情報保護學會論文誌
第15卷 第4號, 2005. 8

90/150 셀룰라 오토마타에 의해 생성되는 PN 수열들 사이의 상대적 위상이동차에 대한 알고리즘*

조 성 진,[1†] 최 언 숙,[2‡] 김 한 두[3]
[1]부경대학교, [2]영산대학교, [3]인제대학교

Algorithm for The Relative Phase Shifts between PN Sequences Generated by 90/150 Cellular Automata*

Sung-Jin Cho,[1†] Un-Sook Choi,[2‡] Han-Doo Kim[3]
[1]Pukyong National University, [2]Youngsan University, [3]Inje University

요 약

이 논문에서는 최대길이를 갖는 90/150 셀룰라 오토마타로부터 얻어진 수열에 대해 대수적으로 연구한다. GF(2) 위에서 최대길이를 갖는 n-셀 90/150 셀룰라 오토마타는 길이가 2^n-1인 수열을 생성한다. 이러한 셀룰라 오토마타의 임의의 셀에 대한 출력수열은 다른 셀에 대한 출력수열의 위치를 이동함으로써 얻어질 수 있다. LFSR과는 달리, 셀룰라 오토마타의 셀들에 대한 출력수열들의 위상이동차는 일반적으로 셀룰라 오토마타의 단계들 사이에서 다르다. 본 논문에서는 이러한 셀들 사이의 상대적인 위상이동차를 계산하는 알고리즘을 제시한다. 이 알고리즘은 Sarkar의 알고리즘과 달리 Shank의 알고리즘을 이용하지 않으며, 원하는 위치의 위상이동차를 계산하기 위하여 이전 셀의 위치의 위상이동차를 계산할 필요가 없으며 수행시간은 $O(2^n)$이다.

ABSTRACT

Every cell position of a maximum-length 90/150 cellular automata(CA) generates the same pseudo-noise(PN) sequence corresponding to the characteristic polynomial of the CA with a phase shift. Unlike LFSRs, the phase shift is generally different between stages of a CA. In this paper, we propose an algorithm to compute relative phase shifts between stage of a CA. Our algorithm does not need Shank's algorithm to compute relative phase shifts and does not need any previous phase shifts to compute a phase shift. Moreover it is done in time $O(2^n)$.

Keywords : *90/150 CA, Phase shifts, PN sequences, Primitive polynomials*

Ⅰ. 서 론

LFSR의 대안으로 제안된 셀룰라 오토마타(CA)[1]는 LFSR과 달리 고품질의 PN 수열을 생성할 수 있음[2,3]이 밝혀짐에 따라, CA는 테스트 패턴 생성, 의사 난수열 생성기, 암호 및 서명과 같은 분야에서 응용되고 있다.[4-18] 가산 CA의 상태전이 행동분석은 대수적 분석이 가능하다.[6,7] 가산 CA중 GF(2) 위에서 최대길이를 갖는 n-셀 90/150 CA의 각 셀들은 주기가 2^n-1인 PN 수열을 생성한다. 이러한 CA의 임의의 셀에 대한 출력수열은 다른 셀에 대한

접수일 : 2005년 1월 17일 ; 채택일 : 2005년 7월 25일
* 본 논문은 2003년도 인제대학교 학술 연구 조성비 보조에 의한 것임.
† 주저자, sjcho@pknu.ac.kr
‡ 교신저자, choies@ysu.ac.kr

출력수열의 위치를 이동함으로써 얻을 수 있다. 그리고 LFSR과 달리, CA의 셀들에 대한 출력수열들의 위상이동차는 일반적으로 CA의 단계들 사이에서 다르다. Sarkar는 위상이동차를 구하는 알고리즘을 제안하였다.[5] 이 알고리즘은 CA 수열의 연구를 위하여 적절한 대수적 구조를 전개함으로써 구하였다. 이러한 CA에 의해 생성되는 PN수열은 BIST구조와 안전한 스트림 암호의 설계에 응용된다. 특히, 후자의 경우는 CA 수열의 적당한 부분집합에 속하는 임의의 두 수열 사이의 위상이동차가 CA의 길이에서 지수적으로 커지는 부분집합을 택할 수 있다는 사실에 근거하고 있다. 그러나 Sarkar의 알고리즘에는 몇가지 문제점들이 있다. 첫째, 그의 알고리즘은 상대적 위상이동차를 구하기 위하여 반드시 Shank의 알고리즘을 이용해야 한다는 것인데 Shank의 알고리즘은 셀의 수가 50을 넘어가면 계산이 불가능하다고 알려져 있어서 Sarkar의 알고리즘으로 셀의 수가 50을 넘는 CA에 의해서 생성되는 PN수열들 간의 상대적 위상이동차를 구하는 것은 사실상 불가능하다. 둘째, Sarkar의 알고리즘을 이용하여 상대적 위상이동차를 구하려면 그 이전의 모든 셀들의 상대적 위상이동차를 알아야만 하는 불편함이 있다.

본 논문에서는 최대길이를 갖는 90/150 CA에 의해서 생성되는 수열에 관해 대수적으로 연구하고, 최대길이를 갖는 90/150 CA의 각 셀에서 생성된 수열의 위상이동차에 이를 적용한다. 이러한 응용으로부터, 행(row)위상이동차라는 새로운 개념을 도입하여 Sarkar[5]의 방법을 개선한 위상이동차를 구하는 새로운 알고리즘을 제안한다.

II. 최대길이를 갖는 90/150 셀룰라 오토마타에 의해 생성된 수열의 분석

CA는 규칙적인 방법에 의해 공간적으로 배열된 셀들이 상호 연결되어 이루어진다. 여기서, 각 셀의 상태전이는 그 셀의 이웃에 의존한다. Wolfram[1]에 의해 조사된 CA의 구조는 셀들이 이산격자로 간주될 수 있다. 단, 각 셀의 값은 0 또는 1로 가정하고, 한 셀의 다음 상태는 자신과 인접한 두 셀(3-이웃)에 의존한다고 하자.

규칙 90과 150은 다음과 같이 주어진다.

$$\text{규칙 } 90 : \ q_i^{t+1} = q^t_{i-1} \oplus q^t_{i+1}$$

$$\text{규칙 } 150 : \ q_i^{t+1} = q^t_{i-1} \oplus q^t_i \oplus q^t_{i+1}$$

단, $\oplus$는 XOR 논리이고 q_i^t는 t번째 시간에서 i번째 CA 셀의 상태를 나타내고, q^t_{i-1}와 q^t_{i+1}는 자신의 왼쪽과 오른쪽 이웃 상태를 가리킨다. 이 절에서는 두 개의 원소를 가지는 유한체 GF(2)위에서 최대길이를 갖는 90/150 CA에 의해 생성된 수열의 성질에 대해 조사한다.

다음의 $n\times n$ 삼중대각행렬 T_n을 생각해보자.

$$T_n=\begin{pmatrix} a_1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & a_3 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & a_{n-1} & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & a_n \end{pmatrix}$$

단, $a_1, a_2, \cdots, a_n$은 GF(2)에 속하는 원소이다. T_n을 하나의 n-셀 90/150 CA에 대한 상태전이행렬(state transition matrix)이라 하는데, $T_n=\langle a_1, a_2, \cdots, a_n\rangle$으로 나타내기로 하자.

예로서, 만약 $T_6=\langle 1,0,0,0,0,0\rangle$이 주어진 6-셀 90/150 CA인 C에 대한 상태전이행렬이면, 특성다항식은 $f(x)=x^6+x^5+x^4+x+1$이고 이는 원시다항식이다. 따라서 C는 최대길이를 갖는 90/150 CA이다. 다음 그림은 C의 구조를 보여준다.

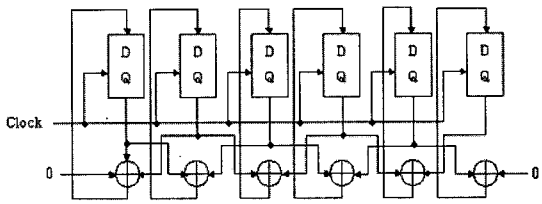


그림 1. 상태전이행렬 T_6을 가지는 90/150 CA C의 구조

Tezuka와 Fushimi[4]는 주어진 원시다항식 $f(x)$에 대하여, $f(x)$를 특성다항식으로 하는 최대길이를 갖는 90/150 CA는 정확히 두 개가 존재함을 주장하였다. 만약 $T_n=\langle a_1, a_2, \cdots, a_n\rangle$이 $f(x)$에 대응하는 상태전이행렬이면, 나머지 상태전이행렬은 $T_n'=\langle a_n, a_{n-1}, \cdots, a_1\rangle$이다.

예를 들어, $f(x)=x^6+x^5+x^4+x+1$이면, $T_6=\langle 1,0,0,0,0,0\rangle$와 $T_6'=\langle 0,0,0,0,0,1\rangle$이 $f(x)$에 대응하는 상태전이행렬이다.

〈보조정리 1[19]〉 상태전이행렬이 T_n인 임의의 n-셀 90/150 CA에 대하여, T_n에 대한 최소 다항식은 T_n에 대한 특성다항식과 같다.

〈정리 2〉 최대길이를 갖는 주어진 n-셀 90/150 CA에 대한 상태전이행렬을 T_n이라 하고, v_0는 F_2^n에 속하는 0아닌 벡터라 하자. 단, $F_2^n = \{(b_1, b_2, \cdots, b_n)^t | b_i \in GF(2), 1 \le i \le n\}$. $t \ge 1$에 대해 $v_t = T_n v_{t-1}$이라 정의하면, 수열 V: $v_0, v_1, v_2, \cdots$은 최대주기 $2^n - 1$을 가진다.

(증명) T_n에 대한 특성다항식을 $f(x)$라 하자. 주어진 0이 아닌 벡터 $v \in F_2^n$에 대하여, $f_v(x)$를 v에 대한 최소다항식이라 하자. 보조정리 1에 의해 0이 아닌 모든 벡터 $v \in F_2^n$에 대하여 $f_v(x) = f(x)$가 성립한다. 만약 r이 수열 V의 주기이면 $T_n^r v_0 = v_0$이므로, $f_{v_0}(x)$는 $x^r - 1$을 나눈다. 한편, $f_{v_0}(x) = f(x)$이고 $f(x)$가 원시이므로, $r = 2^n - 1$ 이다. □

〈정의 3[20,21]〉 $f(x) = c_0 + c_1 x + \cdots + \cdots + c_{n-1}x^{n-1} + x^n$ $(c_0, c_1, \cdots, c_{n-1} \in GF(2))$이 n 차 원시다항식이면, $f(x)$는 주기가 $2^n - 1$인 주기수열을 생성한다. 이 수열을 PN수열이라 한다.

정리 2와 정의 3은 T_n이 최대길이를 갖는 주어진 n-셀 90/150 CA에 대한 상태전이행렬이고 $v_t = (v_t^0, v_t^1, \cdots, v_t^{n-1})^t \in F_2^n$이면, $v_t^i (0 \le i \le n-1)$가 PN 수열임을 말해준다.

〈정리 4〉 T_n을 최대길이를 갖는 n-셀 90/150 CA의 상태전이행렬이라 하면, 다음을 만족하는 p가 존재한다. $(1 \le p \le 2^n - 2)$

$$I_n \oplus T_n = T_n^p$$

(증명) $f(x)$를 T_n에 대한 특성다항식이라 하고 $f(\alpha) = 0$이라 하자. 한편, $f(x)$는 원시이므로 $\{0, 1, \alpha, \cdots, \alpha^{2^n-2}\}$는 α에 의해 생성된 유한체이다. 따라서 $1 + \alpha = \alpha^p$를 만족하는 p $(1 \le p \le 2^n - 2)$가 존재한다. 한편, α는 T_n의 고유벡터이므로, $I_n \oplus T_n = T_n^p$을 만족한다. □

〈따름정리 5〉 T_n을 최대길이를 갖는 n-셀 90/150 CA의 상태전이행렬이라 하면

$$T_n^k \oplus T_n^{k+1} = I_n$$

을 만족하는 k $(1 \le k \le 2^n - 2)$가 존재한다.

(증명) 정리 4에 의하여 $I_n \oplus T_n = T_n^p$를 만족하는 p $(1 \le p \le 2^{n-2})$가 존재하므로

$$T_n^{2^n-1-p}(I_n \oplus T_n) = T_n^{2^n-1} = I_n$$

이 성립한다. 여기서 $k = 2^n - 1 - p$라 두면, $T_n^k(I_n \oplus T_n) = T_n^k \oplus T_n^{k+1} = I_n$ 이 되어 증명된다. □

〈예제 6〉 다음과 같은 상태전이행렬 T_6를 갖는 6-셀 90/150 CA를 생각해보자.

$$T_6 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

T_6의 특성다항식은 $f(x) = x^6 + x^5 + x^4 + x + 1$ 이고, 이는 원시다항식이다. 여기서 $T_6^{24} \oplus T_6^{25} = I_6$ 이 성립한다.

Ⅲ. CA 수열의 특성

이 절에서 최대길이를 갖는 90/150 CA의 특별한 셀에 의해 생성된 수열에 관하여 연구한다. 각 셀 위치는 PN 수열을 생성한다[8]. LFSR과는 달리, 일반적으로 위상이동차는 CA의 단계들 사이에서 다르다.

이제부터는 T_n을 간단히 T로 나타내기로 한다.

〈보조정리 7〉 T가 최대길이를 갖는 n-셀

90/150 CA의 상태전이행렬이면, T^h와 T^m의 i 번째 행은 항상 다르다. 단, $0 \le i \le n-1$이고 $1 \le h < m \le 2^n-2$이다.

(증명) $w_0=(0,0,\cdots,0,1,0,\cdots,0)$을 T의 초기 벡터라 하고 $w_r = w_{r-1}T\ (r \ge 1)$라 정의하자. 그리고 T^h와 T^m의 i번째 행이 같다고 가정하자. 단, $0 \le i \le n-1$이고 $1 \le h < m \le 2^n-2$이다. 그러면

$$w_h = w_0 T^h = w_0 T^m = w_m$$

이다. 한편, $w_0, w_1, \cdots, w_{2^n-2}$은 모두 다르므로, $w_h \neq w_m$이다. 따라서 T^h와 T^m의 i행은 항상 다르다. □

다음 정리는 최대길이를 갖는 90/150 CA의 단계들 사이에서 위상이동차가 다름을 보여준다.

〈정리 8〉 T를 최대길이를 갖는 n-셀 90/150 CA의 상태전이행렬이라 하고, $w_0 \neq (0,0,\cdots,0)$을 T의 초기벡터라 하자. 그러면 임의의 $1 \le i < j \le n-1$에 대하여 다음을 만족하는 정수 h가 존재한다. (단, q_i^t는 시간 t에서의 i번째 셀의 상태를 나타낸다.)

$$q_j^{t+h} = q_i^t, \quad t \ge 0$$

(증명) $f(x)$가 T의 n차의 원시인 특성다항식이면, $\{q_i^t\}$와 $\{q_j^t\}$는 n계 동차 선형점화수열이다. 그리고 $\{q_i^t\}$와 $\{q_j^t\}$의 주기 역시 2^n-1이다.

$w_i = (q_0^i, \cdots, q^i{}_{n-1})$, $0 \le i \le 2^n-2$ 라 두면, 보조정리 7에 의하여 모든 w_i들은 모두 0이 아니면서 서로 다르다. 한편, 각 셀 위치는 PN 수열을 생성하므로, 모든 $t \ge 0$에 대하여 $q_j^{t+h} = q_i^t$를 만족하는 정수 h가 존재한다. □

T를 최대길이를 갖는 주어진 n-셀 90/150 CA의 상태전이행렬이라 하고, $w_0 = (1,0,\cdots,0)$를 T의 초기벡터라 하자. 그러면 T에 의해 생성된 n개의 독립인 PN 수열을 열로서 갖는 $(2^n-1)\times n$ 행렬 A를 얻는다. B^i를 A에서 i번째 열을 제거하여 얻은 $(2^n-1)\times(n-1)$ 행렬이라 하면, B^i는 모두가 0인 $(n-1)$쌍은 단 하나, 나머지 0아닌 $(n-1)$쌍은 두 개씩 포함한다. 이 경우에 B^0에 속하는 첫 번째 벡터는 $(0,0,\cdots,0)$이다.

예로서, $T=\langle 0,1,1\rangle$인 경우에 A와 B^i(i = 0,1,2)는 다음의 표 1에서 보는 바와 같다.

표 1. $T=\langle 0,1,1\rangle$에 대한 행렬 A와 B^i

	A	B^0	B^1	B^2
0	100	**00**	10	10
1	010	10	**00**	01
2	111	11	11	11
3	110	10	10	11
4	101	01	11	10
5	001	01	01	**00**
6	011	11	01	01

이제, B^i에 관한 B^0의 행위상이동차로서 B^i에 속하는 모두 0인 행벡터의 위치를 정의하자. 표 1에서 B^1과 B^2에 관한 B^0의 행위상이동차는 각각 1과 5이다. 즉, B^0에 관한 B^1과 B^2의 행위상이동차는 각각 $-1 \equiv 6 \pmod 7$과 $-5 \equiv 2 \pmod 7$이다.

〈정리 9〉 T가 최대길이를 갖는 n-셀 90/150 CA의 상태전이행렬이면 다음 식을 만족하는 정수 r_i $(0 \le i \le n-1)$가 존재한다.

$$T^{r_i} w_0^t \oplus T^{r_i+1} w_0^t = (0,0,\cdots,0,1,0,\cdots,0)^t$$

(증명) $T^{q_i} w_0^t = (0,0,\cdots,0,1,0,\cdots,0)^t$ 가 성립하는 q_i를 구할 수 있다. 정리 4에 의해 $I_n \oplus T = T^p$를 만족하는 p를 계산하고 $r_i \equiv q_i - p \pmod{2^n-1}$ 라 두면, 이 r_i가 구하는 정수이다. □

다음의 따름정리에 의해 B^i에서 모두가 0인 $(n-1)$쌍의 위치를 구할 수 있다.

〈따름정리 10〉 T는 최대길이를 갖는 n-셀 90/150 CA의 상태전이행렬이고 r_i가 정리 9에서 존재하는 정수라 하면, B^i에서 모두가 0인 쌍은 (r_i+p)번째 벡터이다. 단, p는 정리 4에서의 정수이다.

다음 정리는 위상이동차를 구하는 방법을 제시해 준다.

〈정리 11〉 T를 최대길이를 갖는 n-셀 90/150 CA C의 상태전이행렬이라 하고 u_i를 0번째 셀에 관한 C의 $i\,(0\le i\le n-1)$번째 셀의 위상이동차라 하면, 다음을 만족한다.(단 r_i와 p는 각각 정리 9와 정리 4에서의 정수이다.)

$$u_i \equiv -(r_i+p) \pmod{2^n-1}$$

(증명) A는 T에 의해서 생성된 n개의 독립인 PN 수열을 열로서 갖는 $(2^n-1)\times n$ 행렬이고, $(1,0,\cdots,0)$은 T의 초기구성이라 하자. 각 i $(0\le i\le n-1)$에 대하여, B^i를 A에서 i번째 열을 제거하여 얻은 $(2^n-1)\times(n-1)$ 행렬이라 하자. k_i를 B^i에 관한 B^0의 행위상이동차라고 하면, $k_0=0$이고 $-k_i \pmod{2^n-1}$은 B^0에 관한 B^i의 행위상이동차이다. 한편, T가 대칭행렬(sysmmetric matrix)이므로, 0셀에 관한 i번째 셀의 위상이동차는 B^0에 관한 B^i의 위상이동차와 같다. 따름정리 10에 의하여

$$T^{r_i+p}(1,0,\cdots,0)^t = (0,0,\cdots,0,1,0,\cdots,0)^t$$

이고 따라서 $k_i=r_i+p$이 성립한다. 한편, C가 최대길이를 갖는 CA이므로, T는 가역이다. 그러므로

$$T^{-(r_i+p)}(0,0,\cdots,0,1,0,\cdots,0)^t = (1,0,\cdots,0)^t$$

이고, 다음이 성립한다.

$$u_i \equiv -(r_i+p) \pmod{2^n-1}\ .\ \square$$

〈예제 12〉 $T=\langle 1,0,0,0,0,0\rangle$라 하면, T의 특성다항식은 $x^6+x^5+x^4+x+1$ 이고 $I_6 \oplus T = T^{39}$이 성립한다. 한편, $T^0(1,0,0,0,0,0)^t=(1,0,0,0,0,0)^t$이므로, $q_0=0$이다. 따라서

$r_0=q_0-p=-39\equiv 24 \pmod{63}$ 이다. 실제로, $T^{24}(1,0,0,0,0,0)^t \oplus T^{25}(1,0,0,0,0,0)^t=(1,0,0,0,0,0)^t$ 이다.

한편, $T^{39}(1,0,0,0,0,0)^t=(1,0,0,0,0,0)^t$이므로 $r_1=q_1-p\equiv 0 \pmod{63}$ 이다. 같은 방법으로 다음을 구할 수 있다. $r_2=59$, $r_3=8$, $r_4=57$ 그리고 $r_5=56$ 한편, 정리 11에 의해 $u_i\equiv -(r_i+p) \pmod{63}$이므로, 위상이동차는 다음과 같다.

$$u_0=0,\ u_1=24,\ u_2=28,\ u_3=16,\ u_4=30,\ u_5=31$$

Ⅳ. 위상이동차 계산을 위한 알고리즘 제안 및 비교

4.1 기존 알고리즘과의 비교

다음은 Sarkar의 알고리즘이다[5]. Sarkar의 알고리즘은 주어진 원시 다항식 $f(x)$를 특성다항식으로 갖는 CA의 전이행렬 T에 대하여 $(xT-I)X=0 \bmod f^*(x)$를 푼다. $f(x)$의 상반 다항식 $f^*(x)$를 이용하여 $f^*(x)=0$을 만족하는 해 α를 이용하여 GF(2^n) 유한체를 구성한다. 예를 들어 3-셀 90/150 CA의 전이행렬이 $T=\begin{pmatrix}0&1&0\\1&1&0\\0&1&1\end{pmatrix}$일 때, T의 특성다항식은 $f(x)=x^3+x+1$이다. 특성다항식의 상반다항식은 $f^*(x)=x^3+x^2+1$이다. 그러므로 $(xT-I)X=0 \bmod f^*(x)$은 다음과 같다.

$$(xT-I)X=\begin{pmatrix}1&x&0\\x&1+x&0\\0&x&1+x\end{pmatrix}\begin{pmatrix}1\\x^a\\x^b\end{pmatrix}=0 \bmod f^*(x)$$

위 행렬방정식을 연립방정식으로 나타내면 다음과 같다.

$$\begin{cases}1+x^{a+1}=0 & (1)\\ x+x^a+x^{a+1}=0 & (2)\\ x^{a+1}+x^b+x^{b+1}=0 & (3)\end{cases}$$

식 (1)을 풀면 $a=6$이고, (1)의 결과를 이용하

여 식 (2)를 풀면 $b=2$이다. 따라서 0셀에 대한 1셀, 2셀의 위상이동차는 각각 6과 2이다.

이와 같이 Sarkar의 알고리즘은 먼저 $f^*(x)$를 이용하여 $GF(2^n)$의 유한체를 생성하고, $(xT-I)X=0 \mod f^*(x)$를 순차적으로 풀어야 한다. 다시 말해서 0셀에 대한 i번째 열의 위상이동차를 구하기 위해서는 이전의 모든 값을 알아야만 계산할 수 있다. 또한 이 알고리즘의 풀이법은 Shank의 알고리즘을 이용하고 있으므로 Shank의 알고리즘이 가지고 있는 제약조건인 셀의 크기가 50이하라는 조건을 그대로 가지고 있다. 그러나 본 논문에서 제안한 알고리즘은 알고리즘을 수행하는 데 있어 Shank의 알고리즘이 필요하지 않으며, 0셀에 대한 i번째 열의 위상이동차를 구하기 위해서 이전의 어떤 위상이동차도 필요하지 않다. 또한 Shank의 알고리즘을 사용하지 않으므로 충분히 큰 n에 대해서도 실제적으로 아주 유용하다.

Sarkar의 알고리즘을 수행하기 위해 요구되는 계산량은 $f^*(x)$를 이용하여 $GF(2^n)$을 구성하기 위하여 $O(2^n)$이 요구되고 방정식을 푸는데 $O(n2^n)$이 요구된다. 그러나 본 논문에서 제안한 알고리즘을 수행하기 위해 요구되는 계산량은 $O(2^n)$이다.

4.2 알고리즘 제안

이제, 최대길이를 갖는 주어진 n-셀 90/150 CA에서의 위상이동차를 구하는 알고리즘을 제시한다. 이 알고리즘의 정당성은 정리 11에 있다.

표 2는 제안된 알고리즘에 따라 32차까지 계산한 0셀에 대한 주어진 CA의 위상이동차를 나타낸 것이다.

[Algorithm FindPhaseShifts]

입력: $n\times n$ 상태전이행렬 T, 초기벡터 $w=(1,0,\cdots,0)$
출력: phaseshift[n].

단계 1. mark mark $_{1\times n}$ by 0 ; mark[0]=1;
power=1; phaseshift[0]=0.
단계 2. While (all mark $\neq$1) do step 3 to step 5.
단계 3. $w^l = Tw^l$. /* Run the CA */
단계 4. If (w contains single 1)
then mark[position of 1]=1;
phaseshift[position of 1] $\equiv$ - power (mod 2^n-1).
단계 5. power=power+1.

표 2. 0셀에 대한 CA의 위상이동차

차수	CA 규칙	위상이동차
3	110	0, 4, 5
4	0101	0, 14, 5, 9
5	01111	0, 30, 20, 4, 22
6	000110	0, 62, 51, 60, 22, 23
7	1011001	0, 120, 71, 112, 19, 68, 75
8	01001011	0, 254, 147, 56, 131, 66, 126, 68
16	0001111001001000	0, 65534, 8108, 65532, 3385, 64168, 61463, 41934, 2370, 54822, 47229, 1810, 63957, 6533, 63959, 63960
32	00001100010001111 00001100000000110	0, 4294967294, 3963262907, 4294967292, 2182065471, 3478064023, 2842396500, 3797410740, 2636154424, 1477132997, 2453647807, 3833928247, 4122644326, 2445882768, 3715941894, 3131603603, 3781145264, 724531189, 1964528637, 1178642835, 1437488410, 2132417369, 2228497937, 2438002527, 3823282243, 3142683718, 4037203264, 3657430022, 496625232, 3264387886, 25871502, 25871503

V. 결 론

본 논문에서 우리는 최대길이를 갖는 90/150 CA에 대한 성질을 조사하였으며, 이러한 결과들을 최대길이를 갖는 90/150 CA에 의해서 생성된 PN 수열의 위상이동차에 응용하여 Sarkar[5]의 방법과 다른 새로운 위상이동차 계산 알고리즘을 제안하였다. Sarkar의 알고리즘은 0번째 셀에 대한 i번째 셀의 위상이동차를 구하기 위해 이전 셀의 위상이동차를 알아야만 계산할 수 있다. 무엇보다 방정식을 풀기 위해 Shank의 알고리즘을 이용해야만 하기 때문에 셀의 크기에 제한을 받는다. 그러나 본 논문에서 제안한 알고리즘은 0번째 셀에 대한 i번째 셀의 위상이동차를 독립적으로 계산할 수 있으며 셀의 크기에도 제약을 받지 않는다. 또한 제안한 알고리즘을 수행하기 위해 요구되는 계산량도 $O(2^n)$으로 Sarkar에 의해 제안된 알고리즘의 계산량 $O(n2^n)$보다 효과적임을 보였다.

참 고 문 헌

[1] S. Wolfram, "Statistical Mechanics of

Cellular Automata", Rev. Mod. Phys. 55, pp. 601-644, 1983.

[2] P.H. Bardell, "Analysis of Cellular Automata Used as Pseudorandom Pattern Generators", Proc. IEEE int. Test. Conf. pp.762-767, 1990.

[3] A.K. Das and P.P. Chaudhuri, "Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation", IEEE Trans. Comput. 42, pp. 340-352, 1993.

[4] S. Tezuka and M. Fushimi, "A method of designing cellular automata as pseudorandom number generators for built-in self-test for VLSI", Contemporary Mathematica 168, pp.363-367, 1994.

[5] P. Sarkar, "Computing Shifts in 90/150 cellular automata sequences", Finite Fields Their Appl. 42, pp. 340-352, 2003.

[6] S.J. Cho, U.S. Choi and H.D. Kim, "Analysis of complemented CA derived from a linear TPMACA", Computers and Mathematics with Applications 45, pp.689-698, 2003.

[7] 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 Computer Modelling 36, pp. 979-986, 2002.

[8] S. Nandi and P.P. Chaudhuri, "Additive Cellular Automata as an on-chip test pattern generator", Test Symposium 1993, Proceedings of the Second Asian, IEEE, pp.166-171, 1993.

[9] P. Sarkar, "The filter-combiner model for memoryless synchronous stream ciphers", in Proceedings of Crypto 2002, Lecture Notes in Computer Science, Springer, Berlin 2442, pp. 533-548, 2002.

[10] 전준철, 김현성, 이형목, 유기영, "GF(2^m)상의 셀룰라 오토마타를 이용한 VLSI 구조", 정보보호학회논문지, 12(6), pp. 87-94, 2002.

[11] 홍진, 이동훈, 지성택, "LFSM 기반의 비선형 필터 모델의 특성", 정보보호학회논문지, 14(2), pp.75-83, 2004.

[12] 최언숙, 조성진, "최대길이를 갖는 셀룰라 오토마타의 생성", 정보보호학회논문지, 14(6), pp.25-30, 2004.

[13] 조성진, 최언숙, 황윤희, 김한두, 표용수, "GF(2p) 위에서의 SACA의 상태전이 분석", 정보보호학회논문지, 15(2), pp.105-111, 2005.

[14] 조태남, 이상호, "(2,4)-트리를 이요한 그룹키 관리", 정보보호학회논문지, 11(4), pp.77-89, 2001.

[15] 박영호, 이경현, "이동네트워크 환경에서 그룹키 관리구조", 정보보호학회논문지, 12(2), pp.89-100, 2002.

[16] 권정욱, 황정연, 김현정, 이동훈, 임종인, "일방향 함수와 XOR을 이용한 효율적인 그룹키 관리 프로토콜: ELKH", 정보보호학회논문지, 12(6), pp.93-1121, 2002.

[17] 이상원, 천정희, 김용대, "Pairing을 이용한 트리 기반 그룹키 합의 프로토콜", 정보보호학회논문지, 13(3), pp.101-110, 2003.

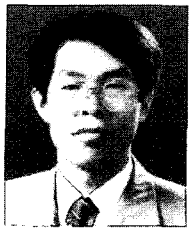
[18] 박영희, 정병천, 이윤호, 김희열, 이재원, 윤현수, "Diffie-Hallman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프로토콜", 정보보호학회논문지, 13(5), pp.3-15, 2003.

[19] M. Serra, T. Slater, J.C. Muzio and D.M. Miller, The analysis of one dimensional linear cellular automata and their aliasing properties, IEEE Trans Computer-Aided Design, 9, pp. 767-778, 1990.

[20] S.W. Golomb, Shift Register Sequences, Holden Day, 1967.

[21] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

〈著者紹介〉



조 성 진 (Sung-Jin Cho) 정회원
1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년~현재: 부경대학교 수리과학부 정교수
〈관심분야〉 셀룰라 오토마타론, 정보보호, 부호이론

최 언 숙 (Un-Sook Choi)
1992년 2월: 성균관대학교 산업공학과 학사
2000년 2월: 부경대학교 응용수학과 석사
2004년 2월: 부경대학교 응용수학과 박사
2004년 3월~현재: 영산대학교 자유전공학부 단임교수
〈관심분야〉 셀룰라 오토마타론, 정보보호, 부호이론

김 한 두 (Han-Doo Kim)
1982년 2월: 고려대학교 수학과 학사
1984년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1989년~현재: 인제대학교 컴퓨터 응용과학부 정교수
〈관심분야〉 전산수학, 셀룰라 오토마타론