전이규칙 195,153,51을 갖는 Uniform/Hybrid 여원 그룹 셀룰라 오토마타의 특성화

황윤희* · 조성진* · 최언숙** · 김석태*

*부경대학교

**영산대학교

Characterization of Uniform/Hybrid Complemented Group Cellular Automata with Rules 195/153/51

Yoon-Hee Hwang* · Sung-Jin Cho* · Un-Sook Choi** · Seok-Tae Kim*

*Pukyong National University

**Youngsan University

E-mail : yhhwang@mail1.pknu.ac.kr

요 약

오늘날 무선 통신의 출현과 PDA, 스마트 카드와 같은 휴대용 장치의 등장으로 휴대용 장치에 보안과 개인 정보 보호에 대한 필요성이 대두되면서 여기에 암호학의 적용은 주요 관심사가 되고 있다. 특히, 암·복호화를 공유할 수 있는 하드웨어 구현이 주목을 받고 있다. LFSR의 대안으로 제안된 셀룰라 오토마타(Cellular Automata, 이하 CA)는 전용의 하드웨어를 사용하지 않고 실행 가능 하도록 프로그램화 될 수 있다. 그러나 이러한 CA는 일반화와 분석이 어렵다는 단점이 있다. 본 논문에서는 모든 상태의 주기가 동일하고 최대로 분리되는 전이규칙 195,153,51을 갖는 uniform/hybrid 여원 그룹 CA를 분석하여 특성화한다. 이는 암호학에서 키 공유 프로토콜에 이용될 수 있다.

ABSTRACT

Recently, the advent of wireless communication and other handheld devices like Personal Digital Assistants and smart cards have made in implementation of cryptosystems a major issue. One important aspect of modern day ciphers is the scope for hardware sharing between the encryption and decryption algorithm. The cellular Automata which have been proposed as an alternative to linear feedback shift registers(LFSRs) can be programmed to perform the operations without using any dedicated hardware. But to generalize and analyze CA is not easy. In this paper, we characterizes uniform/hybird complemented group CA with rules 195/153/51 that divide the entire state space into smaller spaces of maximal equal lengths. This properties can be useful in constructing key agreement algorithm.

Ⅰ. 서 론

셀룰라 오토마타(Cellular Automat, 이하 CA)는 J. Von Neumann에 의하여 스스로 조직화하고 재생산이 가능한 모델로 소개되었다[1]. 이후 CA는 Wolfram에 의해 셀이라 불리는 메모리 배열로 소개되었고, 셀의 상태가 자신을 포함한 인접 이웃 셀 상태의 국소적인 상호작용에 의해 동시에 갱신되는 시스템으로 제안하였다[2]. CA는 간단하고 규칙적이며 작은 단위로 확장 연결이 가능하여 VLSI 하드웨어 구현이 용이하다. 이러한 CA는 LFSR의 대안으로 제안되었으며, test pattern generation, 의사 난수열 생성기, 오류정정부호, 신호분석기, 암호 등 많은 분야에 응용되고 있다[3-9]. 이러한 CA는 여러 가지 장점에도 불구하고 LFSR과 달리 일반화와 분석이 어렵다.

* 본 연구는 한국과학재단 목적기초연구지원사업 (R01-2003-000-10663-0)에 의해 수행되었습니다.

Mukhopadhyay 등은 전이규칙이 53인 uniform 여원 그룹 CA의 상태 전이 그래프에서 모든 상태의 주기가 동일하고 최대로 분리되는 성질을 분석하여 이를 키 공유 알고리즘에 이용하였다[10].

본 논문에서는 이러한 키 공유 알고리즘을 구성하는데 유용한 성질을 가지는 특별한 전이규칙들과 각각에 대응하는 여원벡터를 특성화한다.

본 논문의 구성은 다음과 같다. 2장에서는 전이규칙이 60, 102이거나 204인 uniform/hybrid 그룹 CA의 구조에 대해 분석하고, 3장에서는 이러한 그룹 CA에서 키 공유 알고리즘에 유용한 성질을 가지게 하는 여원벡터에 의해 유도된 195, 153이거나 51인 uniform/hybrid 여원 그룹 CA의 구조를 분석한다. 4장에서는 결론을 맺는다.

II. 전이규칙 60, 102, 204를 갖는 uniform/hybrid 그룹 CA의 특성화

본 절에서는 전이규칙 60, 102, 204를 갖는 uniform/hybrid 그룹 CA에 대해 특성화한다.

CA에서 셀의 다음 상태는 전이규칙에 따라 정해진다. 본 논문에서는 각 셀들은 자기 자신과 이웃 셀들의 함수 값에 의해 다음 상태가 결정되는 동시에 갱신되는 3-이웃 CA를 다룬다. 시간 t에서 i번째 셀의 상태가 $x_i(t)$라면 전이함수는 다음과 같이 나타낼 수 있다.

$$x_i(t+1) = f(x_{i-1}(t), x_i(t), x_{i+1}(t))$$

여기서 f는 다음 상태를 결정하는 함수, 즉 전이규칙이라 할 수 있다. 그룹 CA란 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 CA이다. 그룹 CA의 전이규칙은 여러 가지가 있을 수 있다. 본 절에서 특성화하고자 하는 그룹 CA의 전이규칙은 다음과 같다.

표 1. 그룹 CA의 전이규칙

전이규칙	전이함수
60	$x_i(t+1) = x_{i-1}(t) \oplus x_i(t)$
102	$x_i(t+1) = x_i(t) \oplus x_{i+1}(t)$
204	$x_i(t+1) = x_i(t)$

n-셀 CA의 전이규칙이 모두 같으면 uniform CA라 하고 그렇지 않으면 hybrid CA라고 한다.

<정리 1> 전이규칙이 60, 102이거나 204인 uniform CA는 그룹 CA이다.

<정리 2> 전이규칙이 60, 102 이거나 204인 hybrid CA가 그룹 CA이기 위한 필요충분조건은 102와 60의 전이규칙이 연이어 나오지 않는 것이다.

<정리 3> 전이규칙이 60, 102이거나 204인 n-셀 uniform/hybrid 그룹 CA의 특성다항식 $c(x)$와 최소다항식 $m(x)$는 각각 다음과 같다. (단, $l \leq n$)

표 2. 특성다항식과 최소다항식

	uniform CA			hybrid CA
$c(x)$	60	102	204	$(x+1)^n$
	$(x+1)^n$	$(x+1)^n$	$(x+1)^n$	
$m(x)$	$(x+1)^n$	$(x+1)^n$	$(x+1)$	$(x+1)^l$

<정리 4> 전이규칙이 60, 102이거나 204인 n-셀 hybrid 그룹 CA에서 전이규칙 204가 k번째 셀에 한 번 적용되는 경우, 최소다항식의 차수 l은 다음과 같다.

표 3. k에 따른 최소다항식의 차수

전이규칙	k의 조건	l
<60,…,60, 204,60,…,60>	$k-1 \geq n-k+1$	$k-1$
	$k-1 < n-k+1$	$n-k+1$
<102,…,102, 204,102,…,102>	$k \geq n-k$	k
	$k < n-k$	$n-k$
<60,…,60, 204,102,…,102>	$k-1 \geq n-k$	$k-1$
	$k-1 < n-k$	$n-k$
<102,…,102, 204,60,…,60>	$k \geq n-k+1$	k
	$k < n-k+1$	$n-k+1$

<정리 5> 전이규칙이 60, 102이거나 204인 n-셀 uniform CA의 주기는 각각 다음과 같다.

① $n = 2^a$이면 주기는 n이다.
② $n \neq 2^a$ $(2^{a-1} < n < 2^a)$이면
주기는 2^a이다.

<정리 6> 전이규칙이 60, 102이거나 204인 n-셀 hybrid 그룹 CA의 최소다항식의 차수가 l이면 주기는 각각 다음과 같다.

① $l=2^n$이면, 주기는 l이다.
② $l\neq 2^n$ $(2^{n-1}<l<2^n)$이면,
주기는 2^n이다.

<예제 1> 전이규칙이 <60,60,204,102> 인 hybrid 그룹 CA의 최소다항식은 정리 5에 의해서 $m(x)=(x+1)^2$이고, 최소다항식의 차수 $l=2^1$이므로 정리 6에 의해서 주기는 2가 된다. 다음은 이러한 그룹 CA의 상태 전이 그래프이다.

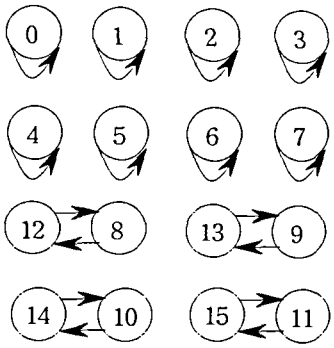

그림 1. 전이규칙 <60,60,204,102>인 그룹 CA

III. 전이규칙 195,153,51을 갖는 uniform/hybrid 여원 그룹 CA의 특성화

본 절에서는 전이규칙 195, 153, 51을 갖는 uniform/hybrid 여원 그룹 CA에 대해 특성화한다.

여원 CA의 i번째 셀에 적용되는 규칙이 여원 규칙이면 i번째 셀의 전이함수는 다음과 같다. 다음과 같이 나타낼 수 있다.

$$\overline{x_i(t+1)}=f(x_{i-1}(t),x_i(t),x_{i+1}(t))\oplus 1$$

본 절에서 특성화하고자 하는 그룹 CA의 전이규칙은 다음과 같다.

표 4. 그룹 CA의 전이규칙

전이규칙	전이함수
195	$x_i(t+1)=\overline{x_{i-1}(t)\oplus x_i(t)}$
153	$x_i(t+1)=\overline{x_i(t)\oplus x_{i+1}(t)}$
51	$x_i(t+1)=\overline{x_i(t)}$

<정리 7>[11] 선형 그룹 CA의 여원 CA도 그룹CA이다.

<정리 8> 전이규칙이 60, 102이거나 204인 n-셀 uniform/hybrid 그룹 CA의 최소다항식의 차수가 m이면, 0이 아닌 여원벡터에 의해 유도된 전이규칙이 195, 153이거나 51인 n-셀 uniform/hybrid 여원 그룹 CA의 주기는 m이거나 $2m$이다.

<정리 9> 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA에서 유도되는 전이규칙이 195, 153이거나 51인 n-셀 uniform/hybrid 여원 그룹 CA의 상태 전이 그래프에서 여원벡터 $F(\neq 0)$가 다음과 같은 경우에 사이클들의 주기가 모두 같아진다.

①전이규칙이 60인 경우
$F=(1,a_2,\cdots,a_n)$, $a_i=0$ *or* 1

②전이규칙이 102인 경우
$F=(b_1,b_2,\cdots,1)$, $b_i=0$ *or* 1

③전이규칙이 204인 경우
$F=(c_1,c_2,\cdots,c_n)$, $c_i=0$ *or* 1

<정리 10> 전이규칙이 60, 102이거나 204인 n-셀 hybrid 그룹 CA에서 전이규칙 204가 k번째 셀에 한 번 적용되는 경우 유도되는 전이규칙이 195, 153이거나 51인 n-셀 uniform/hybrid 여원 그룹 CA의 상태 전이 그래프에서 여원벡터 $F(\neq 0)$가 다음과 같은 경우에 사이클들의 주기가 모두 같아진다.

①전이규칙이 <60,⋯,60,204,60,⋯,60>인 경우
㉠ $k-1\geq n-k+1$인 경우
$F=(1,a_2,\cdots,a_n)$
㉡ $k-1<n-k+1$인 경우
$F=(a_1,\cdots,a_{k-1},1,a_{k+1},\cdots,a_{n-1})$

②전이규칙이<102,⋯,102,204,102,⋯,102>인 경우
㉠ $k\geq n-k$인 경우
$F=(a_1,\cdots,a_{k-1},1,a_{k+1},\cdots,a_{n-1})$
㉡ $k<n-k$인 경우
$F=(a_1,\cdots,a_{n-1},1)$

③전이규칙이 <60,⋯,60,204,102,⋯,102>인 경우
㉠ $k-1\geq n-k$인 경우
$F=(1,a_2,\cdots,a_n)$
㉡ $k-1<n-k$인 경우

$$F=(a_1,\cdots,a_{n-1},1)$$

④전이규칙이 <102,…,102,204,60,…,60>인 경우

㉠ $k\geq n-k+1$인 경우

$$F=(a_1,\cdots,a_{k-1},1,a_{k+1},\cdots,a_{n-1})$$

㉡ $k<n-k+1$인 경우

$$F=(a_1,\cdots,a_{k-1},1,a_{k+1},\cdots,a_{n-1})$$

<예제 2> 예제 1의 그룹 CA에서 여원벡터 $F=(1,0,0,0)$에 의해 유도된 여원 그룹 CA는 정리 10에 의해서 주기가 모두 4인 사이클들로 분리된다. 다음은 이러한 여원 그룹 CA의 상태 전이 그래프이다.

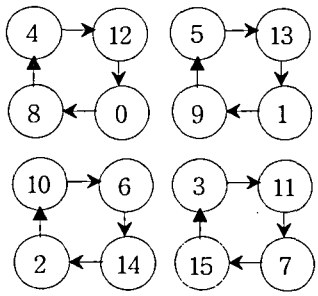

그림 2. 전이규칙 <195,60,204,102>인 여원 그룹 CA

Ⅳ. 결 론

본 논문에서는 전이규칙이 60, 102이거나 204인 uniform/hybrid 그룹 CA의 특성다항식, 최소다항식 그리고 주기에 대해 특성화하였다. 또한 특정한 여원벡터들에 의해서 유도된 95, 153이거나 51인 uniform/hybrid 여원 그룹 CA의 구조를 특성화하였다. 이는 기존의 방법을 보다 일반화한 것으로 키 공유프로토콜에 이용될 수 있다.

참고문헌

[1] J. Von Neumann, "Theory of Self-reproducting automata", University of Illinois Press Urbana, 1966.

[2] S. Wolfram, "Cellular automata and complexity", Addison-Welsly Publishing Company, 1994.

[3] P. Dasgupta, S. Chattopadhyay, P.P. Chaudhuri and I. Sengupta, "Cellular Automata-based recursive pseudoexhaustive test pattern generator, IEEE Transactions of Computers, Vol. 50, No. 2, pp. 177-185, 2001.

[4] P.D. Hortensius, R.D. McLeod and H.C. Card, "Cellular automata based pseudorandom number generators for built-in self test, IEEE Trans. on DAS of Integrated Circuits and System, Vol. 8, pp. 842-859, 1989.

[5] C. N. Zang, M. Deng and R. Mason, " Two improved algorithms and hardware implementations for key distribution using extended programmable cellular automata", Computer Security Applications Conference, Proceedings, 14th Annual, pp. 244-249, 1998.

[6] S. Bhattacharjee, S. Sinha, S. Chattopadhyay and P.P. Chaudhuri, " Cellular automata based scheme for solution of Boolean equations, IEEE, Proc.-Comput. Digit. Tech., Vol. 143, No. 3, pp. 174-180, 1996.

[7] S.J. Cho, U.S. Choi, Y.H. Lee, H.D. Kim, Y.S. Pyo, K.S. Kim and S.H. Heo, Copmuting hase Shifts of Maximum-Length 90/150 Cellular Automata Sequences, LNCS 3305, pp. 31-39, 2004.

[8] S.J. Cho, U.S. Choi, and H.D. Kim, Analysis of Complemented CA Deried from a Linear TPMACA, Computers and Mathematics with Applications, Vol. 45, pp. 689-698, 2003.

[9] S.J. Cho, U.S. Choi, and H.D. Kim, Behavior of Complemented CA whose complement vector is acyclic in a Linear TPMACA, Mathematical and Modelling, Vol. 36, pp. 979-986, 2002.

[10] D. Mukhopadhyay and D.R. Chowdhury, " Characterization of a class of complemented Group Cellular Automata", ACRI 2004, LNCS 3305, pp. 775-784, 2004.

[11] P.P. Chaudhuri, D.R. Chowdhury, S. Nandi and S. Chattopadhyay, "Additive cellular automata theory and applications", IEEE Computer Society Press, Vol. 1, California, USA, 1997.