최대길이를 생성하는 LFSM의 위상이동차+

김한두*, 황윤희**, 권숙희***, 최언숙****, 조성진*****

*인제대학교 컴퓨터응용과학부, **부경대학교 정보보호학과,

***부경대학교 응용수학과, ****동명대학교 멀티미디어공학과,

*****부경대학교 수리과학부

Phase Shifts of Maximum-Length LFSM

Han-Doo Kim*, Yoon-Hee Hwang**, Suk-Hee Kwon***

Un-Sook Choi****, Sung-Jin Cho*****

*School of Computer Aided Science, Inje Univ.

**Dept. of Information Security, Pukyong National Univ.

***Dept. of Applied Mathematics, Pukyong National Univ.

****Dept. of Multimedia Engineering, Tongmyong Univ.

*****Division of Mathematical Sciences, Pukyong National Univ.

요 약

본 논문에서는 최대길이를 생성하는 LFSM의 위상이동차를 동반행렬의 특성다항식을 이용하여 계산하는 알고리즘을 제안한다.

I. 서론

이진 Linear Finite State Machine(이하, LFSM)은 수학적으로 분석이 가능한 이진수열을 효율적으로 발생할 수 있는 장치로 이에 기반한 스트림 암호(stream ciphers)는 하드웨어를 이용한 구현이 용이하며, 주기가 길고 또한 우수한 통계적 특성을 지니고 있기 때문에 키 수열 생성기의 설계에 폭 넓게 이용되고 있다[1,2]. LFSM의 하나인 최대길이를 갖는 90/150 셀룰라 오토마타(Cellular Automata, 이하 CA)의 위상이동차(phase shift)에 관한 연구는 Cho 등에 의해서 연구되었다[3-6].

본 논문에서는 최대길이를 생성하는 LFSM의 위상이동차를 동반행렬의 특성다항식을 이용하여 계산하는 알고리즘을 제안한다.

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

II. LFSM의 동반행렬

n개의 n차 LFSR로 이루어진 LFSM은 $X_t = TX_{t-1}$로 표현할 수 있다. 여기서, X_i는 시간 i에서의 $n\times 1$ 상태벡터이고 T는 LFSM의 $GF(2)$위에서의 $n\times n$ 전이행렬이다. 특히, LFSM의 전이행렬 T는 특성다항식과 최소다항식이 같은 동반행렬로 표현할 수 있다. T의 특성다항식이 $f(x)= x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + 1$ 이면, 동반행렬 T는 다음과 같다.

$$T=\begin{pmatrix} a_{n-1} & 1 & 0 & \cdots & 0 \\ a_{n-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_1 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

본 논문에서는 최대길이를 생성하는 LFSM으로 제한한다.

예제 1> 특성다항식이 $f(x)=x^3+x+1$인 LFSM의 동반행렬은 $T=\begin{pmatrix}0&1&0\\1&0&1\\1&0&0\end{pmatrix}$이고 T에 의한 $(0,0,1)^t$의 다음 상태는 $T(0,0,1)^t=(0,1,0)^t$이다. 이렇게 해서 얻어진 상태들을 행벡터로 나열하면 다음과 같은 7×3 행렬을 얻는다.

$$\begin{matrix}\mathbf{0}&0&1\\0&1&\mathbf{0}\\1&0&0\\0&1&1\\1&1&0\\1&1&1\\1&\mathbf{0}&1\end{matrix}$$

이렇게 얻어진 행렬의 1열에 대한 2열과 3열의 위상이동차는 각각 6과 1이다.

III. LFSM의 위상이동차

3장에서는 최대길이를 생성하는 LFSM의 위상이동차를 구한다.

일반적으로 n차 특성다항식 $f(x)=x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_2x^2+a_1x+1$을 갖는 LFSM의 동반행렬 T와 초기벡터 $X_0=(0,0,\cdots,0,1)^t$에 의해 얻어진 상태들을 행벡터로 나열하면 다음과 같은 $(2^n-1)\times n$ 행렬을 얻는다.

$$\begin{matrix}0&0&\cdots&0&0&1\\0&0&\cdots&0&1&0\\\vdots&\vdots&&\vdots&\vdots&\vdots\\1&0&\cdots&0&0&0\\a_{n-1}&a_{n-2}&\cdots&a_2&a_1&1\\\vdots&\vdots&&\vdots&\vdots&\vdots\\1&a_{n-1}&\cdots&a_3&a_2&a_1\end{matrix}$$

1열에 대한 $i(1\le i\le n)$열의 위상이동차를 $ps(i)$라 두면 $ps(1)=0$, $ps(n)=1$임을 쉽게 알 수 있다.

정리 2> 동반행렬 T의 1열의 $a_i(1\le i\le n)$들이 다음과 같다고 하자.

$$(a_{n-1},a_{n-2},\cdots,a_1)=(\overbrace{0,\cdots,0}^{m-1},1,\cdots)$$

그러면 $ps(i)=2^n-i$ $(2\le i\le m)$이다.

보조정리 3> $T^k\oplus T^{k+1}=I$이면 $T^k\oplus T^{k+2}=T^{2^n-1-k}$이다.

정리 4> $i=\max\{j\mid a_j=1,\ 1\le j\le n-1\}$이고 $T^k\oplus T^{k+(n-i)}=I$이면 $ps(n-i+1)=k$이다.

따름정리 5> i) $a_i=1$, $a_{i-1}=0$이면
$ps(n-i+2)=ps(n-i+1)-1$이다.
ii) $a_i=1$, $a_{i-1}=a_{i-2}=a_{i-m}=0$이면
$ps(n-i+j)=ps(n-i+1)-(j-1)$ 이다.
$(2\le j\le m+1)$

정리 6> $a_i=1$, $a_{i-1}=\cdots=a_1=0$이고 $T^k\oplus T^{k-i}=I$이면 $ps(n-i)=k+1$이다.

정리 7> $a_{n-1}=a_{n-2}=\cdots=a_{n-m+1}=1$, $a_{n-m}=0$이고 $T^k\oplus T^{k+1}\oplus\cdots\oplus T^{k+(m-2)-i}=I(0\le i\le m-4)$ 이면 $ps(m-1-i)=k$이다.

정리 8> $a_1=a_2=\cdots=a_m=0$, $a_{m+1}=1$이면 $ps(i)=n+1-i$ $(n-m\le i\le n-1)$이다.

정리 9> $p=\min\{j\mid a_j=1,1\le j\le n-1\}$이고 $T^k\oplus T^{k+p}=I$라 하자. $a_p=1$, $a_{p+1}=0$ $(1\le p\le n-3)$이면 $ps(n-p-1)=ps(n-p)+1$이다.

정리 10> $a_1=a_2=\cdots=a_m=1, a_{m+1}=0$이고 $T^k\oplus T^{k+1}\oplus\cdots\oplus T^{k+m}=I$이면 다음을 만족한다.
$ps(n-m+i)=k+(m-i)+1$ $(0\le i\le m-1)$

예제 11> 특성다항식이 $f(x)=x^7+x^4+x^3$

$+x^2+1$인 최대길이를 생성하는 LFSM의 경우, 즉, $(a_6,a_5,a_4,a_3,a_2,a_1)=(0,0,1,1,1,0)$인 경우에 $ps(1)=0, ps(7)=1$이고, 정리 2에 의하여 $ps(2)=126, ps(3)=125$ 이다. $T^7\oplus T^4 = T^3\oplus T^2\oplus I = T^{42}$이고, $T^{89}(T^3\oplus I)=I$ 이므로 정리 4에 의하여 $ps(4)=89$이다. 정리 8에 의하여 $ps(6)=2$ 이다. $T^{20}\oplus T^{18}= T^{18}(T^2\oplus I) = I$이므로 정리 9에 의하여 $ps(5)=21$이다.

IV. LFSM의 위상이동차를 구하는 알고리즘

표 1은 3장의 정리 및 보조정리를 이용하여 최대길이를 생성하는 LFSM의 위상이동차를 구하는 알고리즘이다.

V. 결론

본 논문에서는 동반행렬의 특성다항식을 이용하여 최대길이를 갖는 n개의 n차 LFSR로 이루어진 LFSM의 위상이동차에 대한 몇 가지 정리를 얻었고, 이를 이용하여 LFSM의 위상이동차를 구하는 알고리즘을 제안하였다.

[참고문헌]

[1] J. Hong, D.H. Lee, S. Chee and P. Sarkar, Vulnerability of nonlinear filter generators based on linear finite state machine, FSE 2004, LNCS 3017, pp. 193-209, 2004.

[2] M.J. Mihaljevic, M.P.C. Fossorier and H. Imai, Cryptanalysis of keystream generator by decimated sample based algebraic and fast correlation attacks, INDOCRYPT 2005, LNCS 3797, pp. 155-168, 2005.

[3] S.J. Cho, U.S. Choi and H.D. Kim, Analysis of complemented CA derived from a linear TPMACA, Vol. 45, pp. 689-698, 2003.

[4] P.H. Bardell, Analysis of cellular automata used as pseudorandom pattern generators, Proc. IEEE int. Test. Conf., pp. 762-767, 1990.

[5] 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., Vol. 42, pp. 340-352, 1993.

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

[표1] LFSM의 위상이동차

<Algorithm. LFSM의 위상이동차>

Input : 동반행렬 T의 1열 $(a_{n-1}, a_{n-2}, \cdots, a_1, a_0)$

Output : i열의 위상이동차 $ps(i)$ $(2 \le i \le n-1)$

$ps(1) = 2^n - 1$, $ps(n) = 1$, $count = 0$, $upper = n-1$

$count = n-2$가 될 때까지 수행하라.

Step 1. Find $m = Min\{j | a_j = 1, 1 \le j < M\}$

Step 2. For $h = 1$ to $m-1$

begin

$ps(n-h) = h+1$

$count = count + 1$

endfor

Step 3. $ps(n-m) = k$ s.t. $T^k \oplus T^{k-m} = I$

$count = count + 1$

Step 4. Find $M = Max\{j | a_j = 1, m \le j \le upper\}$

Step 5. For $l = M+1$ to $n-1$

begin

$ps(n-l+1) = ps(n-l) - 1$

$count = count + 1$

endfor

Step 6. $ps(n-M+1) = k$ s.t. $T^k \oplus T^{k+(n-M)} = I$

$count = count + 1$

Step 7. $temp = a_M$, $run = 1$, $p = M-1$

While $temp = 1$

begin

$temp = temp \times a_p$

If $temp = 1$ then

begin

$ps(n-M+run+1) = k$ s.t. $T^k \oplus T^{k+1} \oplus \cdots \oplus T^{k+run} = I$

$run = run + 1$

$count = count + 1$

endif

$p = p - 1$

endwhile.

Step 8. $upper = M-1$ go to Step 4.

END