하이브리드 가산 셀룰라 오토마타의 분석

조성진* · 최언숙** · 김한두*** · 황윤희* · 김진경* · 김봉수*
*부경대학교 · **동명대학교 · ***인제대학교

Analysis of Hybrid Additive Cellular Automata

Sung-Jin Cho* · Han-Doo Kim** · Un-Sook Choi***
· Yoon-Hee Hwang* · Jin-Gyoung Kim* · Bong-Soo Kim*
*Pukyong National Univ. · **Tongmyong Univ. · ***Inje Univ.
E-mail : sjcho@pknu.ac.kr

요 약

Anghelescu 등은 전이규칙 51, 60 (또는 102) 만을 사용하는 주기가 8인 8셀 하이브리드 가산 셀룰라 오토마타를 이용하여 블록 암호시스템을 제안하였다. 그러나 이 암호시스템에 사용되는 셀룰라 오토마타중에서 암호시스템의 요구사항인 모든 상태들이 같은 길이의 사이클로 쪼개져야 한다는 요구조건을 만족시키지 못하는 셀룰라 오토마타가 존재한다. 본 논문에서는 이러한 문제점을 분석하고 개선된 방법을 제안한다.

ABSTRACT

Anghelescu et al. proposed a block cryptosystem based on 8-cell hybrid additive cellular automata with cycle length 8 using state transition rules 51, 60 (or 102). All states must divided into the same cycles in the diagram of the cellular automata. But there exist cellular automata which don't satisfy this condition in Anghelescu et al.'s cryptosystem. In this paper we analyze hybrid additive cellular automata and propose an improved method.

키워드

Hybrid Additive Cellular Automata, Group Cellular Automata, Linear Cellular Automata

Ⅰ. 서 론

암호의 종류에는 암호화 키와 복호화 키가 같은 대칭키 암호와 암호화 키와 복호화 키가 다른 비대칭키 암호가 있다. 대칭키 암호에는 평문을 일정한 단위로 나누어서 각 블록마다 암호화 과정을 수행하는 블록 암호와 평문과 같은 키스트림을 생성하여 평문과 키를 비트단위로 합하여 암호문을 얻는 스트림 암호가 있다. 이 중에서 블록암호는 스트림 암호에 비해 기밀성이 요구되는 분야뿐만 아니라 해쉬함수 또는 인증 방식에도 응용될 수 있는 등 응용 분야가 다양하며 알고리즘의 종류도 매우 다양하다.

†본 연구는 한국과학재단 목적기초연구지원사업(R01-2006-000-10260-0)에 의해 수행되었습니다.

셀룰라 오토마타 (이하 CA)는 셀의 상태가 자기 자신 및 인접한 셀의 상태의 국소적인 상호작용에 의하여 동시에 갱신되는 시스템으로 간단하고 규칙적이며 작은 단위로 확장 연결할 수 있는 구조이기 때문에 하드웨어 구현에 적합하다.

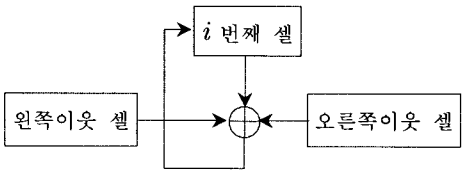
이러한 CA는 테스트 패턴 생성, 의사난수 생성기, 오류정정부호기, 암호, 신호분석 등 많은 분야에 응용되었다. CA가 LFSR보다 난수성이 우수하지만 LFSR에 비하여 분석이 어려우며 CA를 합성하는 방법이 어렵다. 이러한 문제를 해결하기 위하여 여러 해 동안 많은 연구자들이 다항식으로부터 CA를 합성하는 방법에 대한 연구를 수행하였다[1~4].

무선 통신의 출현과 PDA, 스마트카드와 같은 휴대용 장치의 발전으로 인해 이에 대한 보안과 개인 정보보호에 대한 필요성이 대두되면서 암호

화와 복호화를 공유할 수 있는 하드웨어 구현이 주목받고 있다. CA는 전용 하드웨어를 사용하지 않고 실행 가능하도록 프로그램화 될 수 있어서 여기에 이용할 수 있다. Mukhopadhyay 등[5]은 전이규칙 102에서 셀 상태가 모두 1인 여원벡터에 의해 유도된 여원 uniform 그룹 CA를 분석하고, 이러한 성질을 이용하여 키 공유 프로토콜에 적용하였다. Cho 등[6]은 전이규칙 204와 60 (또는 102)를 갖는 CA의 특성다항식과 최소다항식을 분석하여 여원벡터에 대응하여 사이클 구조를 분석하여 Mukhopadhyay[5]의 연구결과를 확장하였다. Anghelescu 등[7]은 전이규칙 51, 60 (또는 102)을 가지고 사이클 길이가 일정한 8셀 CA를 이용하여 짧은 주기의 블록 암호화와 복호화가 동시에 되는 키를 만드는 방법을 설계하였으나, 이때 사용된 CA중에서 사이클의 길이가 일정하지 않는 CA가 존재한다. 본 논문에서는 이러한 문제점을 갖는 CA에 대하여 분석하고 이를 보안하는 CA를 제안하고자 한다.

II. 배경지식 및 관련연구

CA란 이산 시간의 동적 시스템으로 셀이라는 기본 단위 메모리의 배열로 이루어진다. 이 시스템에서 셀의 다음 상태는 어떤 규칙에 따라 정해진다. 즉, 각 셀들은 자기 자신과 이웃 셀의 함수값에 의해 다음 상태가 결정되어 동시에 갱신된다. CA는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 알맞다. Wolfram은 모든 셀이 선형으로 배열되어 있으며 각 셀이 0과 1, 두 상태를 가지고 그림 1과 같이 다음 상태가 자기 자신과 인접한 두 이웃에 의하여 갱신되는 3-이웃 (3-neighbourhood)CA를 제안하였다.



<그림 1> 3-이웃 선형 CA의 셀 구조

세 개의 이웃을 가지는 CA에 대한 다음 상태 전이 함수는 다음과 같이 나타낸다.

$$q_i(t+1) = f\,(q_{i-1}(t), q_i(t), q_{i+1}(t))$$

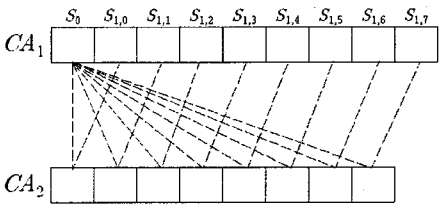
여기서 $q_i(t)$는 시간 t에서 i번째 셀의 상태를 나타내고, f는 결합논리를 가지는 국소전이 함수이다. f는 3개의 변수를 가지는 Boolean 함수로 2^{2^3}개가 있으며 이것을 CA의 전이규칙이라고 한다. 표 1에서와 같이 본 논문에서 사용되는 선형 CA 전이규칙은 60, 102, 204이고 여원 CA 전이규칙은 195, 153, 51를 사용한다.

[표 1] 전이규칙

전이규칙	전이함수
60	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
204	$q_i(t+1) = q_i(t)$
195	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t)}$
153	$q_i(t+1) = \overline{q_i(t) \oplus q_{i+1}(t)}$
51	$q_i(t+1) = \overline{q_i(t)}$

Anghelescu 등은 두 개의 CA의 조합을 사용해서 암호시스템을 실현화 하였다. 그들은 키스트림 생성기로써 의사난수열생성기인 전이규칙 90과 150을 갖는 CA를 사용하였다. 이 CA는 블록암호에서 실시간 키로 제공되어 사용되어진다. 그들의 블록 알고리즘은 전이규칙 51과 60 (또는 102)를 갖는 CA를 사용하여 구성되었다[7].

최대주기를 가지는 선형 CA를 이용하여 일정한 주기를 가지는 여원 CA를 만드는 방법으로 그림 2와 같이 9셀 CA의 첫 번째 셀의 출력은 S_0를 생성하는데 사용되고 나머지 8셀의 출력은 S_1을 생성하는데 사용 되어 두 번째 8셀 CA의 전이규칙이 생성된다. 이때 S_{1j}는 CA_2의 j번째 셀에 대응하는 S_1이다($0 \le j \le 7$).



<그림 2> 블록암호 시스템의 CA 구조

표 2는 S_0, S_1에 의해 생성되는 CA_2의 각 셀의 전이규칙이다. 표 2에서 S_0가 0이면 전이규칙이 모두 51로써 이러한 CA의 상태전이 그래프의 사이클의 길이는 2이다.

[표 2] 생성되는 CA의 전이규칙

S_0	$S_{1,j}$	생성되는 전이규칙
0	0	51
0	1	51
1	0	60
1	1	102

표 3에서 전이규칙이 51과 60 (또는 102)인 8셀 CA의 모든 종류는 512개 이고, 이 중에서 156개 만이 주기가 8인 최대 동일주기를 갖는 CA가 된다.

[표 3] 생성되는 CA의 사이클 길이와 개수

전이규칙	사이클				
	길이	2	4	8	16
51,60(102)	개수	7	327	156	2

III. Analysis of HGCA

<정리 1> $\mathbb{C}$를 전이규칙 204 와 60 (또는 102)을 갖는 n-셀 선형 하이브리드 그룹 CA라 하면 $\mathbb{C}$의 상태전이행렬 T의 특성다항식은

$$c(x)=(x+1)^n$$

이다.

정리 1에 의하여 전이규칙 204 와 60 (또는 102)를 갖는 선형 하이브리드 그룹 CA는 다음에 제시된 룰 벡터(Rule Vector) $RV_i(i=1,2)$의 조합으로만 이루어진다.

$$RV_1 = < 60, \cdots, 60, 204, 60, \cdots, 60 >$$

$$RV_2 = < 102, \cdots, 102, 204, 102, \cdots, 102 >$$

<정리 2> $\mathbb{C}$를 n-셀 선형 하이브리드 그룹 CA라 하고, $m(x)$를 $\mathbb{C}$의 상태전이행렬 T의 최소다항식이라 하자. 다음 각각의 $RV_i(i=1,2)$에 대하여 $m(x)=(x+1)^p$이다.

(1) $RV_1 = < \overbrace{60,\cdots,60}^{a개}, 204, \overbrace{60,\cdots,60}^{b개} >$
$p=\max\{a,b+1\}$

(2) $RV_2 = < \overbrace{102,\cdots,102}^{a개}, 204, \overbrace{102,\cdots,102}^{b개} >$
$p=\max\{a+1,b\}$

표 4는 8셀 CA에서 사이클의 구조가 동일한 CA중에서 일부이다. 여기서 $m(x)$를 $\mathbb{C}$의 상태전이행렬 T의 최소다항식이라 하면 $m(x)=(x+1)^p$이고, 여기서 최소다항식의 p을 결정하는 것은 연이은 전이규칙 60에서 가장 긴 것 중에서 그 위치가 앞에서부터 연이어 있을 경우는 그 수만큼이 p가 되고 중간부터 연이어 있을 경우는 그 수에 +1한 수만큼이 p가 되어 최소다항식이 결정된다. (전이규칙이 102일 때도 유사하다.)

[표 4] 사이클의 구조가 동일한 CA중 일부

CA룰	사이클 길이				특성다항식	최소다항식
	2	4	8	16		
00001001		64			$(x-1)^8$	$(x-1)^4$
00010000			32			$(x-1)^5$
00011001		64				$(x-1)^3$
00100000			32			$(x-1)^6$
00111001		64				$(x-1)^3$
01000000			32			$(x-1)^7$
01111111	128					$(x-1)$
10000000				16		$(x-1)^8$
10000001			32			$(x-1)^7$

* 0은 전이규칙 60을 말하고 1은 전이규칙 204을 말한다.

<정리 3> $\mathbb{C}$를 $RV_i(i=1,2)$를 갖는 n-셀 선형 하이브리드 그룹 CA라 하고, T를 $\mathbb{C}$의 상태전이행렬로 최소다항식이 $m(x)=(x+1)^p$라 하자. $\mathbb{C}'$를 다음과 같이 각각의 여원벡터 $F_i(i=1,2)$에 대응하여 $\mathbb{C}$에서 유도된 여원 하이브리드 그룹 CA라 하자.

(1) RV_1:

$$F_1=\begin{cases}(1,f_2,\cdots,f_n)^t, & a\geq b+1\\ (f_1,\cdots,f_a,1,f_{a+2},\cdots,f_n)^t, & a<b+1\end{cases}$$

(2) RV_2:

$$F_2=\begin{cases}(f_1,\cdots,f_a,1,f_{a+2},\cdots,f_n)^t, & a\geq b+1\\ (f_1,\cdots,f_n,1)^t, & a<b+1\end{cases}$$

이때 $\mathrm{ord}(T)=2^d$이라면 다음이 성립한다.

(1) $\mathbb{C}'$에 있는 모든 사이클의 길이는 같다.

(2) $\mathrm{ord}(\overline{T})=\begin{cases}2^d, & 2^{d-1}<p<2d,\\ 2^{d+1}, & p=2^d.\end{cases}$

8셀에서 전이규칙 60이 연이어 5개 이상 나올 경우 사이클의 길이가 같은 주기로 나누어지지 않는다. 이때 첫 셀에 여원을 넣은 모든 여원벡터에 대하여 사이클의 길이가 8로 동일한 같은 주기로 나누어진다.

표 5는 8셀 CA중에서 사이클의 구조가 동일하지 않는 CA만을 정리한 것이다. 여기서

$$F=(1,a_1,a_2,a_3,a_4,a_5,a_6,a_7),\ (a_i=0,1)$$

로 두면 최대동일주기를 갖는 CA가 된다. 이때 사이클의 구조는 32(8)이 된다. (전이규칙이 102일 때도 유사하다.)

[표 5] 사이클의 구조가 동일하지 않는 CA

CA룰	사이클 길이			특성다항식	최소다항식
	2	4	8		
00000000	1	3	30	$(x-1)^8$	$(x-1)^8$
00000001	4	6	28		$(x-1)^7$
00000010		16	24		$(x-1)^6$
00000011	8	12	24		$(x-1)^6$
00000100		32	16		$(x-1)^5$
00000101		32	16		$(x-1)^5$
00000110		32	16		$(x-1)^5$
00000111	16	24	16		$(x-1)^5$
00011111	64	32			$(x-1)^3$

* 0은 전이규칙 60을 말하고 1은 전이규칙 51을 말한다.

<예제 1>

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

전이규칙이 <60,60,60,60,60,204,204,204>인 위 행렬의 특성다항식은 x^8+1이고 최소다항식은 $(x+1)^5$으로써 사이클의 구조는 16(2), 24(4), 16(8)인데, 정리 3에 의해서

$$F=(1, a_1, a_2, a_3, a_4, a_5, a_6, a_7)\ ,\ (a_i=0,1)$$

로 두면 최대동일주기를 갖는 CA가 된다. 이때 사이클의 구조는 32(8)이 된다.

<예제 2>

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

전이규칙이 <102,102,102,102,102,204,204,204>인 위 행렬의 특성다항식은 x^8+1이고 최소다항식은 $(x+1)^6$으로써 사이클의 구조는 16(2), 24(4), 16(8)인데, 정리 3에 의해서

$$F=(a_1, a_2, a_3, a_4, a_5, 1, a_6, a_7)\ ,\ (a_i=0,1)$$

로 두면 최대동일주기를 갖는 CA가 된다. 이때 사이클의 구조는 32(8)이 된다.

Ⅳ. 결 론

Anghelescu 등은 전이규칙 51, 60 (또는 102)만을 사용하는 주기가 8인 8셀 하이브리드 가산 CA를 이용하여 블록 암호시스템을 제안하였다. 그러나 이 암호시스템에 사용되는 CA중에서 암호시스템의 요구사항인 모든 상태들이 같은 길이의 사이클로 쪼개져야 한다는 요구조건을 만족시키지 못하는 CA가 존재한다. 본 논문에서는 이러한 문제점을 분석하고 개선된 방법을 제안하였다.

참고문헌

[1] M. Serra, T. Slater, "A Lanczos Algorithm in a Finite Field and its Application," J. Combinatorial Math. and Combinatorial Computing, Vol. 17, pp. 11-32, 1990.

[2] K. Cattell and J. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol. 15, pp. 325-335, 1996.

[3] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim and S.H. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol. 26(9), pp. 1720-1724, 2007.

[4] S.J. Cho, U.S. Choi, Y.H. Hwang and H.D. Kim "Analysis of hybrid group cellular automata," ACRI 2006, LNCS, 4173, pp. 222-231, 2006.

[5] D.Mukhopadhyay and D.R. Chowdhury, "Characterization of a class of complemented group cellular automata," LNCS, 3305, pp. 775-784, 2004.

[6] S.J. Cho, U.S. Choi, H.D. Kim and Y.H. Hwang "Analysis of complemented CA derived from linear hybrid group CA," Computers & Mathematics with Applications, Vol. 53(1), pp. 54-63, 2007.

[7] A. Petre, I. Silviu, S. Emil, "Block Encryption Using Hybrid Additive Cellular Automata," Hybrid Intelligent Systems, 2007. HIS 2007. 7th International Conference on 17-19 Sept, pp. 132-137, 2007.