셀룰라 오토마타를 이용한 블록 암호 알고리즘

이준석[†] · 장화식[††] · 이경현[†††]

요 약

본 논문에서는 LFSR(Linear Feedback Shift Register)의 대안으로 소개되고 있는 셀룰라 오토마타(CA : Cellular Automata)를 소개하고 이를 이용한 새로운 블록 암호 알고리즘을 제안한다. 제안된 블록 암호 알고리즘의 성능과 안전성 평가를 위해 쇄도효과와 수행속도에 대해 표준 블록 암호 알고리즘과 비교를 수행하고 또한 차분 분석법(Differential Cryptanalysis)에 대하여 제안 알고리즘에 대한 축소된 버전으로 평가를 수행한다. 부가적으로 제안 암호 알고리즘의 출력 비트열에 대하여 FIPS PUB 140-2(Federal Information Processing Standards Publication 140-2)의 랜덤 수열에 대한 통계적 검정을 수행함으로써 출력 수열이 랜덤함을 보인다.

A Block Cipher Algorithm based on Cellular Automata

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

ABSTRACT

In this paper, we introduce cellular automata and propose a new block cipher algorithm based on cellular automata. For the evaluation of performance and security, we compare the results of the proposed algorithm with them of the standard block ciphers such as DES, Rijndael regarding on avalanche effects and processing time, and analyze the differential cryptanalysis for a reduction version of the proposed algorithm. In addition, we perform the statistical tests in FIPS PUB 140-2(Federal Information Processing Standards Publication 140-2) for the output bit sequences of proposed algorithm to guarantee the randomness property.

Key words: 셀룰라 오토마타(Cellular Automata), 블럭 암호(Block Cipher)

1. 서 론

셀룰라 오토마타는 Von Neumann에 의하여 처음 소개되었고, Wolfram에 의해서 수학적 기초를 마련하였다[1]. 또한 Wolfram은 암호학에 셀룰라 오토마타를 처음으로 도입하였다[2]. 이후 셀룰라 오토마타에 대한 많은 분석과 연구가 이루어졌으며[3,4] 부울 방정식의 해법, BIST 구조, 의사랜덤 수열생성기, 암호알고리즘, 등과 같은 많은 응용분야에 셀룰라 오토마타가 활용되었다[5-9].

특히 Chaudhuri 등은 다차원 셀룰라 오토마타를 제안하였으며, 그룹 셀룰라 오토마타(Group CA)를 구성할 수 있는 선형 법칙(Linear Rules)을 이용한 하이브리드 셀룰라 오토마타(Hybrid CA)를 구성함으로써 같은 길이의 사이클을 이용하여 여러 개의 기본변환(Fundamental Transformations)을 정의하고, 이를 연속적으로 적용함으로써 n-비트 메시지 블록을 암호화하는 블록 암호 알고리즘을 제안하였다. 이 구조는 복호시 암호화에 적용된 기본변환을 역순으로 적용함으로써 특별한 복호 알고리즘 없이 손쉽게 메시지를 복호할 수 있는 특징을 갖는다. 또한, Muzio 등은 최대 주기를 갖는 LFSR에 대응하는 셀룰라 오토마타를 특별한 선형 법칙을 이용한 PCA(Programmable CA)로 구성할 수 있음을 보고하였다[10,11]. 최근에는 Phase shifter를 가지는

[†] 준회원, 부경대학교 대학원 전자계산학과
[††] 준회원, 대덕대학 컴퓨터정보통신계열
[†††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부

LFSR과 셀룰라 오토마타에 대한 비교 분석 결과가 보고되어 있다[12,13].

기존 연구 결과에 따르면 랜덤성 관점에서 셀룰라 오토마타는 LFSR에 비하여 매우 복잡한 천이과정을 가짐으로써 우수한 랜덤성을 가지는 것으로 알려져 있다. 따라서 본 논문에서는 셀룰라 오토마타를 이용한 새로운 블록 암호 알고리즘을 제안하고 이의 안전성과 성능 평가를 위해 표준 블록 암호 알고리즘인 DES와 Rijndael 알고리즘과의 수행속도 및 쇄도 효과를 비교하며 차분 분석법(Differential Cryptanalysis)에 대하여 제안 알고리즘에 대한 축소된 버전으로 평가를 수행한다. 또한 제안된 암호 알고리즘의 출력 수열에 대한 랜덤성 보장을 위한 한가지 방법으로써, 현재 가장 많이 사용되고 있는 출력 비트열에 대한 FIPS PUB 140-2(Federal Information Processing Standards Publication 140-2)의 랜덤 수열에 대한 통계적 검정을 수행함으로써 출력 수열이 랜덤함을 보인다.

2. 셀룰라 오토마타

2.1 셀룰라 오토마타의 정의 및 종류

셀룰라 오토마타(Cellular Automata)는 특별한 법칙에 의해 동시에 국소적인 상호작용을 가지는 동일한 셀들이 규칙적으로 배열되어져 있는 유한상태머신(Finite State Machine)이다. [그림 1]은 1차원 배열을 가지는 1-D(One-Dimensional) 셀룰라 오토마타의 예를 보여준다. 여기서, 각 셀들의 차기 상태는 천이함수 또는 법칙에 의존하여 갱신된다.

각 셀에 적용된 상태 천이법칙은 아래 식으로 표현할 수 있다.

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

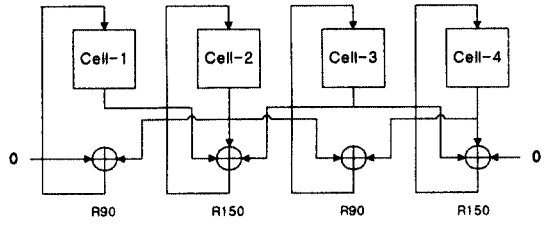


그림 1. 4-셀 1-차원 셀룰라 오토마타의 구조

여기서, s_i^t는 시간 t에서 i번째 셀의 상태 값을 의미하고, f는 상태 천이함수를 나타낸다. 그러므로, 3-이웃 셀룰라 오토마타일 경우 시간 t+1에서의 i번째 셀의 상태 값은 시간 t에서의 i-1, i, i+1번째 셀의 상태 값에 의존하여 결정된다. 상태 천이함수는 일반적으로 아래 표와 같이 법칙으로써 표현한다.

표 1. 상태천이 법칙의 예

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

[표 1]에서 첫 번째 행은 3개의 이웃으로 2^3개의 가능한 상태를 나타낸다. 두 번째 행 이하는 특별한 천이법칙에 대한 상태 값을 나타내고 있다. 따라서, 3-이웃 셀룰라 오토마타에서 가능한 법칙의 개수는 2^{2^3}이다. 또한 법칙 90에서 표현되는 90은 2진 상태 값에 대응하는 10진 값과 동일하다. 또한 이들 법칙은 부울 방정식으로 표현할 수 있다. 위 [표 1]에서 보여진 법칙들에 대한 부울 방정식은 아래 식과 같다.

$$\textit{Rule } 90 \quad s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t$$

$$\textit{Rule } 150 \quad s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$$

$$\textit{Rule } 60 \quad s_i^{t+1} = s_{i-1}^t \oplus s_i^t$$

$$\textit{Rule } 102 \quad s_i^{t+1} = s_i^t \oplus s_{i+1}^t$$

부울방정식에 적용된 연산에 따라서 셀룰라 오토마타를 선형 셀룰라 오토마타, 비선형 셀룰라 오토마타, 등으로 구분하고 있다. 선형 셀룰라 오토마타란 적용된 연산이 XOR/XNOR만으로 구성된 것을 의미하고, 그 외의 연산이 적용된 셀룰라 오토마타는 비선형 셀룰라 오토마타이다. 또한 모든 셀에 동일한 법칙이 적용된 셀룰라 오토마타를 Uniform 셀룰라 오토마타라고 하고, 적용된 법칙이 2개 이상일 경우 Hybrid 셀룰라 오토마타라고 부른다.

각 셀의 상태 천이에서 고려해야 할 또 다른 것은 셀룰라 오토마타를 구성하는 양끝의 셀에서 존재하

지 않는 이웃에 대한 가정이다. 즉, 1-차원 셀룰라 오토마타에 대하여, 첫 번째 셀의 왼쪽 이웃과 마지막 셀의 오른쪽 이웃이 존재하지 않기 때문에 이에 대한 가정을 정의해야 한다. 이를 경계조건(Boundary Condition)이라고 한다. 경제조건에 따라 CA를 NBCA(Null Boundary CA), PBCA(Periodic Boundary CA), IBCA(Intermediate Boundary CA)로 분류한다. 또한 셀룰라 오토마타의 구성에 따라 1차원, 2차원, 3차원 셀룰라 오타마타로 구분할 수 있다.

2.2 셀룰라 오토마타를 이용한 기존 블록 암호 알고리즘

이 절에서는 셀룰라 오토마타를 기반으로 하여 기존에 제안된 Chaudhuri의 알고리즘과 DES 구조를 따르지만 F-함수와 키 생성 부분을 셀룰라 오토마타를 이용하여 구성한 Srisuchinwong의 블록 암호 알고리즘을 간단하게 소개한다.

[5]에서 Chaudhuri 등이 제안한 셀룰라 오토마타 기반 블록 암호 알고리즘은 구성된 셀룰라 오토마타의 특성방정식이 최대 주기를 갖지 않으면서 그룹 특성을 가지도록 구성하고, 암호화하기 위한 F-함수를 involution 특성을 이용할 수 있도록 기본변환(Fundamental Transformations)으로 정의함으로써 다양한 암호화 함수를 선택할 수 있도록 설계함으로써 랜덤성을 높이고 있고, 복호시 적용된 기본변환의 순서를 역순으로 적용함으로써 간단히 메시지를 복호할 수 있는 장점이 있다. 또한 암호화 강도에 따라 암호화 함수의 개수를 조절할 수 있어 보다 효율적으로 적용할 수 있다. 하지만 이 구조에서 제안된 셀룰라 오토마타의 법칙은 3개의 이웃으로 구성하고 있고 제한된 선형 법칙만을 이용하고 있다. 따라서 셀룰라 오토마타를 구성하기 위해 적용된 선형법칙을 알 수 있다면 쉽게 블록사이즈에 대한 적용된 기본변환을 유추할 수 있다는 단점과 비교적 큰 사이즈의 메시지 블록에 적용하기에는 기본 변환을 찾기가 쉽지 않다는 단점이 있을 수 있다.

[9]에서 Srisuchinwong 등이 제안한 블록 암호 알고리즘은 전체적으로 DES와 유사한 구조를 따르고 있지만, 라운드 수는 12라운드, 적용된 메시지 블록의 사이즈는 16-비트이다. 이 구조에서 이용하고 있는 셀룰라 오토마타의 법칙은 출력 블록의 비선형성을 높이기 위해 비선형 법칙을 적용하고 있다. 제안된 구조는 12개의 라운드 키를 생성하기 위해서 Autonomous CA를 이용하고, 메시지 블록을 암호화하기 위해서 F-함수로써 사용된 구조는 Nonautonomous CA이다. 즉, 메시지를 암호화하기 위해 외부 입력으로써 라운드 키를 사용하고 있다. 또한 F-함수 부분의 Nonautonomous CA는 비선형 법칙을 이용하여 구성함으로써 암호학적으로 우수함을 보이고 있다. 하지만, 16비트 블록을 암호화하기 위해 적용된 비밀키가 96-비트가 필요함으로써 메시지 블록 크기에 비해 비밀키의 크기가 다소 크다 할 수 있고, 또한 연속적으로 메시지를 암호화하기 위해서는 라운드 키의 적용에 있어서 매우 정확하게 동기가 맞춰져야만 한다는 단점을 가지고 있다.

3. 새로운 블록 암호 알고리즘

제안된 블록 암호 알고리즘은 셀룰라 오토마타를 기반으로 한 128비트 Feistel 구조 블록 암호 알고리즘이다. 비밀키의 크기 역시 128비트이며 전체 알고리즘의 라운드 수는 16라운드이다. Feistel 구조의 특성을 이용함으로써 복호화 과정에서 고려해야하는 역함수를 고려하지 않아도 되는 장점과 하드웨어 구현 시 복호화를 위한 영역 오브헤드를 감소시킬 수 있는 장점을 얻기 위함이다. 또한 제안된 알고리즘은 고속 연산을 수행하기 위해 잠재적으로 속도 저하에 영향을 줄 수 있는 복잡한 연산을 피하고 bit-wise 연산과 라운드 키에 의존하는 rotate 연산만을 이용하였다.

3.1 1-라운드 알고리즘

1-라운드 암호화 과정은 평문 메시지를 128비트 평문 블록으로 나누어 알고리즘의 입력 값으로 사용한다. 라운드 연산을 수행하기 전 초기화키를 이용하여 아래와 같은 연산을 수행한다.

128비트 메시지 블록은 각각 32비트 서브 블록 P_i로 나누어져 라운드 키 K_j를 이용한 초기연산을 수행한다. 여기에서 사용되는 연산은 라운드 키와의 bit-wise XOR 연산이다. 이를 식으로 나타내면 아래와 같다.

$$B_i = P_i \oplus K_j \quad (i,\ j = 0, 1, 2, 3)$$

또한 마지막 라운드(16 라운드)를 마치고 암호문 출력을 위해 이와 같은 동일한 연산을 수행한다.

이를 각각 4개의 32비트 서브 블록 B_i의 초기 값으로 로드하고 첫 번째 라운드 연산을 수행한다. 라운드 연산은 4개의 32비트 라운드 키 K_{4r+j} $(j = 0, 1, 2, 3)$와 서브 블록 B_i $(i = 0, 1, 2, 3)$를 아래와 같은 과정을 통하여 암호화한다.

$$B_0' = LRot(F(B_0, K_{4r}), K_{4r+2}) \oplus B_1$$

$$B_1' = B_2$$

$$B_2' = LRot(F(B_2, K_{4r+1}), K_{4r+3}) \oplus B_3$$

$$B_3' = B_0$$

여기서 $LRot(B_i, K_j)$는 라운드 키 K_j의 최하위 비트 4비트 값에 의존한 B_i 값의 레프트 로테이터 연산을 의미하며, ⊕는 bit-wise XOR 연산을 의미하고, $F(B_i, K_j)$는 라운드 키 K_j를 이용한 라운드 함수를 서브 블록 B_i에 적용함을 의미한다. [그림 2]는 1-라운드 연산 구조를 나타낸다.

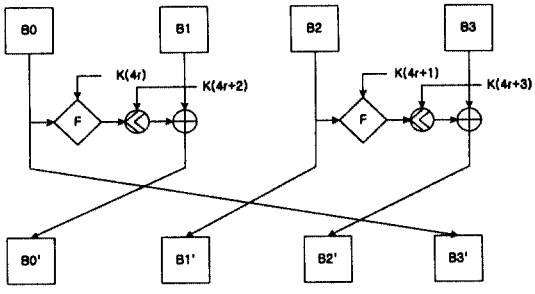


그림 2. 1-라운드 연산 블록도

3.2 라운드 함수 F

일반적으로 블록 암호 알고리즘은 라운드 함수 내에 있는 S-box가 비선형 특성을 가지도록 설계되어진다. 제안된 알고리즘은 라운드 함수 자체를 라운드 키에 의존한 비선형 셀룰라 오토마타의 갱신 법칙을 이용하여 구성함으로써 뛰어난 비선형성을 가질 수 있는 특징을 지닌다. 제안된 알고리즘의 라운드 함수 $F(B_i, K_j)$는 B_0, B_2의 32비트 상태 값을 셀룰라 오토마타의 현재 상태 값으로 간주하고 라운드 키 K_{4r+i} $(i = 0, 1)$를 상태 천이법칙으로 적용하는 1-차원 Null boundary 비선형 셀룰라 오토마타를 이용한다. 즉, 라운드 키의 비트 값에 의존하여 갱신 법칙을 서로 다르게 적용하게 된다. 여기서 적용된 셀 갱신 법칙은 비선형 특성을 나타내는 법칙 78과 법칙 92를 사용하였다. 적용된 두 갱신법칙은 비선형 특성을 나타낼 뿐 아니라 출력 값이 0과 1을 고르게 나타내는 균형함수(Balanced function)이다. 아래 식은 이들의 표현식을 나타낸다.

$$Rule\ 78 = (\overline{s_{i-1}} \cdot s_{i+1}) + (s_i \cdot \overline{s_{i+1}})$$

$$Rule\ 92 = (\overline{s_{i-1}} \cdot s_i) + (s_{i-1} \cdot \overline{s_{i+1}})$$

여기서 s_i는 i번째 셀의 상태 값을 의미한다. ·는 AND 연산을 +는 OR 연산을 각각 의미한다. 즉, 위의 두 법칙은 AND, OR, NOT 연산을 함께 사용하는 셀룰라 오토마타의 3-이웃 비선형 법칙이다.

3.3 키 생성 알고리즘

각 라운드에 적용될 라운드 키는 4개이다. 또한 초기 상태에서 적용된 연산과 최종 라운드 이후에 적용된 연산을 위하여 각각 4개의 키가 필요하다. 따라서 전체 라운드 키의 개수는 전체 72개가 요구된다. 이는 128차 원시다항식을 특성다항식으로 갖는 1차원 셀룰라 오토마타를 이용하여 구성한 라운드 키 생성 알고리즘을 통해서 128비트 비밀키로부터 얻을 수 있다. 다음 식은 특성다항식과 각 셀에 적용된 법칙을 나타낸다.

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

$$d = (4888\ 2FBD\ 6703\ 1A7A\ 7A79\ C0E6\ BDF4\ 1112)$$

여기서, $p(x)$는 최대 주기를 갖는 128차 기약다항식이며, d는 셀에 적용된 갱신법칙을 16진수로 표현한 것이다. 즉, '4'는 2진수 '0100'과 동일한 표현이며 여기서 '0'일 경우 법칙 90, '1'일 경우 법칙 150을 해당 셀에 적용한다.

따라서, 각 라운드마다 128셀 1차원 LHCA(Linear Hybrid CA)의 갱신 값을 이용하여 32비트 라운드키, K_j $(j = 0, 1, 2, \cdots, 70, 71)$를 아래와 같은 방법으로 생성한다.

(1) 128비트 비밀키를 셀룰라 오토마타의 초기 상태 값으로 로드한다.

(2) 갱신법칙 d를 이용하여 셀룰라 오토마타의 상태 값을 갱신한다.

(3) 4개의 32비트 블록으로 나누고 다음과 같이 각 블록의 상태 값을 갱신한다.

$$K'_{4r} = K_{4r} \oplus K_{4r+1}$$

$$K'_{4r+1} = K_{4r+1} \oplus K_{4r+2}$$

$$K'_{4r+2} = K_{4r+2} \oplus K_{4r+3}$$

$$K'_{4r+3} = K_{4r+3} \oplus K_{4r}$$

(4) 생성된 32비트 상태 값의 LSB 4비트의 값을 이용하여 라이트 로테이터를 수행한 후 다음 라운드의 라운드 키로 사용한다.

(5) 결과를 셀룰라 오토마타의 초기 상태 값으로 로드하고 위 과정을 r+2회 반복 수행하여 모든 라운드 키를 생성한다.

[그림 3]는 제안된 블록 암호 알고리즘의 전체 블록도이다.

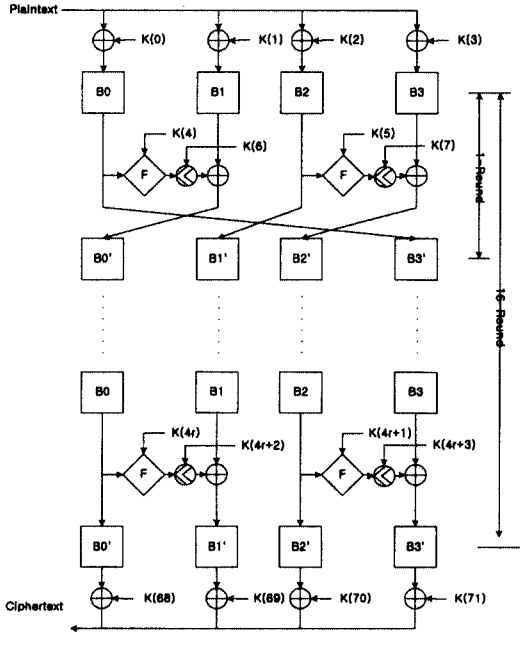


그림 3. 알고리즘의 전체 블록도

4. 알고리즘의 평가

이 장에서는 제안된 블록 암호 알고리즘의 성능과 안전성에 대하여 분석한다. 안전성 평가를 위해 제안된 알고리즘의 축소 버전에 대한 차분 분석법(Differential Cryptanalysis)과 FIPS PUB 140-2[14]에서 제시하고 있는 랜덤 수열에 대한 통계 검정을 실시한다. 또한 평문과 키에 대한 출력의 쇄도효과(Avalanche Effect)를 수행하고, 표준 블록 암호 알고리즘인 DES, Rijndael과의 수행 속도를 비교하여 결과를 제시한다.

4.1 성능 분석

이 절에서는 표준 블록 암호 알고리즘으로 잘 알려진 DES, Rijndael 블록 암호 알고리즘과의 수행속도와 쇄도효과 검정을 수행한다.

4.1.1 수행속도 비교

제안 알고리즘과 표준 블록 암호 알고리즘과의 수행속도 비교를 위해 100,000회의 암호화와 키 생성 과정을 수행하여 비교 결과를 [표 2]에 제시하였다. 제안 알고리즘은 DES에 비해 출력의 크기가 2배이므로 DES에 대하여 상당히 빠른 속도를 나타내지만 차세대 표준 블록 암호로 선정된 Rijndael에 대하여는 상당히 느리다. 이는 Rijndael 알고리즘이 AES 선정을 위해 코드가 최적화되었다고 하더라도 추후 개선되어야 할 부분이다. 하지만 하드웨어 구현에서는 셀룰라 오토마타의 셀 갱신이 한 번의 동작으로 모든 셀을 갱신할 수 있기 때문에 보다 우수한 결과를 보일 것으로 예상된다.

표 2. 수행속도 비교

구분	제안 알고리즘	DES	Rijndael
암호화	166	333	11
키 생성	224	122	23

4.1.2 쇄도효과 검정

제안 알고리즘과 표준 블록 암호 알고리즘인 DES, Rijndael 블록 암호 알고리즘과의 쇄도효과를 비교하였다. 비교를 위해 동일한 수준의 평문과 비밀키 크기를 사용하였다. 아래 [표 3]은 그 결과를 보여준다. 모든 알고리즘이 우수한 쇄도효과를 나타내고 있음을 알 수 있다.

4.2 안전성 분석

이 절에서는 제안 알고리즘의 축소된 버전에 대한

표 3. 쇄도효과 검정 비교

구분	제안 알고리즘	DES	Rijndael
평문	64	31	63
비밀키	63	32	64

차분 분석과 출력 비트열에 대한 FIPS PUB 140-2에서 권고하는 통계적 검증을 수행한다.

4.2.1 축소된 버전에 대한 차분 분석 적용 결과

차분 해독법(DC : Differential Cryptanalysis)이 1990년 Biham과 Shamir에 의해서 처음 소개된 이후 안전하다고 알려져 있던 블록 암호 알고리즘들이 실제로 이 공격법에 대하여 취약함이 드러나고 있다. 따라서, 반복라운드 구조를 갖는 블록암호 알고리즘을 설계할 경우 반드시 차분 해독법에 대하여 고려해야 한다. 본 절에서는 제안된 알고리즘의 차분 해독법에 대하여 살펴본다.

제안된 알고리즘은 라운드 함수 내부에 S-box를 두지 않고, F-함수 자체가 셀룰라 오토마타의 비선형 천이 법칙을 이용한 천이특성을 사용하고 있기 때문에 S-box에 대한 차분을 다룰 수는 없다. 또한 F-함수의 입력이 32비트이기 때문에 모든 차분에 대하여 분석하는 것은 계산적으로 불가능하다. 그리고, F-함수의 적용은 라운드 함수에 적용되는 라운드 키에 의존하고 있기 때문에 라운드 함수 F에 대한 전체적인 분석을 다루기는 매우 힘들다. 따라서, 여기서는 차분 분석을 위해 F-함수를 4비트 입력과 4비트 출력을 갖는 함수로 축소하여 분석하고자 한다. F-함수가 4비트 입출력을 가짐으로써 이론적으로 가능한 입력 차분과 출력 차분은 각각 16가지가 존재할 수 있다.

key : 0(0000)

Results

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	:1
1	0	8	0	8	0	0	0	0	0	0	0	0	0	0	0	0	:2
2	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	0	:4
3	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	:4
4	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	:8
5	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	:8
6	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	:4
7	0	4	0	0	0	0	0	4	0	0	0	4	0	4	0	0	:4
8	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	:4
9	0	4	0	0	0	0	0	4	0	0	0	4	0	4	0	0	:4
A	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	:8
B	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	:8
C	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	:4
D	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	:4
E	0	0	0	0	0	0	8	0	0	0	8	0	0	0	0	0	:2
F	0	0	0	0	0	4	0	4	0	4	0	4	0	0	0	0	:4
total																	:73

이를 4비트의 가능한 모든 라운드 키를 적용하여 입력 차분과 출력 차분에 대한 분포 특성을 구성하였다. 위의 값은 라운드 키를 k=0(0000)로 주었을 때 F-함수의 입력 차분과 출력 차분의 분포를 보여주고 있다. 여기서, 각 행은 입력 차분을 나타내며, 각 열은 출력 차분을 의미한다. 그리고, 각각의 값은 입력 차분과 출력 차분에 대한 카운트를 의미한다.

전체 256(16×16)개 경우 중에서 73개의 경우만이 존재함을 알 수 있고 이는 라운드 키에 따라 다소 차이가 있지만 가능한 라운드 키 16가지를 모두 적용하였을 경우 평균적으로 72.8을 나타낸다. 그리고 이는 전체 테이블의 28.4%에 해당한다. DES의 S-box(약 80%)와 비교하면 많은 차이가 나지만 DES의 경우 S-box의 입력이 6비트임을 감안하면 결코 적은 수치가 아니다.

가장 이상적인 입출력 차분의 분포는 입력 차분에 대한 출력 차분이 각각 2개의 쌍을 갖는 8개의 가능한 출력 차분으로 나타나는 것이다. 암호 알고리즘의 설계 시 이러한 이상적인 분포를 가지도록 암호 알고리즘을 설계하는 것은 매우 어려운 문제이다.

축소된 F-함수의 경우 전체적으로 이상적인 결과를 보이지는 않지만 4개 또는 8개의 순서쌍을 가지는 출력 차분의 경우가 다수(13회) 나타남으로써 균일한 차분 분포를 나타낼 수 있을 것으로 보인다. 축소된 F-함수의 분석이 전체 F-함수에서도 동일한 효과로 나타날 것으로 생각되지는 않지만 축소된 F-함수의 차분 분포가 다소 고른 분포를 나타낸다는 것은 차분 공격이 성공할 확률을 매우 낮출 수 있을 것으로 기대되어 실제 F-함수에 있어서도 차분 공격이 가능한 characteristics을 찾을 확률이 매우 낮다는

것을 예상할 수 있다.

4.2.2 출력 수열에 대한 통계적 검정

FIPS PUB 140-2는 FIPS PUB 140-1을 수정 보완하여 2001년 6월에 공포된 표준안으로써 암호학적 모듈이 가져야 할 통계적 검정의 기준을 제시하고 있다. [표 4]는 FIPS PUB 140-2의 기준과 제안 알고리즘의 검정 값을 보여준다.

표 4. FIPS PUB 140-2 통계 검정 결과

검정		FIPS PUB 140-2	제안알고리즘
Monobit Test		9,725~10,275	10,047
Poker Test		2.16<x<46.17	28.0
Runs Test	1	2343~2657	2511(2556)
	2	1135~1365	1278(1195)
	3	542~708	628(663)
	4	251~373	327(302)
	5	111~201	160(163)
	6+	111~201	129(154)
Long Run Test		0	0

(1) The Monobit Test

이 검정은 20,000비트 출력 수열에 대한 '1'의 개수를 카운트하는 것이다. 검정결과가 허용오차 2.75% 이하(9,725~10,275개)가 되어야 검정을 통과한다.

(2) The Poker Test

이 검정은 20,000비트 수열을 4비트씩 나누어 가능한 패턴들이 균일하게 분포하는 것을 검정한다. 이 검정은 아래 식에 의해 그 결과가 2.16~46.17 일 경우 검정을 통과한다. 여기서 i는 가능한 4비트 패턴이다.

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

(3) The Runs Test

이 검정은 20,000비트 수열에 대하여 0과 1의 연속인 런의 개수가 [표 2]에서 제시된 값에 대하여 만족하여야 검정을 통과한다. 즉, 12가지의 모든 카운트가 모두 만족해야만 한다. 여기서 6+의 의미는 런의 길이가 6이상인 모든 런의 개수를 의미한다.

(4) The Long Run Test

이 검정은 20,000비트 검정 수열에 대하여 런의 길이가 26이상인 런이 존재하지 않아야만 통과할 수 있다.

이외 자기상관검정의 수행 결과 또한 d=8, 5% 유의수준(3.842)에 대하여 검정값 0.253으로 만족한 결과를 보여주었다.

5. 결 론

본 논문에서는 셀룰라 오토마타를 기반으로 하는 새로운 블록 암호 알고리즘을 제안하였다. 셀룰라 오토마타의 병렬성과 랜덤성에 기인하여 고속 동작을 위한 새로운 접근이 가능할 것으로 예상되고 비선형 셀 갱신 법칙을 사용함으로써 보다 우수한 랜덤성을 가질 수 있음을 보였다. 또한 알고리즘 구조 측면에서 제안된 블록 암호 알고리즘은 매우 간단한 연산을 이용하였고 알고리즘 구조상 단지 3-이웃에 대한 의존도만을 가짐으로써 하드웨어 구현에서도 유리한 이점을 가지면서 셀룰라 오토마타의 복잡한 천이 특성을 이용한 간단한 알고리즘으로 설계될 수 있음을 보였다. 알고리즘의 안전성과 성능 평가를 위해 주요한 블록 암호 안전성 평가요소인 차분 공격법을 축소된 버전에 적용하였으며 키와 평문에 대한 암호문의 쇄도효과 결과를 기술하였다. 또한 출력 수열의 랜덤성 평가를 위한 통계적 검정을 수행하였으며 기존 표준 블록 암호 알고리즘과의 수행속도 비교를 통해 성능을 평가하였다.

차후 연구로써 제안 알고리즘의 안전성 향상을 위한 다차원 셀 구조에의 응용 및 안전성 평가를 위한 선형 분석법의 적용, 하드웨어 구현을 통한 실제 구현 속도의 측정 등이 보완되어야 할 것으로 평가된다. 본 논문은 보다 고속성이 요구되는 다양한 암호 알고리즘의 응용을 위한 새로운 암호 프리미티브(Cryptographic primitive)로써 역할을 수행할 수 있을 것으로 기대된다.

참 고 문 헌

[1] S. Wolfram, *Cellular Automata and Complexity*, Addison Wesely Publishing Company, 1994.

[2] S. Wolfram, "Cryptography with Cellular Automata", *in Advances in Cryptology: Crypto '85 Proceedings, Lecture Notes and Computer Science*, vol.218, pp.429-432 (Springer-Verlag, 1986)

[3] A.K. Das, A. Ganguly, A. Dasgupta, S. Bhawmik, P.P. Chaudhuri, "Efficient characterization of cellular automata", *IEE Proceeding E, Computer and Digital Techniques*, vol.137, no.1, pp.81-87, Jan. 1990.

[4] K. Cattell, M. Serra, "Analysis of One-Dimensional Multiple-Value Linear Cellular Automata", *IEEE Proceedings of the 20th International Symposium on Multiple Valued Logic*, pp.402-409, 1990.

[5] P.P. Chaudhuri, A.R. Chowdhury, S. Nandi, S. Chattopadhyay, *Additive Cellular Automata: Theory and Applications, Volume 1*, IEEE Computer Society Press, 1997.

[6] S. Bhattacharjee, S. Sinha, C. Chattopadhyay, P.P. Chaudhuri, "Cellular automata based scheme for solution of Boolean equations", *IEE Proceedings E, Computer and Digital Techniques*, vol.143, no.3, 1996.

[7] M. Mihaljevic, H. Imai, "A Family of Fast Keystream Generations based on Programmable Linear Cellular Automata over GF(q) and Time-Variant Table", *IEICE Transactions on Fundamentals*, vol.E82-A, no.1, pp.32-39, 1999.

[8] M. Mihaljevic, Y. Zhang, H. Imai, "A Fast and Secure Stream Cipher based on Cellular Automata over GF(q)", *IEEE Global Telecommunications Conference, GLOBECOM '98*, vol.6, pp.3250-3255, 1998.

[9] B. Srisuchinwong, T.A. York, Ph. Taslides, "A Symmetric Cipher using autonomous and non-autonomous cellular automata", *IEEE Global Telecommunications Conference, GLOBECOM '95*, pp.1172-1177, 1995.

[10] K. Cattell, J. Muzio, "Analysis of One-Dimensional Linear Hybrid Cellular Automata over GF(q)", *IEEE Transactions on Computers*, vol.45, no.7, pp.782-792, 1996.

[11] K. Cattell, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol.15, no.3, pp.325-335, 1996.

[12] J. Rajski, G. Mrugalski, J. Tyszer, "Comparative Study of CA-based PRPGs and LFSRs with Phase Shifters", *IEEE Proceedings of 17th VLSI Test Symposium*, pp.236-245.

[13] P.S. Cardoso, M. Strum, J.R. Amazonas W.J. Chau, "Comparison between Quasi-Uniform Linear Cellular Automata and Linear Feedback Shift Registers as Test Pattern Generators for Built-In Self Test Applications", *IEEE Proceedings of 12th Symposium on Integrated Circuits and Systems Design*, pp.198-201, 1999.

[14] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

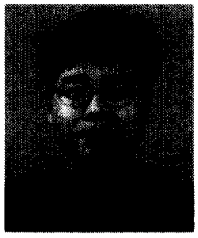
이 준 석

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 석사
2000년 2월 부경대학교 대학원 전자계산학과 박사수료
1996년 3월~1999년 8월 제주관광대학 사무자동화과 전임강사
2000년 3월~현재 대덕대학 컴퓨터정보통신계열 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