Constructions for favorable sequences family using Sidelnikov sequences

ITA 2014
Feb. 10-14

Hong-Yeop Song
Yonsei University
Seoul, Korea

Dae San Kim
Sogang University
Seoul, Korea
Motivation

- Synchronization, Distinguishing users, Interference minimization, Higher resolution RADAR,…

- 1969 – Sidelnikov (autocorrelation property only)

- 2007~Present – Sequence families from Sidelnikov sequences

Purpose

- Sequence families with larger size
- Sequence families with lower correlation magnitude
Brief History and Main Contribution

(SONG-07) Sequence family constructions from Sidelnikov sequences have been considered, by using constant multiples

(NO-08, YANG-09) Family size increased by additionally using shift-and-adds

(GONG-10) 2-D array structure of size \((q - 1) \times \left(\frac{q^2-1}{q-1}\right)\)

(KIM-10) 2-D array structure of size \((q - 1) \times \left(\frac{q^d-1}{q-1}\right)\) with \((d, q - 1) = 1\)

(This paper) 2-D array structure of size \((q - 1) \times \left(\frac{q^d-1}{q-1}\right)\)

without \((d, q - 1) = 1\)

maintaining the family size “comparable” to the above

and the correlation bound the same as the above
Notation

- $p$: prime
- $q = p^n$: prime power or prime
- $GF(q)$: finite field of order $q$
- $GF(q^d)$: finite field of order $q^d$ with $2 \leq d < (\sqrt{q} - \frac{2}{\sqrt{q}} + 1)/2$
- $\alpha$: arbitrary but fixed primitive element of $GF(q^d)$
- $\beta = \alpha^{(q^d-1)/(q-1)}$: the primitive element of $GF(q)$
- $\omega_M$: complex $M^{th}$ root of unity, where $M|q - 1$
- $\psi$: the **multiplicative character of order** $M$ from $GF(q)$, defined by

$$
\psi(x) = \exp\left(\frac{2\pi i}{M} \log_{\beta} x\right) = \omega_M^{\log_{\beta} x}
$$

and

$$
\psi(0) = 1.
$$
Sidelnikov Sequences of period $q-1$

- $\text{GF}(q)$ = finite field of size $q$ where $q = p^n$
- $\beta$ = primitive element of $\text{GF}(q)$
- $M$ = a divisor of $q - 1$
- **Coset Partition**
  - $D_0$: the set of $M$-th powers in $\text{GF}(q)^*$
  - $D_k = \beta^k \cdot D_0$ for $0 \leq k \leq M-1$

- An $M$-ary Sidelnikov sequence of period $q - 1$ is defined as, for $t = 0, 1, 2, \ldots, q-2$,

\[
s(t) = \begin{cases} 
0, & \text{if } \beta^t + 1 = 0 \\
 k, & \text{if } \beta^t + 1 \in D_k 
\end{cases}
\]
(Example) $p = q = 13, \quad M = 3, \quad \beta = 2$

- $D_0 = 2^0 \cdot D_0 = \{1, 5, 8, 12\} = \text{cubic residues mod } 13$
- $D_1 = 2^1 \cdot D_0 = \{2, 10, 3, 11\}$
- $D_2 = 2^2 \cdot D_0 = \{4, 7, 6, 9\}$

<table>
<thead>
<tr>
<th>$t$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta^t = 2^t$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>$\beta^t + 1$</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>7</td>
<td>0</td>
<td>12</td>
<td>10</td>
<td>6</td>
<td>11</td>
<td>8</td>
</tr>
<tr>
<td>belongs to</td>
<td>$D_1$</td>
<td>$D_1$</td>
<td>$\text{?}$</td>
<td>$D_1$</td>
<td>$D_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S(t)$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
$$s(t) \equiv \log_\beta (\beta^t + 1) \pmod{12}$$

Is this ADDONE table of the finite field GF(13)?

<table>
<thead>
<tr>
<th>t</th>
<th>$\beta^t$</th>
<th>$\beta^t + 1$</th>
<th>$\log_\beta (\beta^t + 1)$ (mod 12)</th>
<th>(mod 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>$\beta = 2$</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>$\beta^2 = 4$</td>
<td>5</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>$\beta^3 = 8$</td>
<td>9</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>$\beta^4 = 16 = 3$</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>$\beta^5 = 6$</td>
<td>7</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>$\beta^6 = 12$</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>12</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>8</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
Sidelnikov Sequences
(alternative definition)

The M-ary Sidelnikov sequence \( s(t) \) of period \( q - 1 \) is defined by, for \( 0 \leq t \leq q - 2 \),

\[
s(t) \equiv \log_\beta (\beta^t + 1) \mod M,
\]

where we assume that \( \log_\beta(0) = 0 \).
2-D array structure of size \((q - 1) \times \left(\frac{q^2-1}{q-1}\right)\)

Write a Sidelnikov sequence of period \(q^2 - 1\) as an array of size \((q - 1) \times (q + 1)\).

1) the first column sequence is always a constant-multiple of a Sidelnikov sequence of period \(q - 1\).
2) other column sequences of period \(q - 1\) (not necessarily Sidelnikov sequences) have GOOD correlations
   - NOT ONLY with each other
   - BUT ALSO with previously constructed family members of period \(q - 1\) if they are not cyclically equivalent to each other.

→ Nontrivial increase in the family size
Theorem (Gong-10)

Let $\mathcal{U}$ be the set of sequences of period $q - 1$ given as follows:

\[
\mathcal{U} = \{cs(t) | 1 \leq c \leq M - 1\} \cup \left\{c_0s(t) + c_1s(t + l_1) | 1 \leq l_1 \leq \left\lfloor \frac{q - 1}{2} \right\rfloor \right\} \cup \left\{c_2v_{l_2}(t) | 1 \leq l_2 \leq \left\lfloor \frac{q}{2} \right\rfloor \right\}.
\]

Then,

1. The maximum correlation of $\mathcal{U}$ is upper bounded by $3\sqrt{q} + 5$.
2. This family have size $\frac{M(M-1)(q-2)}{2} + M - 1$.

If $v_l(t)$ is the column sequence of the $(q-1) \times (q+1)$ array of a Sidelnikov sequence of period $q^2 - 1$ given by

\[
\log_\alpha(\alpha^t + 1) \mod M,
\]

Then $s(t)$ must be the Sidelnikov sequence of period $q - 1$ given by

\[
\log_\beta(\beta^t + 1) \mod M \text{ where } \beta = \alpha^{(q^2-1)/(q-1)} = \alpha^{q+1}.
\]
Kim’s Generalization

D.S. Kim, 2010: A family of sequences with large size and good correlation property arising from M-ary Sidelnikov sequences of period $q^d - 1$, arXiv:1009.1225v1 [cs.IT]

Why not considering a sidelnikov sequence of period $q^3 - 1$, $q^4 - 1$ or $q^d - 1$ in general in the first place and then using an array of size $(q - 1) \times \left(\frac{q^d - 1}{q - 1}\right)$?
Key Observation – Theorem and remark

- To analyze the column sequences of the array, one has to represent the Sidelnikov sequence of period $q^d - 1$ using a primitive element of GF($q$).

- **THEOREM:**

  Let $\alpha$ be a primitive element of GF($q^d$).
  
  $\beta = \alpha^{(q^d-1)/(q-1)}$: the primitive element of GF($q$)

  For period $q^d - 1$, we have
  
  $$s(t) \equiv \log_{\beta}N(\alpha^t + 1) \mod M.$$  

- **REMARK:** when $d = 2$, it becomes that

  $$N(\alpha^t + 1) = (\alpha^t + 1)^{\frac{q^2-1}{q-1}} = (\alpha^t + 1)^{q+1} = (\alpha^t + 1)^q(\alpha^t + 1)$$

  $$= \alpha^{(q+1)t} + \alpha^{qt} + \alpha^t + 1 = \beta^t + 1 + \text{Tr}(\alpha^t)$$
Let $\alpha$ be a primitive element of $\text{GF}(q^d)$.

For period $q^d - 1$, denote $y(t) \equiv \log_\alpha (\alpha^t + 1) \mod q^d - 1$.

Assume that $N(\alpha^t + 1) \neq 0$. Then $N(\alpha^t + 1) = \beta^{x(t)}$.

This gives:

$$\frac{q^d-1}{q-1} y(t) \equiv \frac{q^d-1}{q-1} \log_\alpha (\alpha^t + 1) \equiv \log_\alpha (\alpha^t + 1) \frac{q^d-1}{q-1}$$

$$\equiv \log_\alpha N(\alpha^t + 1) \equiv \log_\alpha \beta^{x(t)} \equiv \log_\alpha \alpha^{\frac{q^d-1}{q-1}x(t)}$$

$$\equiv \frac{q^d-1}{q-1} x(t) \mod q^d - 1$$

Since $\left(\frac{q^d-1}{q-1}, q^d - 1\right) = \frac{q^d-1}{q-1}$, we have:

$$x(t) \equiv y(t) \equiv \log_\beta N(\alpha^t + 1) \mod q - 1 \text{ (and hence, mod } M).$$
Columns of the Array Structure

Let \( d \geq 2 \), and write a Sidelnikov sequence of period \( q^d - 1 \) as an array of size \((q - 1) \times \frac{q^d - 1}{q-1}\). Then, the column sequences \( v_l(t) \) of the array can be represented as

\[
v_l(t) \equiv \log_{\beta} f_l(\beta^t) \pmod{M}
\]

where \( f_l(x) = N(\alpha^lx + 1) \).

**Proof:**

\[
v_l(t) \equiv s \left( \frac{q^d - 1}{q-1} t + l \right) \equiv \log_{\beta} N(\alpha^{q^d-1}_t t + l) \equiv \log_{\beta} N(\alpha^l \beta^t + 1)
\]
Cyclic Equivalence of Columns

Let \( d \geq 2 \), and write a Sidelnikov sequence of period \( q^d - 1 \) as an array of size \((q - 1) \times (\frac{q^d - 1}{q - 1})\). The column sequences are denoted by \( v_l(t) \) for \( l = 0, 1, 2, \ldots, \frac{q^d - 1}{q - 1} - 1 \).

Then,

1. For \( l = 0 \), \( v_0(t) \equiv d \log_\beta (\beta^t + 1) \mod M \)
2. For \( l \neq 0 \), \( v_l(t) \equiv v_{lq}(t) \mod M \)

where \( lq \) is computed \( \mod \frac{q^d - 1}{q - 1} \)
Family of Column Sequences

Assume that \((d, q - 1) = 1, \ d < \frac{\sqrt{q} - \frac{2}{\sqrt{q}} + 1}{2}\).

Construct a family
\[
\Sigma = \{ \ \text{cv}_l(t) \mid 1 \leq c < M \text{ and } l \in \Lambda \setminus \{0\} \}
\]
where \(\Lambda\) is the set of all the representatives of \(q\)-cyclotomic cosets mod \(\frac{q^d - 1}{q - 1}\).

Then
① \( |C_{\text{max}}(\Sigma)| \leq (2d - 1)\sqrt{q} + 1. \)

② The asymptotic size of the family is \(\frac{(M-1)q^{d-1}}{d}\) as \(q \to \infty\).
### Importance of \( \gcd(d, q - 1) \)

<table>
<thead>
<tr>
<th>q</th>
<th>( \gcd(q - 1, 3) )</th>
<th>( \gcd(q - 1, 4) )</th>
<th>q</th>
<th>( \gcd(q - 1, 3) )</th>
<th>( \gcd(q - 1, 4) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>3</td>
<td>X</td>
<td>61</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>37</td>
<td>3</td>
<td>X</td>
<td>64</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>41</td>
<td>1</td>
<td>X</td>
<td>67</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>43</td>
<td>3</td>
<td>X</td>
<td>71</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>47</td>
<td>1</td>
<td>X</td>
<td>73</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>49</td>
<td>3</td>
<td>X</td>
<td>79</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>53</td>
<td>1</td>
<td>4</td>
<td>81</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>59</td>
<td>1</td>
<td>2</td>
<td>83</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Can we remove the condition \((d, q-1) = 1\)?

- \(q\)-cyclotomic coset mod \(q^d - 1\)
  - Natural

- \(q\)-cyclotomic coset mod \(\frac{q^d - 1}{q - 1}\)
  - Define \(\Lambda \setminus \{0\}\)
  - Kim-10

- \(q\)-cyclotomic coset mod \(\frac{q^d - 1}{q - 1}\) with full size \(d\)
  - Define \(\Lambda' \setminus \{0\}\)
  - Key Idea

Example (\(q = 7, \ d = 2\))

- 7-cyclotomic coset mod 48
  - There exists 23 cosets of size 2 except \(\{0\}, \{7\}\)

- 7-cyclotomic coset mod 8
  - \(\{0\}, \{1,7\}, \{2,6\}, \{3,5\}, \{4\}\)
  - \(\Lambda \setminus \{0\} = \{1,2,3,4\}\)

- 7-cyclotomic coset mod 8 of size \(d(=2)\)
  - \(\{1,7\}, \{2,6\}, \{3,5\}\)
  - \(\Lambda' \setminus \{0\} = \{1,2,3\}\)
For $2 \leq d < \frac{\sqrt{q} - \frac{2}{\sqrt{q}} + 1}{2}$, the sequences in the family
\[ \Sigma' = \{cv_l(t) | 1 \leq c < M, l \in \Lambda' \setminus \{0\} \} \]
are cyclically inequivalent.

Further, we have
\[ |C_{max}(\Sigma')| \leq (2d - 1)\sqrt{q} + 1, \]
and
\[ (M - 1)|\Lambda'| = |\Sigma'| \cong |\Sigma| = (M - 1)|\Lambda| \]
Range of $d$

$d \leq \text{Floor} \left( \frac{\sqrt{q} - 2}{\sqrt{q} + 1} \right) / 2$

Kim-10 and this paper

Gong-10
Example for case \((q - 1, d) \neq 1\)

Let \(q = 7, M = 6, d = 3\). Consider finite field \(GF(343)\). Then 6-ary Sidelnikov sequence \(s(t)\) of period 48 is represented by \(6 \times 57\) array as follows:

\[
s(t) = [v_0(t), v_1(t), \ldots, v_{55}(t), v_{56}(t)]
\]

- \(v_l(t) = v_{lq}(t)\).
- In above figure, \(v_{19}(t)\) and \(v_{38}(t)\) are sequences of period 2.
- In general, we can not use all the representatives since \((q - 1, d) \neq 1\).
Proof of Main Theorem

Suppose that $c_1 v_{l_1}(t) = c_2 v_{l_2}(t + \tau)$ for some $\tau (0 \leq \tau < q - 1)$. Then,

$$q - 1 = \sum_{t=0}^{q-2} \omega_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)} = \sum_{t=0}^{q-2} \psi^{c_1}(f_{l_1}(\beta^t))\psi^{M-c_2}(f_{l_2}(\beta^{t+\tau}))$$

$$= \sum_{x \in GF(q)} \psi_1(\beta^l p_{l_1}(x))\psi_2(\beta^{l_2} \cdot \beta^{\tau d} \cdot \beta^{-\tau d} p_{l_2}(\beta^{\tau} x)) - 1$$

where $\psi_1 = \psi^{c_1}$ and $\psi_2 = \psi^{M-c_2}$ and $p_l(x) = \beta^{-l} f_l(x)$.

Claim

$$\left| \sum_{x \in GF(q)} \psi_1(\beta^l p_{l_1}(x))\psi_2(\beta^{l_2} \cdot \beta^{\tau d} \cdot \beta^{-\tau d} p_{l_2}(\beta^{\tau} x)) \right| \leq (2d - 1)\sqrt{q}$$

If the above claim is true, then $q - 1 \leq (2d - 1)\sqrt{q} + 1$.

This is impossible because of our assumption $d < (\sqrt{q} - \frac{\sqrt{q}}{2} + 1)/2$. 
Weil bound

Let $f_1(x), \ldots, f_m(x)$ be distinct monic irreducible polynomial over $\text{GF}(q)$ with degrees $d_1, \ldots, d_m$, with $e_j$ the number of distinct roots in $\text{GF}(q)$ of $f_j(x)$.

Let $\psi_1, \ldots, \psi_m$ be nontrivial multiplicative characters of $\text{GF}(q)$, with $\psi_j(0) = 1$.

Then for every $a_i \in \mathbb{F}_q \setminus \{0\}$, we have the estimate

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x)) \right| \leq \left( \sum_{i=1}^m d_i - 1 \right) \sqrt{q} + \sum_{i=1}^m e_i.$$
For the proof of claim, we have to show that the following statement is true:

- Let \( l_1, l_2 \) be elements in \( \Lambda'\backslash\{0\} \), and let \( \tau(0 \leq \tau < q - 1) \) be an integer. Then \( p_{l_1}(x) \) and \( \beta^{-\tau d} p_{l_2}(\beta^\tau x) \) are distinct irreducible polynomials over \( GF(q) \), unless \( l_1 = l_2 \) and \( \tau = 0 \).

Note that \( p_l(x) \) is alternative form of \( f_l(x) = N(\alpha^lx + 1) \).

For each \( l \left( 0 \leq l < \frac{q^{d-1}}{q-1} \right) \),

\[
f_l(x) = \beta^l N(x + \alpha^{-l})
= \beta^l (x + \alpha^{-l})(x + \alpha^{-lq}) \cdots (x + \alpha^{-lq^{d-1}})
= \beta^l p_l(x)^{d/d_l}
\]

where \( p_l(x) \) is the minimal polynomial over \( GF(q) \) of \( -\alpha^{-l} \) of degree \( d_l \). And if \( l \in \Lambda' \), then \( d = d_l = m_l \). So, \( f_l(x) = \beta^l p_l(x) \).
Proof of the statement

- Assume that they are the same.

\[ \beta^{-\tau d} p_{l_2}(\beta^\tau x) = (x + \alpha^{-l_2} \beta^{-\tau})(x + \alpha^{-l_2 q} \beta^{-\tau}) \cdots (x + \alpha^{-l_2 q^{d-1}} \beta^{-\tau}) \text{ imply } \alpha^{-l_1} = \alpha^{-l_2 q^s} \beta^{-\tau} \text{ for some nonnegative integer } s \left( s < d \right). \]

- Hence \( l_1 \equiv l_2 q^s + \tau \left( \frac{q^{d-1}}{q-1} \right) \mod q^d - 1. \)

- So, \( l_1 \equiv l_2 q^s \mod \frac{q^{d-1}}{q-1}, \text{ and } l_1 = l_2. \)

- Now \( l_1 \equiv l_1 q^s \mod \frac{q^{d-1}}{q-1}, \text{ and hence } s = 0 \text{ since } m_{l_1} = d. \)

- In all, \( l_1 \equiv l_1 + \tau \left( \frac{q^{d-1}}{q-1} \right) \mod q^d - 1. \)

- This implies \( q - 1 \mid \tau, \text{ and therefore } \tau = 0. \)
Remaining steps for the family construction are straightforward

\[ \Lambda \rightarrow \Lambda' \]
by removing the representatives of the cosets of size *smaller* than \( d \)

\[ \Sigma \rightarrow \Sigma' \]

\[ \Sigma_{\text{ext}} \rightarrow \Sigma'_{\text{ext}} \]
by adding the constant multiples of the Sidelnikov sequence of period \( q-1 \) using \( \beta \) as well as some of their shift-and-add’s
Example for $q = 199$, $L = q - 1 = 198$ for $M = 2$ and $M = 198$

| $M$ | $d$ | $(d, q - 1)$ | $|\Lambda|$ or $|\Lambda'|$ | $|\Sigma|$ or $|\Sigma'|$ | $|\Sigma^{ext}|$ or $|\Sigma'^{ext}|$ | $(2d - 1)\sqrt{q} + 1$ or $3\sqrt{q} + 3$ |
|-----|-----|--------------|-----------------|-----------------|-----------------|-----------------|
| 2   | 2   | 2            | 99              | 99              | 198             | 45.32           |
| 3   | 3   | 13266        | 13266           | 13365           |                 | 71.53           |
| 4   | 2   | 1980000      | 1980000         | 1980099         |                 | 99.75           |
| 5   | 1   | 315231920    | 315231920       | 315232019       |                 | 127.96          |
| 6   | 6   | 52275946734  | 52275946734     | 52275946833     |                 | 156.17          |
|     |     |              |                 |                 |                 |                 |
| 2   | 2   | 2            | 99              | 19503           | 3842288         | 45.32           |
| 3   | 3   | 13266        | 2613402         | 6436187         |                 | 71.53           |
| 4   | 2   | 1980000      | 390060000       | 393882785       |                 | 99.75           |
| 5   | 1   | 315231920    | 62100688240     | 62104511025     |                 | 127.96          |
| 6   | 6   | 52275946734  | 10298361506598  | 10298365329383  |                 | 156.17          |
## Summary

<table>
<thead>
<tr>
<th>Author</th>
<th>Family size</th>
<th>Correlation bound</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sidelnikov ‘69</td>
<td>1</td>
<td>$\frac{4}{(\text{regardless of } q \text{ and } M)}$</td>
<td>By construction</td>
</tr>
<tr>
<td>Song ‘07</td>
<td>$M - 1$</td>
<td>$\sqrt{q} + 3$</td>
<td>Constant Multiple</td>
</tr>
<tr>
<td>No &amp; Yang ‘08-’09</td>
<td>$M - 1 + \frac{(M-1)^2(q-1)}{2} + 0$</td>
<td>$3\sqrt{q} + 5$</td>
<td>+ Shift-and-add</td>
</tr>
<tr>
<td>Gong ‘10</td>
<td>$\left(M - 1 + \frac{(M-1)^2(q-1)}{2}\right) + \frac{(M-1)(q-1)}{2}$</td>
<td>$3\sqrt{q} + 5$</td>
<td>+ Column sequence</td>
</tr>
<tr>
<td>Kim ‘10</td>
<td>$\approx \left(M - 1 + \frac{(M-1)^2(q-1)}{2}\right) + \frac{(M-1)q^{d-1}}{d}$</td>
<td>$(2d - 1)\sqrt{q} + 1$</td>
<td>Extension of Gong, With $(d,q-1)=1$</td>
</tr>
<tr>
<td>IT Trans submission</td>
<td>comparable</td>
<td>comparable</td>
<td>Variation of Kim, Without $(d,q-1)=1$</td>
</tr>
</tbody>
</table>
Thanks for your attention...

Any questions?