On the cycle decomposition of the WG-NLFSR

Li Yujuan [1†] & Shen Wenhua [2]& Wang Huaifu [3]& Zhou Peipei [4]

Science and Technology on Information Assurance Laboratory, Beijing, 100072, P.R. China
email: [1]liyj@amss.ac.cn, [2]xxbz@163.com [3]wanghf@mmrc.iss.ac.cn, [4]zhoupeipei08@mails.gucas.ac.cn

Abstract Recently, Kalikinkar Mandal and Guang Gong presented a family of nonlinear pseudo-random number generators using Welch-Gong Transformations in their paper [6]. They also performed the cycle decomposition of the WG-NLFSR recurrence relations over different finite fields by computer simulations where the nonlinear recurrence relation is composed of a characteristic polynomial and a WG permutation. In this paper, we mainly prove that the state transition transformation of the WG-NLFSR is an even permutation. We also prove that the number of the cycles in the cycle decomposition of WG-NLFSR is even. And we apply our results to the filtering WG7-NLFSR to prove that the period of the sequences generated by WG7-NLFSR can not be maximum.

Keywords: cycle decomposition, WG-NLFSR, permutation

1 Introduction

Unlike the LFSR sequences which are well studied and understood [1,2,4], the randomness properties of a sequence generated by an arbitrary NLFSR are not known and hard to determine. As an example, the cycle decomposition of an arbitrary NLFSR is not well understood, because it is hard to determine the number of cycles and the lengths of the cycles in a cycle decomposition of the NLFSR. In the theory of NLFSRs, the cycle decomposition of NLFSRs is an important property to look at first, since each cycle can be considered as a sequence and the length of the cycle determines the period of the sequence.

In their paper[6], Kalikinkar Mandal, and Guang Gong presented a family of pseudorandom sequence generators, named the filtering nonlinear feedback shift registers using Welch-Gong (WG) transformations (henceforth called filtering WG-NLFSR). They also performed the cycle decomposition of WG-NLFSR recurrence relations over different finite fields by computer simulations where the nonlinear recurrence relation is composed of a characteristic polynomial and a WG permutation. In this paper, we would like to propose some general theories of the cycle decomposition of NLFSR, especially for filtering WG-NLFSR. Also we would like to use our results to analyze some related objects such as WG7-NLFSR in [6].

The article is organized as follows. In section 2, we recall the general model of the filtering WG-NLFSR. In section 3 and 4, we give our main results. In section 5, we use our results to analyze the filtering WG7-NLFSR. In section 6, we give the conclusion.

2 General Description of the Filtering WG-NLFSR

Keep the notations in [6]. The readers can refer to [6] for some details on the filtering WG-NLFSR. For the WG-NLFSR, an architecture of the WG-NLFSR is shown in Figure. 1. Let

† Corresponding author

$\mathbf{a} = \{a_i\}_{i\geqslant 0}$, $a_i \in \mathbb{F}_{2^t}$ be a sequence generated by the $n-$stage nonlinear recurrence relation, which is defined as

$$a_{n+k} = c_0 a_k + \cdots + c_{n-1} a_{n-1+k} + WGP(a_{n-1+k}), a_i \in \mathbb{F}_{2^t}, k \geqslant 0. \quad (1)$$

where $WGP(x)$ is the WG permutation and $(a_0, a_1, \cdots, a_{n-1})$ is the initial state. The filtering WG-NLFSR sequence $\{b_i\}_{i\geqslant 0}$ is defined by $b_i = WG(a_i)$, where $WG(x)$ is the WG transformation.

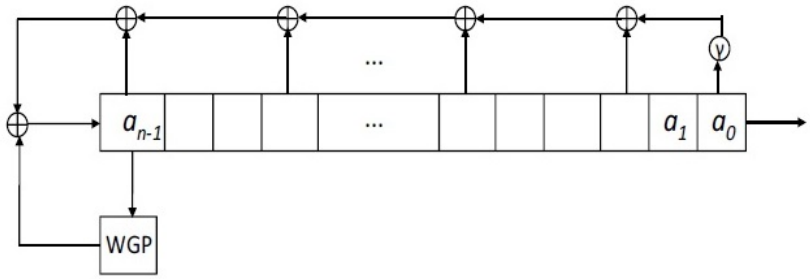

Figure 1: An Architecture of the WG-NLFSR

Let

$$T(a_0, \cdots, a_{n-1}) = (a_1, \cdots, a_{n-1}, c_0 a_0 + \cdots + c_{n-1} a_{n-1} + WGP(a_{n-1}).$$

Then T is a permutation from $\mathbb{F}_{2^t}^n$ to $\mathbb{F}_{2^t}^n$ when $c_0 \neq 0$. We call it the state transition transformation of the WG-NLFSR.

In [6], the authors said that it was not hard to show the period of $\{b_i\}_{i\geqslant 0}$ produced by the filtering WG-NLFSR was the same as the period of a. So analyzing the period of the sequence a is equivalent to analyzing the period of the sequence b. Since the state transition transformation T of the WG-NLFSR is a permutation when $c_0 \neq 0$, analyzing the cycle decomposition of the state transition transformation T of the WG-NLFSR is equivalent to analyzing the period of the sequence a. From now on, we suppose that $c_0 \neq 0$.

3 The parity of the state transition transformation of the WG-NLFSR

By algebra theory, we know that each permutation σ in the symmetric group $\mathcal{S}_n$ can be written as a product of disjoint cycles. Suppose that $\sigma = \prod_{i=1}^{n} i * k_i$, here k_i is the number of the $i-$cycle, i represents the cycle with length i. Then $\sum_{i=1}^{n} i k_i = n$ and the number of cycles of σ is $\sum_{i=1}^{n} k_i$. When two permutations $\sigma = \prod_{i=1}^{n} k_i$ and $\varsigma = \prod_{i=1}^{n} h_i$ in the symmetric group $\mathcal{S}_n$ are conjugate , i.e., there exits a permutation τ such that $\sigma = \tau^{-1}\varsigma\tau$, then their cycle decompositions have the same type, i.e., for $1 \leqslant i \leqslant n$, $k_i = h_i$. A permutation is called an even (odd) permutation if it can be written as a product of 2-cycle of even (odd)number. For example, if i is even, then the i-cycle is an odd permutation otherwise it is an even permutation. The product of two even or odd permutations is an even permutation. The product of an even and an odd permutations is an odd permutation.

In this part, we mainly prove that the state transition transformation T of the WG-NLFSR is an even permutation. First we define some permutations of the n-dimensional vector space $\mathbb{F}_{2^t}^n$ over the finite field $\mathbb{F}_{2^t}$, here $t > 0$, $n \geqslant 2$ are positive integers.

Let

$$T_{L_1}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, a_{n-1} + a_{n-2}).$$

$$T_{WGP}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, WGP(a_{n-2}), a_{n-1}).$$

$$T_{WGP^{-1}}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, WGP^{-1}(a_{n-2}), a_{n-1}).$$

It is obvious that $T_{WGP}^{-1} = T_{WGP^{-1}}$.

Let $T_{L_2}(a_0, a_1, \cdots, a_{n-1}) = (a_1, a_2, \cdots, a_{n-1}, c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1})$. Since $c_0 \neq 0$, T_{L_2} is a permutation on $\mathbb{F}_{2^t}^n$. Now we can write T as the composition of the permutations defined above.

Lemma 1. The state transition transformation T of the WG-NLFSR is the composition of $T_{WGP}^{-1}, T_{L_1}, T_{WGP}$ and T_{L_2}, i.e., $T = T_{WGP}^{-1} \circ T_{L_1} \circ T_{WGP} \circ T_{L_2}$, where $\circ$ denotes the composition of maps.

Proof. $T_{WGP}^{-1} \circ T_{L_1} \circ T_{WGP} \circ T_{L_2}(a_0, a_1, \cdots, a_{n-1})$

$$\begin{aligned}
&= T_{WGP}^{-1} \circ T_{L_1} \circ T_{WGP}(a_1, a_2, \cdots, a_{n-1}, c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1}) \\
&= T_{WGP}^{-1} \circ T_{L_1}(a_1, a_2, \cdots, WGP(a_{n-1}), c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1}) \\
&= T_{WGP}^{-1}(a_1, a_2, \cdots, WGP(a_{n-1}), c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1} + WGP(a_{n-1})) \\
&= (a_1, a_2, \cdots, a_{n-1}, c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1} + WGP(a_{n-1})) \\
&= T(a_0, a_1, \cdots, a_{n-1}).
\end{aligned}$$

Hence, $T = T_{WGP}^{-1} \circ T_{L_1} \circ T_{WGP} \circ T_{L_2}$. □

Lemma 2 Let $T_L = T_{WGP^{-1}} T_{L_1} T_{WGP}$. Then T_L is even.

Proof. In order to prove T_L is even, we need to prove T_{L_1} is even. $T_{L_1}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, a_{n-1} + a_{n-2})$. When $a_{n-2} = 0$, T_{L_1} has $(2^t)^{n-1}$ fixed points. When $a_{n-2} \neq 0$, T_{L_1} is the composition of $\frac{1}{2}((2^t)^n - (2^t)^{n-1})$ transpositions

$$((a_0, a_1, \cdots, a_{n-1}), (a_0, a_1, \cdots, a_{n-2}, a_{n-1} + a_{n-2})).$$

So T_{L_1} is even. Thus T_L is even. □

Let T_τ be the permutation of the n-dimensional vector space $\mathbb{F}_{2^t}^n$.

$$T_\tau(a_0, a_1, \cdots, a_{n-1}) = (a_1, a_2, \cdots, a_{n-1}, a_0).$$

Where $t > 1$, $n \geqslant 2$ are positive integers. T_τ is the so-called pure circulation. In the following, we first extend some results of the $n-$stage pure cycling register (PCR_n) over $\mathbb{F}_2$ to the general finite field of characteristic 2. And then prove that the pure circulation T_τ is an even permutation.

Theorem 1[2]. The period of $n-$stage pure cycling register (PCR_n) sequences over the finite field $\mathbb{F}_2$ must be a factor of n. Let d be a positive factor of n. Then the number of cycles

of length d in the state diagram of PCR_n is

$$M(d) = \frac{1}{d}\sum_{d'|d}\mu(d')2^{d/d'}$$

where the sum takes over all the positive factors of d, and $\mu(d)$ is the Möbius function, then the number of cycles in the state diagram of PCR_n is

$$Z(n) = \frac{1}{n}\sum_{d|n}\phi(d)2^{n/d}$$

where the sum takes over all the positive factors of n, and $\phi(d)$ is Euler function. When $n \neq 2$, $Z(n)$ must be even.

Theorem 1 is on the result of $n-$stage pure cycling register (PCR_n) sequences over the finite field $\mathbb{F}_2$. For the finite field of characteristic 2, the result is similar. But not the same. For $\mathbb{F}_2$, one can check that $M(d)$ may not be even, but for finite field $\mathbb{F}_{2^t}$ $(t > 1)$, we will prove in the following theorem that $M(d)$ is always even.

Theorem 2 The period of $n-$stage pure cycling register (PCR_n) sequences over the finite field $\mathbb{F}_{2^t}$ $(t > 1)$ must be a factor of n. Let d be a positive factor of n. Then the number of cycles of length d in the state diagram of PCR_n is

$$M(d) = \frac{1}{d}\sum_{d'|d}\mu(d')(2^t)^{d/d'}$$

where the sum takes over all positive factors of d, and $\mu(d)$ is the Möbius function. Furthermore $M(d)$ is even.

Proof. Let $\{a_i\}_{i\geqslant 0}$ be an arbitrary sequence generated by PCR_n. Then $a_{n+k} = a_k$, $k = 0, 1, 2, \cdots$. This proves that the period of the sequence $\{a_i\}_{i\geqslant 0}$ must be a factor of n.

Let d be a positive factor of n. Let $(a_1, a_2, \cdots, a_n)$ be a state of PCR_n and the period of it be a factor of d, then $(a_1, a_2, \cdots, a_n) = (a_{d+1}, a_{d+2}, \cdots, a_n, a_1, a_2, \ldots, a_d)$. So

$$a_i = a_{i+d} = a_{2d+i} = \cdots = a_{(n/d-1)d+i}, i = 1, 2, \cdots, d.$$

That is,

$$(a_1, a_2, \cdots, a_n) = (\underbrace{a_1, a_2, \cdots, a_d}, \underbrace{a_1, a_2, \cdots, a_d}, \cdots, \underbrace{a_1, a_2, \cdots, a_d}).$$

On the contrary, if $(a_1, a_2, \cdots, a_d)$ be an arbitrary d-tuple , then the period of the state $(a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, a_d, a_1, a_2, \cdots, a_d, \cdots, a_1, a_2, \cdots, a_d)$ must be a factor of d. Hence PCR_n has $(2^t)^d$ states whose periods are factors of d. On the other side, the number of the states whose periods are factors of d is

$$\sum_{d'|d} d'M(d'),$$

where the sum takes over all positive factors of d. Thus

$$\sum_{d'|d} d'M(d') = (2^t)^d.$$

By the Möbius inversion formula, we have

$$M(d) = \frac{1}{d}\sum_{d'|d}\mu(d')(2^t)^{d/d'}.$$

In the following we will prove that $M(d)$ is even. When d is odd, by the above formula, we have

$$dM(d) = \sum_{d'|d}\mu(d')(2^t)^{d/d'}.$$

So $M(d)$ must be even. When $d = 2^k$, $k > 0$,

$$M(2^k) = \frac{1}{2^k}\sum_{d'|2^k}\mu(d')(2^t)^{2^k/d'} = \frac{1}{2^k}((2^t)^{2^k} - (2^t)^{2^{k-1}}),$$

so $M(d)$ is even since $k > 0$, $t > 1$. When $d = 2^k m$, $(k > 0)$, $\gcd(m, 2) = 1$,

$$\begin{aligned} M(2^k m) &= \frac{1}{2^k m}\sum_{d'|2^k m}\mu(d')(2^t)^{2^k m/d'} \\ &= \frac{1}{m}\sum_{d'|2^k m}\mu(d')2^{(2^k mt/d')-k} \end{aligned}$$

If $k = 1$, then $2^k mt/d' - k = 2mt/d' - 1 \geqslant t - 1 \geqslant 1$. So $2^{(2^k mt/d')-k}$ is even. If $k \geqslant 2$, let $d' = 2^l m'$, where $m'|m, l \leqslant k$. If $l \geqslant 2$, then $\mu(d') = 0$. If $l \leqslant 1$, then $2^k mt/d' - k = 2^(k-l)mt/m' - 1 \geqslant 2^(k-l)t - k > 1$ So $2^{(2^k mt/d')-k}$ is also even. Hence, the numerator of the right part of above equation is always even while the denominator is odd, so $M(d)$ is even. □

Corollary 1. The permutation $T_\tau(a_0, a_1, \cdots, a_{n-1}) = (a_1, \cdots, a_{n-1}, a_0)$ of $\mathbb{F}_{2^t}^n$ is even.

Proof. By Theorem 2, the length of every cycle of the permutation is a factor of n. Let d be a positive factor of n, then $M(d)$ which is the number of the cycles with length d is even. Represent T_τ as the product of disjoint cycles, then for every factor d of n, there are even number cycles of length d. Write $T_\tau = \Pi d * M(d)$. If d is odd, then all the d-cycles are even permutations. If d is even, then all the d-cycle are odd permutation. However, the number of the cycles with length d is even. So the product of all d-cycle is an even permutation. Thus T_τ is an even permutation following from that the product of two even permutations is an even permutation. □

Lemma 3. The permutation T_{L_2} is an even permutation.

Proof. Let $T_{c_0}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, c_0 a_{n-1})$. And let $T_{L_3}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, a_{n-1} + c_1 a_0 + \cdots + c_{n-1}a_{n-2})$. Then they are all permutations of $\mathbb{F}_{2^t}^n$ and $T_{L_2} = T_{L_3} \circ T_{c_0} \circ T_\tau$. Since T_τ is an even permutation by corollary 1, if we prove that T_{c_0} and T_{L_3} are all even permutations, then so is T_{L_2}.

For T_{c_0}, if $c_0 = 1$, then T_{c_0} is the identity mapping. If $c_0 > 1$, denote the order of c_0 is r, then T_{c_0} has $2^t(n-1)$ fixed points and $2^t(n-1)(2^t-1)$ r-cycle. Since $2^t(n-1)(2^t-1)$ is even when $n > 1$ and $t > 1$. T_{c_0} is an even permutation whatever r is even or odd.

For T_{L_3}, let $h = \#\{i|c_i \neq 0, 1 \leqslant i \leqslant n-1\}$. If $h = 0$, then T_{L_3} is the identity mapping, then T_{L_3} is even. If $h \neq 0$. It does not lose the generality to suppose that $c_1 \neq 0$. For

$(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_{2^t}^n$, if $a_0 = c_1^{-1} \sum_{i=2}^{n-1} c_i a_{i-1}$, then $(a_0, a_1, \cdots, a_{n-1})$ is the fixed point of T_{L_3}. So T_{L_3} has $(2^t)^{n-1}$ fixed points. If $a_0 \neq c_1^{-1} \sum_{i=2}^{n-1} c_i a_{i-1}$, then $T_{L_3}^2(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-1})$. Hence T_{L_3} is the composition of $\frac{1}{2}((2^t)^n - (2^t)^{n-1})$ transpositions. Obviously, $\frac{1}{2}((2^t)^n - (2^t)^{n-1})$ is even when $n > 1$ and $t > 1$. So T_{L_3} is also an even permutation. □

Applying the above lemmas, we can give our first main result.

Theorem 3 The state transition transformation T is an even permutation of $\mathbb{F}_{2^t}^n$ when $t, n > 1$.

Proof. By Lemma 1, we have $T = T_{WGP}^{-1} \circ T_{L_1} \circ T_{WGP} \circ T_{L_2}$. By lemma 2, $T_L = T_{WGP}^{-1} \circ T_{L_1} \circ T_{WGP}$ is an even permutation of $\mathbb{F}_{2^t}^n$. By lemma 3, T_{L_2} is an even permutation. So T is an even permutation of $\mathbb{F}_{2^t}^n$ when $t, n > 1$. □

4 The cycle decomposition of the WG-NLFSR

In this part, we first give the relationships among the parity of a permutation of a set , the parity of the number of cycles in the cycle decomposition of the permutation and the number of the elements of the set. Then we apply the result to prove that the parity of the number of cycles in the cycle decomposition of the state transition transformation T is even.

Suppose that Ω is an arbitrary nonempty set. And π is an arbitrary permutation of Ω. Let $|\Omega|$ represent the number of elements of the set Ω, b represent the parity of the permutation π ($b = 0$ or 1, 0 represents even permutation, 1 represents odd permutation), N represent the number of cycles in the cycle decomposition of π. Then we have

Theorem 4 The parity of N is the same as the parity of $|\Omega| + b$.

Proof. Let the cycle structure of the permutation π be $\{1 * k_1, 2 * k_2, \cdots, m * k_m\}$, here $1 \leqslant m \leqslant |\Omega|$, $k_i (i = 1, 2, \cdots, m)$ are positive numbers. Then the number of the cycles in the cycle structure is $N = k_1 + k_2 + \cdots + k_m$. Since π is a permutation of Ω, we have $k_1 + 2k_2 + \cdots + t \cdot k_m = |\Omega|$. So the parity of $|\Omega|$ is the same as the parity of $k_1 + k_3 + k_5 + \cdots$.

When $b = 0$, i.e., π is an even permutation, then the number of k-cycle when k is even must be even, i.e., $k_2 + k_4 + \cdots$ is even. So the parity of $N = k_1 + k_2 + k_3 + \cdots + k_m$ is the same as $|\Omega|$.

When $b = 1$, i.e., π is an odd permutation, then the number of k-cycles when k is even must be odd, i.e. $k_2 + k_4 + \cdots$ is odd, hence $N = k_1 + k_2 + k_3 + \cdots + k_m$ is the same as $|\Omega| + 1$. □

By theorem 4, we can directly have the following corollaries.

Corollary 2 For every even permutation π of $\mathbb{F}_{2^t}^n$, the number of cycles in its cycle decomposition is even.

Corollary 3 The number of cycles in the cycle decomposition of T is even.

Proof. By theorem 3, T is an even permutation, then by corollary 2, the number of cycles in the cycle decomposition of T is even. □

5 The filtering WG7-NLFSR

The readers can refer to [6] for more details. The mathematical details of the filtering WG7-NLFSR which is similar to the WG-7 stream cipher [5]. The filtering WG7-NLFSR is composed of a nonlinear feedback shift register of length 23 and the WG transformation over the finite field $\mathbb{F}_{2^7}$. The finite field $\mathbb{F}_{2^7}$ is defined by the primitive polynomial $t(x) = x^7 + x + 1$ over $\mathbb{F}_2$.

Let $h(x) = x + x^{33} + x^{39} + x^{41} + x^{104}$. The nonlinear WG permutation with decimation 3, from $\mathbb{F}_{2^7}$ to $\mathbb{F}_{2^7}$, is defined by $WGP7(x^3) = h(x^3 + 1) + 1$, and the WG transformation over $\mathbb{F}_{2^7}$ is defined as $WG7(x) = Tr(WGP7(x^3)) = Tr(x^3 + x^9 + x^{21} + x^{57} + x^{87})$, $x \in \mathbb{F}_{2^7}$.

Here $Tr(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32} + x^{64}$ is the mapping from $\mathbb{F}_{2^7}$ to $\mathbb{F}_2$. We denote by $\{a_i\}$ the sequence generated by the following NLFSR, which is defined as

$$a_{i+23} = \gamma a_i + a_{i+11} + WGP7(a_{i+22}); a_i \in \mathbb{F}_{2^7}, \qquad (2)$$

where $p(x) = x^{23} + x^{11} + \gamma$ is a primitive polynomial over $\mathbb{F}_{2^7}$ and $t(\gamma) = 0$. A binary filtering WG-NLFSR sequence $\{s_i\}$ is produced by filtering through the WG transformation WG7, i.e., $s_i = WG7(a_i)$, $i \geqslant 0$.

Set $q = 2^7$. Recall that $T(a_0, a_1, \cdots, a_{22}) = (a_1, a_2, \cdots, \gamma a_i + a_{i+11} + WGP7(a_{i+22}), a_i \in \mathbb{F}_q$.

Theorem 5 The period of the sequences which generated by $WG7-$ NLFSR is less than $2^{161} - 1$ ($161 = (2^7)^{23}$). The number of cycles in the cycle structure of T is at least 4.

Proof. In order to prove the result we need to show that the length of the longest cycle in the cycle structure of $WG7-$NLFSR is less than $2^{161} - 1$. We know that $\{0, \cdots, 0\}$ is a fixed point of T. Hence the period of the sequences which produced by T is less than or equal to $q^n - 1$. If there exists some $a \in \mathbb{F}_q^*$ such that $\gamma a = WGP7(a)$, then $T(a, \cdots, a) = (a, \cdots, a)$. Fortunately it is easy to compute that $WGP7(a) = \gamma a$, when $a = \gamma^6 + \gamma^5 + \gamma^2 + \gamma + 1$. By Theorem 3.3, 3.4., the period of the sequences which generated by $WG7-$ NLFSR is less than $2^{161} - 1$ and there are at least 4 cycles in the cycle structure of T. □

6 Conclusions

In the paper[6], the authors presented a family of pseudorandom number generators named the filtering WG-NLFSR and the filtering WG7-NLFSR for EPC C1 Gen2 RFID tags. They investigated the periodicity of the filtering WG-NLFSR sequence by performing the complete cycle decomposition of the WG-NLFSR recurrence relations and by conducting an empirical study on the period distribution of WG-NLFSR sequences. In our paper we first investigate the cycle decomposition of the WG-NLFSR by the theories of permutations. And our results can be applied to a more general case. And we hope that it will be useful when we study the nonlinear feedback shift registers.

References

[1] Solomon W.Golomb, *Shift Register Sequences*, ©Copyright 1967 by Holden-Day, Inc..

[2] Z.X. Wan and Z.D. Dai, *Nonlinear feedback shift registers*,1975.

[3] Guang Gong, Member, IEEE, and Amr M. Youssef, *Cryptographic Properties of the WelchCGong Transformation Sequence Generators*, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 48, NO. 11, NOVEMBER 2002.

[4] AS. W. Golomb, and G. Gong, *Signal Design for Good Correlation: For Wire- less Communication, Cryptography, and Radar*, Cambridge University Press, New York, NY, USA, 2004.

[5] Y. Luo, Q. Chai, G. Gong, and X. Lai, *WG-7: A Lightweight Stream Cipher with Good Cryptographic Properties* , IEEE Global Communications Conference GLOBECOM 2010, pp. 1-6, 2010.

[6] Kalikinkar Mandal, and Guang Gong, *Filtering Nonlinear Feedback Shift Registers using Welch-Gong Transformations for Securing RFID Applications*, QSHINE 2013: 643-657. ISBN: 9783642379482.

[7] Yassir Nawaz and Guang Gong, *The WG stream cipher*.

[8] Xinxin Fan and Guang Gong, *Specification of the stream Cipher WG-16 Based Confidentiality and Integrity Algorithms*.