REFERENCES

[1] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967.

[2] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1983.

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, revised ed. New York: McGraw-Hill, 1994.

[4] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 561.

[5] R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology: The Science of Information Integrity*, G. J. Simmons, Ed. New York: IEEE Press, 1992, pp. 65–134.

[6] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[7] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, Jan. 1969.

[8] E. J. Groth, "Generation of binary sequences with controllable complexity," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 288–296, May 1971.

[9] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732–736, Nov. 1976.

[10] R. Göttfert and H. Niederreiter, "On the linear complexity of products of shift-register sequences," in *Proc. Advances in Cryptology-EUROCRYPT '93*. Berlin, Germany: Springer-Verlag, 1993, pp. 151–158.

[11] ——, "On the minimal polynomial of the product of linear recurring sequences," *Finite Fields Applic.*, vol. 1, pp. 204–218, Apr. 1995.

[12] J. L. Massey and S. Serconek, "Linear complexity of periodic sequences: A general theory," in *Proc. Advances in Cryptology-CRYPTO '96*. Berlin, Germany: Springer-Verlag, 1996, pp. 358–371.

[13] N. Zierler and W. H. Mills, "Products of linear recurring sequences," *J. Algebra*, vol. 27, pp. 147–157, 1973.

[14] J. L. Massey and S. Serconek, "A fourier transform approach to the linear complexity of nonlinearly filtered sequences," in *Proc. Advances in Cryptology-CRYPTO '94*. Berlin, Germany: Springer-Verlag, 1994, pp. 332–340.

[15] J. D. Golić, "On the linear complexity of functions of periodic GF(q) sequences," *IEEE Trans. Inform. Theory*, vol. 35, pp. 69–75, Jan. 1989.

[16] R. A. Rueppel and O. J. Staffelbach, "Products of linear recurring sequences with maximum complexity," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 124–131, Jan. 1987.

[17] R. A. Rueppel, *Analysis and Design of Stream Ciphers (Communications and Control Engineering Series)*. Berlin, Germany: Springer–Verlag, 1986.

[18] A. Lempel, "Analysis and synthesis of polynomials and sequences over GF(2)," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 297–303, May 1971.

[19] N. Kalouptsidis, *Signal Processing Systems (Telecommunications and Signal Processing Series)*. New York: Wiley, 1996.

[20] B. Benjauthrit and I. S. Reed, "Galois switching functions and their applications," *IEEE Trans. Comput.*, vol. C-25, pp. 78–86, Jan. 1976.

[21] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclop. Math. Its Applic.*, 2nd ed. Cambridge, U.K: Cambridge Univ. Press, 1996, vol. 20.

[22] T. Herlestam, "On functions of linear shift register sequences," in *Proc. Advances in Cryptology–EUROCRYPT '85*. Berlin, Germany: Springer-Verlag, 1985, pp. 119–129.

[23] J. Bernasconi and C. G. Günther, "Analysis of a nonlinear feedforward logic for binary sequence generators," in *Proc. Advances in Cryptology–EUROCRYPT '85*. Berlin, Germany: Springer-Verlag, 1985, pp. 161–166.

[24] N. Kalouptsidis and M. Manolarakis, "Sequences of linear feedback shift registers with nonlinear feedforward logic," *Proc. Inst. Elec. Eng.*, vol. 130, pp. 174–176, Sept. 1983.

[25] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: North–Holland Math. Library/Elsevier Science, 1998, vol. 55.

[26] N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2758–2764, Oct. 2002.

[27] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k–error linear complexity," *IEEE Trans. Inform. Theory*, vol. 46, pp. 694–698, Mar. 2000.

New Families of Binary Sequences With Low Correlation

Sang-Hyo Kim, *Student Member, IEEE*, and Jong-Seon No, *Member, IEEE*

***Abstract*—In this correspondence, for a positive integer n, new families $\mathcal{S}$ and $\mathcal{U}$ of binary sequences of period $2^n - 1$ with low correlations are proposed, where for some positive integer e, $\mathcal{S}$ is defined for odd $\frac{n}{e}$ and $\mathcal{U}$ for even $\frac{n}{e}$. The family $\mathcal{S}$ has four-valued correlations and is a generalization of the family of Gold-like sequences introduced by Boztas and Kumar. The family $\mathcal{U}$, which is also a generalization of the sequence family defined by Udaya has six-valued correlations. The relationship between Gold-like sequences and Gold sequences is the same as the relationship between the family $\mathcal{S}$ and the family constructed from the binary sequences partially contributed by Gold [2], Kasami [4], and Welch [13]. Using a lifting idea [9] for the families $\mathcal{S}$ and $\mathcal{U}$, families of binary sequences with the same correlation distributions and large linear span are also constructed.**

***Index Terms*—Correlation, Gold sequences, Gold-like sequences, pseudo-noise sequences, sequences.**

I. INTRODUCTION

For over 40 years, many families of binary sequences of period 2^n-1 with optimal correlations [2], [5], [9] have been found, where n is a positive integer. The Gold sequence family is the best known binary sequence family with optimal correlations. It has a four-valued correlation function, which satisfies the Sidelnikov bound. For an odd integer n, Boztas and Kumar discovered a family of binary sequences, the so-called Gold-like sequences [1] with optimal correlation, whose correlation distribution is identical to that of Gold sequences. For even n, Udaya [14] introduced families of binary sequences with six-valued correlations. In fact, these families correspond to Gold-like sequences for even n. In this correspondence, the four-valued correlations or the six-valued correlations in the sequence families include the in-phase autocorrelation value $2^n - 1$ and thus, excluding the inphase autocorrelation value, the four-valued correlations or the six-valued correlations become the three-valued correlations or the five-valued correlations, respectively. The maximum magnitude of correlation values (except for the in-phase autocorrelation value) of the sequences defined by Udaya is the same as that of Gold sequences for even n. Pairs of m-sequences and their decimated sequences with three-valued cross correlations were introduced by Gold [2], Kasami [4], and Welch [13]. Those sequences can be used to construct a family of binary sequences (referred to as *GKW sequences*) of period $2^n - 1$ with four-valued correlations [3] for a positive integer e such that $\frac{n}{e}$ is an odd integer. This becomes the Gold sequences when $e = 1$.

In this correspondence, combining the construction methods of Gold-like sequences and GKW sequences, a new family $\mathcal{S}$ of binary sequences of period $2^n - 1$ is constructed for a positive integer e such that $\frac{n}{e}$ is an odd integer. The new family $\mathcal{S}$ has four-valued correlations, which are the same as those of GKW sequences. When $e = 1$, this family becomes the Gold-like sequence family. Using the

Manuscript received December 21, 2001; revised June 17, 2003. This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Lausanne, Switzerland, June/July 2002.

The authors are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul, 151-744 Korea (e-mail: kimsh@ccl.snu.ac.kr; jsno@snu.ac.kr).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2003.818399

same method of construction as was used for the family $\mathcal{S}$, but for an integer e such that $\frac{n}{e}$ is an even integer, we also construct a new family $\mathcal{U}$ of binary sequences of period 2^n-1. It turns out that the new family $\mathcal{U}$ has six-valued correlations. The sequence family $\mathcal{U}$ for $e=1$ is the family of binary sequences by Udaya. Applying a lifting idea [9] to the families $\mathcal{S}$ and $\mathcal{U}$, two new families $\mathcal{S}^E$ and $\mathcal{U}^E$ of binary sequences with the same correlation distributions and large linear span are also constructed.

The remainder of the correspondence is organized as follows. Section II discusses several known families of binary sequences with good correlations. Section III introduces the new families of binary sequences with four-valued correlations. Section IV presents the new families of binary sequences with six-valued correlations.

II. Preliminaries

Let F_{2^n} be the finite field with 2^n elements. Then the trace function from F_{2^n} to F_{2^m} is defined by

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

where $x\in F_{2^n}$ and $m|n$. The trace function satisfies the following:

i) $\mathrm{tr}_m^n(ax+by)=a\,\mathrm{tr}_m^n(x)+b\,\mathrm{tr}_m^n(y)$, for all $a,b\in F_{2^m}$, $x,y\in F_{2^n}$;

ii) $\mathrm{tr}_m^n(x^{2^m})=\mathrm{tr}_m^n(x)$, for all $x\in F_{2^n}$.

Let $f(\underline{v})$ be a function defined on the vector space V_2^n of binary $\{0,1\}$ n-tuples. Such a function $f(\underline{v})$ is called a *Boolean function* if it takes on the values $\{0,1\}$. The *Fourier transform* $F(\underline{\lambda})$ of the Boolean function $f(\underline{v})$ and its inverse Fourier transform are defined by

$$F(\underline{\lambda})=\sum_{\underline{v}\in V_2^n}(-1)^{f(\underline{v})+\underline{\lambda}\cdot\underline{v}^T},\qquad \text{for } \underline{\lambda}\in V_2^n$$

$$(-1)^{f(\underline{v})}=\frac{1}{2^n}\sum_{\underline{\lambda}\in V_2^n}F(\underline{\lambda})(-1)^{\underline{\lambda}\cdot\underline{v}^T},\qquad \text{for } \underline{v}\in V_2^n$$

where $\underline{v}^T$ stands for the transpose of $\underline{v}$ and $\underline{\lambda}\cdot\underline{v}^T$ denotes the inner product of the two row vectors $\underline{\lambda}$ and $\underline{v}$. Rothaus [12] defined the bent functions as follows.

A Boolean function $f(\underline{v})$ defined on the vector space V_2^n is *bent* if the Fourier transform $F(\underline{\lambda})$ of $f(\underline{v})$ takes on the values $\{+\sqrt{2^n},-\sqrt{2^n}\}$ for all $\underline{\lambda}\in V_2^n$.

Olsen, Scholtz, and Welch [11] introduced the *trace transform* of functions defined on F_{2^n}. Let $g(x)$ be a function from F_{2^n} to F_2. The trace transform $G(\lambda)$ of $g(x)$ and its inverse trace transform are defined by

$$G(\lambda)=\sum_{x\in F_{2^n}}(-1)^{g(x)+\mathrm{tr}_1^n(x\lambda)}$$

$$(-1)^{g(x)}=\frac{1}{2^n}\sum_{\lambda\in F_{2^n}}G(\lambda)(-1)^{\mathrm{tr}_1^n(x\lambda)}.$$

By using a basis of F_{2^n}, every function from F_{2^n} to F_2, called Boolean function on F_{2^n}, can be expressed as a Boolean function on V_2^n. Throughout this correspondence, the trace transform of a Boolean function on F_{2^n} is equivalent to the Fourier transform of the associated Boolean function on V_2^n, and thus the bent functions can be defined on F_{2^n} [3]. A Boolean function $f(x)$ on F_{2^n} is a *quadratic form* if it is expressible as a homogeneous degree two polynomial on V_2^n [3]. Thus, it is clear that $\sum_i \mathrm{tr}_1^n(x^{2^i+1})$ is a quadratic form. A binary quadratic form which is alternating and bilinear is called *symplectic* [7]. It can be shown that the distribution of trace transform values of a quadratic Boolean function on F_{2^n} is determined from the rank of its symplectic form.

Theorem 1 (Helleseth and Kumar[3]): Let $f(x)$ be a quadratic Boolean function on F_{2^n}. If the rank of $f(x)$ is $2h$, $2\le 2h\le n$, then the distribution of the trace transform values is given by

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

Let $\mathcal{C}$ be a family of M binary sequences of period N

$$\mathcal{C}=\{s_i(t)\,|\,0\le i\le M-1,\ 0\le t\le N-1\}.$$

Then, the correlation function between two sequences in $\mathcal{C}$ is

$$C_{i,j}(\tau)=\sum_{t=0}^{N-1}(-1)^{s_i(t)+s_j(t+\tau)},\qquad 0\le i,j\le M-1,\ 0\le\tau\le N-1. \quad (1)$$

Let α be a primitive element of F_{2^n} and $f(x)$ be a Boolean function on F_{2^n}. By replacing x by α^t, the Boolean function $f(x)$ on F_{2^n} defines a binary sequence of period $N=2^n-1$ denoted by

$$s_f(t)=f(\alpha^t),\qquad t=0,1,2,\ldots,2^n-2.$$

For example, an m-sequence of period 2^n-1 and its decimated sequences are defined by the functions $\mathrm{tr}_1^n(x)$ and $\mathrm{tr}_1^n(x^d)$. In this correspondence, we deal with sequences defined by quadratic Boolean functions on F_{2^n}.

All sequence families considered in this paper are constructed by using the trace function $a(x)=\mathrm{tr}_1^n(x)$ and some quadratic form $b(x)$ as follows:

$$\mathcal{C}=\{f_i(x)\,|\,0\le i\le 2^n,\ x\in F_{2^n}^*\} \quad (2)$$

where

$$f_i(x)=\begin{cases}a(v_ix)+b(x), & \text{for } 0\le i\le 2^n-1\\ a(x), & \text{for } i=2^n\end{cases}$$

and $\{v_0,v_1,\ldots,v_{2^n-1}\}$ is an enumeration of the elements in F_{2^n}. Further, it is assumed that the quadratic form $b(x)$ is represented as

$$b(x)=\sum_{i\in I}\mathrm{tr}_1^n(x^{d_i})$$

where I is an index set and d_i has Hamming weight 2 in its 2-adic expression. The correlation function between two sequences defined by $f_i(x)$ and $f_j(x)$ can be given by the function from F_{2^n} to the set of integers Z as

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

where $\delta=\alpha^\tau\in F_{2^n}^*$ and it can be expressed as a trace transform

$$\begin{aligned}R_{i,j}(\delta)&=\sum_{x\in F_{2^n}^*}(-1)^{\mathrm{tr}_1^n([v_i+v_j]x)+g(x)}\\&=-(-1)^{g(0)}+\sum_{x\in F_{2^n}}(-1)^{\mathrm{tr}_1^n(x\lambda)+g(x)}\\&=-1+G(\lambda)\end{aligned}$$

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

Gold [2], Kasami [4], and Welch [13] found pairs of binary m-sequences with three-valued crosscorrelation functions.

Theorem 2 (Gold [2], Kasami [4], and Welch [13]): Let

$$e=\gcd(n,k),\qquad 1\le k\le n-1$$

and $\frac{n}{e}$ be an odd integer. Let

$$d = 2^k + 1 \quad \text{or} \quad d = 2^{2k} - 2^k + 1.$$

Then the cross correlation of m-sequence $\mathrm{tr}_1^n(x)$ and its decimated sequence $\mathrm{tr}_1^n(x^d)$ takes on the following distribution:

$$\begin{cases} -1 + 2^{\frac{(n+e)}{2}}, & 2^{n-e-1} + 2^{\frac{(n-e-2)}{2}} \text{ times} \\ -1, & 2^n - 2^{n-e} - 1 \text{ times} \\ -1 - 2^{\frac{(n+e)}{2}}, & 2^{n-e-1} - 2^{\frac{(n-e-2)}{2}} \text{ times.} \end{cases} \tag{3}$$

When $e = 1$, the m-sequence and its decimated sequence in Theorem 2 become a preferred pair, which is defined as a pair of binary m-sequences with three-valued cross-correlation function of values -1, $-1 + 2^{\lfloor (n+2)/2 \rfloor}$, $-1 - 2^{\lfloor (n+2)/2 \rfloor}$ [3]. Using (2), these two sequences make the family of Gold sequences. Using the pair of binary sequences in Theorem 2, the family $\mathcal{K}$ of GKW sequences with family size $2^n + 1$ can be constructed from the sequences defined by

$$k_i(x) = \begin{cases} \mathrm{tr}_1^n(v_i x) + \mathrm{tr}_1^n(x^d), & \text{for } 0 \le i \le 2^n - 1 \\ \mathrm{tr}_1^n(x), & \text{for } i = 2^n \end{cases}$$

and has four-valued correlations which are the same as the values in (3) except for the in-phase autocorrelation value $2^n - 1$.

When $e = 1$, the GKW sequence family $\mathcal{K}$ is the Gold sequence family. Boztas and Kumar [1] introduced the family of binary sequences, called Gold-like sequences with four-valued correlations identical to those of Gold sequences [1].

Definition 3 (Boztas and Kumar [1]): For an odd integer $n = 2m + 1 \ge 3$, a family $\mathcal{G}_o$ of Gold-like sequences is the set of $2^n + 1$ sequences defined by

$$g_i(x) = \begin{cases} \mathrm{tr}_1^n(v_i x) + \sum_{k=1}^{m} \mathrm{tr}_1^n(x^{2^k+1}), & \text{for } 0 \le i \le 2^n - 1 \\ \mathrm{tr}_1^n(x), & \text{for } i = 2^n. \end{cases}$$

Theorem 4 (Boztas and Kumar [1]): The distribution of the correlation values of the family $\mathcal{G}_o$ of Gold-like sequences is

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

Udaya introduced families of binary sequences for even n with six-valued correlations.

Definition 5 (Udaya [14]): For an even integer $n = 2m \ge 4$, the family $\mathcal{G}_e$ is the set of $2^n + 1$ sequences defined by

$$g_i(x) = \begin{cases} \mathrm{tr}_1^n(v_i x) + \sum_{k=1}^{m-1} \mathrm{tr}_1^n(x^{2^k+1}) + \mathrm{tr}_1^m(x^{2^m+1}), & \text{for } 0 \le i \le 2^n - 1 \\ \mathrm{tr}_1^n(x), & \text{for } i = 2^n. \end{cases}$$

Theorem 6 (Udaya [14]): For the family $\mathcal{G}_e$, the distribution of correlation values is given as follows:

$$R_{i,j}(\delta) = \begin{cases} 2^n - 1, & 2^n + 1 \text{ times} \\ -1, & 2^{2n-1}(2^{n-1} + 2^{n-2}) + 2^{2n} - 2 \text{ times} \\ -1 + 2^m, & (2^{2n-1} - 2)(2^{n-1} + 2^{m-1}) \text{ times} \\ -1 - 2^m, & (2^{2n-1} - 2)(2^{n-1} - 2^{m-1}) \text{ times} \\ -1 + 2^{m+1}, & 2^{2n-1}(2^{n-3} + 2^{m-2}) \text{ times} \\ -1 - 2^{m+1}, & 2^{2n-1}(2^{n-3} - 2^{m-2}) \text{ times.} \end{cases} \tag{4}$$

In addition, it has been proven that the functions defined in Definition 5 are bent.

Theorem 7: (Kim and No[6]) : The function defined by

$$b(x) = \mathrm{tr}_1^n(yx) + \sum_{k=1}^{m-1} \mathrm{tr}_1^n(x^{2^k+1}) + \mathrm{tr}_1^m(x^{2^m+1}) \tag{5}$$

is a quadratic bent function on F_{2^n}, where $y \in F_{2^n}$. □

In the next section, Theorem 2 is modified to construct a new family of binary sequences with four-valued correlation distribution identical to that of the GKW sequence family $\mathcal{K}$. It is a generalization of the Gold-like sequences introduced by Boztas and Kumar.

III. Families of Binary Sequences With Four-Valued Correlations

Let $e = \gcd(n, k)$ and $\frac{n}{e} = m$ be an odd integer, where $m \ge 3$. The Boolean function $p(x)$ on F_{2^n} is defined by

$$p(x) = \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n(x^{2^{ki}+1}). \tag{6}$$

Then the function $p(x)$ can be rewritten as follows.

Lemma 8: The Boolean function $p(x)$ can be rewritten as

$$p(x) = \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n(x^{2^{ei}+1}). \tag{7}$$

Proof: Let $k = el$, where $\gcd(l, m) = 1$. Let

$$d_i \equiv eli \bmod n \quad \text{or} \quad d_i \equiv -eli \bmod n$$

such that $e \le d_i \le \frac{m-1}{2}e$. Then each d_i is a multiple of e. Since $\mathrm{tr}_1^n(x^{2^n}) = \mathrm{tr}_1^n(x)$ and $\mathrm{tr}_1^n(x^{2^d+1}) = \mathrm{tr}_1^n(x^{2^{n-d}+1})$, (6) can be rewritten as

$$p(x) = \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n(x^{2^{eli}+1}) = \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n(x^{2^{d_i}+1}). \tag{8}$$

Now, it is sufficient to show that all d_i's in (8) are distinct.

Assume that $d_i = d_j$ for $i \ne j$. Then

$$eli - elj = el(i - j) \equiv 0 \bmod n$$

or

$$eli + elj = el(i + j) \equiv 0 \bmod n.$$

But, neither $i - j$ nor $i + j$ can be a multiple of m because $1 \le i, j \le \frac{m-1}{2}$. This contradicts the assumption. Therefore, all the trace functions in (8) are distinct. □

The Boolean function $p(x)$ has an associated symplectic form because it is quadratic. Thus, the distribution of the trace transform values of $p(x)$ is determined by the rank of the associated symplectic form.

Theorem 9: The distribution of the trace transform values of $p(x)$ in (7) is given as

$$\begin{cases} 2^{\frac{n+e}{2}}, & 2^{n-e-1} + 2^{\frac{n-e-2}{2}} \text{ times} \\ 0, & 2^n - 2^{n-e} \text{ times} \\ -2^{\frac{n+e}{2}}, & 2^{n-e-1} - 2^{\frac{n-e-2}{2}} \text{ times.} \end{cases}$$

Proof: To find the distribution of the trace transform of $p(x)$, the rank of the symplectic form associated with $p(x)$ can be calculated. The bilinear form $B_p(x, z)$ of $p(x)$ is defined by

$$B_p(x, z) = p(x) + p(z) + p(x + z)$$

where $x, z \in F_{2^n}$. Plugging (7) into $B_p(x,z)$, $B_p(x,z)$ can be rewritten as

$$\begin{aligned}B_p(x,z) &= \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(x^{1+2^{ei}}\right) + \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(z^{1+2^{ei}}\right) \\ &\quad + \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left((x+z)^{1+2^{ei}}\right) \\ &= \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(zx^{2^{ei}} + z^{2^{ei}}x\right) \\ &= \sum_{i=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n\left(x(z^{2^{e(m-i)}} + z^{2^{ei}})\right) \\ &= \mathrm{tr}_1^n\left(x\mathrm{tr}_e^n(z) + xz\right) \\ &= \mathrm{tr}_1^n\left(x\left[\mathrm{tr}_e^n(z) + z\right]\right).\end{aligned}$$

In order to find the rank of the symplectic form associated with $p(x)$, it is sufficient to find the number of elements $z \in F_{2^n}$ satisfying

$$B_p(x,z) = 0, \qquad \text{for all } x \in F_{2^n}$$

which corresponds to finding the number of solutions z in F_{2^n} to $\mathrm{tr}_e^n(z) + z = 0$ (see [7, Ch. 15]). Because $\frac{n}{e}$ is odd, for $z \in F_{2^e}$, $\mathrm{tr}_e^n(z) = z\mathrm{tr}_e^n(1) = z$ and for $z \in F_{2^n}\backslash F_{2^e}$, $\mathrm{tr}_e^n(z) \neq z$. Thus, there exist 2^e solutions to $\mathrm{tr}_e^n(z) + z = 0$. Therefore, the rank of the symplectic form associated with $p(x)$ is $n - e = (m-1)e$. Then the trace transform values and their distribution can be easily obtained by using Theorem 1. □

Similarly to the GKW sequence family $\mathcal{K}$, a new family of binary sequences can be constructed by using the Boolean function $p(x)$ on F_{2^n} and the trace function $\mathrm{tr}_1^n(x)$.

Definition 10: Let k and n be positive integers. Let $e = \gcd(n,k)$ and $\frac{n}{e} = m$ be an odd integer, where $m \geq 3$. The family $\mathcal{S}$ of binary sequences is the set of sequences of period $2^n - 1$ defined by

$$s_i(x) = \begin{cases} \mathrm{tr}_1^n(v_i x) + \sum_{j=1}^{\frac{m-1}{2}} \mathrm{tr}_1^n(x^{2^{ej}+1}), & \text{for } 0 \leq i \leq 2^n - 1 \\ \mathrm{tr}_1^n(x), & \text{for } i = 2^n. \end{cases}$$

When $e = 1$, the new sequence family $\mathcal{S}$ in the Definition 10 is the Gold-like sequence family $\mathcal{G}_o$ defined by Boztas and Kumar. This relationship is exactly the same as that of the GKW sequence family $\mathcal{K}$ and the Gold sequence family. Further, it will be proved that the newly defined family of binary sequences $\mathcal{S}$ has four-valued correlation distribution which is the same as that of the GKW sequence family $\mathcal{K}$.

Theorem 11: The distribution of the correlation values of the family $\mathcal{S}$ is given as

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

Proof: The proof follows the proof of the correlation distribution of the Gold-like sequence family defined by Boztas and Kumar [1]. The proof can be divided into five cases as follows.

Case 1): $\delta = \alpha^0 = 1, i = j$:
It is a trivial case and thus,

$$R_{i,j}(\delta) = 2^n - 1,\ 2^n + 1 \text{ times.}$$

Case 2): $\delta \neq 1, i = j = 2^n$:
The sequence defined by $s_{2^n}(x)$ is an m-sequence and

$$R_{i,j}(\delta) = -1,\ 2^n - 2 \text{ times.}$$

Case 3): $\delta = 1, i \neq j, 0 \leq i, j \leq 2^n - 1$:
From the linearity of the trace function

$$\begin{aligned}R_{i,j}(\delta) &= \sum_{x \in F_{2^n}^*} (-1)^{s_i(\delta x) + s_j(x)} \\ &= \sum_{x \in F_{2^n}^*} (-1)^{\mathrm{tr}_1^n([v_i + v_j]x)} \\ &= -1,\ 2^n(2^n - 1) \text{ times .}\end{aligned}$$

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

$$R_{2^n,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{\mathrm{tr}_1^n([\delta + v_j]x) + p(x)} \tag{9}$$

where $p(x)$ is given in (7). Then the correlation function in (9) can be rewritten in terms of the trace transform of $p(x)$ as

$$R_{2^n,j}(\delta) = -1 + \sum_{x \in F_{2^n}} (-1)^{p(x) + \mathrm{tr}_1^n(x\lambda)}, \qquad \lambda \in F_{2^n}$$

where $\lambda = \delta + v_j$. The distribution of the trace transform of $p(x)$ is already given in Theorem 9. Therefore, the distribution of correlation function for a fixed δ is given as

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

As δ varies over $F_{2^n}^*$, the distribution is

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

The case of $i \neq 2^n$ and $j = 2^n$ has the same distribution.
Case 5): $\delta \in F_{2^n}\backslash\{0,1\}$ and $0 \leq i, j \leq 2^n - 1$:
In this case, we have

$$s_i(\delta x) + s_j(x) = p(\delta x) + p(x) + \mathrm{tr}_1^n([\delta v_i + v_j]x).$$

Actually, the correlation function is equivalent to the trace transform of a function $q(x)$ which is given as

$$q(x) = p(\delta x) + p(x).$$

In order to compute the distribution of the correlation values, the rank of the symplectic form associated with $q(x)$ must be found and it is enough to count the number of z in F_{2^n} satisfying

$$B_q(x,z) = 0, \qquad \text{for all } x \in F_{2^n}$$

where

$$B_q(x,z) = q(x) + q(z) + q(x+z).$$

Plugging $p(x)$ into $B_q(x,z)$, we have

$$B_q(x,z) = \mathrm{tr}_1^n\left(x[\delta^2 z + \delta\mathrm{tr}_e^n(\delta z) + \mathrm{tr}_e^n(z) + z]\right).$$

The rank can be computed by determining the number of solutions to

$$\delta^2 z + \delta\mathrm{tr}_e^n(\delta z) + \mathrm{tr}_e^n(z) + z = 0. \tag{10}$$

Let $\mathrm{tr}_e^n(\delta z) = a$ and $\mathrm{tr}_e^n(z) = b$, where $a, b \in F_{2^e}$. Then (10) can be rewritten as

$$\delta^2 z + a\delta + z + b = 0.$$

As $\delta \neq 1$, the expression of z can be obtained as follows:

$$z = \frac{a\delta + b}{\delta^2 + 1}.$$

To satisfy the conditions $\mathrm{tr}_e^n(\delta z) = a$ and $\mathrm{tr}_e^n(z) = b$, the obtained solutions have to satisfy the following equations:

$$\mathrm{tr}_e^n(\delta z) = \mathrm{tr}_e^n\left(\frac{a\delta^2 + b\delta}{\delta^2 + 1}\right) = a$$
$$\mathrm{tr}_e^n(z) = \mathrm{tr}_e^n\left(\frac{a\delta + b}{\delta^2 + 1}\right) = b.$$

Let $\mathrm{tr}_e^n(\frac{1}{\delta+1}) = X$. Then $\mathrm{tr}_e^n(\frac{1}{\delta^2+1}) = X^2$. Thus, the above conditions can be rewritten as

$$aX^2 + b(X^2 + X) = (a+b)X^2 + bX = 0 \quad (11)$$
$$a(X^2 + X) + bX^2 = (a+b)X^2 + aX = b. \quad (12)$$

All solutions to (10) must satisfy (11) and (12). Now, we consider the following three cases.

i) $X = \mathrm{tr}_e^n\left(\frac{1}{1+\delta}\right) = 0$:
To satisfy conditions (11) and (12), we must have $b = 0$. Therefore, $z = \frac{a\delta}{\delta^2+1}$. As a varies over F_{2^e}, the number of solutions is 2^e.

ii) $X = \mathrm{tr}_e^n\left(\frac{1}{1+\delta}\right) = 1$:
To satisfy the conditions, we must have $a = 0$. Therefore, $z = \frac{b}{\delta^2+1}$. As b also varies over F_{2^e}, the number of solutions is 2^e.

iii) $X = \mathrm{tr}_e^n\left(\frac{1}{\delta+1}\right) \in F_{2^e} \backslash \{0, 1\}$:
From (11), $a = \frac{X+1}{X}b$ can be obtained. The value $a = \frac{X+1}{X}b$ always satisfies (12). Therefore, the solution z can be rewritten as

$$z = \frac{\delta\frac{X+1}{X}b + b}{\delta^2 + 1} = \frac{\delta\frac{X+1}{X} + 1}{\delta^2 + 1}b.$$

From the condition $X = \mathrm{tr}_e^n\left(\frac{1}{\delta+1}\right)$, it is easy to check that $\delta\frac{X+1}{X} + 1$ is nonzero. Similarly to the previous cases, the number of solutions is 2^e since b varies over F_{2^e}.

For each of the preceding three cases, the number of solutions is 2^e. Therefore, the rank of the associated symplectic form is $n - e$. It is the same as that of $p(x)$. From the distribution in Case 4), the distribution can be computed as follows:

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

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

Using the lifting idea of the extended sequences introduced by No, Yang, Chung, and Song [10], families of binary sequences with the same four-valued correlations as the family $\mathcal{S}$ can be constructed as follows.

Theorem 12: Let n and k be positive integers such that $\gcd(n, k) = e$ and $\frac{n}{e} = m$ be an odd integer, where $m \geq 3$. Let r be an integer such that $\gcd(2^e - 1, r) = 1, 1 \leq r < 2^e - 1$. Assume that the binary sequence of period $2^e - 1$ defined by the function

$$h(x) = \sum_{a_k \in I} \mathrm{tr}_1^e(x^{a_k}), \qquad \text{for } x \in F_{2^e}^*$$

has the ideal autocorrelation property, where I is an index set. Then, the family $\mathcal{S}^E$ of the binary sequences defined by

$$s_i^r(x) = \begin{cases} \sum_{a_k \in I} \mathrm{tr}_1^e([\mathrm{tr}_e^n([v_i x]^2) + \sum_{j=1}^{\frac{m-1}{2}} \mathrm{tr}_e^n(x^{2^{ej}+1})]^{ra_k}), \\ \qquad \text{for } 0 \leq i \leq 2^n - 1 \\ \sum_{a_k \in I} \mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^{ra_k}), \qquad \text{for } i = 2^n \end{cases}$$

has the same correlation distribution as that of the family $\mathcal{S}$.

The proof is omitted because it is similar to the proof in [10].

IV. Families of Binary Sequences With Six-Valued Correlations

This section introduces a construction method of sequence families of period $2^n - 1$ for even $\frac{n}{e} = m$, which have six-valued correlations. It is a generalization of the binary sequence family $\mathcal{G}_e$ by Udaya for even n given in Definition 5.

Similarly to Theorem 7, a new bent function is given as in the following theorem.

Theorem 13: Let $\gcd(n, k) = e$ and $\frac{n}{e} = m$ be an even positive integer, where $m \geq 4$. Then the Boolean function $r(x)$ on F_{2^n} defined by

$$r(x) = \sum_{i=1}^{\frac{m}{2}-1} \mathrm{tr}_1^n(x^{1+2^{ki}}) + \mathrm{tr}_1^{\frac{n}{2}}(x^{1+2^{\frac{n}{2}}}) \quad (13)$$

is a quadratic bent function.

Proof: It is clear that $r(x)$ is a quadratic form. The theorem is proved by finding the rank of the associated symplectic form of $r(x)$. Let $k = el$, where $\gcd(m, l) = 1$. Similarly to the proof of Lemma 8, it can be shown that

$$r(x) = \sum_{i=1}^{\frac{m}{2}-1} \mathrm{tr}_1^n(x^{1+2^{ei}}) + \mathrm{tr}_1^{\frac{n}{2}}(x^{1+2^{\frac{n}{2}}}). \quad (14)$$

In order to find the rank of the associated symplectic form of $r(x)$, the bilinear form of $r(x)$ given by

$$B_r(x, z) = r(x) + r(z) + r(x + z)$$

must be investigated. Plugging (14) into $B_r(x, z)$, $B_r(x, z)$ can be rewritten as

$$B_r(x, z) = \mathrm{tr}_1^n(x[\mathrm{tr}_e^n(z) + z])$$

whose derivation is similar to the case of $B_p(x, z)$ for odd $\frac{n}{e}$.

In order to determine the rank of the associated symplectic form of $r(x)$, the number of z satisfying $B_r(x, z) = 0$ for all x must be found, that is, the number of z satisfying $\mathrm{tr}_e^n(z) + z = 0$. For $z \in F_{2^e}^*$, $\mathrm{tr}_e^n(z) = 0$ and, thus, $\mathrm{tr}_e^n(z) + z \neq 0$. If $z \notin F_{2^e}$, then $\mathrm{tr}_e^n(z) + z \neq 0$. Therefore, $z = 0$ is the only solution for $\mathrm{tr}_e^n(z) + z = 0$. Thus, the rank of the associated symplectic form of $r(x)$ is n. Therefore, $r(x)$ is a quadratic bent function. □

Using the function $r(x)$ in (13), the new sequence family can be defined as follows.

Definition 14: Let k and n be positive integers. Let $e = \gcd(n,k)$ and $\frac{n}{e} = m$ be an even integer, where $m \geq 4$. The family $\mathcal{U}$ of binary sequences with family size $2^n + 1$ is the set of binary sequences of period $2^n - 1$ defined by

$$u_i(x) = \begin{cases} \mathrm{tr}_1^n(v_i x) + \sum_{j=1}^{\frac{m}{2}-1} \mathrm{tr}_1^n(x^{2^{ej}+1}) + \mathrm{tr}_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}}+1}), \\ \qquad\qquad \text{for } 0 \leq i \leq 2^n - 1 \\ \mathrm{tr}_1^n(x), \qquad\qquad \text{for } i = 2^n. \end{cases} \tag{15}$$

In the following theorem, we prove that the family $\mathcal{U}$ has six-valued correlations.

Theorem 15: The family $\mathcal{U}$ of binary sequences of period $2^n - 1$ with family size $2^n + 1$ has the distribution of correlation values as follows:

$$R_{i,j}(\delta) = \begin{cases} 2^n - 1, & 2^n + 1 \text{ times} \\ -1, & 2^{2n-e}(2^n - 2^{n-2e}) + (2^{2n} - 2) \text{ times} \\ -1 + 2^{\frac{n+2e}{2}}, & 2^{2n-e}(2^{n-2e-1} + 2^{\frac{n-2e-2}{2}}) \text{ times} \\ -1 - 2^{\frac{n+2e}{2}}, & 2^{2n-e}(2^{n-2e-1} - 2^{\frac{n-2e-2}{2}}) \text{ times} \\ -1 + 2^{\frac{n}{2}}, & (2^{2n} - 2^{2n-e} - 2)(2^{n-1} + 2^{\frac{n}{2}-1}) \text{ times} \\ -1 - 2^{\frac{n}{2}}, & (2^{2n} - 2^{2n-e} - 2)(2^{n-1} - 2^{\frac{n}{2}-1}) \text{ times.} \end{cases} \tag{16}$$

Proof: The proof is similar to that of Theorem 11. The proof can be divided into the following five cases.

The first three cases are exactly the same as those of Theorem 11.

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

For a fixed δ

$$R_{2^n,j}(\delta) = \sum_{x \in F_{2^n}^*} (-1)^{\mathrm{tr}_1^n([\delta + v_j]x) + r(x)} \tag{17}$$

where $r(x)$ is given in (13). Thus, the correlation function in (17) is rewritten as the trace transform of $r(x)$

$$R_{2^n,j}(\delta) = -1 + \sum_{x \in F_{2^n}} (-1)^{r(x) + \mathrm{tr}_1^n(x\lambda)}, \qquad \lambda \in F_{2^n}$$

where $\lambda = \delta + v_j$. It has already been proved that the Boolean function associated with $r(x)$ is a bent function. The distribution of the trace transform values of $r(x)$ can be derived by using Theorem 1. Therefore, the distribution of correlation values in this case is given as

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

Case 5): $\delta \in F_{2^n} \backslash \{0,1\}$ and $0 \leq i,j \leq 2^n - 1$:

In this case, we have

$$u_i(\delta x) + u_j(x) = r(\delta x) + r(x) + \mathrm{tr}_1^n([\delta v_i + v_j]x).$$

In fact, the correlation function is equivalent to the trace transform of $q(x)$ which is given as

$$q(x) = r(\delta x) + r(x).$$

Similarly to the proof in Theorem 11, the rank of the symplectic form associated with $q(x)$ must be found and it is sufficient to count the number of $z \in F_{2^n}$ satisfying

$$B_q(x,z) = 0, \qquad \text{for all } x \in F_{2^n}$$

where

$$B_q(x,z) = q(x) + q(z) + q(x+z).$$

Plugging $r(x)$ into $B_q(x,z)$

$$\begin{aligned} B_q(x,z) =& \mathrm{tr}_1^n(x[\mathrm{tr}_e^n(z) + z]) + \mathrm{tr}_1^n(x\delta[\mathrm{tr}_e^n(z\delta) + z\delta]) \\ =& \mathrm{tr}_1^n(x[z\delta^2 + \delta \mathrm{tr}_e^n(z\delta) + z + \mathrm{tr}_e^n(z)]). \end{aligned}$$

Thus, it is sufficient to find the number of solutions to

$$z\delta^2 + \delta \mathrm{tr}_e^n(z\delta) + z + \mathrm{tr}_e^n(z) = 0. \tag{18}$$

Note that $\delta \neq 0, 1$. Let $\mathrm{tr}_e^n(\delta z) = a$ and $\mathrm{tr}_e^n(z) = b$, where $a, b \in F_{2^e}$. Then (18) is rewritten as

$$\delta^2 z + a\delta + z + b = 0. \tag{19}$$

As $\delta \neq 1$, z is obtained as

$$z = \frac{a\delta + b}{\delta^2 + 1}.$$

To satisfy the conditions $\mathrm{tr}_e^n(\delta z) = a$ and $\mathrm{tr}_e^n(z) = b$, the obtained solutions have to satisfy the following equations:

$$\mathrm{tr}_e^n(\delta z) = \mathrm{tr}_e^n\left(\frac{a\delta^2 + by}{\delta^2 + 1}\right) = a \tag{20}$$

$$\mathrm{tr}_e^n(z) = \mathrm{tr}_e^n\left(\frac{a\delta + b}{\delta^2 + 1}\right) = b. \tag{21}$$

Let $\mathrm{tr}_e^n(\frac{1}{\delta+1}) = X$. Then $\mathrm{tr}_e^n(\frac{1}{\delta^2+1}) = X^2$. Since

$$\mathrm{tr}_e^n(1) = \mathrm{tr}_e^n\left(\frac{1+\delta^2}{1+\delta^2}\right) = 0$$

$\mathrm{tr}_e^n(\frac{1}{\delta^2+1})$ is equal to $\mathrm{tr}_e^n(\frac{\delta^2}{\delta^2+1}) = X^2$. Thus, the conditions in (20) and (21) are rewritten as

$$aX^2 + b(X^2 + X) = (a+b)X^2 + bX = a \tag{22}$$

$$a(X^2 + X) + bX^2 = (a+b)X^2 + aX = b. \tag{23}$$

All solutions to (18) must satisfy (22) and (23). Consider the following three cases.

i) $X = \mathrm{tr}_e^n(\frac{1}{1+\delta}) = 0$:
In this case, (22) and (23) reduce to $a = 0$ and $b = 0$. Thus, the unique solution of (19) is $z = 0$ and thus the rank is n.

ii) $X = \mathrm{tr}_e^n(\frac{1}{1+\delta}) = 1$:
Putting $X = 1$ into (22) and (23), all a, b in F_{2^e} satisfy the equations. Thus, the number of solutions $z = \frac{a\delta+b}{\delta^2+1}$ is equal to 2^{2e} and the rank of the associated symplectic form is $n - 2e$.

iii) $X = \mathrm{tr}_e^n(\frac{1}{1+\delta}) \in F_{2^k} \backslash \{0,1\}$:
The summation of both sides of (22) and (23) is given as

$$(a+b)X = a + b.$$

Since $X \neq 1$, $a + b = 0$ is obtained. If $b = a$ is put in (22), then $aX = a$. From the assumption $X \neq 1$, it is clear that $a = b = 0$. Therefore, the only solution in this case is $z = 0$ and the rank of the associated symplectic form is n.

Note that $\frac{1}{1+\delta} \neq 0, 1$ and $\mathrm{tr}_e^n(0) = 0$ and $\mathrm{tr}_e^n(1) = 0$ for even $m = \frac{n}{e}$. As δ varies in $F_{2^n}^*$, $\mathrm{tr}_e^n(\frac{1}{1+\delta})$ has the following distribution:

$$\mathrm{tr}_e^n\left(\frac{1}{\delta+1}\right) = \begin{cases} 0, & 2^{n-e} - 2 \text{ times} \\ 1, & 2^{n-e} \text{ times} \\ X, & 2^{n-e} \text{ times, for all } X \in F_{2^e} \backslash \{0,1\}. \end{cases}$$

TABLE I
COMPARISON OF THE FAMILIES OF BINARY SEQUENCES WITH LOW CORRELATION

	$a(x)$	$b(x)$	$C_{\max}$	Family size
Gold	$\mathrm{tr}_1^n(x)$	$\mathrm{tr}_1^n(x^d)$	$1+2^{\frac{n+1}{2}}$	2^n+1
$\mathcal{K}$	$\mathrm{tr}_1^n(x)$	$\mathrm{tr}_1^n(x^d)$	$1+2^{\frac{n+e}{2}}$	2^n+1
$\mathcal{G}_o$	$\mathrm{tr}_1^n(x)$	$\sum_{k=1}^{\frac{n-1}{2}} \mathrm{tr}_1^n(x^{2^k+1})$	$1+2^{\frac{n+1}{2}}$	2^n+1
$\mathcal{G}_e$	$\mathrm{tr}_1^n(x)$	$\sum_{k=1}^{\frac{n}{2}-1} \mathrm{tr}_1^n(x^{2^k+1})+\mathrm{tr}_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}}+1})$	$1+2^{\frac{n+2}{2}}$	2^n+1
$\mathcal{S}$	$\mathrm{tr}_1^n(x)$	$\sum_{k=1}^{\frac{\frac{n}{e}-1}{2}} \mathrm{tr}_1^n(x^{2^{ek}+1})$	$1+2^{\frac{n+e}{2}}$	2^n+1
$\mathcal{U}$	$\mathrm{tr}_1^n(x)$	$\sum_{k=1}^{\frac{n}{2e}-1} \mathrm{tr}_1^n(x^{2^{ek}+1})+\mathrm{tr}_1^{\frac{n}{2}}(x^{2^{\frac{n}{2}}+1})$	$1+2^{\frac{n+2e}{2}}$	2^n+1

Combining the above three cases in Case 5) and Theorem 1, the distribution in this case is obtained as

$$R_{i,j}(\delta)=\begin{cases} -1+2^{\frac{n+2e}{2}}, & 2^n2^{n-e}(2^{n-2e-1}+2^{\frac{n-2e-2}{2}}) \text{ times} \\ -1-2^{\frac{n+2e}{2}}, & 2^n2^{n-e}(2^{n-2e-1}-2^{\frac{n-2e-2}{2}}) \text{ times} \\ -1, & 2^n2^{n-e}(2^n-2^{n-2e}) \text{ times} \\ -1+2^{\frac{n}{2}}, & 2^n(2^n-2^{n-e}-2)(2^{n-1}+2^{\frac{n}{2}-1}) \text{ times} \\ -1-2^{\frac{n}{2}}, & 2^n(2^n-2^{n-e}-2)(2^{n-1}-2^{\frac{n}{2}-1}) \text{ times} \end{cases}$$

where δ varies over $F_{2^n}\backslash\{0,1\}$ and i,j vary from 0 to 2^n-1, respectively. Summing up the distributions of the above five cases, the distribution of correlation values for the sequence family $\mathcal{U}$ is derived as in (16).

Similarly to Theorem 12, families of binary sequences with the same six-valued correlation distribution as the family $\mathcal{U}$ can be constructed as follows.

Theorem 16: Let n and k be positive integers such that $\gcd(n,k)=e$ and $\frac{n}{e}=m$ be an even integer, where $m\geq 4$. Let r be an integer such that $\gcd(2^e-1,r)=1, 1\leq r\leq 2^e-1$. Assume that the binary sequence of period 2^e-1 defined by

$$h(x)=\sum_{a_k\in I}\mathrm{tr}_1^e(x^{a_k}), \qquad \text{for } x\in F_{2^e}^*$$

has the ideal autocorrelation property, where I is an index set. Then the family $\mathcal{U}^E$ of the binary sequences defined by

$$u_i^r(x)=\begin{cases} \sum_{a_k\in I}\mathrm{tr}_1^e([\mathrm{tr}_e^n([v_ix]^2)+\sum_{j=1}^{\frac{m}{2}-1}\mathrm{tr}_e^n(x^{2^{ej}+1})+\mathrm{tr}_e^{\frac{n}{2}}(x^{2^{\frac{n}{2}}+1})]^{ra_k}), & \text{for } 0\leq i\leq 2^n-1 \\ \sum_{a_k\in I}\mathrm{tr}_1^e([\mathrm{tr}_e^n(x)]^{ra_k}), & \text{for } i=2^n \end{cases}$$

has the same correlation distribution as that of the family $\mathcal{U}$.

The proof is also omitted because it is similar to the proof in [10]. The linear spans of the sequences in $\mathcal{U}^E$ are larger than those of of the sequences in $\mathcal{U}$.

The relationship among the several families of binary sequences referred to in this correspondence is summarized in the following remark.

Remark 17: Note that all the sequence families referred in this correspondence except for $\mathcal{S}^E$ and $\mathcal{U}^E$ can be constructed by using the trace function $a(x)=\mathrm{tr}_1^n(x)$ (m-sequence) and some quadratic form $b(x)$ on F_{2^n}. As the Gold-like sequence family $\mathcal{G}_o$ is a special case of $\mathcal{S}$, the sequence family $\mathcal{G}_e$ by Udaya is a special case of $\mathcal{U}$ when $e=1$. Those sequence families are summarized in Table I.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable advice.

REFERENCES

[1] S. Boztas and P. V. Kumar, "Binary sequences with Gold-like correlation but larger linear span," *IEEE Trans. Inform. Theory*, vol. 40, pp. 532–537, Mar. 1994.
[2] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 154–156, Jan. 1968.
[3] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elservier, 1998.
[4] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Sci. Lab., Univ. Illinois, Urbana-Champaign, Tech. Rep. R-285 (AD 632574), 1966.
[5] ——, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in *Combinatorial Mathematics and Its Applications*. Chapel Hill, NC: Univ. North Carolina Press, 1969.
[6] S.-H. Kim and J.-S. No, "On the quaternary sequences of period $\mathbf{2^n-1}$ constructed on the Galois ring," unpublished manuscript, 2000.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[8] J.-S. No, "New cyclic difference sets with singer parameters constructed from $\boldsymbol{d}$ -homogeneous functions," *Des., Codes Cryptogr.*, to be published.
[9] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371–379, Mar 1989.
[10] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "New construction for families of binary sequences with optimal correlation properties," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1596–1602, Sept. 1997.
[11] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 858–864, Nov. 1982.
[12] O. S. Rothaus, "On bent functions," *J. Comb. Thoery, Ser. A*, vol. 20, pp. 300–305, 1976.
[13] H. M. Trachtenberg, "On the crosscorrelation functions of maximal linear recurring sequences," Ph.D. dissertation, Univ. Southern California, Los Angeles, 1970.
[14] P. Udaya, "Polyphase and frequency hopping sequences obtained from finite rings," Ph.D. dissertation, Dept. Elec. Eng., Indian Inst. Technol., Kanpur, 1992.