ON IDEAL \( t \)-TUPLE DISTRIBUTION OF ORTHOGONAL FUNCTIONS IN FILTERING DE BRUIJN GENERATORS

KALIKINKAR MANDAL* AND GUANG GONG

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, CANADA

(Communicated by Sihem Mesnager)

Abstract. Uniformity in binary tuples of various lengths in a pseudorandom sequence is an important randomness property. We consider ideal \( t \)-tuple distribution of a filtering de Bruijn generator consisting of a de Bruijn sequence of period \( 2^n \) and a filtering function in \( m \) variables. We restrict ourselves to the family of orthogonal functions, that correspond to binary sequences with ideal 2-level autocorrelation, used as filtering functions. After the twenty years of discovery of Welch-Gong (WG) transformations, there are no much significant results on randomness of WG transformation sequences. In this article, we present new results on uniformity of the WG transform of orthogonal functions on de Bruijn sequences. First, we introduce a new property, called invariant under the WG transform, of Boolean functions. We have found that there are only two classes of orthogonal functions whose WG transformations preserve \( t \)-tuple uniformity in output sequences, up to \( t = (n - m + 1) \). The conjecture of Mandal et al. in [29] about the ideal tuple distribution on the WG transformation is proved. It is also shown that the Gold functions and quadratic functions can guarantee \( (n - m + 1) \)-tuple distributions. A connection between the ideal tuple distribution and the invariance under WG transform property is established.

1. Introduction

Theoretically ensuring uniformity in producing binary tuples from a source is a fundamental problem in the areas of communication, complexity theory, cryptography and statistics. It is regarded as one of the important randomness properties of a bit generator. In complexity theory, a deterministic randomness extractor is a deterministic function which makes a non-uniform source to a uniform or close to uniform source [1]. For instance, the input source of a randomness extractor is a physical source, which may include a noisy diode based on quantum effects, ring oscillator, and biased or correlated input source. On the other hand, a pseudorandom generator is a deterministic function that accepts a short truly random input and outputs a bit stream usually of longer length. The quality of a pseudorandom generator is characterized by the randomness properties such as long period, balance, equal distribution of runs, uniform tuple distribution, ideal 2-level autocorrelation, and high linear span [19, 20, 21]. In particular, the ability of producing uniformly distributed bit sequences of various lengths is one of the desirable properties of a
A vast amount of effort has been put to generate sequences with the properties long period, balance, 2-level autocorrelation and high linear span for communication and cryptographic applications. For details, see [21]. Let \( f \) be a function from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_2 \). The function \( f \) is called orthogonal if and only if the exponential sum \( \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+f(\lambda x)} = 0 \) for all \( 1 \neq \lambda \in \mathbb{F}_{2^m} \). Any orthogonal function corresponds to a binary sequence with 2-level autocorrelation by mapping \( a_i = f(\alpha^i), i = 0, \ldots, 2^m - 2 \) where \( \alpha \) is a primitive element in \( \mathbb{F}_{2^m} \) [21].

A Welch-Gong (WG) transformation sequence is to apply transform \( \text{WG}_f(x) = f(x+1) + \text{Tr}(1) \) where \( \text{Tr}(x) \) is the trace function from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_2 \), and \( f(x) \) yields a 5-term sequence with 2-level autocorrelation. WG-transformation sequences were discovered by Golomb, Gong and Gaal, together with the other two classes jointly published in [33]. This transform is termed as the Welch-Gong (WG) transformation by Solomon Golomb and appeared in [33] as well. WG transformation sequences with 2-level autocorrelation was first conjectured in 1997 [33]. In their milestone paper [11], Dillon and Dobbertin constructed a general class of two-level
autocorrelation sequences and proved all known conjectured two-level autocorrelation sequences including WG transformation sequences. A detailed investigation of cryptographic properties of WG sequences is presented in [23]. In 2005, Nawaz and Gong proposed the WG stream cipher and submitted to the eStream project in 2005 [14, 32], and completed analysis of security and hardware implementation costs are presented in [31, 42, 35, 16] in sequel. Moreover, the WG stream ciphers have provable randomness properties such as long period, balance, 2-level autocorrelation, known linear complexity, and ideal ℓ-tuple distribution. Since then, a tremendous research on the other parameters, cryptanalysis and hardware implementation of WG stream ciphers are reported in the literature [34, 12, 13, 25, 36, 35, 42, 15].

In this paper, we consider orthogonal functions over binary (extension) finite fields as filtering functions over NLFSRs that generate de Bruijn sequences where the orthogonal functions (not necessarily) ensure 2-level autocorrelation sequences, and we study uniformity in tuple distribution in output filtering sequences. In a WG stream cipher, the WG transformation is used as a filtering function over an LFSR over an extension field. Here we consider a WG transformation as a filtering function over binary NLFSRs where the WG transformations generate 2-level autocorrelation sequences. We also consider the Kasami power functions (defined in Section 2) as filtering functions over NLFSRs as the properties such as Hadamard transform, 2-level autocorrelation of the KPFs are well-studied and which is a rich source of APN functions and almost bent functions.

It is rather surprising that we have found a new property of the WG transformation when we study the uniformity of tuple distributions of those sequences. Note that the WG transformation is involution. What we discovered is that, for odd m, \( f(x) = WG_f(x) = f(x+1) + \text{Tr}(1) \) where \( f(x) = WG_h(x^d) \) and \( h(x) \) is the WG transform of either a 5-term sequence, denoted as \( T_5(x^d) \) or a 3-term sequence, denoted as \( T_3(x^d) \) for a unique decimation number \( d \) with Hamming weight greater than one. Specifically, \( f(x) \) is invariant under the WG transform (WG-invariance) when \( f \in \{WG_{T_5}(x^d),WG_{T_3}(x^d)\} \) where \( d = 2^{m-k+1} - 1 \) with \( 3k \equiv 1 \mod m \), and \( d' = 2^k - 1 \) with \( m = 2k - 1 \). Those decimations are unique. Note that \( WG_{T_3}(x) \) does not have 2-level autocorrelation (decimation does not change the autocorrelation).

In order to show that the decimated WG transformation function is invariant under the WG transformation, we use the properties of the Hadamard transform of the WG transformation functions. For the three-term case, we conjecture that the WG transform of the three-term function is invariant under the WG transform (see Section 3). It is turned out that that the above decimations are the same decimations in [39] where Yu and Gong studied their respective Hadamard transforms of \( WG_{T_5}(x^d) \) and \( T_3(x^d) \). Using this result, we are able to establish that the uniformity in binary tuples of various lengths in the filtering sequences. We show that \( f \in \{WG_{T_5}(x^d),WG_{T_3}(x^d)\} \) guarantees the ideal tuple distribution in the filtering sequences. For the theory of 2-level autocorrelation sequences, i.e., orthogonal functions and their known constructions, the reader is referred to [21].

1.2. Related work. Ideal tuple distributions of LFSR-based nonlinear filtering generators have been studied in the literature [18, 4, 38, 31]. Siegenthaler, Forré and Kleiner in [38] studied the ideal tuple distribution of binary sequences where an LFSR defined over a finite field and the nonlinear filtering function is also defined over the same field. The necessary and sufficient condition for generating a filtering
sequence with uniform tuple distribution is that the filtering function is balanced [38]. Golić [18] investigated the properties of the filtering functions for achieving uniform distribution for LFSR-based filtering generators and proposed a necessary condition and a conjecture on the sufficient condition for the filtering function. Carlet [4] proved the Golić conjecture for the sufficient condition. Smyshlyaev in [41] also proved the Golić conjecture. Recently, Mandal et al. [29] studied the ideal tuple distributions of purely NLFSR-based filtering generators where they employ an NLFSR generating a de Bruijn sequence as a generator and studied the properties of the filtering function for achieving the ideal tuple distribution in the filtering sequence. As a summary, we see that for both LFSR and NLFSR-based filtering generators, the necessary and sufficient conditions for the filtering functions for ensuring the ideal tuple distribution are the same.

1.3. Our contribution. We put our effort to seek for filtering functions of a filtering de Bruijn generator (FDBG) that can guarantee ideal tuple distribution as well as have good and proven cryptographic properties. We first mathematically study the orthogonal functions namely WG transformations, three-term functions and some quadratic functions under a new property called WG-invariance property of a Boolean function. We then apply the WG-invariance orthogonal functions in a FDBG to achieve the ideal tuple distribution in a filtering sequence. Our contributions in this article are summarized as follows:

- **WG-invariance property of WG transformations and three-term functions.** We introduce a new property called invariant under the Welch-Gong (WG) transform or WG-invariance property of a Boolean function, and provide a connection between the $x_0$-independence form and the WG-invariance property. We prove that there exists a WG transformation over $\mathbb{F}_{2^m}$ with decimation $d = 2^{m-k+1} - 1$ that has the invariant under the WG transform property where $k$ is such that $3k \equiv 1 \mod m$ and $m$ is odd. We next define the WG transform of the three-term function over $\mathbb{F}_{2^m}$ with $m = 2k - 1$ and determine the Hadamard transform of the WG transform of three-term functions, which is 5-valued. We conjecture that the WG transform of the three-term function also has the invariance property for the decimation $d = 2^k - 1$. The results on the nonlinearity of both the WG transformation and the WG transform of the three-term functions with the above two decimations are presented.

- **Achieving ideal tuple distribution from WG transformations and the WG transform of three-term functions.** We prove that, for odd $m$, the WG transformations over $\mathbb{F}_{2^m}$ with the invariance property guarantee the ideal tuple distribution in the filtering de Bruijn generator (FDBG). This proof solves the conjecture of Mandal et al. in [29]. Based on the conjecture on the WG transform of three-term functions, we showed the WG transforms of three-term functions have the ideal tuple distribution in the FDBG. For completeness, we consider the quadratic functions and show that the Gold function and quadratic functions are WG-invariant, thus can also be used to achieve ideal tuple distributions in the FDBG.

- **Experimental results on the WG transforms of KPFs.** Considering the Kasami power functions (KPFs) and their WG transforms as filtering functions in a filtering de Bruijn generator, we perform an experiment for testing the ideal tuple distributions for different lengths of the NLFSRs ($9 \leq n \leq 19$).
and different input lengths of KPFs \((8 \leq m \leq 13)\). Our experimental results show that there are no KPFs, along with their WG transforms including all decimations that give the ideal tuple distribution in the FDBG. We conjecture that only the WG transformation and three-term functions have the WG-invariance property in the KPF class.

2. Background

In this section, we present some basic definitions on Boolean functions, a definition of the WG transformation, and a description of the filtering de Bruijn generator and a result on the ideal tuple distribution from \cite{29}.

**Notations.** We use the following notations throughout the paper.

- \(\mathbb{F}_2 = \{0, 1\}\) denotes the Galois field with two elements.
- \(\mathbb{F}_{2^m}\) denotes the finite field defined by the primitive element \(\alpha\) with \(2^m\) elements where \(p(\alpha) = 0\) and \(p(x)\) is a primitive polynomial.
- \(\mathbb{F}_2^m\) denotes the vector space of dimension \(m\) over \(\mathbb{F}_2\).
- \(\text{Tr}(x) = x + x^2 + \cdots + x^{2^m-1}\) denotes the trace function from \(\mathbb{F}_{2^m}\) to \(\mathbb{F}_2\).
- \(n\) denotes the length of an NLFSR and \(m\) denotes the input size of the filtering function.

2.1. Basic Definitions on Boolean Functions. An \(m\)-variable Boolean function is a mapping from \(\mathbb{F}_2^m\) to \(\mathbb{F}_2\). If \(\lambda = (\lambda_0, \cdots, \lambda_{m-1})\) and \(x = (x_0, \cdots, x_{m-1})\) belong to \(\mathbb{F}_2^m\), the inner product of \(\lambda\) and \(x\), denoted by \(\lambda \cdot x\), is given by \(\sum_{i=0}^{m-1} \lambda_i x_i\).

There is a one-to-one correspondence between a Boolean function and its univariate polynomial representation defined in Section 2.1.1 \cite{21}. Note that the summation is in a finite field either \(\mathbb{F}_2\) or \(\mathbb{F}_{2^m}\). We use \(f\) to represent a Boolean function in \(m\) variables and its univariate polynomial representation from \(\mathbb{F}_{2^m}\) to \(\mathbb{F}_2\).

**Definition 2.1.** Let \(f : \mathbb{F}_2^m \to \mathbb{F}_2\) be a Boolean function in \(m\) variables. The algebraic normal form (ANF) of \(f\) is defined by

\[
f(x_0, \cdots, x_{m-1}) = \sum_{I \in \mathcal{P}} a_I x^I, \quad a_I \in \mathbb{F}_2\]

where \(\mathcal{P}\) is the power set of \(\{0, \cdots, m-1\}\) and \(x^I = \prod_{i \in I} x_i\) and \(I = \{i_0, \cdots, i_{m-1}\}\).

**Definition 2.2.** \cite{5, 21} The Walsh-Hadamard transform of a Boolean function \(f\) is defined as

\[
\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x) + \lambda \cdot x}, \quad \lambda \in \mathbb{F}_2^m.
\]

When \(f\) is defined over \(\mathbb{F}_{2^m}\), the Walsh-Hadamard transform or Hadamard transform of the Boolean function \(f\) is defined as

\[
\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x) + \text{Tr}(\lambda x)}, \quad \lambda \in \mathbb{F}_{2^m}.
\]

The nonlinearity of \(f\) is defined as \(NL(f) = 2^{m-1} - \max_{\lambda \in \mathbb{F}_{2^m}} |\hat{f}(\lambda)|\).

**Definition 2.3.** \cite{21} A function \(f(x)\) is called an orthogonal function if

\[
\sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(\lambda x) + f(x)} = \begin{cases} 2^m & \text{if } \lambda = 1 \\ 0 & \text{if } \lambda \neq 1. \end{cases}
\]
Definition 2.4. [39] Let \( u(x) \) and \( v(x) \) be two orthogonal functions over \( \mathbb{F}_{2^m} \). The crosscorrelation between \( u(x) \) and \( v(x) \), denoted by \( C_{u,v} \), is defined as \( C_{u,v}(\lambda) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{u(x)+v(x)} \lambda \in \mathbb{F}_{2^m} \). When \( v(x) = \text{Tr}(x) \), \( C_{u,\text{Tr}} \) is the Hadamard transform of \( u(x) \), i.e., \( C_{u,\text{Tr}}(\lambda) = \hat{u}(\lambda) \). Moreover, when \( u(x) \) and \( v(x) \) are trace functions, we denote \( C_{u,v} \) by \( H_e(\lambda^t) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(\lambda^tx) + \text{Tr}(x^e)} \), gcd\((e, 2^m - 1) = 1\).

2.1.1. Representation of boolean functions in univariate polynomials with trace. Let \( f(x) \) be a Boolean function from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_2 \). Then \( f(x) \) can be represented as

\[
f(x) = \sum_{i=1}^r \text{Tr}_i(x^{t_i})
\]

where \( t_i \) is a coset leader modulo \( 2^{m_i} - 1 \) and \( m_i|m \). Let \( \alpha = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\} \) be the basis of \( \mathbb{F}_{2^m} \) over \( \mathbb{F}_2 \). Then \( x \in \mathbb{F}_{2^m} \) can be written as \( x = x_0\alpha_0 + x_1\alpha_1 + \cdots x_{m-1}\alpha_{m-1} \) and \( f(x) = f(x_0\alpha_0 + x_1\alpha_1 + \cdots x_{m-1}\alpha_{m-1}) = f_\alpha(x_0, x_1, \ldots, x_{m-1}) \), which is the Boolean representation of \( f \). In the present article, we take only the polynomial basis \( \{1, \alpha, \ldots, \alpha^{m-1}\} \) of \( \mathbb{F}_{2^m} \) and consider the functions with the trace representation. We emphasize that at many places in this article we will use the term Boolean representation of \( f(x) \), we actually mean it by we are interested only in the variable \( x_0 \) and its coefficient in its ANF representation.

2.2. Kasami power function (KPF) construction. Let \( m \) be a positive integer and \( k \) and \( k' \) be such that \( kk' \equiv 1 \mod m \), \( k < m \) and gcd\((k, m) = 1\). Let \( R(x) \) be a permutation polynomial over \( \mathbb{F}_{2^m} \), which is recursively defined as [11, 21]

\[
R_{k'}(x) = \sum_{i=1}^{k'} A_i(x) + V_{k'}(x)
\]

where \( A_i(x) \) and \( V_i(x) \) are defined below:

\[
A_1(x) = x, \quad A_2(x) = x^{2^k+1}
\]

\[
A_{i+2} = x^{2^{(i+1)k}} A_{i+1}(x) + x^{2^{(i+1)k} - 2^{i+k}} A_i(x), \quad i \geq 1
\]

\[
V_0(x) = 0, \quad V_2(x) = x^{2^k-1}
\]

\[
V_{i+2} = x^{2^{(i+1)k}} V_{i+1}(x) + x^{2^{(i+1)k} - 2^{i+k}} V_i(x), \quad i \geq 1
\]

Furthermore, \( R_{k'}(x) \) is a permutation over \( \mathbb{F}_{2^m} \). This is known as a Kasami power function construction.

2.3. The Welch-Gong (WG) transformation and its generalization. Let \( m \) be a positive integer and \( k \) be a positive integer such that \( 3k \equiv 1 \mod m \). Denoting \( q_1 = 2^k + 1 \), \( q_2 = 2^{2k} + 2^k + 1 \), \( q_3 = 2^{2k} - 2^k + 1 \) and \( q_2 = 2^{2k} + 2^k - 1 \), the function \( u(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4} \) is defined from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_{2^m} \), which is a permutation over \( \mathbb{F}_{2^m} \) [21]. In fact, \( u(x) = R_3(x) \). The Welch-Gong (WG) transformation [23] from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_2 \) is defined as

\[
\text{WG}(x) = \text{Tr}(u(x + 1) + 1).
\]

The trace representation of the WG transformation is given in Facts 1 and 2. Let \( d \) be a positive integer such that \( \gcd(d, 2^m - 1) = 1 \) and \( d \leq 2^m - 2 \). The \( d \)-th decimation of \( \text{WG}(x) \) is given by \( \text{WG}(x^d) \).
Fact 1. [28] Let $k$ be a positive integer such that $3k \equiv 1 \pmod{m}$ and $m \equiv 2 \pmod{3}$. Then

$$WG(x) = Tr(u(x + 1) + 1) = \sum_{i \in I} Tr(x^i)$$

where $I = I_1 \cup I_2$, $I_1 = \{2^{2k-1} + 2^{k-1} + 2 + j : 0 \leq j \leq 2^{k-1} - 3\}$ and $I_2 = \{2^{2k} + 2 \cdot j + 1 : 1 \leq j \leq 2^{k-1} - 1\}$.

Fact 2. [28] Let $k$ be a positive integer such that $3k \equiv 1 \pmod{m}$ and $m \equiv 1 \pmod{3}$. Then

$$WG(x) = Tr(u(x + 1) + 1) = \sum_{i \in I} Tr(x^i)$$

where $I = I_1 \cup I_2 \cup I_3 \cup I_4$, $I_1 = \{2^{\frac{k+1}{2}} + 2 + i : 0 \leq i \leq 2^{\frac{k+1}{2}} - 2\}$, $I_2 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k+1}{2}}(2^{i+1} - 1) + 2^i - 1) : 0 \leq j \leq \frac{k-2}{2}, 1 \leq i \leq 2^j\}$, $I_3 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k+1}{2}}(2^{i+1} - 1) + 2^i - 1) : 1 \leq i \leq 2^{\frac{k+1}{1}}\}$ and $I_4 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k+1}{2}}(2^{i+1} - 1) + 2^i - 1) : 2 \leq i \leq 2^{\frac{k+1}{2}}\}$.

In [33], an alternative representation of the WG transformation can be found, which is given in Fact 3. However, we use the representations of WG in Facts 1 and 2. Note that in general $u(x) \neq v(x)$, but $Tr(u(x + 1) + 1) = Tr(v(x + 1) + 1)$ where $u(x)$ is a permutation over $\mathbb{F}_{2^m}$.

Fact 3. [33] Let $m \equiv 3 \pmod{p}$ be a positive integer. For $m = 3s - 1$, defining $r_1 = 2^s + 1$, $r_2 = 2^{2s-1} + 2^{s-1} + 1$, $r_3 = 2^{2s-1} - 2^{s-1} + 1$ and $r_4 = 2^{2s-1} + 2^{s-1} - 1$ and for $m = 3s - 2$, defining $r_1 = 2^{s-1} + 1$, $r_2 = 2^{2s-2} + 2^{s-1} + 1$, $r_3 = 2^{2s-2} - 2^{s-1} + 1$ and $r_4 = 2^{2s-1} - 2^{s-1} + 1$. The function $v : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m}$ is defined by $v(x) = x + x^{r_1} + x^{r_2} + x^{r_3} + x^{r_4}$. The WG transformation is defined as $WG(x) = Tr(v(x + 1) + 1)$.

We now extend the concept of the WG transformation to any function over $\mathbb{F}_{p^m}$.

**Definition 2.5.** Let $p > 1$ and $g(x)$ be a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^\ell}$. We define $f(x) : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_{p^\ell}$ where $\ell | m$ as

$$f(x) = Tr^m_{\ell}(g(x - a) - b)$$

where $Tr^m_{\ell}(x)$ is the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^\ell}$. This is referred to as a WG transform of $g(x)$, denoted by $WG_g(x)$. When $p = 2$ and $a = b = 1$, it becomes the original WG transformation.

The WG transform of $R_{k'}(x)$ over $\mathbb{F}_{2^m}$ is given by

$$WG_{R_{k'}}(x) = Tr(R_{k'}(x + 1) + 1), x \in \mathbb{F}_{2^m}$$

where $R_{k'}(x) = \sum_{t=1}^{r'} A_t(x) + V_{k'}(x)$ and $A_t(x)$ and $V_{k'}(x)$ are defined in Section 2.2.

In this article we consider $Tr(R_{k'}(x))$ and the WG transform of $Tr(R_{k'}(x))$. For $k' = 2$ and 3, $R_{k'}(x)$ gives the 3-term, $T3(x) = Tr(R_{2}(x))$, sequences, and the 5-term, $T5(x) = Tr(R_{3}(x))$, sequences with 2-level autocorrelation, respectively. Note that only the WG transform sequence of $T5(x)$ (i.e, $WG_{R_3}(x)$) has 2-level autocorrelation, but not the others. In this paper, we keep the term “WG transformation” for the WG transform of the 5-term functions.
2.4. Filtering de Bruijn generators. We describe the construction of the filtering de Bruijn sequence generator (FDBG) and the condition on the filtering function for achieving the ideal \(t\)-tuple distribution of the filtering sequence from [29].

2.4.1. Description of the FDBG. Let \(a = \{a_i\}_{i \geq 0}\) be a binary de Bruijn (DB) sequence generated by a nonlinear feedback shift register (NLFSR) of length \(n\), whose recurrence relation is given by

\[
a_{n+i} = F(a_i, a_{i+1}, \ldots, a_{i+n-1}) = a_i + F'(a_{i+1}, \ldots, a_{i+n-1}), \quad a_i \in \mathbb{F}_2, \quad i \geq 0
\]

where \(F(x_0, x_1, \ldots, x_{n-1})\) is the feedback function defined from \(\mathbb{F}_2^n\) to \(\mathbb{F}_2\). Efficient implementation of an NLFSR of any length that generates a de Bruijn sequence can be found in [27, 43]. Let \((i_0, i_1, \ldots, i_{m-1})\) with \(0 \leq i_0 < i_1 < \cdots < i_{m-1} \leq n - 1\) be the tap position of the NLFSR. We construct \(m\)-tuples from \(a\) by selecting \(m\) bits from the positions \((i_0, \ldots, i_{m-1})\) of the NLFSR as \(a_i = (a_{i_0}, a_{i_1}, \ldots, a_{i_{m-1}})\) which is regarded as an element of \(\mathbb{F}_2^m, i \geq 0\). Let \(f\) be a Boolean function in \(m\) variables defined over \(\mathbb{F}_2^m\). The filtering sequence \(b = \{b_i\}_{i \geq 0}\) is constructed from the de Bruijn sequence \(a\) as

\[
b_i = f(a_i), \quad i \geq 0.
\]

We call sequence \(b\) a filtering de Bruijn sequence. As the period of sequence \(a\) is \(2^n\), the period of \(b\) is also \(2^n\). Figure 1 depicts a block diagram of a filtering de Bruijn generator. As the NLFSR generates uniformly distributed \(t\)-tuples with \(1 \leq t \leq n\) (\(a\)), which is a uniform source, we are interested in uniformity on the binary \(t\)-tuple distribution of \(b\).

![Figure 1. Block diagram of a filtering de Bruijn generator (FDBG)](image)

2.4.2. Known results on ideal tuple distributions of the FDBG. We start by providing a definition of the ideal tuple distribution of a binary sequence.

**Definition 2.6.** Let \(b = \{b_i\}\) be a binary sequence of period \(2^n\). A \(t\)-tuple from \(b\) is constructed as \((b_i, b_{i+1}, \ldots, b_{i+t-1})\), \(i \geq 0\). We say the sequence \(b\) has \(t\)-tuple distribution if every \(t\)-tuple \((b_i, b_{i+1}, \ldots, b_{i+t-1})\) occurs \(2^{n-t}\) times in a period of the sequence. The sequence \(b\) has an ideal \(\ell\)-tuple distribution if \(b\) has \(t\)-tuple distribution for all \(1 \leq t \leq \ell\).
Note that if the filtering function $f(\cdot)$ is balanced, then the sequence $b$ is balanced, i.e., it has 1-tuple distribution. Lemma 2.7 states the condition on the filtering function for having ideal $t$-tuple distribution of $b$ with $t \geq 1$ and the maximum value of $t$. We extensively use this result to guarantee the ideal tuple distribution of a filtering sequence. In this article we always consider the last $m$ positions of the NLFSR as the input to the filtering function.

**Lemma 2.7.** [29] Let $f$ be a filtering function and $(i_0, i_1, \cdots, i_{m-1}) = (n-m, \cdots, n-1)$, i.e., the last $m$ positions be the tap positions in the FDBG. The filtering de Bruijn sequence has an ideal $(n-m+1)$-tuple distribution if and only if the ANF representation of $f$ has the form $f(x_0, \cdots, x_{m-1}) = x_0 + g(x_1, \cdots, x_{m-1})$, where $g$ is a Boolean function in $(m-1)$ variables.

### 3. Invariance of the WG Transformation

In this section, we introduce the concept of the invariance under the WG transform (or WG-invariant) of a Boolean function. We consider the WG transformations and the WG transform of three-term functions. We use the Hadamard transform of Boolean functions as a tool. Then, we present some results on the $x_0$-independence of a Boolean function, and finally find a relation with the WG-invariance property.

#### 3.1. Relation between the Hadamard transforms of $f$ and $WG_f$.

We first define the invariant under the WG transform. Let $f(x)$ be a Boolean function with the trace representation from $F_{2^m}$ to $F_2$. Notice that we denote the WG transform of a function $f$ by $WG_f(x) = f(x+1) + \text{Tr}(1)$. From now on, when we write a function $f$ in the subscript of $WG$, i.e., $WG_f$, we mean it by the WG transform of $f$.

**Definition 3.1.** Let $f(x)$ be a Boolean function with the trace representation. We say a function $f(x)$ is **invariant** under the WG transform (or WG-invariant) if the WG transform of $f(x)$ is the function itself for $m$ odd or its complement for $m$ even, i.e.,

$$WG_f(x) = \begin{cases} f(x) & m \text{ odd} \\ f(x) + 1 & m \text{ even}. \end{cases}$$

Similarly, we say a function $f(x)$ is **complementary invariant** under the WG transform (or complementary WG-invariance) if the WG transform of $f(x)$ is the complementary function for $m$ odd or itself for $m$ even, i.e.,

$$WG_f(x) = \begin{cases} f(x) + 1 & m \text{ odd} \\ f(x) & m \text{ even}. \end{cases}$$

As the WG transform of a Boolean function is another Boolean function, we shall find a relation between the Hadamard transforms of the Boolean function $f$ and $WG_f$, and use that to study the invariance property and determine the nonlinearity of $WG_f$.

**Lemma 3.2.** Let $f(x)$ be a function from $F_{2^m}$ to $F_2$ and $WG_f(x)$ be the WG transform of $f$, i.e., $WG_f(x) = f(x+1) + \text{Tr}(1)$. Then

$$WG_f(\lambda) = (-1)^{\text{Tr}((\lambda+1)f(\lambda)), \forall \lambda \in F_{2^m}}.$$  

Furthermore, for $m$ odd, the following conditions are equivalent: $f$ is WG-invariant, i.e.,
1) \( WG_f(x) = f(x) \)
2) \( \hat{WG}_f(\lambda) = \hat{f}(\lambda) \)
3) \( \hat{f}(\lambda) \neq 0 \) implies \( \text{Tr}(\lambda) = 1 \).

**Proof.** The Hadamard transform of a Boolean function \( f \) is defined as
\[
\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+\text{Tr}(\lambda x)}.
\]
The Hadamard transform of \( WG_f(x) \) is given by
\[
\hat{WG}_f(\lambda) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+\text{Tr}(\lambda x)}
= \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+\text{Tr}(\lambda(x+1))+\text{Tr}(\lambda+1)}
= (-1)^{\text{Tr}(\lambda+1)} \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+\text{Tr}(\lambda(x+1))}
= (-1)^{\text{Tr}(\lambda+1)} \sum_{y \in \mathbb{F}_2^m} (-1)^{f(y)+\text{Tr}(\lambda y)},
\]
(6)
The conditions (1) and (2) are equivalent by definition. For odd \( m \), \( \text{Tr}(1) = 1 \).
When \( \hat{f}(\lambda) \neq 0, \hat{WG}_f(\lambda) = \hat{f}(\lambda) \) implies \( \text{Tr}(\lambda + 1) = 0 \) and hence \( \text{Tr}(\lambda) = 1 \).  

The lemma asserts that the range of the Hadamard transform (absolute) values for the Boolean function and its WG transform is the same. Next, we investigate the invariance property of the WG transformations.

3.2. \( x_0 \)-**Independence of Boolean functions.** We now exhibit a general form of a Boolean function in terms of variable \( x_0 \). A special form of a Boolean function in \( x_0 \), called \( x_0 \)-independence, is defined below.

**Definition 3.3.** Let \( f \) be a Boolean function in \( m \) variables. We say \( f(x) \) has \( x_0 \)-independence form if \( f(x) \) can be written as \( f(x) = x_0 + g(x_1, \ldots, x_{m-1}) \) where \( g \) is independent of \( x_0 \).

In terms of the truth table, the \( x_0 \)-independence can be interpreted as follows:
A function \( f \) has an \( x_0 \)-independence form if \( f(\alpha^i) = f(\alpha^{Z(i)}) + 1 \) where \( Z(i) \) is the Zech logarithm satisfying \( \alpha^{Z(i)} = \alpha^i + 1 \).

**Proposition 1.** Let \( f(x) \) be a function from \( \mathbb{F}_2^m \) to \( \mathbb{F}_2 \). Then the function \( f(x) \) can be written as \( f(x) = x_0 \text{Tr}(1) + x_0 f(z) + \text{WG}_f(z) + f(z) \) where \( x = x_0 + z \in \mathbb{F}_2^m \).

**Proof.** Let \( x = x_0 + z \in \mathbb{F}_2^m, x_0 \in \mathbb{F}_2 \). Without loss of generality \( f(x) \) can be written as
\[
f(x) = x_0 g(z) + h(z)
\]
(7)
where \( g(z), h(z) \) are functions in only \( z \)-variable, which is independent of \( x_0 \). When \( x = z \) and \( x = 1 + z \), Eq. (7) can be written as
\[
f(z) = h(z)
\]
(8)
\[
f(1 + z) = g(z) + h(z)
\]
(9)
Summing Eqs. (8) and (9), \( g(z) \) can be written as \( g(z) = f(z) + f(1+z) \).
Substituting the values of \( g(z) \) and \( h(z) \) in Eq. (7), \( f(x) \) can be written as
\[
\begin{align*}
f(x) &= x_0(f(z) + f(1+z)) + f(z) \\
&= x_0 \text{Tr}(1) + x_0(f(z) + f(1+z) + \text{Tr}(1)) + f(z) \\
&= x_0 \text{Tr}(1) + x_0(f(z) + \text{WG}_f(z)) + f(z).
\end{align*}
\]
where \( \text{WG}_f(x) = f(x+1) + \text{Tr}(1) \) is the WG transform of \( f \). Hence the proof. \( \square \)

We now establish a relation between the \( x_0 \)-independence form and the WG-invariance property of a Boolean function as follows.

**Theorem 3.4.** Let \( m \) be odd and \( f \) be a Boolean function in \( m \) variables. The function \( f(x) \) has the \( x_0 \)-independence form if and only if \( f \) is invariance under the WG transform (WG-invariance).

**Proof.** Let \( f(x) \) have the \( x_0 \)-independence form. Then \( f(x) \) can be written as \( f(x) = x_0 + g(x_1, \ldots, x_{n-1}) \) for some \( g \). The WG transform of \( f(x) \) is given by
\[
\begin{align*}
\text{WG}_f(x) &= f(x+1) + \text{Tr}(1) = x_0 + 1 + g(x_1, \ldots, x_{n-1}) + \text{Tr}(1) \\
&= x_0 + g(x_1, \ldots, x_{n-1}) = f(x)
\end{align*}
\]
as for odd \( m \), \( \text{Tr}(1) = 1 \). This proves the necessary condition.

Conversely, we assume that \( f \) is invariant under the WG transform. According to Proposition 1, for odd \( m \), \( f(x) \) can be written as \( f(x) = x_0 + x_0(f(z) + \text{WG}_f(z)) + f(z) \). Since \( f(x) = \text{WG}_f(x) \), so does \( f(z) = \text{WG}_f(z) \), and hence \( f(x) = x_0 + g(x_1, \ldots, x_{m-1}) \) where \( g(x_1, \ldots, x_{m-1}) = f(z) \), which is independent of \( x_0 \). Hence the result is established. \( \square \)

3.3. **Invariance of the Decimated WG Transformation.** We study the invariance property of the WG transformation with decimation \( d = 2^{m-k+1} - 1 \). Considering \( f(x) = \text{WG}(x^d) \) and the function \( \text{WG}_f(x) = f(x+1) + \text{Tr}(1) = f(x+1) + 1 \) for odd \( m \). The main result of this subsection is to find the invariant under the WG transform of \( f(x) \) for odd \( m \).

**3.3.1. Connection between WG Decimations.** For \( m \equiv 2 \mod 3 \), \( m = 3k-1 \) and for \( m \equiv 1 \mod 3 \), \( 2m = 3k - 1 \). Then the decimation \( d = 2^{m-k+1} - 1 \) can be written as
\[
\begin{align*}
d = \begin{cases} 
2^{2k} - 1 & \text{if } m \equiv 2 \mod 3 \\
2^{k+1} - 1 & \text{if } m \equiv 1 \mod 3.
\end{cases}
\end{align*}
\]

In Section 2.3, we mentioned that there are two ways to define the WG transformations (see Facts 1 and 2 and Fact 3) where the exponents are calculated using either \( m = 3s \pm 1 \) or \( 3k \equiv 1 \mod m \). In [39], Yu and Gong proved the Hadamard transform of the decimated WG transformation (see Fact 5) where the decimation is \( d_1 = \frac{2^{2s} - 2^{s+1} + 1}{2^s + 1} \). We provide a connection between the decimations \( d_1 \) and \( d \) defined by Eq. (10) for both definitions of the WG transformation in the following proposition.

**Proposition 2.** Let \( m \) be odd and \( m = 3s \pm 1 \). Define \( d_1 = \frac{2^{2s} - 2^{s+1} + 1}{2^s + 1} \). Let \( 3k \equiv 1 \mod m \). The relation between \( d_1 \) and \( d \) is given by \( d_1 = 2^{k \cdot d} \) where
\[
\ell = \begin{cases} 
0 & \text{if } k = s \\
k - s - 1 & \text{if } k = 2s + 1.
\end{cases}
\]
Proof. There are two cases to consider for odd values of $m$.

**Case 1. $m \equiv 2 \mod 3$.** When $m = 3s - 1$ and $3k \equiv 1 \mod m$, we have $k = s$. The exponent $d$ can be written as $d = 2^k - 1$. Furthermore, we have

$$d_1 = \frac{2^k - 2^k + 1}{(2^k + 1)(2^k - 1)} = \frac{2^k - 2^k + 1}{2^k + 2^k - 2^k + 1} = 1$$

as $2^{3k-1} = 1$. Thus, $d_1 = d = 2^\ell \cdot d$ with $\ell = 0$.

**Case 2. $m \equiv 1 \mod 3$.** When $m = 3s + 1$ and $3k \equiv 2 \mod m$, we have $k = 2s + 1$, implying $s = \frac{k-1}{2}$. The exponent $d$ can be written in terms of $k$ as $d = 2^k \cdot d$. Thus, we have

$$d_1 = \frac{2^{k-1} - 2^{k-1} + 1}{(\frac{2^{k-1}}{2} + 1)(\frac{2^{k-1}}{2} - 1)} = \frac{2^{k-1} - 2^{k-1} + 1}{2^k + 2^{k-1} - 2^{k-1} + 1} = 1$$

as $2^{3k-1} = 1$. Thus $d_1 = 2^\ell \cdot d$ where $\ell = \frac{k-1}{2} = k - s - 1$. Hence the proof. \qed

### 3.3.2. Invariance property of $WG(x^d)$. To prove $f(x)$ is invariant under the WG transform, we show that the Walsh spectra of $f(x)$ and $WG(f(x))$ at every point are identical. In the following, we prove this result, but before that we state two results on the Hadamard transform of the WG transformation from [10, 23, 39]. In [39], Yu and Gong presented the Hadamard transform of $WG(x^d)$ when $m = 3s \pm 1$, but the values of $\lambda$ for which the Hadamard transform value equals zero or nonzero were not known. In Lemma 3.5, we explicitly present the values of $\lambda$ in terms of the trace function for which the Hadamard transform values are zeros and nonzeros and use this result to prove the invariant under the WG transform property of the WG transformation.

**Fact 4.** [23] Let $m = 3s \pm 1$. For the WG transformation $WG(x) = Tr(v(x + 1) + 1)$ over $\mathbb{F}_{2^m}$ defined in Fact 3, the Hadamard transform of $WG(x)$ is given by

$$\widehat{WG}(\lambda) = \begin{cases} 
0 & \text{if } Tr(\lambda^c) = 0 \\
\pm 2^{\frac{m+1}{2}} & \text{if } Tr(\lambda^c) = 1
\end{cases}$$

where $c = e^{-1}$ and $e = 2^{2s} - 2^s + 1$.

**Fact 5.** [39] For $m = 3s \pm 1$ and $WG(x) = Tr(v(x + 1) + 1)$, the Hadamard transform of the WG transformation with decimation $d_1 = \frac{2^k}{\mathbb{F}_{2^m}}$ with $e = 2^{2s} - 2^s + 1$, i.e., $WG^{(d_1)}(x) = WG(x^{d_1})$ is 3-valued, i.e., $\{0, \pm 2^{\frac{m+1}{2}}\}$ and $WG^{(d_1)}(\lambda) = H_{c^{-1}}(\lambda^{-d_1}) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr(\lambda^{-d_1}x) + Tr(x^{-1})}$.

**Lemma 3.5.** For $m = 3s \pm 1$ and $WG(x) = Tr(v(x + 1) + 1)$, the Hadamard transform of the WG transformation with decimation $d_1 = \frac{2^k}{\mathbb{F}_{2^m}}$, $e = 2^{2s} - 2^s + 1$, denoted by $WG^{(d_1)}(x) = WG(x^{d_1})$, is given by

$$\widehat{WG^{(d_1)}}(\lambda) = \begin{cases} 
0 & \text{if } Tr(\lambda^c) = 0 \\
\pm 2^{\frac{m+1}{2}} & \text{if } Tr(\lambda^c) = 1
\end{cases}$$

**Proof.** From Fact 5, we write the Hadamard transform of $WG(x^{d_1})$ as

$$\widehat{WG^{(d_1)}}(\lambda) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr(\lambda^{-d_1}x) + Tr(x^{-1})}$$
In [10], Dillon proved the Walsh spectrum of \( \text{Tr}(x^e) \) for which
\[
H(f) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}(x) + \text{Tr}(x^e - 1)} - \lambda(2^e + 1)^{-1}.
\]

Thus, the Walsh spectra of \( f \) are identical at every point. Therefore, \( f \) is invariant under the WG transform.

**Example 1.** Let \( m = 7 \), \( 3k \equiv 1 \) mod \( m \) implying \( k = 5 \). Then \( \text{WG}_{T5}(x) = \text{Tr}(x + (x + 1)^{33} + (x + 1)^{39} + (x + 1)^{41} + (x + 1)^{104}) = \text{Tr}(x + x^3 + x^7 + x^{19} + x^{29}) \) over \( \mathbb{F}_{2^7} \). For decimation \( d = 2^{7-5+1} - 1 = 7 \), the decimated WG transformation is given by \( f(x) = \text{WG}_{T5}(x^d) = \text{WG}_{T5}(x^e) = \text{Tr}(x^3 + x^7 + x^{21} + x^{49} + x^{76}) \). It can be shown that \( \text{WG}_f(x) = \text{Tr}((1 + x)^3 + (1 + x)^7 + (1 + x)^{21} + (1 + x)^{49} + (1 + x)^{76} + 1) = f(x) \).

As a consequence of Theorem 3.6, we have the following result on the nonlinearity of the WG transformation when its exponents are defined using \( k \) satisfying \( 3k \equiv 1 \) mod \( m \).
Thus the nonlinearity of $WG(x^d)$ is $2^{m-1} - 2^{\frac{m-1}{2}}$.

Proof. According to Theorem 3.6, the Walsh spectrum of $WG(x^d)$ is $\{0, \pm 2^\frac{m-1}{2}\}$. Thus the nonlinearity of $WG(x^d)$ is $2^{m-1} - 2^{\frac{m-1}{2}}$. Hence the result follows.

3.4. Invariance of the WG transform of three-term function. In this section, we first present a definition of the WG transform of the three-term (T3) function and its decimation. We then determine the Hadamard transform and investigate the invariance property of the WG transform of the three-term function.

3.4.1. WG transform of three-term function. Three-term functions (T3) are constructed by setting $k' = 2$ in $R_k(x)$ defined in Section 2.2. Let $m = 2k - 1$, $k \geq 2$ and $R_2(x) = x + x^{q_1} + x^{q_2}$ where $q_1 = 2^k + 1$ and $q_2 = 2^k - 1$ and $k = m+1$. The three-term function (T3) is defined as [11]

$$T3(x) = \text{Tr}(R_2(x)) = \text{Tr}(x + x^{q_1} + x^{q_2}), x \in \mathbb{F}_{2^m}. \tag{11}$$

An alternative definition of the three-term function is

$$w(x) = \text{Tr}(x + x^r + x^{r^2}) \tag{12}$$

where $r = 2^\frac{m-1}{2} + 1$ [22, 33]. Note that $w(x) = T3(x^{2^k+1})$ [11, 21]. The WG transform of $T3(x)$, denoted by $WG_{T3}(x)$, is defined as

$$WG_{T3}(x) = \text{Tr}(R_2(x + 1) + 1) = \text{Tr}(x + (x + 1)^{q_1} + (x + 1)^{q_2}).$$

Let $d$ be a positive integer such that $\gcd(d, 2^m - 1) = 1$. The decimated $WG_{T3}(x)$ with $d$-th decimation is defined as

$$f(x) = WG_{T3}(x^d) = \text{Tr}(x^d + (x^d + 1)^{q_1} + (x^d + 1)^{q_2}), x \in \mathbb{F}_{2^m}.$$ 

Note that the functions $WG_{T3}(x)$ and its decimation $WG_{T3}(x^d)$ do not ensure 2-level autocorrelation.

3.4.2. Hadamard transform of $WG_{T3}(x^d)$. In [11], Dillon and Dobbertin proved that the Hadamard transform of $w(x)$ is 3-valued. In [7], Chang et al. proved that the dual of the code $\{(\text{Tr}(ax + bx^r + cx^{r^2})) : a, b, c \in \mathbb{F}_{2^m}\}$ is a triple-error correcting cyclic code, and its weight distribution is at most 5-valued. In [39], Yu and Gong presented the result on the Hadamard transform of $T3(x)$ and decimated $T3(x)$, i.e., $T3(x^d)$ with $d = 2^k - 1$, which is presented in Fact 6. We here determine the Hadamard transform of $f(x) = WG_{T3}(x^d)$ with decimation $d = 2^k - 1$ in Theorem 3.8, before that we present the Hadamard transform values of the WG transforms of $T3(x)$, $w(x)$, and $T3(x^d)$.

Fact 6. [39] Let $m = 2k - 1$ and $T3(x)$ be the three-term function. For the decimation $d = 2^k - 1$, the Hadamard transform of $T3(x^d)$ is at most 5-valued, i.e., $\{0, \pm 2^\frac{m-1}{2}, \pm 2^\frac{m+1}{2}\}$.

Lemma 3.7. Let $T3(x)$ and $w(x)$ be as defined in Eqs. (11) and (12), respectively, and $g(x) = T3(x^d)$ with $d = 2^k - 1$. The Hadamard transforms of $WG_w(x)$ and $WG_g(x)$ are as follows:

1) the Hadamard transform of $WG_w(x)$ is 3-valued.
2) the Hadamard transform of $WG_g(x)$ is also at most 5-valued.
In [7], Chang et al. proved that the dual code of \( C \) is given by \( \hat{h}(\lambda) = (-1)^{Tr(\lambda+1)} h(\lambda) \) for any \( h \). This implies that the Hadamard transform value level of \( W G_{f}(x) \) is upper bounded by that of \( h(x) \). Since, according to [21], the Hadamard transform of \( w(x) \) is 3-valued, the Hadamard transform of \( W G_{g}(x) \) is 3-valued. According to [11] and [39], the Hadamard transform of \( g(x) \) is at most 5-valued, therefore the Hadamard transforms of \( W G_{f}(x) \) is at most 5-valued. Hence the proof.

\[ \text{Theorem 3.8. For } m = 2k - 1 \text{ and } d = 2^{k} - 1, \text{ the Hadamard transform of the decimated } WG \text{ transform of the three-term function } f(x) = W G_{T3}(x^{d}) \text{ is 5-valued, i.e., } \{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}. \]

\[ \text{Proof. Recall the definition of } f(x) = W G_{T3}(x^{d}) = Tr(x^{d} + (x^{d} + 1)^{q_{1}} + (x^{d} + 1)^{q_{2}}) \text{ where } q_{1} = 2^{k} + 1, q_{2} = 2^{k} - 1 \text{ and } d = 2^{k} - 1. \text{ The Hadamard transform of } f(x) \text{ is given by} \]

\[ \hat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^{m}}} (-1)^{Tr(\lambda x) + Tr(x^{2^{k-1} + 1} + (x^{2^{k-1} + 1})^{2^{k} + 1} + (x^{2^{k-1} + 1})^{2^{k} - 1})} \]

\[ = \sum_{y \in \mathbb{F}_{2^{m}}} (-1)^{Tr(\lambda(y + 1)^{2^{k-1} + 1} + y + 1 + y^{2^{k-1}} + y^{2^{k} - 1})} \]

where \( y = x^{2^{k-1} + 1} \), implying \( x = (y + 1)^{2^{k}+1} \) as \((2^{k} - 1)^{-1} = 2^{k} + 1 \)

\[ = \sum_{y \in \mathbb{F}_{2^{m}}} (-1)^{Tr(\lambda(y^{2^{k-1}} + y^{2^{k-1}} + y^{2^{k-1}} + y^{2^{k} - 1})} \]

\[ = (-1)^{Tr(\lambda + 1)} \sum_{y \in \mathbb{F}_{2^{m}}} (-1)^{Tr((1 + \lambda)x^{2^{k-1}} + y^{2^{k-1}} + y^{2^{k-1}} + y^{2^{k-1}} + y^{2^{k} - 1})} \]

as \( Tr(\lambda y^{2^{k}}) = Tr(\lambda^{2^{k-1}} y) \)

Let \( x = y^{2^{k-1}} \) \( \implies y = x^{2^{k}+1} \) as \((2^{k} - 1)^{-1} = 2^{k} + 1 \)

\[ = (-1)^{Tr(\lambda + 1)} \sum_{x \in \mathbb{F}_{2^{m}}} (-1)^{Tr(x + (1 + \lambda)x^{2^{k-1}} + (1 + \lambda)y^{2^{k-1}} + (1 + \lambda)y^{2^{k-1}} + y^{2^{k-1}} y^{2^{k-1}})} \].

In [7], Chang et al. proved that the dual code of \( C \) is \( \{ Tr(\lambda x + bx^{r} + cx^{2^{r}}) | a, b, c \in \mathbb{F}_{2^{m}} \} \) where \( r = 2^{k} + 1 \) is a triple-error correcting cyclic code, which has the 5-level weight distribution \( \{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\} \). Therefore, the Hadamard transform of \( f(x) \) is 5-valued. Hence the result.

We summarize the Hadamard transform values of the three-term functions and their (decimated) WG transforms in Table 1. Note that the Hadamard transforms of both \( T3(x^{d}) \) and \( W G_{T3}(x^{d}) \) are 5-valued. The following theorem states the non-linearity of the WG transform of the three-term function and with its decimation.

\[ \text{Theorem 3.9. For } m = 2k - 1 \text{ and } d = 2^{k} - 1, \text{ the nonlinearity of both } W G_{T3}(x) \text{ and } W G_{T3}(x^{d}) \text{ is } 2^{m-1} - 2^{\frac{m+1}{2}}. \]
Table 1. A summary of the Hadamard transform values of three-term functions.

| Functions \( w(x) = T_3(x^{d_3}+1) = \text{Tr}(x + x' + x''') \) | Hadamard Transform values | Ref. |
|---|---|---|
| \( g(x) = T_3(x^{d_3}+1) = \text{Tr}(x + x'' + x''') \) | 3-valued | [11] |
| \( \text{at most 5-valued} \) | | |
| \( W_{G_0}(x) = \text{Tr}(x + (x+1)' + (x+1)''' \) | 3-valued | Lemma 3.7 |
| \( W_{G_1}(x) = \text{Tr}(x + (x+1)'' + (x+1)''' \) | at most 5-valued | Lemma 3.7 |
| \( W_{G_3}(x^d) = \text{Tr}(x^d + (x^d+1)' + (x^d+1)'' \) | at most 5-valued | Theorem 3.8 |

Proof. According to Theorem 3.8, the Walsh spectra of \( W_{G_3}(x) \) and \( W_{G_3}(x^d) \) are \( \{0, \pm 2^{\frac{m-1}{2}}, \pm 2^{\frac{m+1}{2}} \} \). Therefore, the nonlinearity of \( W_{G_3}(x) \) and \( W_{G_3}(x^d) \) is \( 2^{m-1} - 2^{\frac{m+1}{2}} \). Hence the proof.

3.4.3. Invariance of \( W_{G_3}(x) \). We now present a conjecture about the invariance property of the WG transform of the three-term function.

Conjecture 1. For \( f(x) = W_{G_3}(x^d) \) with \( d = 2^k - 1 \) and \( m = 2k - 1 \), \( f(x) \) is invariant under the WG transform.

We have experimentally checked the invariance under the WG transform property of other decimations of \( W_{G_3} \) for \( 5 \leq m \leq 15 \), none of them has the invariance property except the one in Conjecture 1.

4. Ideal tuple distribution of \( W_{G_3}(x^d) \) and \( W_{G_3}(x^d) \) in FDBG

In this section, we study the ideal tuple distribution property of the decimated WG transformations and the WG transform of three-term functions in the filtering de Bruijn generator (FDBG).

4.1. WG Transformations in FDBG. The main result of this subsection is the proof of the conjecture on the ideal tuple distribution for the WG transformation in Theorem 4.2 by Mandal et al. in [29], which establishes the ideal tuple distribution property of the decimated WG transformation. Before proving the main result, we first show the \( x_0 \)-independence of \( WG(x^d) \).

Theorem 4.1. For \( 3k \equiv 1 \mod m \), the WG transformation with decimation \( d = (2^m-k+1) - 1 \), denoted by \( f(x) = WG(x^d) \), can be written as \( f(x) = x_0 + f'(x_1, x_2, \ldots, x_{m-1}) \) where \( x = x_0 + \cdots + x_{m-1}a^{m-1} \in \mathbb{F}_{2^m} \) and \( f'(x_1, \ldots, x_{m-1}) = f(z) \), which is independent of \( x_0 \).

Proof. According to Proposition 1, the decimated WG transformation is written as \( f(z) = x_0 + f'(x_1, x_2, \ldots, x_{m-1}) \) where \( z = x_1a + \cdots + x_{m-1}a^{m-1} \in \mathbb{F}_{2^m} \). As \( WG_f(x) = f(x+1) + \text{Tr}(1) \), applying Theorem 3.6, we have \( f(x) + WG_f(x) = 0 \). Thus, applying \( f(x) + WG_f(x) = 0 \) and \( \text{Tr}(1) = 1 \) for odd \( m \), \( f(x) \) can be written as \( f(x) = x_0 + f(z) \) where \( f(z) = f'(x_1, \ldots, x_{m-1}) \), which is independent of \( x_0 \). Hence the assertion is established.

Example 2 (Continued). Let \( m = 7 \) and \( d = 7 \). Then \( f(x) = W_{G_3}(x^7) = \text{Tr}(x^3 + z^7 + z^21 + z^{49} + z^{76}) = x_0 + x_0(f(z) + WG_f(z)) + \text{Tr}(z^3 + z^7 + z^{21} + z^{49} + z^{76}) = x_0 + \text{Tr}(z^3 + z^7 + z^{21} + z^{49} + z^{76}) \) as \( \text{Tr}(1) = 1 \), \( WG_f(x) = f(x) \), and \( x = x_0 + z \in \mathbb{F}_{2^m} \). Thus, \( f(x) \) has the \( x_0 \)-independence form.
We are now ready to prove Theorem 4.2. Note that we determined the exact value of the decimation in Theorem 4.2.

**Theorem 4.2.** Let \( m \) be odd and \( 3k \equiv 1 \pmod{m} \), and \( \text{WG} : \mathbb{F}_{2^m} \to \mathbb{F}_2 \) be the Welch-Gong transformation defined in Facts 1 and 2. For \( d = 2^m - k + 1 \) and the filtering de Bruijn sequence \( b \) with \( \text{WG}(x^d) \) as filtering function in the FDBG has an ideal \( \ell \)-tuple distribution where \( \ell = (n - m + 1) \) and \( n \) is the length of the NLFSR generating a de Bruijn sequence.

**Proof.** The proof follows by combining Lemma 2.7 and Theorem 4.1. In Theorem 4.1, it is shown that for decimation \( d = 2^m - k + 1 \), the decimated WG transformation \( f(x) = \text{WG}(x^d) \) has the \( x_0 \)-independence form. Applying Lemma 2.7 on \( f(x) \), it follows that the filtering sequence produced by the FDBG with \( f(x) \) as a filtering function has the ideal \( \ell = (n - m + 1) \)-tuple distribution. Hence the result.

**Example 3.** The feedback function \( g(x_0, \ldots, x_6) = x_0 + x_2 + x_4 + x_1x_2 + \prod_{i=1}^{5}(1 + x_i) \) generates a de Bruijn sequence \((a)\) of period \(2^7\). Considering the WG transformation over \( \mathbb{F}_{2^5}\) where \( m = 5 \) and \( k = 2 \), and then \( d = 2^5 - 2 + 1 - 1 = 15 \). The WG transformation over \( \mathbb{F}_{2^5}\) is given by \( \text{WG}_{T_5}(x) = T_r(x + (x + 1)^5 + (x + 1)^{13} + (x + 1)^{19} + (x + 1)^{21}) = T_r(x^{19}) \). The decimated WG transformation is \( f(x) = \text{WG}_{T_5}(x^{15}) = T_r(x^5) = x_0 + x_3 + x_1x_2 + x_1x_4 + x_2x_3 + x_2x_4 \) over \( \mathbb{F}_{2^5}\) as a filtering function in the FDBG where \( \mathbb{F}_{2^5}\) is defined using \( a^5 + a^3 + 1 = 0 \). The de Bruijn sequence of period \(2^7\) is given by

\[
a = 111111100011010000100011001100011000001001011101100101111010101101110110111011011101110111111111110110110111011101101011010101101010110101011010101101010101101010110101
\]

The filtering sequence with filtering function \( f(x) \) over \( a \) is given by

\[
b = 000111111011001111101001110110111111110101001111100111111111110000010110010000011111111100010110011111100000100101111111111100001011011010011010011111110000010010000011111111111101011001011111101011010011001001
\]

The sequence \( b \) has an ideal up to 3-tuple distribution, i.e., all possible binary tuples of length up to 3 occur equally likely.

**Remark 1.** \( \text{WG}(x^d) \) with \( d = 2^m - k + 1 \) has the form \( x_0 + f'(x_1, \ldots, x_{m-1}) \) for any polynomial basis of the finite field. Considering all polynomial bases, defined by primitive polynomials, the number of WG transformations which have the form in Theorem 4.1 is at least \( \frac{\phi(2^m-1)}{m} \) where \( \phi(\cdot) \) is the Euler totient function.

### 4.2. WG Transform of Three-Term Functions in FDBG

We have the following theorem about the ideal tuple distribution of the WG transform of the three-term function when it is used as a filtering function in the FDBG.

**Theorem 4.3.** If Conjecture 1 is true for \( m = 2k - 1 \) and \( d = 2^k - 1 \), the decimated WG transform of three-term function \( T_3(x) \) can be written as \( f(x) = \text{WG}_{T_3}(x^d) = x_0 + f'(x_1, \ldots, x_{m-1}) \) where \( x = x_0 + \cdots + x_{m-1}a^{m-1} \) and \( f' \) is a function in \( (m-1) \) variables and is independent of \( x_0 \) and hence the filtering de Bruijn sequence \( b \) with \( \text{WG}_{T_3}(x^d) \) as filtering function in the FDBG has an ideal \( \ell \)-tuple distribution where \( \ell = (n - m + 1) \) and \( n \) is the length of the NLFSR generating a de Bruijn sequence.

**Proof.** The proof directly follows from Lemma 2.7 and Conjecture 1.
Example 4. Let \( m = 5 \) and \( k = \frac{m+1}{2} = 3 \). The three-term function is \( T3(x) = \text{Tr}(x + x^7 + x^9) \) over \( \mathbb{F}_{2^5} \) and \( \text{WG}_T3(x) = \text{Tr}(x + (x + 1)^7 + (x + 1)^9), x \in \mathbb{F}_{2^5} \). Consider the decimation \( d = 2^k - 1 = 7 \). Then \( f(x) = \text{WG}_T3(x^7) \) is given by

\[
\begin{align*}
f(x) &= \text{Tr}(x^7 + (x^7 + 1)^7 + (x^7 + 1)^9) \\
&= \text{Tr}(1 + x + x^7 + (x^7 + 1)^7) \\
&= \text{Tr}(x + x^4 + x^{18}) = \text{Tr}(x^9).
\end{align*}
\]

The \( x_0 \)-independence form of \( f(x) \) is given by \( f(x) = x_0 + x_1 + x_2 + x_4 + x_1x_2 + x_2x_4 + x_3x_4 \) where \( \mathbb{F}_2^5 \) is defined by \( \alpha^5 + \alpha^3 + 1 = 0 \).

Remark 2. If Conjecture 1 is true, the representation of \( \text{WG}_T3(x^d) = x_0 + f'(x_1, \cdots, x_{m-1}) \) is independent of the basis of \( \mathbb{F}_{2^m} \). For the WG transform of the three-term function \((k' = 2)\), the decimation is also of the form \( d = 2^j - 1 \) with \( J = m - k + 1 = 2k - 1 - k + 1 = k \) where \( m = 2k - 1 \), implying \( 2k \equiv 1 \mod m \).

5. Quadratic Functions as Filtering Functions in FDBG

In this section, we use quadratic functions as filtering functions in the FDBG and present the results on the ideal tuple distribution.

5.1. The Gold Function. The Gold function is defined as [17]

\[
G(x) = \text{Tr}(x^d), x \in \mathbb{F}_{2^m}
\]

where \( d = 2^k + 1, k \leq \frac{m-1}{2} \) and \( \gcd(k, m) = 1 \) is called the Gold exponent. The WG transform of \( G(x) \) is given by

\[
f(x) = \text{Tr}((x + 1)^d + 1) = \text{Tr}(x^d) = G(x).
\]

Thus, the Gold function is invariant under the WG transform. When the Gold function is used as a filtering function, we have the following theorem for the ideal tuple distribution.

Theorem 5.1. For odd \( m \) and \( d = 2^k + 1, k \leq \frac{m-1}{2} \) and \( \gcd(k, m) = 1 \), the filtering de Bruijn sequence with the Gold function as a filtering function, the filtering sequence \( b \) has an ideal \( t \)-tuple distribution where \( t = (n - m + 1) \) and \( n \) is the length of the NLFSR generating a de Bruijn sequence.

Proof. Let \( x = x_0 + x_1 \alpha + \cdots + x_{m-1} \alpha^{m-1} = x_0 + z \in \mathbb{F}_{2^m} \) where \( z = x_1 \alpha + \cdots + x_{m-1} \alpha^{m-1} \). Then \( \text{Tr}(x^d) \) can be written as

\[
\begin{align*}
\text{Tr}(x^d) &= \text{Tr}((x_0 + x_1 \alpha + \cdots + x_{m-1} \alpha^{m-1})^d) \\
&= x_0 + \text{Tr}(z^{2^k+1}), z = x_1 \alpha + \cdots + x_{m-1} \alpha^{m-1}
\end{align*}
\]

as \( \text{Tr}(z) = \text{Tr}(z^{2^k}) \). Therefore the Gold function \( G(x) \) can be written as \( G(x) = x_0 + G'(x_1, \cdots, x_{m-1}) \) where \( G'(x_1, \cdots, x_{m-1}) = \text{Tr}(z^{2^k+1}) \). Applying Lemma 2.7 on the Gold function \( G(x) \) as a filtering function, the filtering sequence \( b \) has an ideal \( (n - m + 1) \)-tuple distribution. \( \square \)
5.2. Quadratic Functions. Let \( m \) be a positive integer. The quadratic Boolean function over \( \mathbb{F}_{2^m} \) is defined as

\[
Q(x) = \sum_i \text{Tr}^{r_i}_1(a_i x^{2^i+1}) + \text{Tr}(c x), \quad c \in \mathbb{F}_{2^m}, a_i \in \mathbb{F}_{2^r}, 0 \leq i \leq \left\lceil \frac{m+1}{2} \right\rceil,
\]

where \( \text{Tr}^{r_i}_1(x) \) is a trace function from \( \mathbb{F}_{2^r} \) to \( \mathbb{F}_2 \) and \( r_i | m \), and \( x^{2^i+1} \) is a function over \( \mathbb{F}_{2^r} \) and \( a_i \in \mathbb{F}_{2^r} \). For proper choices of parameters \( m, i, j, a_i \) and \( c \), \( Q(x) \) can generate the Gold-like sequences introduced by Boztas and Kumar [2] and the sequences of Yu and Gong [40]. For specific definitions of the quadratic function \( Q(x) \) in [2, 40], the results on the Hadamard transform can be found in [2, 40], respectively.

\[\text{Lemma 5.2.}\] \( Q \) is odd and \( Q(x) \) be the quadratic Boolean function defined in Eq. (13). Then \( Q(x) \) is invariant under the WG transform iff \( \sum_i \text{Tr}^{r_i}_1(a_i + a_i^{2^m-1}) = 0 \) and \( \sum_i \text{Tr}^{r_i}_1(a_i + c + 1) = 0. \)

\[\text{Proof.}\] The WG transform of \( Q(x) \), denoted by \( \text{WG}_Q(x) \), is:

\[
\text{WG}_Q(x) = \sum_i \text{Tr}^{r_i}_1(a_i(x+1)^{2^i+1} + c(x+1) + 1)
= \sum_i \text{Tr}^{r_i}_1(a_i x^{2^i+1}) + \text{Tr}(c x) + \sum_i \text{Tr}^{r_i}_1(x(a_i + a_i^{2^m-1})) + \sum_i \text{Tr}^{r_i}_1(a_i + c + 1)
= Q(x) + \sum_i \text{Tr}^{r_i}_1(x(a_i + a_i^{2^m-1})) + \sum_i \text{Tr}^{r_i}_1(a_i + c + 1).
\]

The quadratic function \( Q(x) \) is invariant under the WG transform iff \( \sum_i \text{Tr}^{r_i}_1(x(a_i + a_i^{2^m-1})) + \sum_i \text{Tr}^{r_i}_1(a_i + c + 1) = 0. \) This implies \( \sum_i \text{Tr}^{r_i}_1(a_i + a_i^{2^m-1}) = 0 \) and \( \sum_i \text{Tr}^{r_i}_1(a_i + c + 1) = 0. \) Let \( x = x_0 + x_1 \alpha + \cdots + x_{m-1} \alpha^{m-1} = x_0 + z \in \mathbb{F}_{2^m}. \) Then \( Q(x) \) can be written in terms of \( x_0 \) and \( z \) as

\[
Q(x) = x_0 \left( \sum_i \text{Tr}^{r_i}_1(a_i) + \text{Tr}(c) \right) + x_0 \left( \sum_i \text{Tr}^{r_i}_1(z(a_i + a_i^{2^m-1})) \right) + \sum_i \text{Tr}(a_i z^{2^i+1})
+ \text{Tr}(c z).
\]

Moreover, when \( m \) is odd and \( Q(x) \) is WG-invariant, \( Q(x) \) has the \( x_0 \)-independence form.

We have the following result about the ideal tuple distribution when \( Q(x) \) is used as a filtering function.

\[\text{Theorem 5.3.}\] For \( m \) odd, the filtering de Bruijn sequence \( b \) with the quadratic function \( Q(x) \) defined above as a filtering function has an ideal \( t \)-tuple distribution if \( \sum_i \text{Tr}^{r_i}_1(a_i + a_i^{2^m-1}) = 0 \) and \( \sum_i \text{Tr}^{r_i}_1(a_i + c + 1) = 0 \) where \( t = (n-m+1) \) and \( n \) is the length of the NLFSR generating a de Bruijn sequence.

\[\text{Proof.}\] The proof follows from the fact that, according to Eq. (14) in Lemma 5.2, \( Q(x) \) can be written as \( Q(x) = x_0 + g(x_1, \cdots, x_{m-1}) \) when \( Q(x) \) has the WG-invariance property, and applying Lemma 2.7 where \( Q(x) \) is the filtering function.

\[\text{Remark 3.}\] We note that not all quadratic functions are orthogonal functions. For instance, the Gold or Gold-like functions are orthogonal functions. However, we presented a general result on the ideal tuple distribution for quadratic functions.
6. Experimental results on KPFs

In hope of successfully finding the ideal \((n - m + 1)\)-tuple distribution for the WG transformations and the WG transform of three-term functions with decimation \(d = 2^{m-k+1} - 1\), we consider to check the ideal tuple distribution property of the Kasami power function (KPF) construction (see Section 2.2) in the FDBG, as it is a generalization of the five-term and three-term functions. The reader is referred to [21, 11] for the details about the KPF construction. We denote by \(\text{KPF}\) a generalization of the five-term and three-term functions. The reader is referred to the Kasami power function (KPF) construction (see Section 2.2) in the FDBG, as it is described in Section 2.4 and examined the ideal tuple distribution of the filtering de Bruijn generator. We denote by \(\text{WG}\) the set of all KPFs for different \(k\) to \([21, 11]\) for the details about the KPF construction.

Table 2. Experimental results for ideal \(t\)-tuple distributions of the WG transform of the Kasami power functions for \(k' = 3, 4\) and 5. When \(k' = 3\), \(WG_{R_3}(x^d)\) over \(\mathbb{F}_{2^m}\) is the WG transformation functions.

\[
\begin{array}{|c|c|c|c|c|c|c|}
\hline
\text{Input size } m & \text{NLFSR length } n & \text{\(t\)-tuple dist.} & \text{Input size } m & \text{NLFSR length } n & \text{\(t\)-tuple dist.} \\
\hline
8 & 9 - 19 & 2 & 9 & 10 - 19 & 2 \\
10 & 11 - 19 & 2 & 11 & 12 - 19 & 2 \\
14 & 15 - 19 & 2 & 13 & 14 - 19 & 2 \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|c|c|c|}
\hline
\text{Input size } m & \text{NLFSR length } n & \text{\(t\)-tuple dist.} & \text{Input size } m & \text{NLFSR length } n & \text{\(t\)-tuple dist.} \\
\hline
9 & 10 - 19 & 2 & 8 & 9 - 19 & 2 \\
11 & 12 - 19 & 2 & 12 & 13 - 19 & 2 \\
13 & 14 - 19 & 2 & 14 & 15 - 19 & 2 \\
\hline
\end{array}
\]

Conjecture 2. For \(m\) odd, \(WG_h(x^d), \forall h \in \text{KPF}\) and all decimations except for those two cases in Theorem 3.6 and Conjecture 1, are not invariant or complementary invariant under the WG transform, i.e., for \(f(x) = WG_h(x^d), \forall h \in \text{KPF}\) and \(\forall d, \gcd(d, 2^m - 1) = 1\) and

\[
WG_f(x) = \begin{cases} f(x) & m \text{ odd} \\ f(x) + 1 & m \text{ even.} \end{cases}
\]

or

\[
WG_f(x) = \begin{cases} f(x) + 1 & m \text{ odd} \\ f(x) & m \text{ even.} \end{cases}
\]

An empirical investigation on WG transformations (as filtering functions) over \(\mathbb{F}_{2^m}\) where \(m\) is even was conducted in [29] to check the ideal tuple distribution of filtering de Bruijn sequences. The results show that the filtering de Bruijn generators have up to 2-tuple distribution (\(t = 2\)) (see Table 2a). For odd \(m\), we also use the three-term function \(w(x)\) defined in Section 3.4 and the WG transform of \(w(x)\) over \(\mathbb{F}_{2^m}\) with all decimations as filtering functions in the FDBG. None of the functions has the ideal \(t\)-tuple distribution for \(t = (n - m + 1)\). Moreover, our
experimental results on the five-term functions \( \text{Tr}(R_3(x)) \) as filtering functions in the FDBG show that there is no five-term function with a decimation that ensures the ideal \( t \)-tuple distribution property with \( t = (n - m + 1) \).

We further considered the power functions \( f(x) = \text{Tr}(x^e) \) and \( WG_f(x) \) where \( e \) is a Kasami, Welch, Niho, inverse, or Dobbertin exponent with all decimations. None of them have the ideal tuple distribution property, except those decimations leading to the Gold (exponents) functions.

7. Conclusions and discussions

We have established a connection between the WG-invariance property and the ideal tuple distribution in the FDBG model. A filtering function in the FDBG can ensure the ideal tuple distribution if the (Boolean) filtering function has the \( x_0 \)-independence form. For cryptographic applications, the filtering function should have strong cryptographic properties such as high nonlinearity. In terms of sequences generated by an orthogonal function, the orthogonal property is equivalent to the auto-correlation property of the sequence. Note that any random function with \( x_0 \)-independence form can be used in the FDBG to ensure ideal tuple distribution, but it is hard to guarantee its increased nonlinearity, low-valued correlation property, and orthogonal property. Especially, for a random function, it is hard to ensure low-valued (absolute) Walsh spectrum. Thus, we have started with orthogonal functions such as WG transforms and KPFs whose Hadamard transforms and other properties are well-studied and known, and investigated their ideal tuple distributions in the FDBG. Figure 2 depicts relations among Hadamard transform (HT), WG-invariance (WG-inv), \( x_0 \)-independence, and ideal tuple distribution properties. In Figure 2, we can observe that there is a relation between the Hadamard transform and the WG-invariance property (see Lemma 3.2). However, given any Boolean function \( f \) over \( \mathbb{F}_{2^m} \), it is not easy to theoretically determine the set \( \{ \lambda : \text{Tr}(\lambda) = 1 \text{ when } \hat{f}(\lambda) \neq 0 \} \).

\[ \begin{align*}
\text{Low-valued} & \quad \text{HT} & \quad \text{Tr}(\lambda) = 1 \quad \text{if and only if} \quad \hat{f}(\lambda) \neq 0 \\
T_5, T_3, \text{Quad} & \quad \text{WG-inv} & \quad \text{if for } m \text{ odd} \\
\text{WG, KPF} & \quad \text{WG}_{T_5}(x^d) \quad \text{if } d \quad \text{if } d \quad \text{if } d \\
\text{Quad} & \quad \text{WG}_{T_3}(x^d) & \quad \text{Quad} & \quad \text{Quad} \\
& \quad \text{Ideal Tuple Distribution} & \quad (n - m + 1)
\end{align*} \]

Figure 2. Relations among Hadamard Transform, WG-inv, \( x_0 \)-independence and ideal tuple distribution. \( g(\cdot) \) is independent of \( x_0 \). \( \leftrightarrow \) denotes if and only if condition, \( \rightarrow \) denotes if condition and \( n \) is the NLFSR length.

In this article, we have considered the problem of converting a uniformly distributed pseudorandom sequence into another uniformly distributed sequence where the distribution of binary tuples of various lengths up to \( n \) is taken into consideration. We introduced the invariant under the WG transform property of a Boolean function over a finite field and studied this property on the orthogonal functions. We proved that the decimated WG transformation with \( d = 2^{m-k+1} - 1 \) has the invariance under the WG transform property, which results in an ideal \( t \)-tuple distribution of a filtering sequence up to \( t = (n - m + 1) \) where \( n \) is the length of the NLFSR and \( m \) is the input size of the filtering function. We conjectured that
the WG transform of a three-term function with decimation $d = 2^k - 1$ has the invariance property. Moreover, the ideal tuple distribution of the quadratic functions are studied. The Hadamard transform of the WG transform of a three-term function and the decimated one is determined, which is 5-valued. The results on the nonlinearity of these filtering functions with the above decimations are presented.

In the future work, we shall prove the conjectures on the invariance property of $WG_{T^3}(x^d)$ and the KPFs. We will also develop (algorithmic) techniques to efficiently check whether a Boolean function is invariant under the WG transform. More specifically, given a function $f(x) : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ with univariate polynomial representation, how to efficiently determine whether the function is invariant under the WG transform. From a differential cryptanalysis point of view, the invariance under the WG transform of a Boolean function means its differential at 1 is constant. An interesting question is to investigate how to use the (complementary) WG-invariance property of a (filtering) Boolean function to launch an attack on stream ciphers.

**Acknowledgments**

The authors would like to thank the reviewers for their valuable comments to improve the quality of the paper. This research was supported by the U.S. Department of Commerce, National Institute of Standards and Technology award no. 60NANB16D289.

**References**

[1] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.
[2] S. Boztas and P.V. Kumar, Binary sequences with Gold-like correlation but larger linear span, *IEEE Trans. Inf. Theory*, **40** (1994), 532–537.
[3] N. G. de Bruijn, A combinatorial problem, *Proc. Koninklijke Nederlandse Akademie v. Wetenschappen*, **49** (1946), 758–764.
[4] A. Canteaut, *Analysis and Design of Symmetric Ciphers*, Habilitation for directing Theses, University of Paris 6, 2006. Available from: https://www.rocq.inria.fr/secret/Anne.Canteaut/canteaut-hdr.pdf.
[5] C. Carlet, Boolean functions for cryptography and error correcting codes, Chapter of the monography Boolean models and methods in mathematics, computer science, and engineering, Cambridge University Press, (2010), 257–397.
[6] A. H. Chan, R. A. Games, and E. L. Key, On the complexities of de Bruijn sequences, *Journal of Combinatorial Theory, Series A*, **33** (1982), 233–246.
[7] A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth and P. V. Kumar, On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code, *IEEE Trans. Inf. Theory*, **46** (2000), 680–687.
[8] T. W. Cusick and P. Stǎnicǎ, *Cryptographic Boolean Functions and Applications*, Elsevier/Academic Press, Amsterdam, 2009.
[9] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal information processing standards publication, FIPS PUB 186-2, Reaffirmed, 2000.
[10] J. F. Dillon, Multiplicative difference sets via additive characters, *Designs, Codes and Cryptography*, **17** (1999), 225–235.
[11] J. F. Dillon and H. Dobbertin, New cyclic difference sets with singer parameters, *Finite Fields and Their Applications*, **10** (2004), 342–389.
[12] L. Ding, C. Jin, J. Guan and Q. Wang, Cryptanalysis of lightweight WG-8 stream cipher, *IEEE Trans. Inf. Forensics and Security*, **9** (2014), 645–652.
[13] L. Ding, C. Jin, J. Guan, S. Zhang, T. Cui, D. Han and W. Zhao, Cryptanalysis of WG family of stream ciphers, *Computer Journal*, **58** (2015), 2677–2685.
[14] The eStream project, (2008). Available from: http://www.escrypt.eu.org/stream/project.html.
[15] X. Fan, K. Mandal and G. Gong, WG-8: A lightweight stream cipher for resource-constrained smart devices, 9th International Conference on Quality, Reliability, Security and Robustness in Heterogeneous Networks, Springer Berlin, (2013), 617–632.

[16] X. Fan, N. Zidaric, M. Aagaard and G. Gong, Efficient hardware implementation of the stream cipher WG-16 with composite field arithmetic, The 2013 ACM Workshop on Trustworthy Embedded Devices (TrustED'13), ACM Press, (2013), 21–34.

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

[18] J. Dj Golić, On the security of nonlinear filter generators, in 1996 Proceedings of Fast Software Encryption, Springer, Berlin, Heidelberg, (1996), 173–188.

[19] S. W. Golomb, On the classification of balanced binary sequences of period $2^n - 1$, IEEE Trans. Inf. Theory, 26 (1980), 730–732.

[20] S. W. Golomb, Shift register sequences, Aegean Park Press, Laguna Hills, CA, (1981).

[21] S. W. Golomb and G. Gong, Signal Design for Good Correlation: For wireless Communication, Cryptography and Radar, Cambridge University Press, New York, 2005.

[22] G. Gong, P. Gaal and S. W. Golomb, A suspected infinity class of cyclic Hadamard difference sets, Proceedings of 1997 IEEE Information Theory Workshop, Longyearbyen, Syllbard, Norway, (1997).

[23] G. Gong and A. Youssef, Cryptographic properties of the Welch-Gong transformation sequence generators, IEEE Trans. Inf. Theory, 48 (2002), 2837–2846.

[24] B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, Canadian Journal of Mathematics, 14 (1962), 614–625.

[25] M. Joseph, G. Sekar and R. Balasubramanian, Distinguishing attacks on (ultra-)lightweight WG ciphers, in 5th International Workshop on Lightweight Cryptography for Security and Privacy, LightSec 2016, Springer International Publishing, (2017), 45–59.

[26] K. Mandal and G. Gong, Cryptographically strong de Bruijn sequences with large periods. in Selected Areas in Cryptography, SAC 2012, Lecture Notes in Comput. Sci., Springer, Heidelberg, 7707 (2012), 104–118.

[27] K. Mandal and G. Gong, Feedback reconstruction and implementations of pseudorandom number generators from composited de Bruijn sequences, IEEE Trans. Computers, 65 (2016), 2725–2738.

[28] K. Mandal, G. Gong, X. Fan and M. Aagaard, Optimal parameters for the WG stream cipher family, Cryptography and Communications, 6 (2014), 117–135.

[29] K. Mandal, B. Yang, G. Gong and M. Aagaard, On ideal $t$-tuple distribution of filtering de Bruijn sequence generators, Cryptography and Communications, 10 (2018), 629–641.

[30] J. L. Massey, Shift-register synthesis and BCH decoding, IEEE Trans. Inform. Theory, 15 (1969), 122–127.

[31] Y. Nawaz and G. Gong, WG: A family of stream ciphers with designed randomness properties, Information Sciences, 178 (2008), 1903–1916.

[32] Y. Nawaz and G. Gong, The WG stream cipher, (2005). Available from: http://www.ecrypt.eu.org/stream/p2ciphers/wg/wg_p2.pdf.

[33] J.-S. No, S. W. Golomb, G. Gong, H. K. Lee and P. Gaal, Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation, IEEE Trans. Inform. Theory, 44 (1998), 814–817.

[34] M. A. Orumiehchiha, J. Pieprzyk and R. Steinfeld, Cryptanalysis of WG-7: A lightweight stream cipher, Cryptography Communications, 4 (2012), 277–285.

[35] H. El-Razouk, A. Reyhani-Masoleh and G. Gong, New implementations of the WG stream cipher, IEEE Trans. on VLSI, 22 (2014), 1865–1878.

[36] S. Rönningen, Improving algebraic attacks on stream ciphers based on linear feedback shift register over $F_{2^k}$, Designs Codes Cryptography, 82 (2017), 27–41.

[37] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

[38] T. Siegenthaler, R. Forré and A. W. Klener, Generation of binary sequences with controllable complexity and ideal $r$-tupel distribution, in Advances in Cryptology–EUROCRYPT 87, Lecture Notes in Comput. Sci, 304 (1987), 15–23.

[39] N. Y. Yu and G. Gong, Crosscorrelation properties of binary sequences with ideal two-level autocorrelation, in Proceedings of the 4th International Conference on Sequences and Their Applications (SETA'06), Lecture Notes in Comput. Sci, Springer, Berlin, Heidelberg, 4086 (2006), 104–118.

[40] N. Y. Yu and G. Gong, A new binary sequence family with low correlation and large size, IEEE Trans. Inf. Theory, 52 (2006), 1624–1636.
[41] S. V. Smyshlyaev, Perfectly balanced Boolean functions and Golić conjecture, Journal of Cryptology, 25 (2012), 464–483.
[42] G. Yang, X. Fan, M. Aagaard and G. Gong, Design space exploration of the lightweight stream cipher WG-8 for FPGAs and ASICs, Proceedings of the Workshop on Embedded Systems Security, (2013), 1–10.
[43] B. Yang, K. Mandal, M. D. Aagaard and G. Gong, Efficient composited de Bruijn sequence generators, IEEE Trans. on Computers, 66 (2017), 1354–1368.

Received June 2019; revised November 2020.

E-mail address: kmandal@unb.ca
E-mail address: ggong@uwaterloo.ca