원격 잠금 장치 암호 알고리즘

이 준석†, 박 영호†, 이 경현†
† 부경대학교 전자계산학과, ‡ 부경대학교 컴퓨터멀티미디어공학전공

A Cryptographic Algorithm for Remote Keyless Entry

Jun-Seok Lee†, Young-Ho Park†, Kyung-Hyune Rhee†
† Department of Computer Science, PKNU
‡ Department of Computer and Multimedia Engineering, PKNU

요 약

본 논문은 자동차 등에 사용중인 원격 잠금 장치 등과 같은 간단한 응용에 적합한 고속 동작이 가능하면서 암호학적으로 안전한 새로운 스트림 암호 알고리즘을 제안한다. 스트림 암호 알고리즘에 많이 적용되고 있는 피트백 쉬프트 레지스트(LFSR)에 비하여 암호학적으로 복잡한 천이 과정을 갖는다고 알려져 있는 셀룰라 오토마타(CA)를 이용하여 의사 랜덤 비트 스트림 생성기(PRNG)를 구성하였다. 또한 제안된 PRNG의 안전성 평가를 위해 출력 2진 비트 스트림에 대하여 통계적 검정과 스트림 암호 시스템의 평가를 수행한다.

1. 서론

현재 여러 가지 원격 잠금 장치(Remote Keyless Entry)가 상용화되어 사용중이다. 하지만 여러 가지 문제점이 발견되고 있으며, 특정 분야에 한정되어 사용되고 있어, 보다 광범위한 활용에 대한 기대에 못 미치고 있다. 이에 다양한 공격으로부터 안전하게 보호될 수 있으며, 보다 넓은 범위에 활용할 수 있는 안정적이고 효율적인 알고리즘의 개발이 필요하게 되었다.

따라서 최근까지 널리 사용되어 온 LFSR류의 대안으로 거론되고 있는 셀룰라 오토마타(CA)를 기반으로 하는 스트림 암호 알고리즘을 개발하였다.

CA는 지금까지 발표된 연구 자료들에 의하면 기존의 LFSR에 비하여 보다 복잡한 천이 과정을 가짐으로써 암호학적으로 보다 안전한 것으로 알려져 있다. 특히 같은 길이의 LFSR에 비하여 비도가 우수하고 선형 복잡도가 뛰어난 것으로 보고되고 있다.

최근에는 CA와 다항식과의 연관성에 대한 연구들이 활발하게 진행되고 있으며 이를 이용하여 원시 다항식에 대응하는 CA의 특성 다항식을 구성함으로써 안전성이 뛰어난 PRNG를 구성할 수 있게 되었다.

2. 본문

CA는 Von Neumann과 Wolfram에 의해 스스로 조직화하고 재생산할 수 있는 모델로 소개되었다[1][2]. CA란 동역학계(dynamical system)를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적인 공간을 셀룰라 공간(cellular space)의 기본 단위인 셀(cell)이 취할 수 있는 상태(state)를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용(local Interaction)에 의해서 동시에 갱신되는 시스템이다.

CA는 test pattern generation, pseudo-random number generation, cryptography, error correcting codes, signature analysis 등 많은 응용 분야에서 활용되고 있다[3]. 특히 CA는 인접한 이웃들과 결합 논리로써 서로 연결되어 있고 그 형태가 규칙적인 배열로 구성되기 때문에 랜덤성(randomness)이 좋은 랜덤 패턴(random pattern)을 효과적으로 생성할 수 있다. 그래서 최근에 LFSR의 대안으로 CA가 암호 알고리즘에 대한 새로운 응용으로써 대두되고 있다.

CA는 Wolfram에 의해 처음으로 암호학에 응용되었다[4]. 최근에는 PCA with ROM과 Two Stage PCA로 불리는 GF(2) 상의 선형 셀룰라 오토마타(Linear CA)를 기반으로 한 새로운 키스트림 생성기가 Nandi 등에 의해서 제안되고, 분석되었다[5][6]. 그리고 임의의 기약다항식에 대응하는 CA를 구성하는 방법에 대한 알고리즘이 Kevin, Muzio 등에 의해서 연구되었다[7]. 또한 GF(q)상의 선형 CA에 대하여 활발하게 연구되어지고 있고, Kevin, Muzio 등에 의해서 특성과 구성 방법이 소개되었다[8].

또 다른 CA를 이용한 키스트림 생성기로는 table shuffling을 이용한 RC4의 변형으로써 time-variant table을 갖는 GF(q)상의 CA를 이용한 키스트림 생성기가

Mihaljevic, Imai 등에 의해서 최근에 연구되었다[9].

2.1 1-차원 셀룰라 오토마타(1-D CA)

2.1.1 1-차원 CA의 정의와 표기법

CA의 가장 간단한 구조는 1-차원 CA이다. 이들은 모든 셀들이 선형으로 배열되어져 있고, 가장 중요하게 다루어지고 있는 형태는 2-상태 3-이웃 CA(2-state 3-neighborhood CA)이다. CA를 설명하기 위하여 다음의 표기법을 정의한다.

i : 일차원으로 배열되어 있는 각 셀들의 위치

t : 시간 단계

s_i^t : 시간 t에서 i 번째 셀의 상태

s_i^{t+1} : 시간 $t+1$에서 i 번째 셀의 상태

2.1.2 1-차원 CA의 법칙

CA를 구성하는 차기 상태 전이 함수를 일반적으로 CA 법칙(rule)이라고 말하고, 3-이웃 CA에 대한 차기 상태 전이 함수는 다음과 같이 주어진다.

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

여기서, f는 결합논리를 가지는 국소 전이 함수(local transition function)이다. 그러므로 f는 3개의 변수를 가지는 선형 부울 함수로 간주할 수 있다. 따라서 2^3개의 서로 다른 구성형태가 존재하고, 2^{2^3}개의 상태 전이 함수가 존재한다.

이웃 상태	111	110	101	100	011	010	001	000	rule
다음상태1	0	1	0	1	1	0	1	0	90
다음상태2	1	0	0	1	0	1	1	0	150

CA의 셀들의 상태를 GF(2)의 원소로 다루고 CA의 차기 상태 전이 함수를 위와 같이 표현한다. 여기서 첫 번째 행은 시간 t에서의 3-이웃으로 구성 가능한 8가지 구성형태이고, 두 번째와 세 번째 행은 시간 $t+1$에서 i번째 셀의 갱신된 후의 상태이다.

아래 rule에 대한 결합논리는 다음 식으로 표현할 수 있고 "+"는 XOR(exclusive-OR) 논리를 나타낸다.

rule 90 : $s_i^{t+1} = s_{i-1}^t + s_{i+1}^t$

rule 150 : $s_i^{t+1} = s_{i-1}^t + s_i^t + s_{i+1}^t$

즉, rule 90은 자신의 왼쪽과 오른쪽 셀의 현재 상태에 의존하여 차기 상태를 결정하게된다. 유사하게, rule 150은 자신과 왼쪽, 그리고 오른쪽 이웃의 셀을 이용하여 차기 상태로 갱신하게 된다.

2.1.3 1-차원 CA의 분류

1-차원 CA는 셀들에 적용된 결합논리의 종류에 따라서 linear CA, additive CA, nonadditive CA 등으로 분류할 수 있다.

Linear CA : XOR 논리로만 이루어진 CA

Additive CA : XOR/XNOR 논리의 결합으로 구성된 CA

Nonadditive CA : AND/OR 논리로 이루어진 CA

또한 각각의 셀에 동일한 rule이 적용된 CA를 Uniform CA라고 부르고, 셀에 적용된 rule이 동일하지 않은 경우를 Hybrid CA라고 한다.

그리고 CA의 상태에 따라서 Group CA 또는 Nongroup CA로 구분할 수 있다. Group CA란 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA를 말한다. 그 외의 CA를 Nongroup CA라고 한다.

2.1.4 경계 조건

1-차원 CA의 가장 왼쪽 셀과 가장 오른쪽 셀은 각각 2개의 이웃만을 가지게 된다. 그러므로 세 번째 이웃의 상태를 결정해 주어야 한다. 이러한 제 3 이웃을 결정하는 방법에 따라 3가지 경계조건을 이룬다. 즉, 가장 왼쪽과 오른쪽 셀의 왼쪽과 오른쪽 이웃을 상태 0으로 결정하는 NBCA(Null Boundary CA), 가장 왼쪽 셀과 가장 오른쪽 셀이 연결된 것으로 간주하는 PBCA(Periodic Boundary CA), 그리고 가장 왼쪽(오른쪽) 셀의 다음 상태가 그 자신과 오른쪽(왼쪽) 이웃, 두 번째 오른쪽(왼쪽) 이웃 셀의 현재 상태에 의존하는 IBCA(Intermediate Boundary CA)로 경계조건을 나눈다.

2.1.5 1-차원 CA의 전이행렬과 CA 특성다항식

n개의 셀로 구성되는 1-차원 CA는 선형 연산자 A에 의해서 특성화될 수 있다. 여기서 A는 GF(2) 상에서의 $n \times n$ 행렬로 나타낼 수 있고, A의 i번째 행은 i번째 셀에 적용되는 rule이며 그 셀의 다음상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 표기한다. 예를 들어서, 네 개의 셀을 가진 Null Boundary 1차원 CA의 rule이(90,150,90,150)이라고 하면 전이행렬 A는 다음과 같다.

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

만약 CA의 전이행렬 A가 정칙행렬, 즉 $det(A) = 1$이면 그 CA는 Group CA이다. Group CA는 최대 길이를 갖는 CA와 최대 길이를 갖지 않는 CA로 구분할 수 있다. n개의 셀로 구성된 CA에서 모든 셀의 상태가 0인 경우를 제외하고 $2^n - 1$개의 상태가 하나의 주기에서 나타날 때 최대 길이를 가진다고 한다. 또한 최대 길이를 갖는 CA의 특성다항식은 원시다항식(primitive polynomial)이 된다.

CA의 셀들의 차기 상태는 열 벡터로 나타내어지는 CA의 셀들의 현재 상태에 이 선형 연산자를 적용함으로써 생성된다. 적용되는 연산은 modulo 2의 연산이다. 만약 t번째 시각에서의 CA의 상태가 아래와 같은 열 벡터로 표현한다면

$$s^t = [\, s_1^t\ s_2^t\ \cdots\ s_n^t \,]^T$$

CA의 차기 상태는 다음과 같이 주어진다.

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

또한 이러한 전이 행렬 A에 대하여 CA 특성 다항식은 다음 식으로 구할 수 있다.

$$\Delta = |xI - A|$$

여기서, x는 임의의 값이고, I는 identity 매트릭스, A는 CA 전이 매트릭스이다. $xI - A$를 CA 특성 매트릭스라고 부른다. 또한 특성다항식은 x에 대한 n차 다항식이다.

$$p(x) = |xI - A| = \begin{vmatrix} x & 1 & 0 & 0 \\ 1 & x+1 & 1 & 0 \\ 0 & 1 & x & 1 \\ 0 & 0 & 1 & x+1 \end{vmatrix} = x^4 + x + 1$$

위의 다항식은 위의 예에서 보인 rule(90,150,90,150)의 4-셀 Null-boundary LHCA(Linear Hybrid CA)에 대

한 특성다항식이다.

2.2 새로운 PRNG 알고리즘

이 절에서는 원격 잠금 장치를 위한 새로운 암호 알고리즘을 제안한다. 제안된 알고리즘은 스트림 암호 시스템으로 구성하고, 스트림 암호에서 관심의 대상인 비트 스트림의 생성을 위해 최근에 LFSR의 대안으로 주목받고 있는 셀룰라 오토마타를 이용하였다. 본 논문에서는 구현의 용이성, 원격 잠금 장치 수준에 적절한 안전성, 고속성, 그리고 다양한 응용에의 확장성 등을 고려하여 GF(2)상의 Null-Boundary 1-차원 LHCA를 암호 알고리즘의 기본 구성요소로 선택하였다.

2.2.1 제안된 PRNG의 구조

제안된 암호 시스템의 블럭도는 그림 1과 같다. PRNG의 실질적인 입력이 되는 키는 3개의 128-bit 비밀키를 입력받아 키 생성 함수 F를 이용하여 생성함으로써 키에 대한 안전성을 향상시켰다. 여기서 사용하는 CA의 구성은 최대 주기를 보장하기 위해 128차와 64차의 원시다항식(primitive polynomial)에 대응하는 하나의 128-cell CA와 두 개의 68-cell CA를 이용하여 PRNG를 구성하였다[10][11].

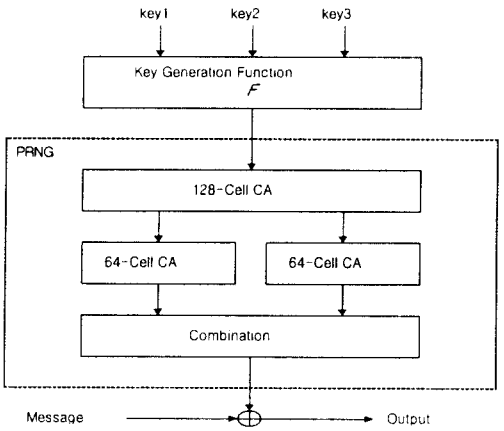

그림 1 제안된 의사 랜덤 비트 생성기

2.2.2 CA의 구성

CA의 구성은 셀의 개수가 $n=128$인 하나의 1-D LHCA와 $n=64$인 두 개의 1-D LHCA로 구성하였다. 각각의 CA는 최대 주기를 보장하기 위해서 128차와 64차 원시다항식을 이용하여 구성하였다.

CA의 차기 상태 전이 법칙은 rule 90과 150으로 제한하였으며, 이웃 의존도는 nearest-neighbor로써 제한하였다. 적용된 경계 조건은 가장 왼쪽(오른쪽) cell의 왼쪽(오른쪽) 입력이 0인 Null Boundary 경계조건으로 제한하였다. 또한 왼쪽 이웃과 오른쪽 이웃의 상태에 항상 의존적이고 자신에 대한 의존도는 d의 값에 의해서 결정되도록 하였다. d는 기약다항식을 rule 90과 150으로 구성된 CA의 특성다항식이 되도록 구성하는 알고리즘에 의해 구성된다.

$$d=[d_1,\ d_2,\ \cdots,\ d_{i-1},\ d_i,\ d_{i+1},\cdots,\ d_{n-1},\ d_n]$$

$$d_i=\begin{cases}1 & i=a,\ b,\ \cdots,\quad 1\le i\le n\\ 0 & otherwise\end{cases}$$

여기서, $i=a,\ b,\ \cdots,$는 구성된 CA의 셀 번호를 나타낸다. $i=a,\ b,\ \cdots,$인 경우 rule 150이 적용되고, 그 외의 경우에는 rule 90이 적용된다. 그림 2는 d_i의 값에 따라서 rule 90과 150을 적절하게 적용할 수 있도록 설계된 CA의 cell 구조를 보여준다.

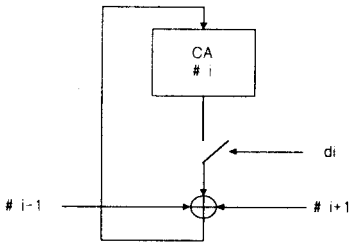

그림 2 CA의 cell 내부 구조

이러한 구조를 갖는 CA의 특성 매트릭스 A는 $n\times n$ 매트릭스로 다음과 같이 three-diagonal 매트릭스로 구성된다.

$$A=\begin{bmatrix} d_1 & 1 & 0 & \cdots & 0 & 0\\ 1 & d_2 & 1 & \ddots & & 0\\ 0 & 1 & d_3 & \ddots & & \vdots\\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots\\ 0 & & & \ddots & d_{n-1} & 1\\ 0 & 0 & \cdots & \cdots & 1 & d_n \end{bmatrix}$$

여기서 $d_i=1\ (i=a,\ b,\ \cdots,)$이고 나머지는 0이다. 따라서, CA의 특성 다항식은 다음과 같이 구할 수 있다.

$$\phi(x)=|xI-A|$$

제안된 PRNG에서 적용한 자신에 대한 의존도 d의 값을 16진 값으로 아래에 표현하였다. 여기서 d_{128}은 128-cell CA의 의존도를 의미하고, d_{64}는 64-cell CA의 의존도를 의미한다.

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

d_{64} = 9D4D ED99 39B7 B2B9

CA에 대응하는 특성다항식은 천이 매트릭스 A를 구성하여 구할 수 있다. 또한 CA의 천이 매트릭스가 three-diagonal 매트릭스로 위와 같은 특별한 구성을 가진다면 특성다항식은 Euclid's Algorithm을 이용한 점화 관계식(recurrence relation)을 이용하여 보다 용이하게 구할 수 있다[12]. 제안된 PRNG에 적용한 특성다항식은 128차와 64차 원시다항식으로 아래와 같다.

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

$$p_{64}(x)=x^{64}+x^4+x^3+x+1$$

2.2.3 키 생성

키 생성(Key Generation)은 3개의 128-bit(16-byte) 비밀키 $x,\ y,\ z$를 입력받아 아래와 같은 키 생성 함수에 의해 생성한다.

$$f_{key}(x,\ y,\ z)=(x\wedge y)\vee(\neg x\wedge z)$$

여기서, $\vee$는 논리 연산 OR, $\wedge$는 논리 연산 AND 그리고 $\neg$는 논리연산 NOT를 의미한다.

생성된 키는 128-cell CA의 초기 값을 설정하기 위

해 CA가 정상 상태에 도달할 수 있도록 충분한 갱신 과정을 거친 후, CA 상태값을 128-cell CA의 초기값으로 설정하고 CA의 천이 법칙에 따라 새로운 상태로 천이한다.

2.2.4 비트 스트림의 생성

비트 스트림의 생성은 다음과 같은 순서로 매우 간단하게 생성된다. 비밀키로 구성한 키 값에 의해 128-cell CA의 초기 값을 설정하고 이를 천이 시킴으로서 다음 상태 값을 얻는다. 동시에 128-cell CA의 출력을 64-bit씩 좌우로 나누어 64-cell CA의 입력 값으로 사용한다. 이를 천이 시켜 64-cell CA의 출력을 얻는다. 여기서 각 64-cell CA의 32번째 cell의 상태 값을 출력으로 내보낸다. 최종적으로 두 개의 64-cell CA의 출력을 조합함으로써 PRNG의 출력을 구성한다.

2.3 제안된 PRNG의 평가

제안된 PRNG의 출력에 대한 임의성을 평가하기 위하여 본 연구실에서 개발한 임의성 평가 통계 검정 프로그램을 이용하여 출력 스트림에 대해 시뮬레이션을 수행하였다. 또한 기존에 가장 빠른 스트림 암호 알고리즘으로 잘 알려져 있는 RC4 알고리즘과 수행 속도를 비교하였다.

2.3.1 빈도 검정(Frequency Test)

통계량의 분포는 자유도 1인 χ^2-분포를 따르며 유의수준 α 에 대한 기각역은 $\chi_0^2 > \chi^2(1, \alpha)$ 이다. 제안된 비트 스트림 생성기의 출력 스트림에 대한 테스트 결과 통계량 $\chi^2 = 0.819$로써 5% 유의수준에 대한 통계량 $\chi_{0.05}^2 = 3.841$을 만족함을 알 수 있다.

2.3.2 계열 검정(Serial Test)

통계량의 분포는 자유도 2인 χ^2-분포를 따르며 유의수준 α에 대한 기각역은 $\chi_0^2 > \chi^2(2, \alpha)$이다. 제안된 알고리즘의 출력 비트 스트림에 대한 테스드 결과 통계량 $\chi^2 = 1.225$로써 5% 유의수준에 대한 통계량 $\chi_{0.05}^2 = 5.991$를 만족함을 알 수 있다.

2.3.3 포커 검정(Poker Test)

통계량의 분포는 자유도 $2^m - 1$인 χ^2-분포를 따르며 유의수준 α에 대한 기각역은 $\chi_0^2 > \chi^2(2^m - 1, \alpha)$ 이다. 테스트 결과 $m = 8$에 대하여 통계량은 $\chi_{m=8}^2 = 282.874$로써 5% 유의수준에 대한 통계량 $\chi_{0.05}^2 = 293.247$을 만족함을 알 수 있다. $m = 16$에 대해서도 통계량은 $\chi_{m=16}^2 = 65733.632$으로써 5% 유의수준에 대한 통계량 $\chi_0^2 = 66131.630$에 대하여 만족한다.

2.3.4 런 검정(Run Test)

통계량의 분포는 자유도 $2(L-1)$인 χ^2-분포를 따르며 유의수준 α에 대한 기각역은 $\chi_0^2 > \chi^2(2(L-1), \alpha)$이다. 여기서 L은 런의 길이를 의미한다. $L = 16$에 대한 테스트 결과 통계량 $\chi_{L=16}^2 = 14.238$로써 5% 유의수준에 대한 통계량 $\chi_{0.05}^2 = 24.995$에 대하여 만족한다.

2.3.5 자기 상관 검정(Auto-Corralation Test)

통계량의 분포는 자유도 1인 χ^2-분포를 따르며 유의수준 α에 대한 기각역은 $\chi_0^2 > \chi^2(1, \alpha)$이다. 제안한 의사 랜덤 비트 스트림 생성기에 대한 테스트 결과 $d = 8, 16$에 대하여 통계량 $\chi_{d=8}^2 = 0.121$, $\chi_{d=16}^2 = 0.009$으로써 5% 유의수준에 대한 통계량 $\chi_{0.05}^2 = 3.841$을 만족하고 있다.

2.3.6 엔트로피 검정(Entropy Test)

랜덤 비트 스트림 생성기에 대한 엔트로피 검정은 통계적 검정에 비해 좀 더 실제적인 암호학적 중요성을 측정한다는 이점 때문에 스트림 암호 시스템의 성능 평가를 위해 사용되고 있다.

엔트로피 검정 결과 검정 통계량 -0.00243으로서 유의수준 5%에 대한 검정역 $-1.96 \leq$통계량≤ 1.96에 대하여 만족함을 알 수 있다.

2.3.7 선형 복잡도 검정(Linear Complexity Test)

제안된 알고리즘의 출력 8000-bit 검정 파일에 대한 선형 복잡도는 4000이다.

2.3.8 선형 복잡도 프로파일 검정

제안된 의사 랜덤 비트 스트림에 대한 선형 복잡도 프로파일 검정의 결과는 다음 그림과 같다. 7920 번째 비트에서 8000 번째 비트까지의 선형 복잡도 프로파일을 보이고 있다. 이 때 7920 번째 비트에서의 선형 복잡도는 3961임을 볼 수 있다.

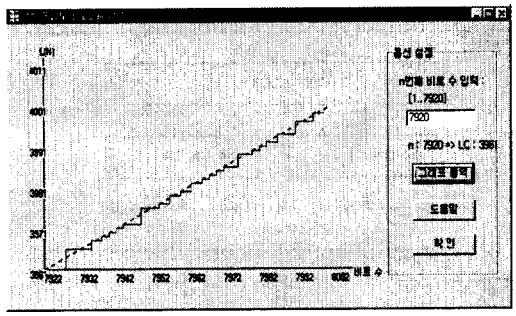

그림 3 선형 복잡도 프로파일 검정 결과

2.3.9 알고리즘의 처리 속도 비교

이 절에서는 기존에 가장 빠른 스트림 암호 알고리즘으로 잘 알려져 있는 RC4 스트림 암호 알고리즘과의 처리 속도를 비교한다. 이를 위한 시뮬레이션은 Pentium Pro(180MHz) CPU와 메모리 64MB를 갖춘 Windows 98 시스템에서 Turbo-C 컴파일러를 이용하여 구현하였다.

표 1 알고리즘의 처리 속도 비교

알고리즘	수행시간(second)
RC4	1.703297
제안 알고리즘(2-bit output)	18.461538
제안 알고리즘(128-bit output)	0.494505

시뮬레이션 결과는 표 1과 같으며 RC4에 비해 매우 느린 것으로 나타난다. 하지만 출력되는 비트 수를 적절하게 제어한다면 RC4에 비해 성능 면에서 뒤떨

어지지 않는다. 즉, RC4의 경우 한 번의 사이클에 128-bit의 출력을 생성하지만 제안된 알고리즘은 단지 2-bit의 출력을 생성한다는 것을 감안한다면 성능 면에서 크게 떨어진다고 볼 수 없다. 즉, 제안한 알고리즘에서는 64-cell CA의 출력 비트 수를 1-bit으로 제한하였지만 이를 8-bit로 수정한다면 RC4의 성능과 유사하게 될 것이다.

3. 결론

제안된 PRNG는 간단한 구조로 구성되어져 있어 하드웨어로 On-chip하기에 용이하고, 처리 속도 면에서도 스트림 암호 알고리즘들 중 가장 빠른 것으로 알려져 있는 RC4 스트림 암호 알고리즘과 유사한 수행 속도를 나타내며 구현 방법에 따라 보다 고속으로 비트 열을 생성할 수 있어 고속의 난수열 생성이 요구되는 고속 암호화 통신 알고리즘에도 적용될 수 있는 장점이 있다. 또한 기존의 LFSR 기반 시스템에 비해 암호학적으로 뛰어난 안전성을 보장한다고 알려져 있는 CA를 기반으로 하여 PRNG를 구성함으로써 복잡한 천이 과정을 가지도록 구성되었다.

제안된 알고리즘의 구성은 구조를 간단하게 하기 위하여 64-cell CA의 전이 법칙을 같은 rule로 구성하였다. 보다 높은 안전성을 요구한다면 각각 다른 rule을 적용하여 구성할 수 있을 것이다.

또한 이미 언급하였듯이, 성능을 강화하고자 한다면 1-bit 출력으로 제한된 64-cell CA의 출력 비트 수를 안전성이 허용되는 범위 내에서 다중 비트 출력으로 구성할 수 있다. 권장하는 64-cell CA의 출력 비트 수는 16-bit 이하이다. 또는 출력 비트를 선택하는 제어 로직을 이용하여 출력 비트를 선택할 수 있도록 조합 회로를 설계하면 보다 뛰어나고 안전한 알고리즘을 얻을 수 있을 것이다.

따라서 안전성과 성능에 대한 trade-off 관계를 이용하여 적용하고자 하는 응용에 알맞도록 조절한다면 보다 효율적인 알고리즘을 얻을 수 있으므로, 기 사용중인 자동차 원격 잠금 장치 뿐 아니라 도어 원격 잠금 장치, 출입 통제 원격화, 개인 식별/인식 등의 간단하면서 높은 안전성을 요구하는 많은 응용에 적용할 수 있을 것으로 판단되어진다. 또한 이러한 여러 가지 응용이 통합된 새로운 제품으로도 개발 가능할 것이다.

또한 제안된 알고리즘은 소프트웨어, 하드웨어 구현 시 큰 오버헤드 없이 약간의 수정을 통하여 블록 암호 및 데이터 무결성 확인이 가능한 해쉬 함수 등에 적용가능하며, 보다 복잡한 암호 시스템의 기본 모듈로 설계될 수 있을 것으로 판단된다.

참고문헌

[1] J. Von Neumann, "Theory of self-reproducing automata", University of Illinois Press Urbana, 1966.
[2] S. Wolfram, "Statistical mechanics of cellular automata", Rev. Modern Physics, vol. 55, no. 3, July 1983.
[3] A. K. Das and P. P. Chaudhuri, "Vector Space Theoretic Analysis of Additive Cellular Automata and Its Application for Pseudoexhaustive Test Pattern Generation", IEEE Trans. Comput., vol. 42, no. 3, pp. 340-352, March 1993.
[4] S. Wolfram, "Cryptography with Cellular Automata", Advances in Cryptology - CRYPTO 85, Lecture Notes in Computer Science, vol. 218, pp. 429-432, 1985.
[5] S. Nandi, B. K. Kar, and P. Pal Chaudhuri, "Theory and application of cellular automata in cryptography", IEEE Trans. Comput., vol. 43, pp. 1346-1357, 1994.
[6] P. P. Chaudhuri, D. R. Chowdhuri, S. Nandi, and S. Chattopadhyay, "Additive Cellular Automata : Theory and Applications", IEEE Press, New York, 1997.
[7] Kevin Cattell and Jon C. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", IEEE Trans. on Computer-Added Design of Integrated Circuits and System, vol. 15, no. 3, March 1996.
[8] K. Cattell and J. C. Muzio, "Analysis of One-Dimensional Linear Hybrid Cellular Automata ove GF(q)", IEEE Trans. Comput., vol. 45, pp. 782-792, 1996.
[9] M. Mihaljevic and 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.
[10] Kevin CAttell and Shujian Zhang, "Minimal Cost One-Dimensional Linear Hybrid Cellular Automata of Degree Through 500", Journal of Electronic Testing: Theory and Applications, 6(2):255-258, April 1995.
[11] Kevin M Cattell, Jon 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, 1995.
[12] Robert J. McEliece, "Finite Fields for Computer Scientists and Engineers", Kluwer Academic Publishers, 1987.