = (4888\ 2FBD\ 6703\ 1A7A\ 7A79\ C0E6\ BDF4\ 1112)$

T를 구성하여 구할 수 있다. 제안된 구조가 3 이웃으로 제한되어져 있기 때문에 특성행렬의 구조는 3중 대각행렬로 나타난다. 또한 셀룰라 오토마타의 천이행렬이 3개의 이웃을 갖는 대각행렬이라면 유클리드 알고리즘을 이용한 점화관계식(Recurrence Relation)을 이용하여 보다 용이하게 구할 수 있다[11].

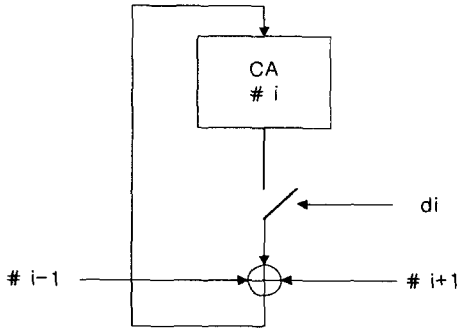


그림 4. 셀의 구조

3.3 키 스트림 생성

제안 알고리즘의 출력 키 스트림의 생성은 다음과 같은 간단한 단계를 거쳐 생성된다.

단계1. 3개의 128비트 비밀키를 입력받아 초기 상태값 생성함수를 통하여 128비트 초기상태를 생성한다.

단계2. 생성된 초기값을 128셀 셀룰라 오토마타의 상태값으로 로드하고 상태를 갱신한다.

단계3. 좌우 64셀의 상태를 각각 64셀 셀룰라 오토마타의 초기값으로 로드한 후 상태를 갱신한다.

단계4. 두 개의 64셀 셀룰라 오토마타의 32번째 셀상태를 XOR 논리를 이용하여 결합한다.

단계5. 결과를 키 스트림으로 출력한다.

단계6. 단계2~단계5를 반복 수행한다.

4. 제안 알고리즘의 평가

이 장에서는 생성된 키 스트림에 대한 랜덤성을 평가한다. 랜덤 수열 생성기의 통계적 검정에 대한

FIPS(Federal Information Processing Standards)의 요구사항은 FIPS PUB 140-2에서 20000비트 출력 수열에 대하여 빈도검정(Monobit Test), 포커검정(Poker Test), 런검정(Runs Test), 롱런검정(Long Run Test)에 대하여 규정하고 있다[8].

본 논문에서는 FIPS 140-2의 검정방법과 스트림 암호 알고리즘의 검정방법인 자기상관검정, 엔트로피 검정, 선형복잡도 검정을 수행하였다[12-15]. 각각의 검정에 대한 결과를 아래에 나타내었다. 모든 검정에서 만족할 만한 결과를 보임을 알 수 있다.

4.1 FIPS PUB 140-2 통계검정

FIPS PUB 140-2 통계검정은 출력 수열 20000 비트에 대하여 다음과 같은 기본검정방법을 제시하였다.

빈도 검정(Monobit Test)은 출력 수열에 대하여 0과 1이 일양적으로 분포하는가를 검정하는 것이다. 1의 개수를 카운트하여 검정결과 9,725~10,275일 경우 빈도검정을 통과하게 된다.

포커 검정(Poker Test)은 n 비트 패턴의 분포가 일양적인가를 검정하는 것이다. 출력 수열을 4비트 블록으로 분할하고 가능한 16가지 패턴의 분포를 카운트하여 아래 식을 이용하여 검정값을 계산한다. 검정결과 2.16~46.17값을 나타낼 경우 포커검정을 통과하게 된다.

$$x=(16/5000)\left(\sum_{i=0}^{15} f(i)^2\right)-5000$$

여기서 i 는 가능한 4비트 패턴을 의미하며 $f(i)$ 는 4비트 블록의 개수이다.

런 검정(Runs Test)은 0 또는 1 의 연속된 길이를 의미하며 길이 6이상의 런에 대하여 6+로 나타낸다. 런 검정은 0 과 1의 런이 랜덤 수열에서 나타나는 것과 유사하게 발생하는가를 검정한다. 검정결과가 표 2에 나타난 기준을 모두 만족하여야만 런 검정을 통과하게된다.

롱런 검정(Long Run Test)의 길이 26이상인 런이 존재하지 않을 경우 검정을 통과하게 된다.

표 2는 FIPS PUB 140-2의 기준과 제안 알고리즘의 검정 결과를 보여준다. 제안 알고리즘의 검정결과가 모두 기준을 만족함을 알 수 있다.

4.2 자기상관 검정(Auto-Correlation Test)

자기상관 검정은 n 비트 이진 비트 스트림에 대하여 d 비트만큼 전이시켜 생성한 스트림과의 상관관계를 조사하는 검정이다. 통계량의 분포는 자유도 1인 x^2-분포를 따른다. 제안 알고리즘에 대한 테스트 결과 128kb 출력 수열에 대하여 $d=8$에 대한 검정값이 $\chi_8^2=0.121$로써 5% 유의수준에 대한 통계량 $\chi_{0.05}^2=3.841$에 대하여 만족함을 알 수 있다.

표 2. FIPS PUB 140-2 통계 검정 결과

Tests		FIPS PUB 140-2	Results
Monobit Test		9725~10275	10011
Poker Test		2.16<x<46.17	8.0
Runs Test	1	2343~2657	2492(2502)
	2	1135~1365	1244(1237)
	3	542~708	619(636)
	4	251~373	339(321)
	5	111~201	162(140)
	6+	111~201	145(165)
Long Run Test		0	0

4.3 엔트로피 검정(Entropy Test)

랜덤 비트 스트림에 대한 엔트로피 검정은 통계적 검정에 비해 좀 더 실제적인 암호학적 중요성을 측정한다는 이점 때문에 스트림 암호 시스템의 성능 평가를 위해 사용되고 있다. 키 소스의 비트 당 엔트로피를 측정함으로써 암호 시스템의 효율적인 키 크기를 측정한다. 제안된 알고리즘의 엔트로피 검정은 검정통계량 -0.00243 으로서 유의수준 5%에 대한 검정역 -1.96 < 통계량 < 1.96을 만족하였다.

4.4 선형복잡도 검정(Linear Complexity Test)

선형복잡도 검정은 주어진 유한 2진 비트 스트림을 생성할 수 있는 가장 짧은 LFSR의 길이를 의미하는 선형복잡도를 결정하기 위한 검정법이다. 일반적으로 랜덤 비트 스트림의 선형복잡도는 비트 스트림 길이의 1/2에 근사된다. 제안된 알고리즘의 선형복잡도는 주어진 8000비트 스트림에 대하여 4000으로서 만족함을 보였다.

5. 결 론

본 논문에서는 LFSR을 대신하여 새로운 기본 구성 요소로 등장한 셀룰라 오토마타를 이용한 스트림 암호 알고리즘을 제안하였다. 제안 알고리즘은 고속

성과 랜덤성을 최대한 이용하기 위해 셀룰라 오토마타의 근본적인 성질을 이용하였다.

제안 알고리즘의 성능 평가를 위해 FIPS에서 제안하는 통계적 검정 외에 자기상관검정과 스트림 암호 알고리즘의 평가 방법인 선형복잡도와 엔트로피 검정을 수행하여 만족할 수 있는 결과를 얻을 수 있었다.

제안 알고리즘은 셀룰라 오토마타를 새로운 암호 알고리즘의 기본요소로 제안함으로써 암호 알고리즘에 대한 새로운 방향을 제시할 수 있을 것으로 기대된다.

참 고 문 헌

[1] A. K. Das, P. P. Chaudhuri, "Vector Space Theoretic Analysis of Additive Cellular Automata and Its Applications for Pseudoexhaustive Test Pattern Generation", *IEEE Trans. Comput.*, vol.42, no.3, pp.340-352, March 1993.

[2] S. Wolfram, "Cryptography with Cellular Automata", *Advances in Cryptology - CRYPTO 85,* LNCS vol.218, pp.429-432, 1985.

[3] S. Nandi, B. K. Kar, P. P. Chaudhuri, "Theory and application of cellular automata in cryptography", *IEEE Trans. Comput.*, vol.43, pp. 1346-1357, 1994.

[4] P. P. Chaudhuri, D. R. Chowdhuri, S. Nandi, S. Chattopadhyay, *Additive Cellular Automata : Theory and Applications*, IEEE Press, New York, 1997.

[5] M. Mihaljevic, H. Imai, "A Family of Fast Keystream Generators Based on Programmable Linear Cellular Automata over GF(q) and Time-Variant Table", *IEICE Trans. Fundamentals*, vol.E82-A, no.1, January 1999.

[6] K. Cattell, J. C. Muzio, "Analysis of One-Dimensional Linear Hybrid Cellular Automata over GF(q)", *IEEE Trans. Comput.*, vol.45, pp.782-792, 1996.

[7] Kevin Cattell, Jon C. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", *IEEE Trans. on Computer-Added Design of Integrated Circuits and System*, vol.5, no.3, March 1996.

[8] http://csrc.nist.gov/publications/fips/

[9] K. Cattell, S. Zhang, "Minimal Cost One-Dimensional Linear Hybrid Cellular Automata of Degree Through 500", *Journal of Electronic Testing: Theory and Applications*, vol.6, no.2, pp.255-258, April 1995.

[10] K. Cattell, J. C. Muzio, "Tables of Cellular Automata for Lowest Weight Primitive Polynomials for Degrees up to 300", *Technical report DCS-163-IR*, Dept. of Computer Science, University of Victoria.

[11] Robert J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[12] 김혜정, 암호 메커니즘의 안전성 평가를 위한 임의성 검정법의 설계 및 분석, 석사학위논문, 부경대학교 대학원, 1999.

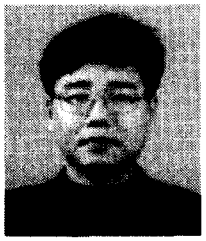
[13] P. L'Ecuyer, "Entropy Tests for Random Number Generators", *ACM Transactions on Modeling and Computer Simulation*, 1997.

[14] R. A. Rueppel, "Linear Complexity and Random Sequences", Lecture Notes in Computer Science, Advances in Cryptoloy - Eurocrypt '85, Springer-Verlag, pp.167-188.

[15] Bruce Schneier, *Applied Cryptography 2nd-Ed,* John Wiley & Sons, Inc. 1996.

이 준 석

1995년 2월 동의대학교 전자통신공학과 졸업
1998년 2월 동의대학교 전자공학과 석사
2001년 2월 부경대학교 전자계산학과 박사수료
관심분야 : 셀룰라 오토마타, 정보보호, 암호이론, 부호이론



장 화 식

1993년 2월 계명대학교 통계학과 졸업
1995년 2월 부경대학교 대학원 전자계산학과 졸업
2000년 2월 부경대학교 대학원 전자계산학과 박사수료
1996년 3월~1999년 8월 제주관광대학 사무자동화과 전임강사
2000년 3월~현재 대덕대학 인터넷정보기술계열 전임강사
관심분야 : 컴퓨터보안, 정보보호, 암호학

이 경 현

1982년 2월 경북대학교 수학교육과 졸업
1985년 2월 한국과학기술원 응용수학과 석사
1992년 8월 한국과학기술원 수학과 박사
1985년 2월~1993년 2월 한국전자통신연구소 연구원, 선임연구원
1993년 3월~현재 부경대학교 전자컴퓨터정보통신공학부 전임, 조교수, 부교수
관심분야 : 암호학, 암호프로토콜, 네트워크보안, 이동네트워크, 그룹키 관리