Another New Family of Gold-Like Sequences

Sankhadip Roy[1*] and Arnab Ganguly[2]
[1]Department of Basic Science and Humanities, University of Engineering and Management, Kolkata-160, India and
[2]Comscore, Reston, Virginia, United States

In this correspondence, for a positive odd integer n, a new family $\mathcal{U}$ of binary sequences with 2^n+1 sequences of length 2^n-1 taking three valued nontrivial correlations -1 and $-1\pm 2^{\frac{n+1}{2}}$ is presented. This family $\mathcal{U}$ is consturcted using the families introduced by Boztas and Kumar[4] , Kim and No [7]. This family has the same correlation distribution as that of the well-known Gold sequences. So this family can be considered as another new class of Gold-like sequences.

Keywords: Binary sequences, Quadratic Boolean functions, Correlation, Gold sequence, Gold-like sequence.

I. INTRODUCTION

Families of binary sequences with low correlation have important applications in code-division multiple access (CDMA), communication systems and cryptographic system([1],[2],[3]). Sidelnikov's bound([9]) is used to test the optimality of sequence families, which states that for any family of k binary sequences of period N, if $k \geq N$, then

$$R_{max} \geq (2N-2)^{\frac{1}{2}},$$

where R_{max} is the maximum magnitude of correlation values except for the in-phase autocorrelation value. The Gold's family ([5]) is the best known binary sequence family which satisfies Sidelnikov's bound. It has correlations $2^n-1, -1, -1\pm 2^{\frac{n+1}{2}}$, where n is odd. But the linear span of Gold sequences is too small to resist attacks based on Berlekamp-Massey algorithm. So the Gold-like families with larger linear span were constructed. The odd case of Gold-like sequence family was discovered by Boztas and Kumar[4], whose correlations are identical to those of Gold sequences. For even n, Udaya[11] introduced families of binary sequences with correlations $2^n-1, -1, -1\pm 2^{\frac{n}{2}}, -1\pm 2^{\frac{n}{2}+1}$ which corresponds to even case of Gold-like sequence family. Later Kim and No [7] further generalized the Gold-like sequences to GKW-like sequences by using the quadratic form technique and constructed families with correlations $2^n-1, -1, -1\pm 2^{\frac{n+e}{2}}$ and $2^n-1, -1, -1\pm 2^{\frac{n}{2}}, -1\pm 2^{\frac{n}{2}+e}$ respectively, where n and e are positive integers, $e|n$.

In this correspondence, we introduce a generalized family of Gold-like sequences by combining the families introduced in [4] and [7]. This new family of optimal binary sequences with 2^n+1 sequences of length 2^n-1 has correlation distribution identical to that of Gold sequence for odd n. So this family can be considered as a new generalized class of Gold-like sequences.

The remainder of the correspondence is organized as follows. In Section 2, we present the necessary preliminaries required for the subsequent sections and also discuss some known families of binary sequences with good correlations. In Section 3, we introduce the new family of binary sequences and our main result. In Section 4 , we investigate the dimensions of the radicals of two quadratic forms. Finally in Section 5, we give the proof of our main result.

II. PRELIMINARIES

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. Then the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is defined by

$$tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{mi}}$$

where $x \in \mathbb{F}_{2^n}$ and $m|n$. The trace function has the following properties:

(i) $tr_m^n(ax+by) = atr_m^n(x) + btr_m^n(x)$, for all $a, b \in \mathbb{F}_{2^m}, x, y \in \mathbb{F}_{2^n}$;

(ii) $tr_m^n(x^{2^m}) = tr_m^n(x)$, for all $x \in \mathbb{F}_{2^n}$.

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and $\lambda \in F_{2^n}$. The *trace transform* $F(\lambda)$ of $f(x)$ is defined by

$$F(\lambda) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+tr_1^n(x\lambda)}.$$

Definition 1. *Let $x = \sum_{i=1}^n x_i\alpha_i$, where $x_i \in \mathbb{F}_2$ and $\alpha_i, i = 1, 2, ..., n$, is a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then the function $f(x)$ over $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is a quadratic form if it can be expressed as*

$$f(x) = f(\sum_{i=1}^n x_i\alpha_i) = \sum_{i=1}^n\sum_{j=1}^n b_{i,j}x_ix_j,$$

where $b_{i,j} \in \mathbb{F}_{2^n}$.

*e-mail : sankhadip.roy@uem.edu.in

The quadratic form has been well analized in [8]. We also recall that the symplectic bilinear form of a quadratic form $f(x)$ is

$$B(x,z) = f(x) + f(z) + f(x+z) \text{ for } x, z \in \mathbb{F}_{2^n}.$$

Finding the dimension of the radical of a quadratic form is very crucial for our result. The radical of the quadratic form $f(x)$ is the number of sloutions of $x \in \mathbb{F}_{2^n}$ to

$$B(x,z) = f(x) + f(z) + f(x+z) = 0 \text{ for all } z \in \mathbb{F}_{2^n}.$$

The following lemma establishes the relation between the trace transform and the dimension of the radical of a quadratic form.

Lemma 1. *(Helleseth and Kumar [6]) Let $f(x)$ be a quadratic Boolean function on $\mathbb{F}_{2^n}$. If the rank of $f(x)$ is $2h$, $2 \leq 2h \leq n$, then the distribution of the trace transform values is given by*

$$F(\lambda) = \begin{cases} 2^{n-h}, & 2^{2h-1} + 2^{h-1} times \\ 0, & 2^n - 2^{2h} times \\ -2^{n-h}, & 2^{2h-1} - 2^{h-1} times \end{cases}$$

where rank is the co-dimension of the radical of $f(x)$.

All the sequence families considered in this paper are constructed by using the trace function $a(x) = tr_1^n(x)$ and some quadratic form $b(x)$ as follows:

$$C = \{f_i(x) | 0 \leq i \leq 2^n, x \in \mathbb{F}_{2^n}^*\}$$

where

$$f_i(x) = \begin{cases} a(v_i x) + b(x), & 0 \leq i \leq 2^n - 1 \\ a(x), & i = 2^n. \end{cases}$$

and $\{v_0, v_1, ..., v_{2^n-1}\}$ is an enumeration of the elements in $\mathbb{F}_{2^n}$.

The correlation function between two sequences defined by $f_i(x)$ and $f_j(x)$ can be given by the function from $\mathbb{F}_{2^n}$ to the set of integers $\mathbb{Z}$ as

$$R_{i,j}(\delta) = \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{f_i(x) + f_j(\delta x)}$$

where $\delta \in \mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. $R_{i,j}(\delta)$ can be expressed as a trace transform

$$\begin{aligned} R_{i,j}(\delta) &= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{tr_1^n([v_i + v_j]x) + g(x)} \\ &= -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_1^n(x\lambda) + g(x)} \\ &= -1 + G(\lambda) \end{aligned}$$

where $g(x) = b(\delta x) + b(x)$ and $\lambda = v_i + v_j \in \mathbb{F}_{2^n}$.

Definition 2. *Let $\frac{n}{e} = m$ be odd. We define the boolean quadratic functions $p(x)$ and $q(x)$ by*
$p(x) = \sum_{l=1}^{\frac{n}{2}-1} tr_1^n(x^{2^l+1})$, $q(x) = \sum_{l=1}^{\frac{m}{2}-1} tr_1^n(x^{2^{el}+1})$.

Lemma 2. *([4]) The associated symplectic form of $p(x)$ is*

$$\begin{aligned} B(x,z) &= p(x) + p(z) + p(x+z) \\ &= tr_1^n[z(tr_1^n(x) + x)]. \end{aligned} \tag{1}$$

Definition 3. *(Boztas and Kumar [4]) For an odd integer $n = 2k+1 \geq 3$, Boztas and Kumar introduced the following family G of Gold-like sequences*

$$g_i(x) = \begin{cases} tr_1^n(v_i x) + p(x), & 0 \leq i \leq 2^n - 1 \\ tr_1^n(x), & i = 2^n. \end{cases}$$

Theorem 1. *(Boztas and Kumar [4]) For the family G , the distribution of correlation values is given as follows:*

$$R_{i,j}(\delta) = \begin{cases} 2^n - 1, & 2^n + 1 \ times \\ -1, & 2^{3n-1} + 2^{2n} - 2^n - 2 \ times \\ -1 + 2^{k+1}, & 2^{2n-2}(2^{2k-1} + 2^{k-1}) \ times \\ -1 - 2^{k+1}, & 2^{2n-2}(2^{2k-1} - 2^{k-1}) \ times. \end{cases}$$

Lemma 3. *([7]) The associated symplectic form of $q(x)$ is*

$$\begin{aligned} B(x,z) &= q(x) + q(z) + q(x+z) \\ &= tr_1^n[z(tr_e^n(x) + x)]. \end{aligned} \tag{2}$$

Definition 4. *(Kim and No [7]) Let $\frac{n}{e} = m$ be an odd integer, where $m \geq 3$. Kim and No introduced the following sequences S which generalized the previous family*

$$s_i(x) = \begin{cases} tr_1^n(v_i x) + q(x), & 0 \leq i \leq 2^n - 1 \\ tr_1^n(x), & i = 2^n. \end{cases}$$

Theorem 2. *(Kim and No [7]) For the family S , the distribution of correlation values is given as follows:*

$$R_{i,j}(\delta) = \begin{cases} 2^n - 1, & 2^n + 1 \ times \\ -1, & (2^n - 2^{n-e}) + 1)(2^{2n} - 2) \ times \\ -1 + 2^{\frac{n+e}{2}}, & (2^{n-e-1} + 2^{\frac{n-e-2}{2}})(2^{2n} - 2) \ times \\ -1 - 2^{\frac{n+e}{2}}, & (2^{n-e-1} - 2^{\frac{n-e-2}{2}})(2^{2n} - 2) \end{cases}$$

III. MAIN RESULT

In this paper we construct a family based on two quadratic forms $p(\lambda x)$ and $q(\zeta x)$ as follows.

Definition 5. *Let $\frac{n}{e} = m \geq 3$ be odd. We define the family $\mathcal{U}$ of binary sequences by*

$$u_i(x) = \begin{cases} tr_1^n(v_i x) + p(\lambda x) + q(\zeta x), & 0 \leq i \leq 2^n - 1 \\ tr_1^n(x), & i = 2^n. \end{cases}$$

where e is also odd, $\lambda, \zeta \in \mathbb{F}_{2^e}$ and $\lambda \neq 0, \lambda \neq \zeta$.

For the correlation property of the family $\mathcal{U}$, we have the following main result.

Theorem 3. *The family $\mathcal{U}$ has the following properties:*

1. *The maximal absolute value of the nontrivial correlation of family $\mathcal{U}$ is bounded by $R_{max} \leq 1 + 2^{\frac{n+1}{2}}$ and so the family is optimal with respect to Sidelnikov bound.*
2. *The correlation distribution is as follows:*

$$R_{i,j}(\delta) = \begin{cases} 2^n - 1, & 2^n + 1 \textit{ times} \\ -1, & 2^{3n-1} + 2^{2n} - 2^n - 2 \textit{ times} \\ -1 + 2^{\frac{n+1}{2}}, & (2^{2n} - 2)(2^{n-2} + 2^{\frac{n-3}{2}}) \textit{times} \\ -1 - 2^{\frac{n+1}{2}}, & (2^{2n} - 2)(2^{n-2} - 2^{\frac{n-3}{2}}) \textit{times.} \end{cases}$$

IV. TWO QUADRATIC FORMS AND THEIR RANKS

A. Quadratic form $p(\lambda x) + q(\zeta x)$

From (1) and (2), the symplectic form of $p(\lambda x)+q(\zeta x)$ is
$B(x, z) = tr_1^n[z(\lambda tr_1^n(\lambda x) + \zeta tr_e^n(\zeta x) + \lambda^2 x + \zeta^2 x)]$.
Now for computing the rank of $p(\lambda x) + q(\zeta x)$, it suffices to find the number of solutions to

$$\lambda tr_1^n(\lambda x) + \zeta tr_e^n(\zeta x) + \lambda^2 x + \zeta^2 x = 0.$$

Let $tr_e^n(x) = a$. Then using the facts that $\zeta \in \mathbb{F}_{2^e}$ and $tr_1^n(x) = tr_1^e(tr_e^n(x))$, we get

$$x = \frac{\lambda tr_1^e(\lambda a) + \zeta^2 a}{\lambda^2 + \zeta^2},$$

which implies $x \in F_{2^e}$. Plugging into $tr_e^n(x) = a$, we get

$$a = \frac{\lambda tr_1^e(\lambda a) + \zeta^2 a}{\lambda^2 + \zeta^2},$$

which simplifies to $tr_1^e(\lambda a) = \lambda a$. So $a\lambda = 0$ or1 which gives $a = 0$ or $\frac{1}{\lambda}$, only two solutions. That is, the rank of the quadratic form $p(\lambda x) + q(\zeta x)$ is $2h = n - 1$.

B. Quadratic form $p(\lambda x) + q(\zeta x) + p(\delta\lambda x) + q(\delta\zeta x)$

Let $\delta \neq 1 \in F_{2^n}$ be a constant. From (1) and (2) , the associated symplectic form is

$$\begin{aligned} B(x, z) &= tr_1^n[z(\delta\lambda tr_1^n(\delta\lambda x) + \lambda tr_1^n(\lambda x) + \zeta\delta tr_e^n(\zeta\delta x) \\ &+ \zeta tr_e^n(\zeta x) + (\lambda^2 + \zeta^2)(1 + \delta^2)x)]. \end{aligned}$$

So we need to count the solutions to
$\delta\lambda tr_1^n(\delta\lambda x) + \lambda tr_1^n(\lambda x) + \zeta\delta tr_e^n(\zeta\delta x) + \zeta tr_e^n(\zeta x)$
$+(\lambda^2+\zeta^2)(1+\delta^2)x = 0$. Let $tr_e^n(x) = a$ and $tr_e^n(\delta x) = b$. Then

$$x = \frac{\zeta^2 a + \lambda tr_1^e(\lambda a) + \delta(\zeta^2 b + \lambda tr_1^e(\lambda b))}{(\lambda^2 + \zeta^2)(1 + \delta^2)}. \qquad (3)$$

Let $X = tr_e^n(\frac{1}{1+\delta})$. So $tr_e^n(\frac{\delta}{1+\delta^2}) = tr_e^n(\frac{1}{1+\delta}) + tr_e^n(\frac{1}{1+\delta^2}) = X+X^2$ and $tr_e^n(\frac{\delta^2}{1+\delta^2}) = tr_e^n(\frac{1}{1+\delta^2}) = X^2+1$. Plugging (3) into $tr_e^n(x) = a$ and $tr_e^n(\delta x) = b$, and using the fact mentioned above, we have

$$\begin{aligned} &(\zeta^2 a + \lambda tr_1^e(\lambda a) + \zeta^2 b + \lambda tr_1^e(\lambda b))X^2 + \\ &(\zeta^2 b + \lambda tr_1^e(\lambda b))X = a(\zeta^2 + \lambda^2), \end{aligned} \qquad (4)$$

$$\begin{aligned} &(\zeta^2 a + \lambda tr_1^e(\lambda a) + \zeta^2 b + \lambda tr_1^e(\lambda b))X^2 + \\ &(\zeta^2 a + \lambda tr_1^e(\lambda a))X = \lambda^2 b + \lambda tr_1^e(\lambda b). \end{aligned} \qquad (5)$$

There are three cases.
1. If $X = 0$, then from (4) and (5), we have $a = 0$ and $tr_1^e(\lambda b) = \lambda b$ which gives $\lambda b = 0$ or 1. So we have only two solutions $(a, b) = (0, 0), (0, \frac{1}{\lambda})$.
2. If $X = 1$, then again we have two solutions $(a, b) = (0, 0), (0, \frac{1}{\lambda})$.
3. If $X = c \in \mathbb{F}_{2^e} \setminus \{0, 1\}$, then from (4) and (5), we get

$$\zeta^2 a+\lambda tr_1^e(\lambda a)+\zeta^2 b+\lambda tr_1^e(\lambda b) = \frac{a(\zeta^2 + \lambda^2) + \lambda^2 b + \lambda tr_1^e(\lambda b)}{c}. \qquad (6)$$

Replacing $\zeta^2 a + \lambda tr_1^e(\lambda a) + \zeta^2 b + \lambda tr_1^e(\lambda b)$ in (4) and (5) with the right hand side of (6) and simplifying, we get

$$c(a + b) = a,$$

$$c((a + b)\lambda^2 + \lambda tr_1^e(\lambda b) + \lambda tr_1^e(\lambda a)) = \lambda^2 b + \lambda tr_1^e(\lambda b).$$

So we have four possibilities:
3.1 $tr_1^e(\lambda a) = 0$ and $tr_1^e(\lambda b) = 0$. Then

$$\begin{aligned} c(a + b) &= a \\ c(a + b) &= b \end{aligned}$$

So $a = b = 0$.
3.2 $tr_1^e(\lambda a) = 1$ and $tr_1^e(\lambda b) = 1$. Then

$$\begin{aligned} c(a + b) &= a \\ c(a + b)\lambda &= \lambda b + 1 \end{aligned}$$

and we have $a = \frac{c}{\lambda}, b = \frac{c+1}{\lambda}$ which lead to a contradiction as $tr_1^e(a\lambda) = tr_1^e(c)$ and $tr_1^e(b\lambda) = tr_1^e(c+1)$.

3.3 $tr_1^e(\lambda a) = 1$ and $tr_1^e(\lambda b) = 0$. Then

$$\begin{aligned} c(a+b) &= a \\ c((a+b)\lambda+1) &= \lambda b \end{aligned}$$

and we have $a = \frac{c^2}{\lambda}, b = \frac{c^2+c}{\lambda}$. This is a solution if $tr_1^e(c) = 1$.

3.4 $tr_1^e(\lambda a) = 0$ and $tr_1^e(\lambda b) = 1$. Then

$$\begin{aligned} c(a+b) &= a \\ c((a+b)\lambda+1) &= \lambda b + 1 \end{aligned}$$

and we have $a = \frac{c^2+c}{\lambda}, b = \frac{c^2+1}{\lambda}$. This is a solution if $tr_1^e(c) = 0$.

Thus, for $X = c \in \mathbb{F}_{2^e} \setminus \{0,1\}$, the associated symplectic form $B(x,z)$ has

1. two solutions $(a,b) = (0,0)$ and $(a,b) = (\frac{c^2}{\lambda}, \frac{c^2+c}{\lambda})$ when $tr_1^e(c) = 1$,
2. two solutions $(a,b) = (0,0)$ and $(a,b) = (\frac{c^2+c}{\lambda}, \frac{c^2+1}{\lambda})$ when $tr_1^e(c) = 0$.

So the rank of $p(\lambda x) + q(\zeta x) + p(\delta\lambda x) + q(\delta\zeta x)$ is $2h = n-1$.

V. PROOF OF THEOREM 3

The proof can be divided into the following five cases.

Case 1: $\delta = 1, i = j$:
It is a trivial case and thus

$$R_{i,j}(\delta) = \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{f_i(x)+f_i(x)} = 2^n-1,\ 2^n+1 \text{ times.}$$

Case 2: $\delta \neq 1, i = j = 2^n$:

$$R_{i,j}(\delta) = \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{tr_1^n(x)+tr_1^n(\delta x)} = \textstyle\sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{tr_1^n([1+\delta]x)} = -1,\ 2^n-2 \text{ times (number of choices for } \delta \neq 0,1).$$

Case 3: $\delta = 1, i \neq j, 0 \leq i,j \leq 2^n-1$:

$$\begin{aligned} R_{i,j}(\delta) &= \sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{u_i(x)+u_j(x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*}(-1)^{tr_1^n((v_i+v_j)x)} \\ &= -1, \qquad 2^n(2^n-1) \text{ times} \end{aligned}$$

Case 4: $i = 2^n, j \neq 2^n$ (or $j = 2^n, i \neq 2^n$):
For fixed δ

$$R_{2^n,j}(\delta) = \textstyle\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n([\delta+v_j]x)+p(\lambda x)+q(\zeta x)} - 1$$

From section 4, we know that the rank of the quadratic form $p(\lambda x) + q(\zeta x)$ is $n-1$. So from Lemma 1, the distribution of correlations for fixed $\delta \in \mathbb{F}_{2^n}^*$ is

$$R_{2^n,j}(\delta) = \begin{cases} -1, & 2^n - 2^{n-1} \text{ times} \\ -1 + 2^{\frac{n+1}{2}}, & 2^{n-2} + 2^{\frac{n-3}{2}} \text{ times} \\ -1 - 2^{\frac{n+1}{2}}, & 2^{n-2} - 2^{\frac{n-3}{2}} \text{ times.} \end{cases}$$

As δ varies over $\mathbb{F}_{2^n}^*$, the distribution becomes

$$R_{2^n,j}(\delta) = \begin{cases} -1, & (2^n - 2^{n-1})(2^n-1) \text{ times} \\ -1 + 2^{\frac{n+1}{2}}, & (2^{n-2} + 2^{\frac{n-3}{2}})(2^n-1) \text{ times} \\ -1 - 2^{\frac{n+1}{2}}, & (2^{n-2} - 2^{\frac{n-3}{2}})(2^n-1) \text{ times.} \end{cases}$$

Case 5: $\delta \in \mathbb{F}_{2^n} \setminus \{0,1\}$ and $0 \leq i,j \leq 2^n-1$:
In this case, we have

$$R_{i,j}(\delta) = \textstyle\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_1^n([\delta v_i+v_j]x)+p(\lambda x)+q(\zeta x)+p(\delta\lambda x)+q(\delta\zeta x)} - 1$$

From section 5, we know the rank of the quadratic form $p(\lambda x) + q(\zeta x) + p(\delta\lambda x) + q(\delta\zeta x)$ is $n-1$. So correlation distributions can be computed from Lemma 1 as

$$R_{i,j}(\delta) = \begin{cases} -1, & (2^n - 2^{n-1})2^n(2^n-2) \text{ times} \\ -1 + 2^{\frac{n+1}{2}}, & (2^{n-2} + 2^{\frac{n-3}{2}}2^n(2^n-2) \text{ times} \\ -1 - 2^{\frac{n+1}{2}}, & (2^{n-2} - 2^{\frac{n-3}{2}})2^n(2^n-2) \text{ times.} \end{cases}$$

Combining the results of the above five cases, the distribution of the correlation values for the sequence family $\mathcal{U}$ can be obtained.

---

[1] Ziemer, R.,Peterson, R., *Digital Communication and spectrum communication systems.*, McMilian, New York (1985).

[2] Gong, G., *New designs for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case*, IEEE Trans. Inform. Theory, **48** (2002),2847-2867.

[3] Fan, P.Z., Darnell, M., *Sequence Design for Communications Applications* , John Wiley, Chichester (1996)

[4] Boztas, S., Kumar, P.V., *Binary sequences with Gold-like correlation but larger linear span*, IEEE Trans. Inform. Theory, **40** (1994),532-537.

[5] Gold, R., *Maximal recursive sequences with 3-valued recursive cross-correlation functions* , IEEE Trans. Inform. Theory, **14** (1968), 154-156.

[6] Helleseth, T. and Kumar, P.V., *"'Sequences with low correlation,"in Handbook of Coding Theory* , V.S. Pless and W.C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier (1998).

[7] Kim, S.H., and No, J.S., *New families of Binary Sequences with low correlation* , IEEE Trans. Inform. Theory, **49**,No.11 (2003), 3059-3065.

[8] Lidl, R. and Niederreiter ,W., *Finite Fields, Encyclopedia of Mathematics and its Application*,Vol 20, Cambridge University Press , Cambridge , 1997.

[9] Sidelnikov, V.M. *On mutual correlations of sequences*, Soviet Math. Dokl. 12, 197-201 (1971).

[10] Tang, X., Helleseth,T., Hu,L., Jiang,W., *A new family of Gold-like sequences*, S.W.Golomb et al.(Eds.):SSC 2007.LNCS 4893,(2007), 62-69.

[11] Udaya, P., *"Polyphase and frequency hopping sequences obtained from finite rings"*, Ph.D. dissertation, Dept. Elec. Eng.,Indian Inst. Technol., Kanpur, 1992.