Linear Complexity of Prime n-Square Sequences

Young-Joon Kim and Hong-Yeop Song

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

2008 IEEE International Symposium on Information Theory,
Sheraton Centre Toronto Hotel, Toronto
July 6-11, 2008

In this talk

- Previous Works
- Definition of Prime n-Square Sequences
- Linear Complexity
- Hardware Implementation
- Concluding Remarks

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, Helleseth, Shan (1998): linear complexity of length p
- Ding (1998): linear complexity of length p^2 (some mistake)
- Kim and Song (1999): linear complexity of length pq
- Kim and Song (2001): trace representation of length p
- 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
- Kim, Song (2008): LC and Autocor. of length 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 (REVIEW)

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

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

-

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

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

Prime Cube Sequences (REVIEW, *Kim et. al*)

Linear Complexity

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

Prime Cube Seq. (REVIEW, *Kim et. al*)

Autocorrelation

1. $p \equiv 1 \pmod 4$

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

2. $p \equiv 3 \pmod 4$

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

What about prime n-Square Sequence?

Construction of Prime n-Square Sequences

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

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

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

where $C_0 = \left(\bigcup_{k=1}^{n} p^{n-k} D_0^{(p^k)}\right)$ and $C_1 = \left(\bigcup_{k=1}^{n} p^{n-k} D_1^{(p^k)}\right)$

Main Result - Linear Complexity

When n is even,

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

When n is odd,

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

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 - Linear Complexity

$$x^{p^n} - 1 = (x-1)\prod_{k=1}^{n} d_0^{(p^k)}(x) \prod_{k=1}^{n} d_1^{(p^k)}(x).$$

where, for $i = 0, 1$, and $k = 1, 2, \cdots, n$

$$d_i^{(p^k)}(x) = \prod_{a \in p^{n-k} D_i^{(p^k)}} (x - \theta^a) \quad \text{of degree} \quad \frac{p^k - p^{k-1}}{2}$$

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

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

Proof of Main Result - Linear Complexity

Key Lemma

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

Then, $$S(\theta^a) = \begin{cases} \frac{p^n+1}{2} \pmod 2, & \text{if } a = 0 \\ \frac{p^{n-k}+1}{2} + t(\theta), & \text{if } a \in p^{n-k} D_0^{(p^k)} \text{ and } k = 1, 2, \ldots, n \\ \frac{p^{n-k}-1}{2} + t(\theta), & \text{if } a \in p^{n-k} D_1^{(p^k)} \text{ and } k = 1, 2, \ldots, n \end{cases}$$

where $t(\theta) = \sum_{i \in p^{n-1} D_1^{(p)}} \theta^i$

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

m : order of 2 mod p^n

Proof of Theorem :

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

- $t(\theta) \in \{0, 1\} \iff 2 \in D_0^{(p)} \iff p \equiv \pm 1 \pmod 8$ [Ding 1998]
- $p^{2k} = (2z+1)^{2k} = \sum_{i=2}^{2k} \binom{2k}{i} (2z)^i + 4kz + 1 \equiv 1 \pmod 4$
- $p^{2k+1} = (2z+1)^{2k+1} = \sum_{i=2}^{2k+1} \binom{2k+1}{i} (2z)^i + 4kz + 2z + 1 \equiv p \pmod 4$

LC : n even

- $p \equiv 1 \bmod 8, \quad t(\theta) \in \{0,1\}$ and $p^{2k} \equiv p^{2k+1} \equiv 1 \pmod 4$

$$S(\theta^a) = \begin{cases} 1, & \text{if } a = 0 \\ 1 + t(\theta), & \text{if } a \in p^{n-k} D_0^{(p^k)} \text{ and } k = 1, 2, \cdots, n \\ t(\theta), & \text{if } a \in p^{n-k} D_1^{(p^k)} \text{ and } k = 1, 2, \cdots, n. \end{cases}$$

Therefore,

$$m(x) = \frac{x^{p^n} - 1}{\gcd(x^{p^n} - 1, S(x))} = \begin{cases} (x-1) \prod_{k=1}^{n} d_0^{(p^k)}(x), & \text{if } t(\theta) = 0 \\ (x-1) \prod_{k=1}^{n} d_1^{(p^k)}(x), & \text{if } t(\theta) = 1 . \end{cases}$$

It follows that

$$L(s^\infty) = \deg(m(x)) = 1 + \sum_{k=1}^{n} \frac{p^k - p^{k-1}}{2} = \frac{p^n + 1}{2}.$$

LC : n even (*continued*)

- $p \equiv 3 \bmod 8, \quad t(\theta) \notin \{0,1\}, \; p^{2k} \equiv 1 \pmod 4$, and $p^{2k+1} \equiv 3 \pmod 4$

$$S(\theta^a) = \begin{cases} 1, & \text{if } a = 0 \\ t(\theta), & \text{if } a \in p^{n-k} D_0^{(p^k)} \text{ and } k = \text{odd} \\ 1 + t(\theta), & \text{if } a \in p^{n-k} D_0^{(p^k)} \text{ and } k = \text{even} \\ 1 + t(\theta), & \text{if } a \in p^{n-k} D_1^{(p^k)} \text{ and } k = \text{odd} \\ t(\theta), & \text{if } a \in p^{n-k} D_1^{(p^k)} \text{ and } k = \text{even.} \end{cases}$$

Therefore,

$$m(x) = \frac{x^{p^n} - 1}{\gcd(x^{p^n} - 1, S(x))} = x^{p^n} - 1.$$

It follows that $L(s^\infty) = \deg(m(x)) = p^n$.

Minimal Polynomial : n even

- $p \equiv 1 \bmod 8$,

$$m(x) = \frac{x^{p^n} - 1}{\gcd(x^{p^n} - 1, S(x))}$$
$$= \begin{cases} (x-1)\prod_{k=1}^{n} d_0^{(p^k)}(x), & \text{if} \quad t(\theta) = 0 \\ (x-1)\prod_{k=1}^{n} d_1^{(p^k)}(x), & \text{if} \quad t(\theta) = 1 \,. \end{cases}$$

- $p \equiv \pm 3 \bmod 8$,

$$m(x) = x^{p^n} - 1.$$

- $p \equiv 7 \bmod 8$,

$$m(x) = \begin{cases} (x-1)\prod_{k=1}^{\frac{n}{2}} d_0^{(p^{2k})}(x)\prod_{k=1}^{\frac{n}{2}} d_1^{(p^{2k-1})}(x), & \text{if} \quad t(\theta) = 0 \\ (x-1)\prod_{k=1}^{\frac{n}{2}} d_0^{(p^{2k-1})}(x)\prod_{k=1}^{\frac{n}{2}} d_1^{(p^{2k})}(x), & \text{if} \quad t(\theta) = 1 \,. \end{cases}$$

Minimal Polynomial : n odd

- $p \equiv 1 \bmod 8$,

$$m(x) = \begin{cases} (x-1)\prod_{k=1}^{n} d_0^{(p^k)}(x), & \text{if} \quad t(\theta)=0 \\ (x-1)\prod_{k=1}^{n} d_1^{(p^k)}(x), & \text{if} \quad t(\theta)=1\ . \end{cases}$$

- $p \equiv 3 \bmod 8$,

$$m(x) = \frac{x^{p^n}-1}{x-1}.$$

- $p \equiv 5 \bmod 8$,

$$m(x) = x^{p^n}-1.$$

- $p \equiv 7 \bmod 8$,

$$m(x) = \begin{cases} \prod_{k=1}^{\frac{n+1}{2}} d_0^{(p^{2k-1})}(x) \prod_{k=1}^{\frac{n-1}{2}} d_1^{(p^{2k})}(x), & \text{if} \quad t(\theta)=0 \\ \prod_{k=1}^{\frac{n-1}{2}} d_0^{(p^{2k})}(x) \prod_{k=1}^{\frac{n+1}{2}} d_1^{(p^{2k-1})}(x), & \text{if} \quad t(\theta)=1\ . \end{cases}$$

Key Lemma

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

Then,
$$S(\theta^a) = \begin{cases} \frac{p^n+1}{2} \pmod 2, & \text{if } a = 0 \\ \frac{p^{n-k}+1}{2} + t(\theta), & \text{if } a \in p^{n-k} D_0^{(p^k)} \text{ and } k = 1, 2, \ldots, n \\ \frac{p^{n-k}-1}{2} + t(\theta), & \text{if } a \in p^{n-k} D_1^{(p^k)} \text{ and } k = 1, 2, \ldots, n \end{cases}$$

where $t(\theta) \triangleq \sum_{i \in p^{n-1} D_1^{(p)}} \theta^i$

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

m : order of 2 mod p^n

Proof of Key Lemma

- When $a = 0$,

$$S(\theta^a) = S(1) = 1 + \sum_{k=1}^{n} |p^{n-k} D_1^{(p^k)}| = \frac{p^n + 1}{2} \pmod 2$$

Proof of Key Lemma

- When $a \in p^{n-k}D_0^{(p^k)} \cup p^{n-k}D_1^{(p^k)}$ for $k = 1, 2, \cdots, n$,
  - For any positive integer i satisfying $n-k+i \le n-1$

$$p^i \cdot p^{n-k}D_0^{(p^k)} \pmod{p^n} = p^{n-k+i}D_0^{(p^{k-i})} \pmod{p^n} \quad \text{and}$$
$$\left| p^i \cdot p^{n-k}D_0^{(p^k)} \pmod{p^n} \right| = p^i \cdot \left| p^{n-k+i}D_0^{(p^{k-i})} \pmod{p^n} \right|. \quad (1)$$

$$\begin{aligned} D_0^{(27)} &= \{1,4,7,10,13,16,19,22,25\}, & D_1^{(27)} &= \{2,5,8,11,14,17,20,23,26\} \\ 3D_0^{(27)} &= \{3,12,21,3,12,21,3,12,21\} & 3D_1^{(27)} &= \{6,15,24,6,15,24,6,15,24\} \\ &\equiv \{3,12,21\} = 3D_0^{(9)}, & &\equiv \{6,15,24\} = 3D_1^{(9)} \\ 9D_0^{(27)} &= \{9,9,9,9,9,9,9,9,9\} & 9D_1^{(27)} &= \{18,18,18,18,18,18,18,18,18\} \\ &\equiv \{9\} = 9D_0^{(3)}, & &\equiv \{18\} = 9D_1^{(3)} \end{aligned}$$

  - For any positive integer i such that $n-k+i \ge n$,

$$p^i \cdot p^{n-k}D_0^{(p^k)} \pmod{p^n} = \{0\} \pmod{p^n}. \quad (2)$$

Proof of Key Lemma

- When $a \in p^{n-k}D_0^{(p^k)} \cup p^{n-k}D_1^{(p^k)}$ for $k = 1, 2, \cdots, n$,

  Let $a = p^{n-k}b$ for some $b \in Z_{p^k}^* = D_0^{(p^k)} \cup D_1^{(p^k)}$.

$$S(\theta^a) = 1 + \Big(\sum_{i \in p^{n-k}D_1^{(p^n)}} + \sum_{i \in p^{n-k+1}D_1^{(p^{n-1})}} + \cdots + \sum_{i \in p^{n-k+n-1}D_1^{(p)}} \Big)\theta^{bi}$$

$$= 1 + p^{n-k} \cdot \big(\underbrace{\sum_{i \in p^{n-k}D_1^{(p^k)}} + \sum_{i \in p^{n-k+1}D_1^{(p^{n-k-1})}} + \cdots + \sum_{i \in p^{n-1}D_1^{(p)}}}_{k \text{ summations } (\because \text{eq. } (1))} \big)\theta^{bi}$$

$$+ \big(\underbrace{\sum_{i \in p^n D_1^{(p^{n-k})}} + \cdots + \sum_{i \in p^{n-k+n-1}D_1^{(p)}}}_{n-k \text{ summations}} \big)\theta^{b \cdot i} \qquad (3)$$

Proof of Key Lemma

- From equation (2), latter $n-k$ summations become $\frac{p^{n-k}-1}{2}$. Therefore, the equation (3) can be simplified as follows.

$$S(\theta^a) = \frac{p^{n-k}+1}{2} + p^{n-k} \cdot \Big(\sum_{i \in p^{n-k} D_1^{(p^k)}} + \sum_{i \in p^{n-k+1} D_1^{(p^{n-k-1})}} + \cdots + \sum_{i \in p^{n-1} D_1^{(p)}} \Big) \theta^{bi}$$

- When $b \in D_0^{(p^k)}$,

  Since $bD_i^{(p^j)} \pmod{p^j} = D_i^{(p^j)} \pmod{p^j}$ for $j = 1, 2, \cdots, k$,

$$bp^{n-j} D_i^{(p^j)} = p^{n-j} D_i^{(p^j)} \quad \text{for } i = 0, 1.$$

- When $b \in D_1^{(p^k)}$,

$$bp^{n-j} D_i^{(p^j)} = p^{n-j} D_{i+1 \pmod 2}^{(p^j)} \quad \text{for } i = 0, 1.$$

Proof of Key Lemma

$$S(\theta^a) = \begin{cases} \frac{p^{n-k}+1}{2} + p^{n-k}\cdot(\sum_{i\in p^{n-k}D_1^{(p^k)}} + \cdots + \sum_{i\in p^{n-1}D_1^{(p)}})\theta^i, & \text{if } b\in D_0^{(p^k)} \\ \frac{p^{n-k}+1}{2} + p^{n-k}\cdot(\sum_{i\in p^{n-k}D_0^{(p^k)}} + \cdots + \sum_{i\in p^{n-1}D_0^{(p)}})\theta^i, & \text{if } b\in D_1^{(p^k)} \end{cases}$$

$$= \begin{cases} \frac{p^{n-k}+1}{2} + t(\theta), & \text{if } b\in D_0^{(p^k)} \\ \frac{p^{n-k}-1}{2} + t(\theta), & \text{if } b\in D_1^{(p^k)} \end{cases}, \quad \text{where } t(\theta) = \sum_{i\in p^{n-1}D_1^{(p)}} \theta^i \qquad (4)$$

Sub Lemma

For $k = 2, \cdots, n$,

$$\sum_{i\in p^{n-k}D_0^{(p^k)}} \theta^i = \sum_{i\in p^{n-k}D_1^{(p^k)}} \theta^i = 0.$$

EXTRA - What about autocorrelation of prime n-Square Sequence?

EXTRA - *IT submitted*

Theorem (Autocorrelation of prime n-square seq. of period p^n)

1. $p \equiv 1 \pmod 4$

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

2. $p \equiv 3 \pmod 4$

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

Hardware Implementation

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

$$V \triangleq 1 \oplus \left\lfloor \left\lfloor \left\{ \frac{a}{\gcd(a, p^{n-1})} \bmod p \right\}^{\frac{p-1}{2}} \bmod p \right\rfloor \bmod 2. \right\rfloor$$

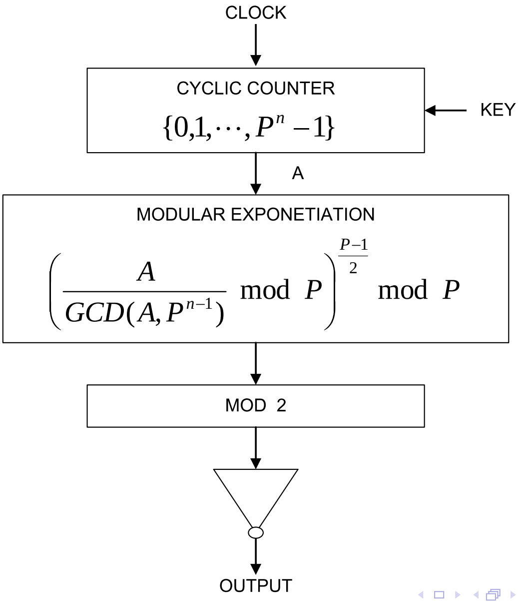
1. $a = 0 \quad : \quad V = 1$
2. $a \in p^{n-k} D_i^{(p^k)} : \gcd(a, p^{n-1}) = p^{n-k}$

So $\left\{ \frac{a}{\gcd(a, p^{n-1})} \bmod p \right\}^{\frac{p-1}{2}} = \{D_i^{(p^k)} \pmod{p}\}^{\frac{p-1}{2}} = \{D_i^{(p)}\}^{\frac{p-1}{2}} = (-1)^i \pmod{p}$

$$s(a) = 1 \oplus \left\{ \frac{a}{\gcd(a, p^{n-1})} \bmod p \right\}^{\frac{p-1}{2}}$$

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

Hardware Implementation



Concluding Remarks

- In this paper, we determine the linear complexity C_L of prime n-square sequences of period p^n by computing of degree of the minimal polynomial.
- The minimal polynomial of these sequences can be changed depending on the value of $t(\theta)$. Nevertheless, we compute the linear complexity completely.

When n is even,

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

When n is odd,

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