On Ideal t-Tuple Distribution of Orthogonal Functions in Filtering De Bruijn Generators

Kalikinkar Mandal and Guang Gong, *Fellow IEEE*

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

Abstract. Uniformity in binary tuples of various lengths in a pseudorandom sequence is an important randomness property. We consider the problem of converting a uniformly distributed (binary t-tuples) pseudorandom sequence into another uniformly distributed (binary t'-tuples) pseudorandom sequence. In particular, an n-stage nonlinear feedback shift register (NLFSR) generating a de Bruijn sequence is considered as a source of generating t-tuples with $1 \leq t \leq n$, and then it is converted into another sequence (called filtering sequence) by applying a filtering function. Note that any filtering function can not be used to achieve uniformity in binary tuples of various lengths t' in the filtering sequence with $2 < t' \leq n$. We restrict ourselves to the family of orthogonal functions used as filtering functions, i.e., those correspond to binary sequences with ideal 2-level autocorrelation, which are also a rich source for known APN functions and almost bent functions. After the twenty years of discovery of Welch-Gong (WG) transformations, there is 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 the output sequences, up to $t = (n - m + 1)$ where m is the input length to the orthogonal functions. The conjecture of Mandal *et al.* in [28] about the uniform tuple distribution on the decimated WG transformation is proved. It is also shown that the Gold functions and the quadratic functions can ensure the ideal $(n - m + 1)$-tuple distribution. Experimental results for the ideal tuple distribution of the Kasami power functions as filtering functions are presented. A connection between the ideal tuple distribution and the invariance under the WG transform property is established.

Keywords. Pseudorandom sequence, De Bruijn sequence, Nonlinear feedback shift register, Ideal tuple distribution, WG transformation, Three-term function, Quadratic function

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 [18, 19, 20]. In particular, the ability of producing uniformly distributed bit sequences of various lengths is one of the desirable properties of a pseudorandom generator. The goal of producing uniformly distributed binary tuples of certain lengths by a pseudorandom generator is the same as that of a randomness extractor. Feedback shift register is a tool for generating pseudorandom sequences, which are of two types namely linear feedback shift registers (LFSRs) and nonlinear feedback shift registers (NLFSRs) [19].

We consider an NLFSR that generates a binary sequence of period 2^n as a uniform source of producing bit sequences. An n-stage NLFSR that generates a sequence of period 2^n is known as a *de Bruijn sequence generator* [3, 19], which guarantees long period 2^n, uniformity on occurrence of ℓ-bit sequences ($1 \leq \ell \leq n$), known as *ideal n-tuple distribution*, and high linear complexity, at least $2^{n-1} + n$ [6]. Although de Bruijn sequences have good randomness properties, they cannot be directly used because of the invertible property of its feedback function, which leads to recovering the seed and that is not permissible in many applications such as cryptographic applications. In this article, we consider the problem of converting a uniformly distributed sequence produced by the NLFSR source to another uniformly distributed source. More precisely, we apply a filtering function to the NLFSR and try to make binary tuples uniformly distributed in the filtering sequence for a suitable choice of a filtering function. A filtering de Bruijn generator consists of an NLFSR generating a de Bruijn sequence as a source of generating a bitstream/sequence and a filtering function distilling the sequences from the source. Of course, the maximum length on the uniformly distributed bit sequences or the ideal tuple distribution will be less than or equal to n. In general, any filtering function cannot be used to achieve the uniformity on ℓ-tuples for large values of $\ell\,(\leq n)$. Like a randomness extractor [1], a suitable filtering function can make a uniformly distributed sequence to another uniformly distributed sequence provided that the input source is uniformly distributed. If the NLFSR source is not uniform, that means it does not generate a de Bruijn (span n) sequence, then even for a suitable choice of a filtering function, the filtering source or sequence will not be uniform. We emphasize that we are interested in those filtering functions whose properties will also be known, which may be suitable for cryptographic applications.

1.1 Problem Statement and Highlights of Our Results

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 [20]. 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 $a_i = f(\alpha^i), i = 0, \cdots, 2^m - 2$ where α is a primitive element in $\mathbb{F}_{2^m}$ [20].

A Welch-Gong (WG) transformation sequence is to apply transform $WG_f(x) = f(x+1)+\mathrm{Tr}(1)$ where $\mathrm{Tr}(x)$ 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 [32]. The Welch-Gong (WG) transformation is named by Solomon Golomb. WG transformation sequences have 2-level autocorrelation, which is first conjectured in 1997 [32], proved by Dillon [9] for odd m and Dillon and Dobbertin [10] in 2004 for even m. A detailed investigation of cryptographic properties of WG sequences is presented in [22]. In the same paper [10], Dillon and Dobbertin also provided a family of binary sequences with 2-level autocorrelation which correspond to the so-called Kasami power functions. In 2005, Nawaz and Gong proposed the WG stream cipher and submitted to the eStream project in 2005 [13, 31], and completed analysis of security and hardware implementation costs are presented in [30, 41, 34, 15] 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 [33, 11, 12, 24, 35, 34, 41, 14].

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, $f(x) = WG_f(x) = f(x+1) + \mathrm{Tr}(1)$ where $f(x) = WG_h(x^d)$ and $h(x)$ is the WG transform of either a 5-term sequence, denoted as $T5(x)$ or a 3-term sequence, denoted as $T3(x)$ for a unique decimation number d with Hamming weight greater than one. Specifically, $f(x)$ is invariant under the WG transform (WG-invariance) when $f \in \{WG_{T5}(x^d), WG_{T3}(x^{d'})\}$ where $d = 2^{m-k+1}-1$ with $3k \equiv 1 \bmod m$, and $d' = 2^k - 1$ with $m = 2k-1$. Those decimations are unique. Note that $WG_{T3}(x)$ 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 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 [38] where Yu and Gong studied their respective Hadamard transforms of $WG_{T5}(x^d)$ and $T3(x^{d'})$. Using this result, we are able to establish that the uniformity in binary tuples of various lengths in the filtering sequences. We show that $f \in \{WG_{T5}(x^d), WG_{T3}(x^{d'})\}$ 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 [20].

1.2 Related Work

Ideal tuple distributions of LFSR-based nonlinear filtering generators have been studied in the literature [17, 4, 37, 30]. Siegenthaler, Forré and Kleiner in [37] 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 [37]. Golić [17] 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. Canteaut [4] proved the Golić conjecture for the sufficient condition. Smyshlyaev in [40] also proved the Golić conjecture. Recently, Mandal *et al.* [28] 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 in filtering a de Bruijn generator that guarantees ideal tuple distribution as well as have good and provable cryptographic properties. In this article, we consider orthogonal functions over finite fields as filtering functions and present our new results on ideal tuple distributions of the WG transform of orthogonal functions on de Bruijn generators. First, we introduce a new property called *invariant under the Welch-Gong (WG) transform* or *WG-invariance* property of a Boolean function and then 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. Second, 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 [28]. Third, we 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 decimations are presented. Finally, we show that the Gold function and quadratic functions are WG-invariant, thus can also be used to achieve ideal tuple distributions in the FDBG. With 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. Our experimental results show that there are no KPFs including all decimations that give the ideal tuple distribution in the FDBG.

The rest of the paper is organized as follows. We define some mathematical functions and provide a brief background on the concepts used in this paper in Section 2. In Section 3, we investigate the invariance under the WG transform of the WG transformations and the WG transform of the three-term function. The results on the ideal tuple distribution of WG transformations and the WG transform of the three-term functions are presented in Section 4. Sections 5 and 6 present the ideal tuple distribution results for quadratic functions, the experimental results, and a conjecture on the KPFs in the FDBG, respectively. In Section 7, we conclude the paper with a discussion and future work.

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 [28].

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 α 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 $\mathbb{F}_2$.
- $\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{m-1}}$ 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 λ 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 [20]. 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 1. *Let $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ be a Boolean function in m variables. The algebraic normal form (ANF) of f is defined by*

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

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. *[5, 20] The* Walsh-Hadamard transform *of a Boolean function f is defined as*

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

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

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

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

Definition 3. *[20] 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 4. *[38] Let $u(x)$ and $v(x)$ be two orthogonal functions. The* crosscorrelation *between $u(x)$ and $v(x)$, denoted by $C_{u,v}$, is defined as $C_{u,v}(\lambda) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{v(\lambda x) + u(x)}, \lambda \in \mathbb{F}_{2^m}$. In particular, when $v(x) = \mathrm{Tr}(x)$, $C_{u,Tr}$ is the Hadamard transform of $u(x)$, i.e, $C_{u,Tr}(\lambda) = \hat{u}(\lambda)$. Moreover, when $u(x)$ and $v(x)$ are trace functions, we denote $C_{u,v}$ by $H_e(\lambda^t) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(\lambda^t x) + \mathrm{Tr}(x^e)}$.*

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

$$f(x) = \sum_{i=1}^{r} \mathrm{Tr}_1^{m_i}(x^{t_i})$$

where t_i is a coset leader modulo $2^{m_i}-1$ and $m_i|m$. Let $\boldsymbol{\alpha} = \{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$ 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 $f(x) = f(x_0\alpha_0 + x_1\alpha_1 + \cdots x_{m-1}\alpha_{m-1}) = f_{\boldsymbol{\alpha}}(x_0, x_1, \cdots, x_{m-1})$, which is the Boolean representation of f. In the present article, we take only the polynomial basis $\{1, \alpha, \cdots, \alpha^{m-1}\}$ 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 $kk' \equiv 1 \bmod m$, $k < m$ and $\gcd(k, m) = 1$. Let $R(x)$ be a permutation polynomial over $\mathbb{F}_{2^m}$, which is recursively defined as [10, 20]

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

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

$$\begin{aligned} A_1(x) &= x,\ A_2(x) = x^{2^k+1} \\ A_{i+2} &= x^{2^{(i+1)k}} A_{i+1}(x) + x^{2^{(i+1)k}-2^{ik}} A_i(x), i \geq 1 \text{ and} \\ V_0(x) &= 0,\ V_2(x) = x^{2^k-1} \\ V_{i+2} &= x^{2^{(i+1)k}} V_{i+1}(x) + x^{2^{(i+1)k}-2^{ik}} V_i(x), i \geq 1 \end{aligned}$$

Furthermore, $R_{k'}(x)$ is a permutation over $\mathbb{F}_{2^m}$.

2.3 The Welch-Gong (WG) Transformation and Its Generalization

Let m be a positive integer and k be a positive integer such that $3k \equiv 1 \bmod m$. 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 $\mathbb{F}_{2^m}$ [20]. In fact, $u(x) = R_3(x)$. The Welch-Gong (WG) transformation [22] from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined as

$$WG(x) = \mathrm{Tr}(WGP(x)) = \mathrm{Tr}(u(x+1)+1)$$

where $WGP(x) = u(x+1)+1$ is called a WG permutation over $\mathbb{F}_{2^m}$. 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 $WG(x)$ is given by $WG(x^d)$.

Fact 1. *[27] Let k be a positive integer such that $3k \equiv 1 \pmod{m}$ and $m \equiv 2 \pmod{3}$. Then*

$$WG(x) = \ \mathrm{Tr}(u(x+1)+1) = \sum_{i \in I} \mathrm{Tr}(x^i) \tag{2}$$

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

$$WG(x) = \mathrm{Tr}(u(x+1)+1) = \sum_{i \in I} \mathrm{Tr}(x^i) \tag{3}$$

where $I = I_1 \cup I_2 \cup I_3 \cup I_4$, $I_1 = \{2^{\frac{k-1}{2}} + 2 + i :\ 0 \leq i \leq 2^{\frac{k-1}{2}} - 2\}$, $I_2 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k-1}{2}}(2^{j+1} - 1) + 2^j - 1) : 0 \leq j \leq \frac{k-7}{2}, 1 \leq i \leq 2^j\}$, $I_3 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k-1}{2}}(2^{\frac{k-3}{2}} - 1) + 2^{\frac{k-5}{2}} - 1) : 1 \leq i \leq 2^{\frac{k-5}{2}}\}$ and $I_4 = \{2^{\frac{k+1}{2}} + 1 + 2(i + 2^{\frac{k-1}{2}}(2^{\frac{k-1}{2}} - 1) + 2^{\frac{k-3}{2}} - 1) : 2 \leq i \leq 2^{\frac{k-3}{2}}\}$.

In [32], 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 $\mathrm{Tr}(u(x+1)+1) = \mathrm{Tr}(v(x+1)+1)$ where $u(x)$ is a permutation over $\mathbb{F}_{2^m}$.

Fact 3. *[32] Let $m \bmod 3 \neq 0$ 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 $v : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is defined by $v(x) = x + x^{r_1} + x^{r_2} + x^{r_3} + x^{r_4}$. The WG transformation is defined as $WG(x) = \mathrm{Tr}(v(x+1)+1)$.*

Below we extend the concepts of the WG transformation to any function over $\mathbb{F}_{p^m}$.

Definition 5. *Let $p > 1$ and $g(x)$ be a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$. We define $f(x) : \mathbb{F}_{p^m} \to \mathbb{F}_{p^\ell}$ where $\ell | m$ as*

$$f(x) = \mathrm{Tr}_\ell^m\big(g(x-a) - b\big) \text{ for fixed } a, b \in \mathbb{F}_{p^m}$$

where $Tr_\ell^m(x)$ 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

$$WG_{R_{k'}}(x) = \mathrm{Tr}(R_{k'}(x+1)+1), x \in \mathbb{F}_{2^m} \tag{4}$$

where $R_{k'}(x) = \sum_{i=1}^{k'} A_i(x) + V_{k'}(x)$ and $A_i(x)$ and $V_{k'}(x)$ are defined in Section 2.2. In this article we consider $\mathrm{Tr}(R_{k'}(x))$ and the WG transform of $\mathrm{Tr}(R_{k'}(x))$. For $k' = 2$ and 3, $R_{k'}(x)$ gives the 3-term, $T3(x) = \mathrm{Tr}(R_2(x))$, sequences, and the 5-term, $T5(x) = \mathrm{Tr}(R_3(x))$, 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 [28].

2.4.1 Description of the FDBG

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

$$\begin{aligned} a_{n+i} &= F(a_i, a_{i+1}, \cdots, a_{i+n-1}) \\ &= a_i + F'(a_{i+1}, \cdots, a_{i+n-1}), a_i \in \mathbb{F}_2, i \geq 0 \end{aligned} \tag{5}$$

where $F(x_0, x_1, \cdots, x_{n-1})$ 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 [26, 42]. Let $(i_0, i_1, \cdots, i_{m-1})$ 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 $\mathbf{a}$ by selecting m bits from the positions $(i_0, \cdots, i_{m-1})$ of the NLFSR as $\mathbf{a}_i = (a_{i_0+i}, \cdots, a_{i_{m-1}+i})$ which is regarded as an element of $\in \mathbb{F}_{2^m}, i \geq 0$. Let f be a Boolean function in m variables defined over $\mathbb{F}_{2^m}$. The filtering sequence $\mathbf{b} = \{b_i\}_{i \geq 0}$ is constructed from the de Bruijn sequence $\mathbf{a}$ as

$$b_i = f(\mathbf{a}_i), i \geq 0.$$

We call sequence $\mathbf{b}$ a *filtering de Bruijn sequence.* As the period of sequence $\mathbf{a}$ is 2^n, the period of $\mathbf{b}$ 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 $1 \leq t \leq n$ ($\mathbf{a}$), which is a uniform source, we are interested in uniformity on the binary t-tuple distribution of $\mathbf{b}$.

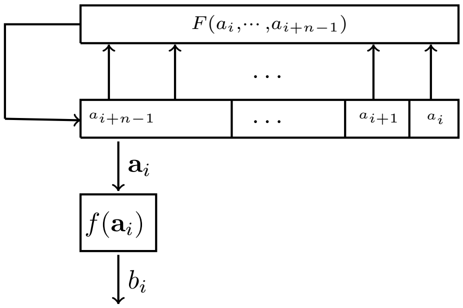

Figure 1: Block diagram of a filtering de Bruijn generator (FDBG)

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 6. *Let $\mathbf{b} = \{b_i\}$ be a binary sequence of period 2^n. A t-tuple from $\mathbf{b}$ is constructed as $(b_i, b_{i+1}, \cdots, b_{i+t-1}), i \geq 0$. We say the sequence $\mathbf{b}$ has* t-tuple distribution *if every t-tuple $(b_i, b_{i+1}, \cdots, b_{i+t-1})$ occurs 2^{n-t} times in a period of the sequence. The sequence $\mathbf{b}$ has an* ideal ℓ-tuple distribution *if $\mathbf{b}$ has t-tuple distribution for all $1 \leq t \leq \ell$.*

Note that if the filtering function $f(\cdot)$ is balanced, then the sequence $\mathbf{b}$ is balanced, i.e., it has 1-tuple distribution. Lemma 1 states the condition on the filtering function for having ideal t-tuple distribution of $\mathbf{b}$ 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 1. *[28] 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.*

In [28], Mandal *et al.* proposed the following conjecture on the ideal t-tuple distribution of $\mathbf{b}$ with the WG transformations as filtering functions.

Conjecture 1. *[28] For odd m, there exist at least $\frac{\phi(2^m-1)}{m}$ WG transformations with decimation $d = 2^J - 1$ (for some J), when used as a filtering function, for which the filtering de Bruijn sequence has ideal $(n-m+1)$-tuple distributions.*

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 of the invariant under the WG transform. Let $f(x)$ be a Boolean function with the trace representation from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Notice that we denote the WG transform of a function f by $WG_f(x) = f(x+1) + \mathrm{Tr}(1)$. 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 7. *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 2. *Let $f(x)$ be a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ and $WG_f(x)$ be the WG transform of f, i.e., $WG_f(x) = f(x+1) + \mathrm{Tr}(1)$. Then*

$$\widehat{WG}_f(\lambda) = (-1)^{\mathrm{Tr}(\lambda+1)} \hat{f}(\lambda), \forall \lambda \in \mathbb{F}_{2^m}.$$

Furthermore, for m odd, the following conditions are equivalent: f is WG-invariant, i.e.,

1) $WG_f(x) = f(x)$

2) $\widehat{WG}_f(\lambda) = \hat{f}(\lambda)$

3) $\hat{f}(\lambda) \neq 0$ *implies* $\mathrm{Tr}(\lambda) = 1$.

Proof. The Hadamard transform of a Boolean function f is defined as

$$\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+\mathrm{Tr}(\lambda x)}.$$

The Hadamard transform of $WG_f(x)$ is given by

$$\begin{aligned}
\widehat{WG}_f(\lambda) &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+\mathrm{Tr}(\lambda x)} \\
&= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x+1)+\mathrm{Tr}(\lambda(x+1))+\mathrm{Tr}(\lambda+1)} \\
&= (-1)^{\mathrm{Tr}(\lambda+1)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x+1)+\mathrm{Tr}(\lambda(x+1))} \\
&= (-1)^{\mathrm{Tr}(\lambda+1)} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{f(y)+\mathrm{Tr}(\lambda y)}, \\
&= (-1)^{\mathrm{Tr}(\lambda+1)} \hat{f}(\lambda). \qquad (6)
\end{aligned}$$

The conditions (1) and (2) are equivalent by definition. For odd m, $\mathrm{Tr}(1) = 1$. When $\hat{f}(\lambda) \neq 0$, $\widehat{WG}_f(\lambda) = \hat{f}(\lambda)$ implies $\mathrm{Tr}(\lambda + 1) = 0$ and hence $\mathrm{Tr}(\lambda) = 1$. □

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 8. *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 $f(x) = x_0 + g(x_1, \cdots, x_{m-1})$ 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 a x_0-independence form iff $f(\alpha^i) = f(\alpha^{Z(i)}) + 1$ 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 $f(x) = x_0\mathrm{Tr}(1) + x_0(f(z) + WG_f(z)) + f(z)$ 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

$$f(x) = x_0 g(z) + h(z) \qquad (7)$$

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

$$f(z) = h(z) \qquad (8)$$

$$f(1 + z) = g(z) + h(z) \qquad (9)$$

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

$$\begin{aligned} f(x) &= x_0(f(z) + f(1+z)) + f(z) \\ &= x_0\mathrm{Tr}(1) + x_0(f(z) + f(1+z) + \mathrm{Tr}(1)) + f(z) \\ &= x_0\mathrm{Tr}(1) + x_0(f(z) + WG_f(z)) + f(z). \end{aligned}$$

where $WG_f(x) = f(x+1) + \mathrm{Tr}(1)$ is the WG transform of f. Hence the proof. □

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

Theorem 1. *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 $f(x) = x_0 + g(x_1, \cdots, x_{n-1})$ for some g. The WG transform of $f(x)$ is given by

$$\begin{aligned} WG_f(x) &= f(x+1) + \mathrm{Tr}(1) = x_0 + 1 + g(x_1, \cdots, x_{n-1}) + \mathrm{Tr}(1) \\ &= x_0 + g(x_1, \cdots, x_{n-1}) = f(x) \end{aligned}$$

as for odd m, $\mathrm{Tr}(1) = 1$. 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 $f(x) = x_0 + x_0(f(z) + WG_f(z)) + f(z)$. Since $f(x) = WG_f(x)$, so does $f(z) = WG_f(z)$, and hence $f(x) = x_0 + g(x_1, \cdots, x_{m-1})$ where $g(x_1, \cdots, x_{m-1}) = f(z)$, which is independent of x_0. Hence the result is established. □

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 $f(x) = WG(x^d)$ and the function $WG_f(x) = f(x+1) + \mathrm{Tr}(1) = f(x+1) + 1$ 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 $m \equiv 2 \bmod 3$, $m = 3k - 1$ and for $m \equiv 1 \bmod 3$, $2m = 3k - 1$. Then the decimation $d = 2^{m-k+1} - 1$ can be written as

$$d = \begin{cases} 2^{2k} - 1 & \text{if } m \equiv 2 \bmod 3 \\ 2^{\frac{k+1}{2}} - 1 & \text{if } m \equiv 1 \bmod 3. \end{cases} \tag{10}$$

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 $3k \equiv 1 \bmod m$. In [38], Yu and Gong proved the Hadamard transform of the decimated WG transformation (see Fact 5) where the decimation is $d_1 = \frac{2^{2s} - 2^s + 1}{2^s + 1}$. 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 $d_1 = \frac{2^{2s}-2^s+1}{2^s+1}$. Let $3k \equiv 1 \bmod m$. The exponent for the tuple distribution is $d = 2^{m-k+1} - 1$. The relation between d_1 and d is given by $d_1 = 2^\ell \cdot d$ 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 $3k \equiv 1 \bmod m$, we have $k = s$. The exponent d can be written as $d = 2^{2k} - 1$. Furthermore, we have

$$\frac{d_1}{d} = \frac{2^{2k} - 2^k + 1}{(2^k + 1)(2^{2k} - 1)} = \frac{2^{2k} - 2^k + 1}{2^{3k} + 2^{2k} - 2^k - 1} = 1$$

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

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

$$\frac{d_1}{d \cdot 2^{\frac{k-1}{2}}} = \frac{2^{k-1} - 2^{\frac{k-1}{2}} + 1}{2^{\frac{3k-1}{2}} + 2^k + 2^{k-1} + 2^{\frac{k-1}{2}}} = \frac{2^{k-1} - 2^{\frac{k-1}{2}} + 1}{2^{k-1} - 2^{\frac{k-1}{2}} + 1} = 1$$

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

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 [9, 22, 38]. In [38], Yu and Gong presented the Hadamard transform of $WG(x^d)$ when $m = 3s \pm 1$, but the values of λ for which the Hadamard transform value equals zero or nonzero were not known. In Lemma 3, we explicitly present the values of λ 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. *[22] Let $m = 3s \pm 1$. For the WG transformation $WG(x) = \mathrm{Tr}(v(x+1)+1)$ over $\mathbb{F}_{2^m}$ defined in Fact 3, the Hadamard transform of $WG(x)$ is given by*

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

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

Fact 5. *[38] For $m = 3s \pm 1$ and $WG(x) = \mathrm{Tr}(v(x+1)+1)$, the Hadamard transform of the WG transformation with decimation $d_1 = \frac{e}{2^s+1}$ 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 $\widehat{WG^{(d_1)}}(\lambda) = H_{e^{-1}}(\lambda^{-d_1}) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(\lambda^{-d_1}x) + \mathrm{Tr}(x^{e^{-1}})}$.*

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

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

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

$$\begin{aligned} \widehat{WG^{(d_1)}}(\lambda) &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(\lambda^{-d_1} x) + \mathrm{Tr}(x^{e^{-1}})} \\ &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(x) + \mathrm{Tr}(x^{e^{-1}} \lambda^{(2^s+1)^{-1}})} \\ &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(\lambda^{(2^s+1)^{-1}} x) + \mathrm{Tr}(x^e)} \\ &= H_e(\lambda^{(2^s+1)^{-1}}). \end{aligned}$$

In [9], Dillon proved the Walsh spectrum of $\mathrm{Tr}(x^e)$ and gave λ in terms of trace for which $H_e(\lambda) = 0$ and $H_e(\lambda) \neq 0$, which is given by [9, 20]

$$H_e(\lambda)^2 = \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda^{2^s+1}) = 0 \\ 2^{m+1} & \text{if } \mathrm{Tr}(\lambda^{2^s+1}) = 1. \end{cases}$$

This implies

$$H_e(\lambda^{(2^k+1)^{-1}}) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda) = 0 \\ \pm 2^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\lambda) = 1. \end{cases}$$

Hence the assertion is established. □

Theorem 2. *For $f(x) = WG(x^d)$ with $d = 2^{m-k+1} - 1$, the Walsh spectra of the functions $WG_f(x)$ and $f(x)$ are identical at every point. In other words, $f(x)$ is invariant under the WG transform.*

Proof. From Lemma 2, we have $\widehat{WG}_f(\lambda) = (-1)^{\mathrm{Tr}(\lambda+1)} \hat{f}(\lambda)$. Applying Proposition 2, for $3k \equiv 1 \bmod m$, we have $d = 2^{m-\ell} d_1$ and $f(x) = WG(x^d) = WG(x^{2^{m-\ell} d_1}) = WG(x^{d_1}) = WG^{(d_1)}(x)$. Using Lemma 3, the Hadamard transform of $f(x)$ is given by

$$\hat{f}(\lambda) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda) = 0 \\ \pm 2^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\lambda) = 1. \end{cases}$$

For odd m, $\mathrm{Tr}(1) = 1$ and the Hadamard transformation of $f(x)$ can be written as

$$\hat{f}(\lambda) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda+1) = 1 \\ \pm 2^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\lambda+1) = 0. \end{cases}$$

Using Eq. (6), the Hadamard transformation of $h(x)$ can be written as

$$\widehat{WG}_f(\lambda) = (-1)^{\mathrm{Tr}(\lambda+1)} \hat{f}(\lambda) = \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda+1) = 1 \\ \pm 2^{\frac{m+1}{2}} & \text{if } \mathrm{Tr}(\lambda+1) = 0. \end{cases}$$

Thus, the Walsh spectra of $f(x)$ and $WG_f(x)$ at every point λ are identical, i.e., $\widehat{WG}_f(\lambda) = \hat{f}(\lambda), \forall \lambda \in \mathbb{F}_{2^m}$. Since the Walsh spectra of $f(x)$ and $WG_f(x)$ are equal at every point, the functions $f(x)$ and $WG_f(x)$ are equal. Therefore, $f(x)$ is invariant under the WG transform. □

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

As a consequence of Theorem 2, we have the following result on the nonlinearity of the WG transformation when its exponents are defined using k satisfying $3k \equiv 1 \bmod m$.

Corollary 1. *For $3k \equiv 1 \bmod m$ and $d = 2^{m-k+1} - 1$, the nonlinearity of $WG(x^d)$ is $2^{m-1} - 2^{\frac{m-1}{2}}$.*

Proof. According to Theorem 2, 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 $k = \frac{m+1}{2}$. The three-term function (T3) is defined as [10]

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

An alternative definition of the three-term function is

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

where $r = 2^{\frac{m-1}{2}} + 1$ [21, 32]. Note that $w(x) = T3(x^{2^k+1})$ [10, 20]. The WG transform of $T3(x)$, denoted by $WG_{T3}(x)$, is defined as

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

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

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

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 [10], Dillon and Dobbertine proved that the Hadamard transform of $w(x)$ is 3-valued. In [7], Chang *et al.* proved that the dual of the code $\{(\mathrm{Tr}(ax + bx^r + cx^{r^2})) : a, b, c \in \mathbb{F}_{2^m}\}$ is a triple-error correcting cyclic code, and its weight distribution is at most 5-valued. In [38], 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 transforms of $T3(x)$ and $f(x) = WG_{T3}(x^d)$ with $d = 2^k - 1$ in Corollary 2 and Theorem 4, respectively. To the best of our knowledge, the Hadamard transform of $T3(x)$ has not appeared in the literature.

Fact 6. *[38] 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., $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$.*

We first present a result on the Hadamard transform of the three-term function with any arbitrary coefficients.

Lemma 4. *Let $h(x) = Tr(\alpha x + \beta x^{q_1} + \gamma x^{q_2}), \alpha, \beta, \gamma \in \mathbb{F}_{2^m}$ where $m = 2k - 1$. The Hadamard transform of $h(x)$ is 5-valued, i.e., $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$.*

Proof. Given

$$h(x) = \mathrm{Tr}(\alpha x + \beta x^{2^k+1} + \gamma x^{2^k-1}), x \in \mathbb{F}_{2^m}. \tag{13}$$

The Hadamard transform of $h(x)$ is

$$\begin{aligned}\widehat{h}(\lambda) &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{h(x)+\mathrm{Tr}(\lambda x)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left((\lambda+\alpha)x + \beta x^{2^k+1} + \gamma x^{2^k-1}\right)}, \lambda \in \mathbb{F}_{2^m} \\ &= \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left((\lambda+\alpha)y^{2^k+1} + \beta y^{(2^k+1)^2} + \gamma y\right)} \\ &\quad \text{where } y = x^{2^k-1}, \text{ implying } x = y^{2^k+1} \text{ as } (2^k-1)^{-1} = 2^k + 1 \\ &= \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left(ay + by^r + cy^{r^2}\right)} \text{ where } r = 2^k + 1\end{aligned}$$

where $a = \gamma$, $b = (\lambda + \alpha)$ and $c = \beta$. Chang *et al.* [7] showed that the dual code of $\mathcal{C} = \{\mathrm{Tr}(ax + bx^r + cx^{r^2}) | a, b, c \in \mathbb{F}_{2^m}\}$ 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 $h(x)$ is 5-valued, i.e., $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$. □

Corollary 2. *Let $T3(x)$ be as defined in Eq. (11). The Hadamard transform of $T3(x)$ is 5-valued, i.e., $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$.*

Proof. The proof follows from Lemma 4 where $\alpha = \beta = \gamma = 1$. □

We now present the Hadamard transform values of the WG transforms of $h(x)$, $T_3(x)$, $w(x)$, and $T3(x^d)$.

Theorem 3. *Let $h(x)$, $T3(x)$ and $w(x)$ be as defined in Eqs. (13), (11) and (12), respectively, and $g(x) = T3(x^d)$ with $d = 2^k - 1$. The Hadamard transform of:*

1) $WG_w(x)$ is 3-valued.

2) $WG_{T3}(x)$ is at most 5-valued.

3) $WG_g(x)$ is also at most 5-valued.

4) $WG_h(x)$ is also at most 5-valued.

Proof. According to Lemma 2, the Hadamard transform of $WG_h(x)$ is $\widehat{WG}_h(\lambda) = (-1)^{Tr(\lambda+1)}\hat{h}(\lambda)$ for any h. This implies that the Hadamard transform value level of $WG_h(x)$ is upper bounded by that of $h(x)$. Since, according to [20], the Hadamard transform of $w(x)$ is 3-valued, the Hadamard transform of $WG_w(x)$ is 3-valued. Compilation of Lemma 4 and Corollary 2 and Lemma 2 demonstrates that the Hadamard transforms of $WG_h(x)$ and $WG_{T3}(x)$ are at most 5-valued. According to [10] and [38], the Hadamard transform of $g(x)$ is at most 5-valued, therefore the Hadamard transform of $WG_g(x)$ is at most 5-valued. Hence the proof. □

Theorem 4. *For $m = 2k - 1$ and $d = 2^k - 1$, the Hadamard transform of the decimated WG transform of the three-term function $f(x) = WG_{T3}(x^d)$ is 5-valued, i.e., $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$.*

Proof. Recall the definition of $f(x) = WG_{T3}(x^d) = \mathrm{Tr}(x^d + (x^d+1)^{q_1} + (x^d+1)^{q_2})$ where $q_1 = 2^k + 1$, $q_2 = 2^k - 1$ and $d = 2^k - 1$. The Hadamard transform of $f(x)$ is given by

$$\begin{aligned}
\widehat{f}(\lambda) &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}(\lambda x)+\mathrm{Tr}\left(x^{2^k-1}+1+(x^{2^k-1}+1)^{2^k+1}+(x^{2^k-1}+1)^{2^k-1}\right)} \\
&= \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left(\lambda(y+1)^{2^k+1}+y+1+y^{2^k+1}+y^{2^k-1}\right)} \\
&\quad \text{where } y = x^{2^k-1}+1, \text{ implying } x = (y+1)^{2^k+1} \text{ as } (2^k-1)^{-1} = 2^k+1 \\
&= \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left(\lambda(y^{2^k+1}+y^{2^k}+y+1)+y+1+y^{2^k+1}+y^{2^k-1}\right)} \\
&= (-1)^{\mathrm{Tr}(\lambda+1)} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left((1+\lambda+\lambda^{2^{k-1}})y+(1+\lambda)y^{2^k+1}+y^{2^k-1}\right)} \text{ as } \mathrm{Tr}(\lambda y^{2^k}) = \mathrm{Tr}(\lambda^{2^{k-1}}y) \\
&\quad \text{Let } x = y^{2^k-1} \implies y = x^{2^k+1} \text{ as } (2^k-1)^{-1} = 2^k+1 \\
&= (-1)^{\mathrm{Tr}(\lambda+1)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}\left(x+(1+\lambda+\lambda^{2^{k-1}})y^{2^k+1}+(1+\lambda)y^{(2^k+1)^2}\right)}.
\end{aligned}$$

In [7], Chang *et al.* proved that the dual code of $\mathcal{C} = \{\mathrm{Tr}(ax + bx^r + cx^{r^2}) | a, b, c \in \mathbb{F}_{2^m}\}$ 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 $WG_{T3}(x^d)$ are 5-valued. The following theorem states the nonlinearity of the WG transform of the three-term function and with its decimation.

Theorem 5. *For $m = 2k - 1$ and $d = 2^k - 1$, the nonlinearity of both $WG_{T3}(x)$ and $WG_{T3}(x^d)$ is $2^{m-1} - 2^{\frac{m+1}{2}}$.*

Proof. According to Theorem 4, the Walsh spectra of $WG_{T3}(x)$ and $WG_{T3}(x^d)$ are $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$. Therefore, the nonlinearity of $WG_{T3}(x)$ and $WG_{T3}(x^d)$ is $2^{m-1} - 2^{\frac{m+1}{2}}$. Hence the proof. □

Table 1: A summary of the Hadamard transform values of three-term functions.

Functions	**Hadamard Transform values**	**Ref.**
$h(x) = \mathrm{Tr}(\alpha x + \beta x^{q_1} + \gamma x^{q_2})$	at most 5-valued	Lemma 4
$T3(x) = \mathrm{Tr}(x + x^{q_1} + x^{q_2})$	at most 5-valued	Corollary 2
$w(x) = T3(x^{2^k+1}) = \mathrm{Tr}(x + x^{q_1} + x^{q_1^2})$	3-valued	[10]
$g(x) = T3(x^{2^k-1}) = \mathrm{Tr}(x + x^{q_2} + x^{q_2^2})$	at most 5-valued	[38]
$WG_h(x) = \mathrm{Tr}(\alpha(x+1) + \beta(x+1)^{q_1} + \gamma(x+1)^{q_2} + 1)$	at most 5-valued	Theorem 3
$WG_{T3}(x) = \mathrm{Tr}(x + (x+1)^{q_1} + (x+1)^{q_2})$	at most 5-valued	Theorem 3
$WG_w(x) = \mathrm{Tr}(x + (x+1)^{q_1} + (x+1)^{q_1^2})$	3-valued	Theorem 3
$WG_g(x) = \mathrm{Tr}(x + (x+1)^{q_2} + (x+1)^{q_2^2})$	at most 5-valued	Theorem 3
$WG_{T3}(x^d) = \mathrm{Tr}(x^d + (x^d+1)^{q1} + (x^d+1)^{q_2})$	at most 5-valued	Theorem 4

3.4.3 Invariance of $WG_{T3}(x)$

We now present a conjecture about the invariance property of the WG transform of the three-term function.

Conjecture 2. *For $f(x) = WG_{T3}(x^d)$ 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 WG_{T3} for $5 \leq m \leq 25$, none of them has the invariance property except the one in Conjecture 2.

4 Ideal Tuple Distribution of $WG_{T5}(x^d)$ and $WG_{T3}(x^d)$ 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.

4.1 WG Transformations in FDBG

We prove Conjecture 1 on the WG transformation, which establishes the required result on the ideal tuple distribution property.

Overview of the Proof of Conjecture 1. Before going into the details, we provide a high-level overview on the proof, which consists of the following steps.

- We claim that, for odd m, the decimation d of $WG(x^d)$ in Conjecture 1 is $d = 2^{m-k+1} - 1$ with $J = (m - k + 1)$ that gives the ideal tuple distribution where k satisfies $3k \equiv 1 \bmod m$.
- For decimation $d = 2^{m-k+1} - 1$, the decimated WG transformation $f(x) = WG(x^d)$ has the following form:

$$f(x) = x_0\mathrm{Tr}(1) + x_0(f(z) + f(z+1) + \mathrm{Tr}(1)) + f(z)$$

  where $x = x_0 + z$ and $z = x_1\alpha + \cdots + x_{m-1}\alpha^{m-1}$.
- Using the invariance property of $f(x)$ for odd m, $g(z) = f(z) + f(z+1) + \mathrm{Tr}(1) = 0$ and hence $f(x)$ has the form $x_0 + f'(x_1, \cdots, x_{m-1})$ where $f'(x_1, \cdots, x_{m-1}) = f(z)$ independent of x_0.

- We apply Lemma 1 in Section 2.4 on $f(x)$ to prove the filtering de Bruijn sequence with $f(x)$ as a filtering function in the FDBG has the ideal $(n-m+1)$-tuple distribution.

We present the main results on the ideal tuple distribution for the WG transformation when it is used as a filtering function in the FDBG. In the following theorem, we show the x_0-independence of $WG(x^d)$.

Theorem 6. *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 $f(x) = x_0 + f'(x_1, x_2, \cdots, x_{m-1})$ where $x = x_0 + x_1\alpha + \cdots + x_{m-1}\alpha^{m-1} \in \mathbb{F}_{2^m}$ and $f'(x_1, \cdots, x_{m-1}) = f(z)$, which is independent of x_0.*

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

Example 2 (Continued)**.** *Let $m = 7$ and $d = 7$. Then $f(x) = WG_{T5}(x^7) = \mathrm{Tr}(x^3 + x^7 + x^{21} + x^{49} + x^{76}) = x_0 + x_0(f(z) + WG_f(z)) + \mathrm{Tr}(z^3 + z^7 + z^{21} + z^{49} + z^{76}) = x_0 + \mathrm{Tr}(z^3 + z^7 + z^{21} + z^{49} + z^{76})$ as $\mathrm{Tr}(1) = 1$, $WG_f(x) = f(x)$, and $x = x_0 + z \in \mathbb{F}_{2^5}$. Thus, $f(x)$ has the x_0-independence form.*

Theorem 7. *Let m be odd and $3k \equiv 1 \mod m$, and $WG : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be the Welch-Gong transformation defined in Facts 1 and 2. For $d = 2^{m-k+1} - 1$ and the filtering de Bruijn sequence $\mathbf{b}$ with $WG(x^d)$ as filtering function in the FDBG has an ideal ℓ-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 1 and Theorem 6. Hence the proof of Conjecture 1. □

Example 3. *The feedback function $g(x_0, \cdots, x_6) = x_0 + x_2 + x_4 + x_1x_2 + \prod_{i=1}^{6}(1 + x_i)$ generates a de Bruijn sequence ($\mathbf{a}$) 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 $WG_{T5}(x) = \mathrm{Tr}(x + (x+1)^5 + (x+1)^{13} + (x+1)^{19} + (x+1)^{21}) = \mathrm{Tr}(x^{19})$. The decimated WG transformation is $f(x) = WG_{T5}(x^{15}) = \mathrm{Tr}(x^3) = x_0 + x_3 + x_1x_2 + x_1x_4 + x_2x_3 + x_2x_4$ over $\mathbb{F}_{2^5}$ as a filtering function in the FDBG where $\mathbb{F}_{2^5}$ is defined using $\alpha^5 + \alpha^3 + 1 = 0$. The de Bruijn sequence of period 2^7 is given by*

$$\begin{aligned}\mathbf{a} =& 1111111000111010001000010110010001100110001010000000100101110110\\ & 0000110111101110010101001001111001110000111110101011011010011010.\end{aligned}$$

The filtering sequence with filtering function $f(x)$ over $\mathbf{a}$ is given by

$$\begin{aligned}\mathbf{b} =& 0001111100101100101101100001101000111111101000010101001011111001\\ & 0110100101000110111001011000011011011100000100111110110010000100.\end{aligned}$$

The sequence $\mathbf{b}$ has an ideal up to 3-tuple distribution, i.e., all possible binary tuples of length up to 3 occur equally likely. □

Remark 1. *$WG(x^d)$ with $d = 2^{m-k+1} - 1$ has the form $x_0 + f'(x_1, \cdots, x_{m-1})$ 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 6 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 8. *If Conjecture 2 is true for $m = 2k - 1$ and $d = 2^k - 1$, the decimated WG transform of three-term function $T3(x)$ can be written as $f(x) = WG_{T3}(x^d) = x_0 + f'(x_1, \cdots, x_{m-1})$ where $x = x_0 + \cdots + x_{m-1}\alpha^{m-1}$ and f' is a function in $(m-1)$ variables and is independent of x_0 and hence the filtering de Bruijn sequence* **b** *with $WG_{T3}(x^d)$ as filtering function in the FDBG has an ideal ℓ-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 1 and Conjecture 2. □

Example 4. *Let $m = 5$ and $k = \frac{m+1}{2} = 3$. The three-term function is $T3(x) = \mathrm{Tr}(x + x^7 + x^9)$ over $\mathbb{F}_{2^5}$ and $WG_{T3}(x) = \mathrm{Tr}(x + (x+1)^7 + (x+1)^9), x \in \mathbb{F}_{2^5}$. Consider the decimation $d = 2^k - 1 = 7$. Then $f(x) = WG_{T3}(x^7)$ is given by*

$$\begin{aligned} f(x) =& \mathrm{Tr}(x^7 + (x^7+1)^7 + (x^7+1)^9) \\ =& \mathrm{Tr}(1 + x + x^7 + (x^7+1)^7) \\ =& \mathrm{Tr}(x + x^4 + x^{18}) = \mathrm{Tr}(x^9). \end{aligned}$$

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 2 is true, the representation of $WG_{T3}(x^d) = x_0 + f'(x_1, \cdots, x_{m-1})$ 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 [16]

$$G(x) = \mathrm{Tr}(x^d), x \in \mathbb{F}_{2^m}$$

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

$$f(x) = \mathrm{Tr}((x+1)^d + 1) = \mathrm{Tr}(x^d) = G(x).$$

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 9. *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* $\mathbf{b}$ *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 $\mathrm{Tr}(x^d)$ can be written as

$$\begin{aligned}\mathrm{Tr}(x^d) &= \mathrm{Tr}((x_0 + x_1\alpha + \cdots + x_{m-1}\alpha^{m-1})^d)\\ &= x_0 + \mathrm{Tr}(z^{2^k+1}), z = x_1\alpha + \cdots + x_{m-1}\alpha^{m-1}\end{aligned}$$

as $\mathrm{Tr}(z) = \mathrm{Tr}(z^{2^k})$. Therefore the Gold function $G(x)$ can be written as $G(x) = x_0 + G'(x_1, \cdots, x_{m-1})$ where $G'(x_1, \cdots, x_{m-1}) = \mathrm{Tr}(z^{2^k+1})$. Applying Lemma 1 on the Gold function $G(x)$ as a filtering function, the filtering sequence $\mathbf{b}$ has an ideal $(n - m + 1)$-tuple distribution. □

5.2 Quadratic Functions

Let m be a positive integer. The quadratic Boolean function over $\mathbb{F}_{2^m}$ is defined as

$$Q(x) = \sum_i \mathrm{Tr}_1^{r_i}(a_i x^{2^i+1}) + \mathrm{Tr}(cx), c \in \mathbb{F}_{2^m}, a_i \in \mathbb{F}_{2^r}, 0 \leq i \leq \lfloor \frac{m+1}{2} \rfloor, \tag{14}$$

where $\mathrm{Tr}_1^{r_i}(x)$ 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 [39]. For specific definitions of the quadratic function $Q(x)$ in [2, 39], the results on the Hadamard transform can be found in [2, 39], respectively.

Lemma 5. *Let m be odd and $Q(x)$ be the quadratic Boolean function defined in Eq. (14). Then $Q(x)$ is invariant under the WG transform iff $\sum_i Tr_1^{r_i}\big(a_i + a_i^{2^{m-i}}\big) = 0$ and $\sum_i Tr_1^{r_i}\big(a_i + c + 1\big) = 0$.*

Proof. The WG transform of $Q(x)$, denoted by $WG_Q(x)$, is:

$$\begin{aligned}WG_Q(x) &= \sum_i \mathrm{Tr}_1^{r_i}(a_i(x+1)^{2^i+1} + c(x+1) + 1)\\ &= \sum_i \mathrm{Tr}_1^{r_i}(a_i x^{2^i+1}) + \mathrm{Tr}(cx) + \sum_i \mathrm{Tr}_1^{r_i}\big(x(a_i + a_i^{2^{m-i}})\big) + \sum_i \mathrm{Tr}_1^{r_i}\big(a_i + c + 1\big)\\ &= Q(x) + \sum_i \mathrm{Tr}_1^{r_i}\big(x(a_i + a_i^{2^{m-i}})\big) + \sum_i \mathrm{Tr}_1^{r_i}\big(a_i + c + 1\big).\end{aligned}$$

The quadratic function $Q(x)$ is invariant under the WG transform iff $\sum_i \mathrm{Tr}_1^{r_i}\big(x(a_i+a_i^{2^{m-i}})\big)+\sum_i \mathrm{Tr}_1^{r_i}\big(a_i+c+1\big) = 0$. This implies $\sum_i \mathrm{Tr}_1^{r_i}\big(a_i + a_i^{2^{m-i}}\big) = 0$ and $\sum_i \mathrm{Tr}_1^{r_i}\big(a_i + c + 1\big) = 0$. 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

$$Q(x) = x_0\Big(\sum_i \mathrm{Tr}_1^{r_i}(a_i) + \mathrm{Tr}(c)\Big) + x_0\big(\sum_i \mathrm{Tr}_1^{r_i}\big(z(a_i + a_i^{2^{m-i}})\big)\big) + \sum_i \mathrm{Tr}(a_i z^{2^i+1}) + \mathrm{Tr}(cz). \tag{15}$$

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.

Theorem 10. *For m odd, the filtering de Bruijn sequence* $\mathbf{b}$ *with the quadratic function $Q(x)$ defined above as a filtering function has an ideal t-tuple distribution if $\sum_i Tr_1^{r_i}\big(a_i + a_i^{2^{m-i}}\big) = 0$ and $\sum_i Tr_1^{r_i}\big(a_i + c + 1\big) = 0$ where $t = (n - m + 1)$ and n is the length of the NLFSR generating a de Bruijn sequence.*

Proof. The proof follows from the fact that, according to Eq. (15) in Lemma 5, $Q(x)$ 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 1 where $Q(x)$ is the filtering function. □

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 [20, 10] for the details about the KPF construction. We denote by KPF the set of all KPFs for different k'. Following the notations in Section 2.2, we consider the cases $k' = 4$ and 5 and the KPFs $h(x) = \mathrm{Tr}(R_{k'}(x))$, $h(x^d)$, and the WG transform of the KPFs $WG_h(x^d)$ including decimations over $\mathbb{F}_{2^m}$ with $9 \leq m \leq 19$. We use the KPFs for the above cases as filtering functions in the filtering de Bruijn generator described in Section 2.4 and examined the ideal tuple distribution of the filtering sequences (see Table 2). Unfortunately, we could not find any KPF and the WG transform of KPFs (including decimations) that give ideal ℓ-tuple distribution with $\ell \geq 3$ for any length of the NLFSR. We present a conjecture about the ideal tuple distribution of the KPFs in Conjecture 3.

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.

(a) When $k' = 3$, $WG_{R_3}(x^d) = \mathrm{Tr}(R_3(x^d + 1) + 1)$. (b) When $k' = 5$, $WG_{R_5}(x^d) = \mathrm{Tr}(R_5(x^d + 1) + 1)$.

Input size m	**NLFSR length n**	**t-tuple dist**	**Input size m**	**NLFSR length n**	**t-tuple dist.**
8	9 – 19	2	9	10 – 19	2
10	11 – 19	2	11	12 – 19	2
14	15 – 19	2	13	14 – 19	2

(c) When $k' = 4$, $WG_{R_4}(x^d) = \mathrm{Tr}(R_4(x^d + 1) + 1)$. (d) When $k' = 5$, $WG_{R_5}(x^d) = \mathrm{Tr}(R_5(x^d + 1) + 1)$.

Input size m	**NLFSR length n**	**t-tuple dist**	**Input size m**	**NLFSR length n**	**t-tuple dist.**
9	10 – 19	2	8	9 – 19	2
11	12 – 19	2	12	13 – 19	2
13	14 – 19	2	14	15 – 19	2

Conjecture 3. *For m odd, $WG_h(x^d)$, $\forall h \in KPF$ and all decimations except for those two cases in Theorem 2 and Conjecture 2, are not invariant or complementary invariant under the WG transform,*

i.e., for $f(x) = WG_h(x^d), \forall h \in KPF$ *and* $\forall d, \gcd(d, 2^m - 1) = 1$ *and*

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

An empirical investigation on WG transformations (as filtering functions) over $\mathbb{F}_{2^m}$ where m is even was conducted in [28] 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 $(\mathrm{Tr}(R_3(x)))$ 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 $f(x) = \mathrm{Tr}(x^e)$ 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 iff 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 2). However, given any Boolean function f over $\mathbb{F}_{2^m}$, it is not easy to theoretically determine the set $\{\lambda : \mathrm{Tr}(\lambda) = 1 \text{ when } \hat{f}(\lambda) \neq 0\}$.

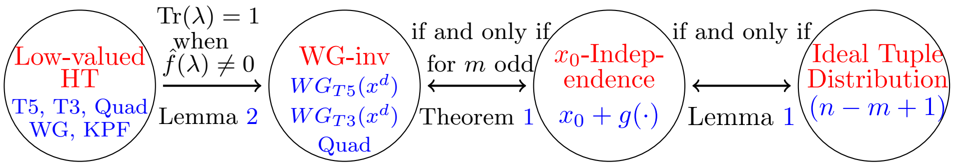

Figure 2: Relations among Hadamard Transform, WG-inv, x_0-independence and ideal tuple distribution. $g(\cdot)$ is independent of x_0. ↔ denotes if and only if condition, → denotes if condition and n is the NLFSR length.

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 $WG_{T3}(x^d)$ 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 $f(x) : \mathbb{F}_{2^m} \to \mathbb{F}_2$ 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.

Acknowledgement

This research is supported by the National Institute of Standards and Technology (NIST).

References

[1] S. Arora and B. Barak. Computational Complexity: A Modern Approach, Cambridge University Press, New York, NY, USA, 2009.

[2] S. Boztas and P.V. Kumar. Binary Sequences with Gold-like Correlation but Larger Linear Span, *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 532 – 537, 1994.

[3] N.G. de Bruijn. A Combinatorial Problem, Proc. Koninklijke Nederlandse Akademie v. Wetenschappen 49, pp. 758 – 764, 1946.

[4] A. Canteaut. Analysis and Design of Symmetric Ciphers, Habilitation for directing Theses, University of Paris 6, 2006. 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, Yves Crama and Peter L. Hammer (eds.), pp. 257 – 397, 2010.

[6] A.H. Chan, R.A. Games, and E.L. Key. On the Complexities of de Bruijn Sequences, *Journal of Combinatorial Theory, Series A*, vol. 33, No. 3, pp. 233 – 246, 1982.

[7] A. Chang and P. Gaal and S.W. Golomb and G. Gong and T. Helleseth and P.V. Kumar. On a Conjectured Ideal Autocorrelation Sequence and a Related Triple-error Correcting Cyclic Code, *IEEE Transactions on Information Theory*, vol. 46, No. 2, pp. 680 – 687, 2000.

[8] T.W. Cusick and P. Stanica. Cryptographic Boolean Functions and Applications. Elsevier/Academic Press, Amsterdam, 2009.

[9] J.F. Dillon. Multiplicative Difference Sets via Additive Characters, *Designs, Codes and Cryptography*, vol. 17, Issue 1, pp. 225 – 235, 1999.

[10] J.F. Dillon and H. Dobbertin. New Cyclic Difference Sets with Singer Parameters, *Finite Fields and Their Applications*, vol. 10, Issue 3, pp. 342 – 389, Elsevier, 2004.

[11] L. Ding, C. Jin, J. Guan and Q. Wang. Cryptanalysis of Lightweight WG-8 Stream Cipher, *IEEE Transactions on Information Forensics and Security*, vol. 9, No. 4, pp. 645 – 652, 2014.

[12] L. Ding, C. Jin, J. Guan, S. Zhang, T. Cui, D. Han, and W. Zhao. Cryptanalysis of WG Family of Stream Ciphers, *Computer Journal* vol. 58, No. 10, pp. 2677 – 2685, 2015.

[13] The eStream Project. http://www.ecrypt.eu.org/stream/project.html, September, 2008.

[14] X. Fan, K. Mandal and G. Gong. WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices, Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013, Revised Selected Papers, pp. 617 – 632, Springer Berlin Heidelberg, 2013.

[15] 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, pp. 21-34, 2013.

[16] R. Gold. Maximal Recursive Sequences with 3-valued Recursive Cross-correlation Functions, *IEEE Transactions on Information Theory*, vol. 14, No. 1, pp. 154 – 156, 1968.

[17] J. Dj Golić. On the Security of Nonlinear Filter Generators, In Gollmann, Dieter (Eds) Fast Software Encryption: Third International Workshop Cambridge, UK, February 21–23 1996 Proceedings, pp. 173 – 188, Springer, Berlin, Heidelberg, 1996,

[18] S.W. Golomb. On the Classification of Balanced Binary Sequences of Period $2^n - 1$, *IEEE Transactions on Information Theory*, vol. 26, No. 6, pp. 730 – 732, 1980.

[19] S.W. Golomb. Shift Register Sequences, Aegean Park Press, Laguna Hills, CA, 1981.

[20] S.W. Golomb, and G. Gong. Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, New York, 2004.

[21] G. Gong, P. Gaal, and S.W. Golomb. A Suspected Infinity Class of Cyclic Hadamard Difference Sets, *the Proceedings of 1997 IEEE Information Theory Workshop*, Longyearbyen, Syalbard, Norway, 1997.

[22] G. Gong and A. Youssef. Cryptographic Properties of the Welch-Gong Transformation Sequence Generators, *IEEE Transactions on Information Theory*, vol. 48, No. 11, pp. 2837 – 2846, 2002.

[23] B. Gordon, W. H. Mills and L.R. Welch. Some New Difference Sets, *Canadian Journal of Mathematics*, vol. 14, pp. 614 – 625, 1962.

[24] M. Joseph, G. Sekar, and R. Balasubramanian. Distinguishing Attacks on (Ultra-)Lightweight WG Ciphers, Lightweight Cryptography for Security and Privacy: 5th International Workshop, LightSec 2016, Aksaray, Turkey, September 21-22, 2016, Revised Selected Papers, pp. 45 – 59, Springer International Publishing, 2017.

[25] K. Mandal and G. Gong. Cryptographically Strong de Bruijn Sequences with Large Periods. In: Knudsen, L.R., Wu, H. (Eds.) SAC 2012. LNCS, vol. 7707, pp. 104 – 118, Springer, Heidelberg, 2012.

[26] K. Mandal and G. Gong. Feedback Reconstruction and Implementations of Pseudorandom Number Generators from Composited De Bruijn Sequences, *IEEE Transactions on Computers*, vol. 65, No. 9, pp. 2725 – 2738, 2016.

[27] K. Mandal, G. Gong, X. Fan and M. Aagaard. Optimal Parameters for the WG Stream Cipher Family, *Cryptography and Communications*, vol. 6, No. 2, pp. 117 – 135, 2014.

[28] K. Mandal, B. Yang, G. Gong and M. Aagaard. On Ideal t-tuple Distribution of Filtering de Bruijn Sequence Generators, *Cryptography and Communications*, vol 10, Issue 4, pp. 629 – 641, 2018.

[29] J.L. Massey. Shift-Register Synthesis and BCH Decoding, *IEEE Trans. Inform. Theory*, vol. 15, No. 1, pp. 122 – 127, 1969.

[30] Y. Nawaz, G. Gong. WG: A Family of Stream Ciphers with Designed Randomness Properties, *Information Sciences*, vol. 178, Issue 7, pp. 1903 – 1916, 2008.

[31] Y. Nawaz and G. Gong. The WG Stream Cipher, 2005. http://www.ecrypt.eu.org/stream/p2ciphers/wg/wg_p2.pdf

[32] 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*, Vol. 44, No. 2, March 1998, pp. 814 – 817, 1998.

[33] M.A. Orumiehchiha, J. Pieprzyk, and R. Steinfeld. Cryptanalysis of WG-7: A Lightweight Stream Cipher, *Cryptography Communications*, vol 4, No. 3-4, pp. 277 – 285, 2012.

[34] H. El-Razouk, A. Reyhani-Masoleh, and G. Gong, New implementations of the WG stream cipher, IEEE Transactions on VLSI, vol. 22, No. 9, 2014,

[35] S. RØnjom. Improving Algebraic Attacks on Stream Ciphers Based on Linear Feedback Shift Register over $\mathbb{F}_{2^k}$, *Designs Codes Cryptography*, vol. 82, No. 1-2, pp. 27 – 41, 2017.

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

[37] T. Siegenthaler, R. Forré and A.W. Kleiner. Generation of Binary Sequences with Controllable Complexity and Ideal r-Tupel Distribution, In: Chaum D., Price W.L. (eds) Advances in Cryptology EUROCRYPT 87. EUROCRYPT 1987. LNCS, vol 304. Springer, Berlin, Heidelberg, 1987.

[38] 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), LNCS 4086, pp. 104 – 118, Springer, Berlin, Heidelberg, 2006.

[39] N.Y. Yu and G. Gong. A new Binary Sequence Family with Low Correlation and Large Size, *IEEE Transactions on Information Theory*, vol. 52, No. 4, pp. 1624 – 1636, 2006.

[40] S.V. Smyshlyaev. Perfectly Balanced Boolean Functions and Golić Conjecture, *Journal of Cryptology*, vol. 25, No. 3, pp. 464 – 483, 2012.

[41] 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, pp. 1 – 10, Article No. 8, 2013.

[42] B. Yang, K. Mandal, M. D. Aagaard and G. Gong. Efficient Composited de Bruijn Sequence Generators, *IEEE Transactions on Computers*, vol. 66, No. 8, pp. 1354 – 1368, 2017.