Linear Complexity and Autocorrelation of Prime Cube Sequences

Young-Joon Kim, Seok-Yong Jin and Hong-Yeop Song

{yj.kim, sy.jin, hysong}@yonsei.ac.kr
Coding and Crypto Lab
Yonsei University, Seoul, KOREA

The 18-th Joint Conference on Communications and Information
(JCCI 2008)
Jeju, Korea - Apr. 23-25, 2008

In this talk

- Previous Works
- Definition of Prime Cube Sequences
- Linear Complexity of Prime Cube Sequences
- Autocorrelation of Prime Cube Sequences
- Hardware Implementation
- Prime n-Square Sequences

Linear Complexity

- $\{s(n)\}$: a sequence of period L over a field F.
- Linear complexity C_L of $\{s(n)\}$: the least positive integer l such that there are constants $c_0 = 1, c_1, \cdots, c_l \in F$ satisfying

$$-s(i) = c_1 s(i-1) + c_2 s(i-2) + \cdots + c_l s(i-l) \quad \text{for all } l \le i < L$$

Importance of Linear complexity

- Length of the shortest linear feedback shift register to reproduce $\{s(n)\}$.
- Large C_L (when $C_L \ge L/2$)

  $\Rightarrow$ Strong against Berlekamp and Massey attack
- Small C_L

  $\Rightarrow$ Implemented easily but weak in cryptographic viewpoint

  (e.g. m-sequence)

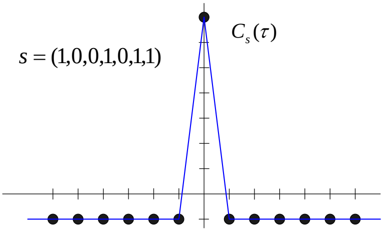
Autocorrelation

- The periodic autocorrelation of a binary sequence $\{s(n)\}$ of period L:

$$C_s(\tau) = \sum_{n=0}^{L} (-1)^{s(n+\tau)-s(n)}, \qquad 0 \le \tau < L.$$

Usage of autocorrelation

1. Determining the presence of a periodic signal which has been buried under noise (User identification)
2. Finding the exact position of repeated pattern (Synchronization)



Previous Works

- Legendre sequences: (classical) cyclotomic sequences of period p
- Ding and Helleseth (1998): period $N = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$
- Ding (1998): linear complexity of length p^2 (some mistake)
- Kim and Song (1999): linear complexity of length pq
- Dai, Gong, Song (2002): trace representation of length pq
- Park, Hong, Chun (2004): linear complexity of length p^2 (corrected)
- Bai, Liu, Xiao (2005): linear complexity of length pq
- Yan, Sun, Xiao (2007): LC and Autocor of length p^2 and pq
- Kim, Jin, Song (2007): LC and Autocor of length p^3 (and p^n ??)

Prime Square Sequence (REVIEW)

- $p = 5$
- $g = 2$: a primitive root of $p^2 = 25$
- Partitions of $\mathbf{Z}_5^*$ and $\mathbf{Z}_{25}^*$,

$$\begin{aligned}
D_0^{(5)} &= (2^2) \pmod 5 &&= \{1,4\} \\
D_1^{(5)} &= 2D_0^{(5)} \pmod 5 &&= \{2,3\} \\
D_0^{(25)} &= (2^2) \pmod{25} &&= \{1,4,6,9,11,14,16,19,21,24\} \\
D_1^{(25)} &= 2D_0^{(25)} \pmod{25} &&= \{2,3,7,8,12,13,17,18,22,23\}
\end{aligned}$$

- $C_0 = D_0^{(25)} \cup 5D_0^{(5)}$ $\quad C_1 = D_1^{(25)} \cup 5D_1^{(5)}$
- Linear Complexity : 25
- Autocorrelation

$$C_s(\tau) = \begin{cases} 25, & \tau = 0 \pmod{25} \\ -7, & \tau \in D_0^{(25)} \\ -3, & \tau \in D_1^{(25)} \\ 17, & \tau \in 5D_0^{(5)} \\ 21, & \tau \in 5D_1^{(5)} \end{cases}$$

Prime Square Sequence (REVIEW, *Yan et.al*)

- Linear Complexity

$$C_L = \begin{cases} \frac{p^2+1}{2}, & p \equiv \pm 1 \pmod 8 \\ p^2, & p \equiv \pm 3 \pmod 8 \end{cases}$$

- Autocorrelation
  1. $p \equiv 1 \pmod 4$

$$C_s(\tau) = \begin{cases} p^2, & \tau = 0 \pmod{p^2} \\ -p-2, & \tau \in D_0^{(p^2)} \\ -p+2, & \tau \in D_1^{(p^2)} \\ p^2-p-3, & \tau \in pD_0^{(p)} \\ p^2-p+1, & \tau \in pD_1^{(p)} \end{cases}$$

  2. $p \equiv 3 \pmod 4$

$$C_s(\tau) = \begin{cases} p^2, & \tau = 0 \pmod{p^2} \\ -1, & \tau \in D_0^{(p^2)} \cup D_1^{(p^2)} \\ p^2-p-1, & \tau \in pD_0^{(p)} \cup pD_1^{(p)} \end{cases}$$

Prime Cube Sequence (EXAMPLE)

- $p = 3$
- $g = 2$: a primitive root of $p^2 = 9$
- Partitions of $\mathbf{Z}_3^*$, $\mathbf{Z}_9^*$, and $\mathbf{Z}_{27}^*$

$$\begin{aligned}
D_0^{(3)} &= (2^2) \pmod 3 &&= \{1\} \\
D_1^{(3)} &= 2D_0^{(3)} \pmod 3 &&= \{2\} \\
D_0^{(9)} &= (2^2) \pmod 9 &&= \{1,4,7\} \\
D_1^{(9)} &= 2D_0^{(9)} \pmod 9 &&= \{2,5,8\} \\
D_0^{(27)} &= (2^2) \pmod{27} &&= \{1,4,7,10,13,16,19,22,25\} \\
D_1^{(27)} &= 2D_0^{(27)} \pmod{27} &&= \{2,5,8,11,14,17,20,23,26\}
\end{aligned}$$

-

$$C_0 = D_0^{(27)} \cup 3D_0^{(9)} \cup 9D_0^{(3)}$$
$$C_1 = D_1^{(27)} \cup 3D_1^{(9)} \cup 9D_1^{(3)}$$

Construction of Prime Cube Sequences

- Construction (Ding, Helleseth '98)
  - p : a prime
  - g : a primitive root of p^2
  - Define

$$D_0^{(p)} = (g^2) \pmod{p}, \qquad D_1^{(p)} = gD_0^{(p)} \pmod{p},$$
$$D_0^{(p^2)} = (g^2) \pmod{p^2}, \qquad D_1^{(p^2)} = gD_0^{(p^2)} \pmod{p^2},$$
$$D_0^{(p^3)} = (g^2) \pmod{p^3}, \qquad D_1^{(p^2)} = gD_0^{(p^3)} \pmod{p^3},$$

$$s(n) = \begin{cases} 0, & \text{if } (i \bmod p^3) \in C_0 \\ 1, & \text{if } (i \bmod p^3) \in C_1 \cup \{0\}. \end{cases}$$

where $C_0 = D_0^{(p^3)} \cup pD_0^{(p^2)} \cup p^2 D_0^{(p)}$ and $C_1 = D_1^{(p^3)} \cup pD_1^{(p^2)} \cup p^2 D_1^{(p)}$

Main Result (1) - Linear Complexity

$$C_L = \begin{cases} \frac{p^3+1}{2}, & \text{if } p \equiv 1 \bmod 8 \\ p^3 - 1, & \text{if } p \equiv 3 \bmod 8 \\ p^3, & \text{if } p \equiv 5 \bmod 8 \\ \frac{p^3-1}{2}, & \text{if } p \equiv 7 \bmod 8. \end{cases}$$

Main Result (2) - Autocorrelation

1. $p \equiv 1 \pmod 4$

$$C_s(\tau) = \begin{cases} p^3, & \tau = 0 \pmod{p^3} \\ p^3 - p - 3, & \tau \in p^2 D_0^{(p)} \\ p^3 - p + 1, & \tau \in p^2 D_1^{(p)} \\ p^3 - p^2 - p - 2, & \tau \in pD_0^{(p^2)} \\ p^3 - p^2 - p + 2, & \tau \in pD_1^{(p^2)} \\ -p^2 - 2, & \tau \in D_0^{(p^3)} \\ -p^2 + 2, & \tau \in D_1^{(p^3)} \end{cases}$$

2. $p \equiv 3 \pmod 4$

$$C_s(\tau) = \begin{cases} p^3, & \tau = 0 \pmod{p^3} \\ p^3 - p - 1, & \tau \in p^2 D_0^{(p)} \cup p^2 D_1^{(p)} \\ p^3 - p^2 - p, & \tau \in pD_0^{(p^2)} \cup pD_1^{(p^2)} \\ -p^2, & \tau \in D_0^{(p^3)} \cup D_1^{(p^3)}. \end{cases}$$

Linear Complexity and Minimal Polynomial

- $\{s(n)\}$: a sequence of period L over a field F.
- Linear complexity of $\{s(n)\}$: the least positive integer l such that there are constants $c_0 = 1, c_1, \cdots, c_l \in F$ satisfying

$$-s(i) = c_1 s(i-1) + c_2 s(i-2) + \cdots + c_l s(i-l) \text{ for all } l \leq i < L$$

- Minimal polynomial of $\{s(n)\}$: $c(x) = c_0 + c_1 x + \cdots + c_l x^l$
- $S(x) \triangleq s(0) + s(1)x + \cdots + s(L-1)x^{L-1}$

Well known facts

1. Mimimal polynomial of $\{s(n)\}$

$$c(x) = (x^L - 1)/\gcd(x^L - 1, S(x))$$

2. Linear complexity of $\{s(n)\}$

$$C_L = L - \deg(\gcd(x^L - 1, S(x)))$$

Proof of Main Result (1) - Linear Complexity

$$x^{p^3} - 1 = (x-1)\, d_0^{(p)}(x)\, d_1^{(p)}(x)\, d_0^{(p^2)}(x)\, d_1^{(p^2)}(x)\, d_0^{(p^3)}(x)\, d_1^{(p^3)}(x)$$

where, for $i = 0, 1$,

$$\begin{aligned} d_i^{(p^3)}(x) &= \prod_{a \in D_i^{(p^3)}} (x - \theta^a) && \text{of degree } \tfrac{p^3 - p^2}{2} \\ d_i^{(p^2)}(x) &= \prod_{a \in pD_i^{(p^2)}} (x - \theta^a) && \text{of degree } \tfrac{p^2 - p}{2} \\ d_i^{(p)}(x) &= \prod_{a \in p^2 D_i^{(p)}} (x - \theta^a) && \text{of degree } \tfrac{p-1}{2} \end{aligned}$$

(m : order of 2 mod p^3, θ : a primitive p^3th root of unity in $GF(2^m)$)

(SIDE): $d_i^{(p^j)}(x)$ is over $GF(2)$ $\iff$ $p \equiv \pm 1 \pmod 8$

Proof of Main Result (1) - Linear Complexity

Lemma

$S(x) = 1 + \sum_{i \in C_1} x^i$

$$\textit{Then,} \quad S(\theta^a) = \begin{cases} \frac{p+1}{2} \pmod 2, & \textit{if } a = 0 \\ S(\theta), & \textit{if } a \in D_0^{(p^3)} \\ S(\theta) + 1, & \textit{if } a \in D_1^{(p^3)} \\ \frac{p+1}{2} + t(\theta), & \textit{if } a \in pD_0^{(p^2)} \\ \frac{p-1}{2} + t(\theta), & \textit{if } a \in pD_1^{(p^2)} \\ 1 + t(\theta), & \textit{if } a \in p^2 D_0^{(p)} \\ t(\theta), & \textit{if } a \in p^2 D_1^{(p)}. \end{cases}$$

where $t(\theta) = \sum_{i \in p^2 D_1^{(p)}} \theta^i$

θ : *a primitive* p^3 *th root of unity in* $GF(2^m)$

m : *order of 2 mod* p^3

Proof of Theorem : $p \equiv 1$ mod 8 case only

From Lemma, whether the equation $S(x) = 0$ has a solution depends on the values $S(\theta), t(\theta)$ and $\frac{p+1}{2}$.

- $t(\theta) \in \{0, 1\} \iff 2 \in D_0^{(p)} \iff p \equiv \pm 1 \pmod 8$ [Ding 1998]
- $S(\theta) \in \{0, 1\} \iff p \equiv \pm 1 \pmod 8$
  - $2 \in D_i^{(p^3)} \iff 2 \in D_i^{(p^2)} \iff 2 \in D_i^{(p)}$ for $i = 0, 1$.
  - $S(\theta)^2 = S(\theta^2) = S(\theta) \quad (\because \quad 2 \in D_0^{(p^3)} \iff p \equiv \pm 1 \pmod 8)$

Proof of Main Result (1) : $p \equiv 1 \bmod 8$ case

$(S(\theta), t(\theta))$	$=$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	
			$S(\theta^a)$			*corres.poly.*
$a = 0$	$\frac{p+1}{2} \pmod 2$	1	1	1	1	$x+1$
$a \in D_0^{(p^3)}$	$S(\theta)$	0	0	1	1	$d_0^{(p^3)}$
$a \in D_1^{(p^3)}$	$S(\theta)+1$	1	1	0	0	$d_1^{(p^3)}$
$a \in pD_0^{(p^2)}$	$\frac{p+1}{2} + t(\theta)$	1	0	1	0	$d_0^{(p^2)}$
$a \in pD_1^{(p^2)}$	$\frac{p-1}{2} + t(\theta)$	0	1	0	1	$d_1^{(p^2)}$
$a \in p^2 D_0^{(p)}$	$1 + t(\theta)$	1	0	1	0	$d_0^{(p)}$
$a \in p^2 D_1^{(p)}$	$t(\theta)$	0	1	0	1	$d_1^{(p)}$

Proof of Main Result (1) : $p \equiv 1 \bmod 8$ case

$$\gcd(x^{p^3}-1, S(x)) = \begin{cases} d_0^{(p^3)}(x) d_1^{(p^2)}(x) d_1^{(p)}(x), & \text{if } S(\theta), t(\theta) = (0,0) \\ d_0^{(p^3)}(x) d_0^{(p^2)}(x) d_0^{(p)}(x), & \text{if } S(\theta), t(\theta) = (0,1) \\ d_1^{(p^3)}(x) d_1^{(p^2)}(x) d_1^{(p)}(x), & \text{if } S(\theta), t(\theta) = (1,0) \\ d_1^{(p^3)}(x) d_0^{(p^2)}(x) d_0^{(p)}(x), & \text{if } S(\theta), t(\theta) = (1,1) \end{cases}$$

It follows that

$$C_L = p^3 - \deg(\gcd(x^{p^3}-1, S(x))) = p^3 - \{\frac{p^3-p^2}{2} + \frac{p^2-p}{2} + \frac{p-1}{2}\} = \frac{p^3+1}{2}.$$

End of Proof ■

Theorem (Autocorrelation of prime cube sequence of period p^3)

1. $p \equiv 1 \pmod 4$

$$C_s(\tau) = \begin{cases} p^3, & \tau = 0 \pmod{p^3} \\ p^3 - p - 3, & \tau \in p^2 D_0^{(p)} \\ p^3 - p + 1, & \tau \in p^2 D_1^{(p)} \\ p^3 - p^2 - p - 2, & \tau \in p D_0^{(p^2)} \\ p^3 - p^2 - p + 2, & \tau \in p D_1^{(p^2)} \\ -p^2 - 2, & \tau \in D_0^{(p^3)} \\ -p^2 + 2, & \tau \in D_1^{(p^3)} \end{cases}$$

2. $p \equiv 3 \pmod 4$

$$C_s(\tau) = \begin{cases} p^3, & \tau = 0 \pmod{p^3} \\ p^3 - p - 1, & \tau \in p^2 D_0^{(p)} \cup p^2 D_1^{(p)} \\ p^3 - p^2 - p, & \tau \in p D_0^{(p^2)} \cup p D_1^{(p^2)} \\ -p^2, & \tau \in D_0^{(p^3)} \cup D_1^{(p^3)}. \end{cases}$$

Proof of Autocorrelation

- The periodic autocorrelation of a binary sequence $\{s(n)\}$ of period L:

$$C_s(\tau) = \sum_{n=0}^{L} (-1)^{s(n+\tau)-s(n)}, \qquad 0 \le \tau < L.$$

- Define

$$d_s(i,j;\tau) = |C_i \cap (C_j + \tau)|, \quad 0 \le \tau < L, \; i,j = 0,1$$

  Here, we use C_1 containing $\{0\}$ (back to paper)

- Note that $C_s(\tau) = p^3 - 4d_s(1,0;\tau)$,

$$\begin{aligned} d_s(1,0;\tau) &= |C_1 \cap (C_0 + \tau)| \\ &= \underbrace{|C_1 \cap (p^2 D_0^{(p)} + \tau)|}_{\triangleq A(\tau)} + \underbrace{|C_1 \cap (pD_0^{(p^2)} + \tau)|}_{\triangleq B(\tau)} + \underbrace{|C_1 \cap (D_0^{(p^3)} + \tau)|}_{\triangleq C(\tau)} \end{aligned}$$

Proof of Autocorrelation

$$A(\tau) = |C_1 \cap (p^2 D_0^{(p)} + \tau)| =$$

$$\underbrace{|\{0\} \cap (p^2 D_0^{(p)} + \tau)|}_{\triangleq A_1(\tau)} + \underbrace{|p^2 D_1^{(p)} \cap (p^2 D_0^{(p)} + \tau)|}_{\triangleq A_2(\tau)} + \underbrace{|p D_1^{(p^2)} \cap (p^2 D_0^{(p)} + \tau)|}_{\triangleq A_3(\tau)} + \underbrace{|D_1^{(p^3)} \cap (p^2 D_0^{(p)} + \tau)|}_{\triangleq A_4(\tau)}$$

$$B(\tau) = |C_1 \cap (p D_0^{(p^2)} + \tau)| =$$

$$|\{0\} \cap (p D_0^{(p^2)} + \tau)| + |p^2 D_1^{(p)} \cap (p D_0^{(p^2)} + \tau)| + |p D_1^{(p^2)} \cap (p D_0^{(p^2)} + \tau)| + |D_1^{(p^3)} \cap (p D_0^{(p^2)} + \tau)|$$

$$C(\tau) = |C_1 \cap (D_0^{(p^3)} + \tau)| =$$

$$|\{0\} \cap (D_0^{(p^3)} + \tau)| + |p^2 D_1^{(p)} \cap (D_0^{(p^3)} + \tau)| + |p D_1^{(p^2)} \cap (D_0^{(p^3)} + \tau)| + |D_1^{(p^3)} \cap (D_0^{(p^3)} + \tau)|$$

Proof of Autocorrelation

$p \equiv 1 \bmod 4$	$A_1(\tau)$	$A_2(\tau)$	$A_3(\tau)$	$A_4(\tau)$	$A(\tau)$
$\tau \in p^2 D_0^{(p)}$	1	$(0,1)_p$	0	0	$\frac{p+3}{4}$
$\tau \in p^2 D_1^{(p)}$	0	$(1,0)_p$	0	0	$\frac{p-1}{4}$
$\tau \in pD_1^{(p^2)}$	0	0	$\frac{p-1}{2}$	0	$\frac{p-1}{2}$
$\tau \in D_1^{(p^3)}$	0	0	0	$\frac{p-1}{2}$	$\frac{p-1}{2}$
otherwise	0	0	0	0	0

$p \equiv 3 \bmod 4$	$A_1(\tau)$	$A_2(\tau)$	$A_3(\tau)$	$A_4(\tau)$	$A(\tau)$
$\tau \in p^2 D_0^{(p)}$	0	$(0,1)_p$	0	0	$\frac{p+1}{4}$
$\tau \in p^2 D_1^{(p)}$	1	$(1,0)_p$	0	0	$\frac{p+1}{4}$
$\tau \in pD_1^{(p^2)}$	0	0	$\frac{p-1}{2}$	0	$\frac{p-1}{2}$
$\tau \in D_1^{(p^3)}$	0	0	0	$\frac{p-1}{2}$	$\frac{p-1}{2}$
otherwise	0	0	0	0	0

Proof of Autocorrelation

$p \equiv 1 \bmod 4$	$B_1(\tau)$	$B_2(\tau)$	$B_3(\tau)$	$B_4(\tau)$	$B(\tau)$
$\tau \in pD_0^{(p^2)}$	1	$\frac{p-1}{2}$	$(0,1)_{p^2}$	0	$\frac{p^2+p+2}{4}$
$\tau \in pD_1^{(p^2)}$	0	0	$(1,0)_{p^2}$	0	$\frac{p(p-1)}{4}$
$\tau \in D_1^{(p^3)}$	0	0	0	$\frac{p^2-p}{2}$	$\frac{p^2-p}{2}$
otherwise	0	0	0	0	0

$p \equiv 3 \bmod 4$	$B_1(\tau)$	$B_2(\tau)$	$B_3(\tau)$	$B_4(\tau)$	$B(\tau)$
$pD_0^{(p^2)}$	0	0	$(0,1)_{p^2}$	0	$\frac{p(p+1)}{4}$
$\tau \in pD_1^{(p^2)}$	1	$\frac{p-1}{2}$	$(1,0)_{p^2}$	0	$\frac{p^2-p+2}{4}$
$\tau \in D_1^{(p^3)}$	0	0	0	$\frac{p^2-p}{2}$	$\frac{p^2-p}{2}$
otherwise	0	0	0	0	0

Proof of Autocorrelation

$p \equiv 1 \bmod 4$	$C_1(\tau)$	$C_2(\tau)$	$C_3(\tau)$	$C_4(\tau)$	$C(\tau)$
$\tau \in D_0^{(p^3)}$	1	$\frac{p-1}{2}$	$\frac{p^2-p}{2}$	$(0,1)_{p^3}$	$\frac{p^3+p^2+2}{4}$
$\tau \in D_1^{(p^3)}$	0	0	0	$(1,0)_{p^3}$	$\frac{p^3-p^2}{4}$
otherwise	0	0	0	0	0

$p \equiv 3 \bmod 4$	$C_1(\tau)$	$C_2(\tau)$	$C_3(\tau)$	$C_4(\tau)$	$C(\tau)$
$\tau \in D_0^{(p^3)}$	0	0	0	$(0,1)_{p^3}$	$\frac{p^3+p^2}{4}$
$\tau \in D_1^{(p^3)}$	1	$\frac{p-1}{2}$	$\frac{p^2-p}{2}$	$(1,0)_{p^3}$	$\frac{p^3-p^2+2}{4}$
otherwise	0	0	0	0	0

Hardware Implementation

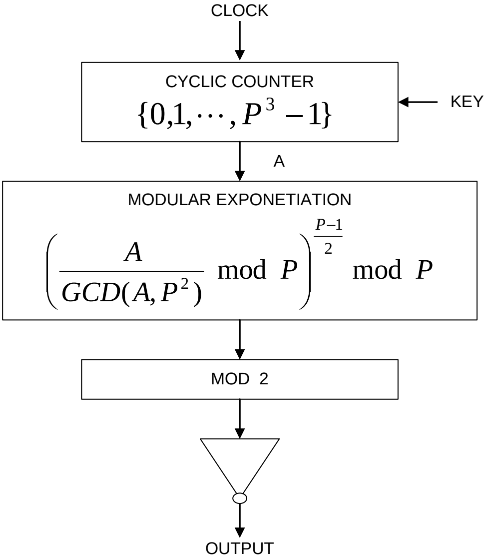
- Cyclic Counter of period p^3
- If $a \in D_i^{(p^k)}$, $a \bmod p \in D_i^{(p)}$ for $i = 0, 1$, $k \in \{0, 1, 2\}$
- For each $0 \le a \le p^3$, consider

$$V \triangleq \left[\left\{ \frac{a}{\gcd(a, p^2)} \bmod p \right\}^{\frac{p-1}{2}} + 1 \right] \bmod p$$

1. $a = 0 \quad : \quad V = 1$
2. $a \in D_i^{(p^3)} : V = (-1)^i + 1 \pmod{p} \equiv \frac{1+(-1)^i}{2} \pmod{2}$
3. $a \in pD_i^{(p^2)} : V = (-1)^i + 1 \pmod{p} \equiv \frac{1+(-1)^i}{2} \pmod{2}$
4. $a \in p^2 D_i^{(p)} : V = (-1)^i + 1 \pmod{p} \equiv \frac{1+(-1)^i}{2} \pmod{2}$

$$\Longrightarrow \quad V = s(a)$$

Hardware Implementation



What about prime n-Square Sequence?

Autocorrelation

$\Rightarrow$ Essentially DONE

by Ding and Helleseth in 1998

Linear Complexity

- We are sure that it is of order p^n
- Can be DONE!

Hardware Implementation (?)