Filtering Nonlinear Feedback Shift Registers Using Welch-Gong Transformations for Securing RFID Applications

Kalikinkar Mandal and Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
{kmandal,ggong}@uwaterloo.ca

Abstract. Pseudorandom number generators play an important role to provide security and privacy on radio frequency identification (RFID) tags. In particular, the EPC Class 1 Generation 2 (EPC C1 Gen2) standard uses a pseudorandom number generator in the tag identification protocol. In this paper, we first present a pseudorandom number generator, named the filtering nonlinear feedback shift register using Welch-Gong (WG) transformations (filtering WG-NLFSR) and the filtering WG7-NLFSR for EPC C1 Gen2 RFID tags. We then investigate the periodicity of a sequence generated by the filtering WG-NLFSR by considering the model, named nonlinear feedback shift registers using Welch-Gong (WG) transformations (WG-NLFSR). The periodicity of WG-NLFSR sequences is investigated in two ways. Firstly, we perform 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 transformation module. Secondly, we conduct an empirical study on the period distribution of the sequences generated by the WG-NLFSR. The empirical study states that a sequence with period bounded below by the square root of the maximum period can be generated by the WG-NLFSR with high probability for any initial state.

Keywords: Nonlinear feedback shift registers, pseudorandom sequence generators, stream ciphers, WG-7 stream cipher.

1 Introduction

A pseudorandom sequence generator is a heart of a stream cipher, which is used for generating random-looking binary keystreams that are used to encrypt binary message streams by XORing the plaintexts with the keystreams in a bit by bit fashion to produce the ciphertexts. In practice, linear and nonlinear feedback shift registers (LFSRs/NLFSRs) have been widely used as basic building blocks for constructing stream ciphers. For instance, well-known stream ciphers, namely Grain, Trivium and Mickey in the eSTREAM project use NLFSRs as their building blocks [4].

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 643–657, 2013.

The randomness properties of a sequence generated by an LFSR have been well studied and understood [5,6], however, 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 and it is hard to determine the number of cycles and the lengths of the cycles in a cycle decomposition of an NLFSR. In the theory of NLFSRs, the cycle decomposition of NLFSRs is an important property to investigate first, since each cycle can be considered as a sequence and the cycles' lengths determine the periods of the sequences.

Several pseudorandom number generators have been proposed in the literature for EPC C1 Gen2 RFID tags [1,12,13,17]. Che *et al.*'s proposal [1] consists of an oscillator-based true random number generator (TRNG) and an LFSR of 16-stage where the TRNG is implemented using an analog circuit. In their design, one true random bit is added to each component of an LFSR generated 16-bit pseudorandom number. Due to the linear structure of the PRNG, the PRNG has been attacked by Melia-Segui *et al.* [13] with high success probability $\frac{(n+1)}{8n}$, wher n is the length of the LFSR. To avoid such an attack, Melia-Segui *et al.* [13] proposed a design by employing eight primitive polynomials to an LFSR where in each clock cycle one primitive polynomial is chosen based on a true random number generator. In [17], Peris-Lopez *et al.* proposed a PRNG named LAMED for RFID tags, which can generate 32-bit random numbers as well as 16-bit random numbers. The internal state of LAMED is 64-bit including a 32-bit key and a 32-bit IV. LAMED always outputs a 32-bit random number, a 16-bit number is obtained by dividing 32-bit number into two equal halves and XORing these two halves together. Recently, Mandal *et al.* [12] designed a PRNG named Warbler based on nonlinear feedback shift registers for RFID tags. In their design, three NLFSRs are used, two of them work over the binary field and the other one is defined over a finite field. The internal state of Warbler consists of 65 bits and 16-bit random numbers are produced by taking disjoint sequences of 16 bits.

In this paper, we present a family of pseudorandom sequence generators, named the filtering nonlinear feedback shift registers using Welch-Gong (WG) transformations (henceforth called filtering WG-NLFSR) for EPC Class 1 Generation 2 RFID tags. In particular, the filtering WG7-NLFSR is composed of a nonlinear feedback shift register of length 23 and a WG transformation module over the field $\mathbb{F}_{2^7}$. Due to the nonlinear state update of the filtering WG-NLFSR, the period of a sequence generated by the filtering WG-NLFSR is not known in general. We investigate the periodicity of a sequence generated by the filtering WG-NLFSR by considering the model, named nonlinear feedback shift registers using Welch-Gong (WG) transformations (WG-NLFSR). The design of the WG-NLFSR was inspired by the key initialization phase of the WG cipher, which was submitted to the eSTREAM project [4,15]. In the WG-NLFSR, the nonlinear recurrence relation is composed of a primitive polynomial and a nonlinear WG permutation. Due to the nonlinear property of the recurrence relation, the WG-NLFSR will be resistant to the powerful cryptanalytic attacks such as algebraic attacks, cube attacks, correlation attacks, and discrete fourier transformation attacks. Another objective of this paper is to study the periodicity of an output sequence produced by the WG-NLFSR. The periodicity of WG-NLFSR sequences is investigated in two steps. Firstly, we perform the complete cycle decomposition for different nonlinear recurrence relations by computer simulations. It is observed that, for a proper selection of a characteristic polynomial, a sequence with period greater than the square root of the maximum period can be generated by the WG-NLFSR. Secondly, we conduct an empirical study for investigating the period distribution of WG-NLFSR sequences. In the empirical study, we consider different WG-NLFSR recurrence relations over different finite fields and compute the probability distribution for different cases. Our empirical study shows that, with high probability, the WG-NLFSR generates sequences with periods bounded below by the square root of the maximum period.

The remainder of the paper is organized as follows. In Section 2, we define some terms and notations that will be used in the paper. In Section 3, we describe a general model of the filtering WG-NLFSR and a pseudorandom number generator, the filtering WG7-NLFSR. In Section 4, we study the periodicity of the WG-NLFSR sequences by performing the cycle decomposition of WG-NLFSR recurrence relations and by conducting an empirical study on the period distribution of WG-NLFSR sequences. Finally, in Section 5, we conclude the paper.

2 Preliminaries

In this section, we define the terms and notations that will be used in this paper to describe the filtering WG-NLFSR.

Notations:

- $\mathbb{F}_2 = \{0, 1\}$: the Galois field with 2 elements.
- $\mathbb{F}_{2^t}$: a finite field with 2^t elements, which is defined by α with $g(\alpha) = 0$, where $g(x)$ be a primitive polynomial of degree t over the field $\mathbb{F}_2$.
- $p(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$: a characteristic polynomial over $\mathbb{F}_{2^t}$.
- $N = 2^{nt} - 1$: the maximum period of a nonzero sequence generated by an n-stage NLFSR over $\mathbb{F}_{2^t}$.
- $\mathbb{S} = \{(x_0, x_1, ..., x_{n-1}) \mid x_i \in \mathbb{F}_{2^t}\}$: the set of all states of the WG-NLFSR with $|\mathbb{S}| = N + 1$.

The Welch-Gong (WG) Transformation

Let $\mathrm{Tr}(x) = x+x^2+x^{2^2}+\cdots+x^{2^{t-1}}$ be the trace function mapping from $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$. Let t be a positive integer with $t \pmod 3 \neq 0$ and $3k \equiv 1 \bmod t$ for some integer k. We define the function h from $\mathbb{F}_{2^t}$ to $\mathbb{F}_{2^t}$ by $h(x) = x+x^{q_1}+x^{q_2}+x^{q_3}+x^{q_4}$ and the exponents are given by $q_1 = 2^k + 1, q_2 = 2^{2k} + 2^k + 1, q_3 = 2^{2k} - 2^k + 1, q_4 = 2^{2k} + 2^k - 1$. Then the function, from $\mathbb{F}_{2^t}$ to $\mathbb{F}_{2^t}$, defined as

$$\mathrm{WGP}(x) = h(x + 1) + 1$$

is known as the *WG permutation* and the function, from $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$, defined by

$$WG(x) = \mathrm{Tr}(\mathrm{WGP}(x)), x \in \mathbb{F}_{2^t}$$

is known as the *WG transformation* [8]. The WG transformation has good cryptographic properties such as high nonlinearity, algebraic degree, and at least 1-order resiliency for a proper choice of basis. Moreover, a WG sequence has high linear complexity.

3 The Filtering WG-NLFSR

In this section we first give a general description of the filtering WG-NLFSR, which has two components including a characteristic polynomial and a WG transformation module. Then we present a pseudorandom number generator named the filtering WG7-NLFSR for EPC C1 Gen 2 RFID tags.

3.1 General Description of the Filtering WG-NLFSR

The filtering WG-NLFSR is a family of word-oriented pseudorandom sequence generators, where an internal state consists of n cells, each of which contains t bits. The total number of bits in an internal state of the filtering WG-NLFSR is $n \cdot t$. Moreover, the internal state is updated by a nonlinear recurrence relation, which is composed of a characteristic polynomial and a nonlinear WG permutation over $\mathbb{F}_{2^t}$. An overview of the architecture is shown in Fig. 1.

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

$$a_{n+k} = c_0 a_k + c_1 a_{k+1} + \cdots + c_{n-1} a_{n-1+k} + \mathrm{WGP}(a_{n-1+k}),\ a_i \in \mathbb{F}_{2^t},\ k \geq 0, \quad (1)$$

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

It is not hard to show that the period of $\{b_i\}$ produced by the filtering WG-NLFSR is the same as the period of $\mathbf{a}$. We note that the output sequence $\mathbf{a}$ cannot directly be used without applying the filter function because after n clock cycles one can have access to the internal state of the NLFSR, which allows an attacker to generate the whole sequence for a key.

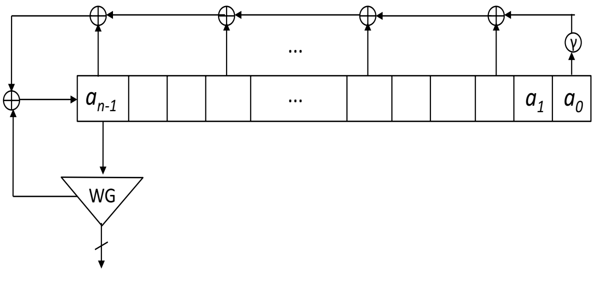


Fig. 1. Architecture of the Filtering WG-NLFSR

3.2 The Filtering WG7-NLFSR

We now give the mathematical details of the filtering WG7-NLFSR which is similar to the WG-7 stream cipher [11]. The main difference between the WG-7 stream cipher and the filtering WG7-NLFSR is that the WG-7 stream cipher uses the nonlinear feedback only at the initialization phase, but the filtering WG7-NLFSR always uses the nonlinear feedback function. 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 $h(x) = x + x^{33} + x^{39} + x^{41} + x^{104}$. Then, the nonlinear WG permutation with decimation 3, from $\mathbb{F}_{2^7}$ to $\mathbb{F}_{2^7}$, is defined by $\mathsf{WGP7}(x^3) = h(x^3 + 1) + 1$, and the WG transformation over $\mathbb{F}_{2^7}$ is defined as

$$\mathsf{WG7}(x) = \mathrm{Tr}(\mathsf{WGP7}(x^3)) = \mathrm{Tr}(x^3 + x^9 + x^{21} + x^{57} + x^{87}), x \in \mathbb{F}_{2^7}$$

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

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

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

The key length and the IV length of the filtering WG7-NLFSR are 80 bits and 81 bits, respectively. We represent an 80-bit key as $K_{0,1,\ldots,79}$ and an 81-bit initial vector as $IV_{0,1,\ldots,80}$. The key and an IV are loaded into the NLFSR as follows. For $0 \leq j \leq 10$, $a_{2j} = (K_{7j,7j+1,7j+2,7j+3}, IV_{7j,7j+1,7j+2})$ and $a_{2j+1} = (K_{7j+4,7j+5,7j+6}, IV_{7j+3,7j+4,7j+5,7j+6})$ and $a_{22} = (K_{77,78,79}, IV_{77,78,79,80})$. After loading the key and the IV, the filtering WG7-NLFSR is run for 46 clock cycles without any output. At 47-th clock cycle, the filtering WG7-NLFSR outputs the first bit.

Due to the nonlinear WG permutation $\mathsf{WGP7}(x)$ in recurrence relation (2), the period of the sequence $\{a_i\}$ is not known in general and is hard to know the exact cycle decomposition because of the large internal state. In Section 4, we will see a general investigation of the periodicity of a sequence produced by a nonlinear recurrence relation of the above type. As the keystream bits are generated by a purely nonlinear feedback function, it will be resistant to powerful cryptanalytic attacks such as algebraic attacks, correlation attacks, cube attacks and discrete fourier transformation attacks [2,7,14,16].

The mathematical functions used in the filtering WG7-NLFSR are the same as the functions used in the WG-7 stream cipher and the nonlinear WG permutation feedback does not increase any extra cost (as it is implemented for the key initialization), the implementation will be the same as the WG-7 stream cipher. For details of the WG-7 stream cipher implementation, we refer the reader to [11]. For easy reference, we reproduce the comparison data given in [11] in Table 8 as Appendix A, which indicates a microcontroller implementation comparison of the WG-7 stream cipher with other ciphers. The implementation includes the 4-bit MARC4 ATAM893-D microcontroller (a in Table 8) and the 8-bit AVR microcontroller ATmega8 (b in Table 8) from Atmel.

3.3 Application of the Filtering WG7-NLFSR

The EPCglobal Class 1 Generation 2 (EPC C1 Gen2) is an RFID standard. The tag identification protocol in the EPC C1 Gen2 standard uses a couple of 16-bit random numbers for identifying low cost passive RFID tags. Passive RFID tags get power from the reader at the beginning of the communication. Most of the existing random number generators are based on an LFSR and a true random number generator. Moreover, a true random number generator consumes more power, occupies more area and the throughput is low. For such resource-constrained environments, the filtering WG7-NLFSR can be used as a pseudorandom number generator for generating 16-bit random numbers. The 16-bit random numbers are generated by taking disjoint 16-bit sequences from the filtering WG7-NLFSR sequence $\{s_i\}$. Based on the implementation given in [11,10], it is confirmed that the filtering WG7-NLFSR is a suitable candidate for RFID tags.

4 Period Analysis of the WG-NLFSR

In order to study the periodicity of a filtering WG-NLFSR sequence, we need to investigate the period property of a sequence produced by recurrence relation (1). We redefine the nonlinear recurrence relation for the WG-NLFSR over the field $\mathbb{F}_{2^t}$ as follows. Let $\mathbf{a} = \{a_i\}_{i\geq 0}, a_i \in \mathbb{F}_{2^t}$ be a sequence generated by an n-stage nonlinear recurrence relation, which is defined as

$$a_{n+k} = c_0 a_k + c_1 a_{k+1} + \cdots + c_{n-1} a_{n-1+k} + \mathrm{WGP}(a_{n-1+k}),\ a_i \in \mathbb{F}_{2^t},\ k \geq 0, \quad (3)$$

where $\mathrm{WGP}(x)$ is the WG permutation, $t \pmod 3 \neq 0$, and $(a_0, a_1, ..., a_{n-1})$ is the *initial state*. We call the nonlinear recurrence relation (3) a *WG-NLFSR recurrence relation*. A block diagram of the WG-NLFSR sequence generator is shown in Fig. 2. Note that a WG-NLFSR recurrence relation is uniquely determined by the characteristic polynomial $p(x)$ and WG permutation. For a fixed WG permutation, the recurrence relation is different if the characteristic polynomial is different.

Due to the nonlinear term $\mathrm{WGP}(\cdot)$ in the recurrence relation (3), the period of the sequence $\mathbf{a}$ is not equal to the period of the polynomial $p(x)$. In particular, the period of $\mathbf{a}$ depends on three factors: the characteristic polynomial $p(x)$, the WG permutation $\mathrm{WGP}(x)$, and the initial state. To investigate the period of sequence $\mathbf{a}$, we need to study the cycle decomposition of the recurrence relation.

Remark 1. In recurrence relation (3), any permutation over a finite field $\mathbb{F}_{2^t}$ can be used. We here used WG permutation as a WG transformation has excellent cryptographic properties and which can be used for both updating the internal state and filtering the output sequences.

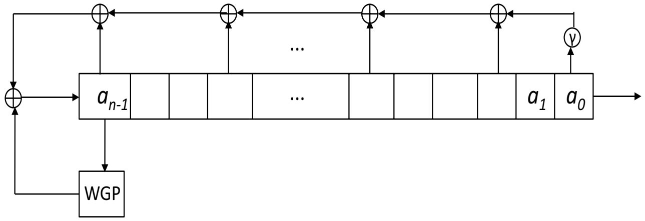


Fig. 2. Architecture of the WG-NLFSR

4.1 Cycle Decomposition of the WG-NLFSR

It is not hard to show that the recurrence relation (3) generates sequences with no branch. Thus, the recurrence relation partitions the whole state space $\mathbb{S}$ into a finite number of disjoint cycles, which is known as the cycle decomposition of the recurrence relation [5]. We denote by Ω the cycle decomposition of the recurrence relation (3), where $\Omega = \{C_1, C_2, \cdots, C_r\}$ with $\mathbb{S} = C_1 \cup C_2 \cup \cdots \cup C_r$ and $C_i \cap C_j = \phi$, $1 \leq i \neq j \leq r$. For an arbitrary recurrence relation, the value of r is not determined. Let $L_i = |C_i|$ be the number of states in $C_i, i = 1, 2, ..., r$. Using any state of C_i, all other states in C_i can be generated by recurrence relation (3). Thus, C_i can be considered as a sequence with period L_i. (For details of cycle decompositions, see [5].)

We here perform computer simulations for investigating the cycle structure of recurrence relation (3). Considering recurrence relation (3) over fields $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$, we present the cycle decompositions for different characteristic polynomials in Tables 1 - 4, where Y represents YES and N represents NO. In tables, the primitive elements α, β and the WG transformations over fields $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$ are defined in Section 4.2. The computer simulations show that for a fixed WGP(x) and a proper selection of a characteristic polynomial, a sequence with period lower bounded by $\sqrt{N}$ can be generated by the recurrence relation (3), where a proper selection of a characteristic polynomial is meant by a characteristic polynomial in the recurrence relation (3) for which the lengths of all cycles are greater than or equal to $\sqrt{N}$. It is noticed that the long period of a sequence generated by recurrence relation (3) does not depend on the irreducibility of the characteristic polynomial. In the recurrence relation, there exists a hidden relation between the coefficients of a characteristic polynomial and the exponents of the WG permutation and that hidden relation can determine a construction of a nonlinear feedback function, which will generate a sequence with a bounded period. Unfortunately, we are not yet able to explore the hidden relation.

4.2 Period Distribution of the WG-NLFSR

In this section, we conduct an empirical study on the period distribution of the sequences generated by recurrence relation (3) by considering the recurrence relation for different characteristic polynomials. In the cycle decomposition, we

Table 1. Complete cycle decompositions of the WG-NLFSR for $n = 3$ over $\mathbb{F}_{2^5}$

Index	Characteristic Polynomial	Irreducible	Cycle decomposition, Ω
1	$1 + \alpha^{14}x + \alpha^{21}x^2 + x^3$	N	23779, 6710, 2276, 1
2	$\alpha^4 + \alpha^{17}x + \alpha^{19}x^2 + x^3$	N	32762, 1, 4
3	$\alpha^{20} + \alpha^2x + \alpha^{25}x^2 + x^3$	Y	15236, 14762, 2769
4	$1 + \alpha^7x + \alpha^{26}x^2 + x^3$	N	23779, 6710, 2276, 1
5	$\alpha^3 + \alpha^{26}x + \alpha^9x^2 + x^3$	N	32750, 4, 2, 3, 1
6	$\alpha^5 + \alpha^{20}x + \alpha^{15}x^2 + x^3$	Y	32754, 4, 3, 5, 1
7	$\alpha^7 + \alpha^{16}x + \alpha^{18}x^2 + x^3$	Y	32762, 4, 1

Table 2. Complete cycle decompositions of the WG-NLFSR for $n = 4$ over $\mathbb{F}_{2^5}$

Index	Characteristic Polynomial	Irreducible	Cycle decomposition, Ω
1	$\alpha + \alpha^4x + \alpha^{26}x^2 + \alpha^{25}x^3 + x^4$	N	39070, 363841, 546171, 99492, 1
2	$\alpha + \alpha^7x + \alpha x^2 + \alpha x^3 + x^4$	N	590707, 379331, 46734, 22986, 8815, 1
3	$\alpha + \alpha^8x + \alpha^2x^2 + \alpha^4x^3 + x^4$	N	615325, 114129, 91408, 227712, 1
4	$\alpha + \alpha^8x + \alpha^{30}x^2 + \alpha^{10}x^3 + x^4$	N	298643, 549045, 141353, 59533, 1
5	$\alpha + \alpha^{18}x + \alpha^4x^2 + \alpha^{22}x^3 + x^4$	N	664966, 54862, 268380, 34846, 25518, 2, 1
6	$\alpha + \alpha^{25}x + \alpha^7x^2 + \alpha^{21}x^3 + x^4$	N	430236, 609318, 3194, 5826, 1
7	$\alpha + \alpha^{28}x + \alpha^5x^2 + \alpha^{25}x^3 + x^4$	N	914718, 91230, 42623, 1, 3
8	$\alpha^3 + \alpha^8x^2 + \alpha^{25}x^3 + x^4$	Y	463471, 585093, 5, 1
9	$\alpha^3 + \alpha^8x + \alpha^{10}x^2 + \alpha^{25}x^3 + x^4$	N	490152, 522883, 30947, 4592, 1
10	$\alpha^3 + \alpha^{20}x + \alpha^{10}x^2 + \alpha^{26}x^3 + x^4$	Y	178444, 870118, 1, 4, 3
11	$\alpha^3 + \alpha^{20}x + \alpha^{13}x^2 + \alpha^{18}x^3 + x^4$	N	636187, 81945, 312587, 17855, 1
12	$\alpha^3 + \alpha^{25}x + \alpha^{18}x^2 + \alpha^{17}x^3 + x^4$	N	62628, 105531, 880413, 2, 1
13	$\alpha^3 + \alpha^{25}x + \alpha^{20}x^2 + \alpha^{22}x^3 + x^4$	N	1048562, 7, 6
*14	$\alpha^5 + \alpha^{14}x + \alpha^{12}x^3 + x^4$	N	1030097, 9736, 8742
15	$\alpha^5 + \alpha^{16}x + \alpha^{14}x^2 + \alpha^3x^3 + x^4$	N	981057, 53724, 13788, 2, 4
16	$\alpha^7 + \alpha^{10}x + \alpha^2x^2 + \alpha^{21}x^3 + x^4$	N	1048570, 4, 1
17	$\alpha^7 + \alpha^{17}x + \alpha^{14}x^2 + \alpha^{15}x^3 + x^4$	N	953457, 80759, 14347, 7, 2, 1
18	$\alpha^7 + \alpha^{19}x + \alpha^{15}x^2 + \alpha^{24}x^3 + x^4$	N	1048572, 2, 1
19	$\alpha^{11} + \alpha x + \alpha^8x^2 + \alpha^8x^3 + x^4$	N	940556, 108007, 9, 1, 2
20	$\alpha^{11} + \alpha^7x + \alpha^4x^2 + \alpha^{28}x^3 + x^4$	N	125158, 635317, 249323, 38772, 1, 3
21	$\alpha^{11} + \alpha^{10}x + \alpha^{26}x^2 + \alpha^{11}x^3 + x^4$	N	554609, 493933, 16, 1
22	$\alpha^{11} + \alpha^{11}x + \alpha^2x^2 + \alpha^{14}x^3 + x^4$	N	696972, 337871, 13730, 1
23	$\alpha^{11} + \alpha^{14}x + \alpha^{18}x^2 + \alpha^8x^3 + x^4$	N	240673, 726854, 81046, 1
24	$\alpha^{11} + \alpha^{15}x + \alpha^3x^2 + \alpha^{12}x^3 + x^4$	Y	1005347, 43222, 3, 1, 2
25	$\alpha^{11} + \alpha^{15}x + \alpha^{20}x^2 + \alpha^9x^3 + x^4$	N	835608, 212956, 9, 1
26	$\alpha^{11} + \alpha^{18}x + \alpha^7x^2 + \alpha^{23}x^3 + x^4$	N	895975, 152596, 2, 1
27	$\alpha^{11} + \alpha^{20}x + \alpha^{21}x^2 + \alpha^{28}x^3 + x^4$	Y	289429, 510434, 84330, 164381, 1
28	$\alpha^{11} + \alpha^{27}x + \alpha^{23}x^2 + \alpha^8x^3 + x^4$	Y	835558, 213010, 2, 4, 1
29	$\alpha^{15} + x + \alpha^{14}x^2 + x^4$	N	1008690, 39884, 1
30	$\alpha^{15} + \alpha^8x + \alpha^{14}x^2 + \alpha^8x^3 + x^4$	N	881607, 166967, 1
31	$\alpha^{15} + \alpha^{15}x + \alpha^8x^2 + \alpha^{20}x^3 + x^4$	N	675115, 373449, 2, 3, 1
32	$\alpha^{15} + \alpha^{16}x + \alpha^{11}x^2 + \alpha^{13}x^3 + x^4$	N	922952, 57138, 44338, 24136, 6, 4, 1
33	$\alpha^{15} + \alpha^{24}x + \alpha^{15}x^2 + \alpha^{25}x^3 + x^4$	Y	1048571, 3, 1

have observed that there exist many characteristic polynomials for which the recurrence relation can generate sequences with periods bounded below by $\sqrt{N}$, where N is the maximum period. However, we do not know the relation between the WG permutation and such characteristic polynomials in general. We here intend to study the probability distribution of period of at least $\sqrt{N}$. That is,

Table 3. Complete cycle decompositions of the WG-NLFSR for $n = 5$ over $\mathbb{F}_{2^5}$

Index	Characteristic Polynomial	Irreducible	Cycle decomposition, Ω
1	$\alpha + \alpha^{18}x^2 + \alpha^{10}x^3 + \alpha^{14}x^4 + x^5$	N	24934939, 8057211, 501740, 60539, 2
2	$\alpha + \alpha^{21}x^2 + \alpha^{26}x^3 + \alpha^{20}x^4 + x^5$	N	33324081, 215923, 14354, 6, 67
3	$\alpha + \alpha x + \alpha^5x^2 + \alpha^{21}x^3 + \alpha^5x^4 + x^5$ N		23683815, 9430226, 180678, 255311, 4401
4	$\alpha + \alpha^{28}x^2 + \alpha^{19}x^3 + \alpha^{19}x^4 + x^5$	Y	33137436, 416935, 29, 23, 1, 6
5	$\alpha + x + \alpha x^2 + \alpha^{22}x^3 + \alpha^9x^4 + x^5$	N	33509677, 42891, 1740, 118, 2, 1
6	$\alpha + \alpha x + x^2 + \alpha^5x^3 + \alpha^{20}x^4 + x^5$	N	32438885, 802371, 136113, 154148, 22912, 1
7	$\alpha + \alpha^4x^2 + \alpha^8x^3 + \alpha^{18}x^4 + x^5$	N	20018544, 12576215, 661370, 252630, 45560, 111, 1
8	$\alpha + \alpha^5x^2 + \alpha^{24}x^3 + x^4 + x^5$	N	31853496, 1026340, 616630, 10591, 46360, 1001, 13
9	$\alpha + \alpha^6x^2 + \alpha^{28}x^3 + \alpha^4x^4 + x^5$	N	27060025, 539828, 5044304, 853141, 57062, 70, 1
10	$\alpha + \alpha^{13}x^2 + \alpha^{14}x^3 + \alpha^4x^4 + x^5$	N	1614083, 26744592, 5172342, 23352, 59, 2, 1
11	$\alpha + \alpha^{16}x^2 + \alpha^2x^3 + \alpha^{24}x^4 + x^5$	N	26604921, 60903, 5881770, 980844, 25982, 4, 7
12	$\alpha + \alpha^{18}x^2 + \alpha^{20}x^3 + \alpha^{24}x^4 + x^5$	N	13669238, 17126821, 2416848, 289074, 52395, 54, 1
13	$\alpha + x + \alpha^{11}x^3 + \alpha^{15}x^4 + x^5$	Y	29770970, 2699894, 1000613, 62602, 20324, 23, 5
14	$\alpha + x + x^2 + \alpha^5x^3 + \alpha^{18}x^4 + x^5$	N	9244135, 9425167, 10061666, 4589985, 233472, 1, 5
15	$\alpha + x + x^2 + \alpha^{22}x^3 + \alpha^{13}x^4 + x^5$	Y	32786392, 758058, 9835, 132, 11, 2, 1
16	$\alpha + x + \alpha x^2 + \alpha^{16}x^3 + \alpha^{20}x^4 + x^5$	N	33188710, 351685, 13861, 166, 6, 2, 1
17	$\alpha + x + \alpha^4x^2 + \alpha^{28}x^3 + \alpha^{18}x^4 + x^5$	Y	33554268, 45, 17, 2, 1, 29, 3
*18	$\alpha + x + \alpha^{11}x^2 + \alpha^{25}x^3 + \alpha^{19}x^4 + x^5$	N	1711633, 17174871, 11626420, 2069636, 659633, 275686, 36552
19	$\alpha + x + \alpha^{12}x^2 + \alpha^{30}x^3 + \alpha^{20}x^4 + x^5$	N	26385451, 704023, 262540, 3728330, 2474077, 8, 2
20	$\alpha + x + \alpha^{13}x^2 + \alpha x^3 + \alpha^{17}x^4 + x^5$	N	31083249, 2470874, 281, 11, 6, 9, 1
21	$\alpha + x + \alpha^{16}x^2 + \alpha^{20}x^3 + \alpha^{30}x^4 + x^5$	N	32645326, 634069, 54804, 88483, 74357, 57391, 1
22	$\alpha + x + \alpha^{19}x^2 + \alpha^{27}x^3 + \alpha^{12}x^4 + x^5$	N	30290671, 609570, 384964, 554062, 1570249, 144914, 1
*23	$\alpha + x + \alpha^{25}x^2 + \alpha x^3 + \alpha^{27}x^4 + x^5$	N	6758906, 19951473, 853356, 5840681, 5929, 75633, 68453
24	$\alpha + \alpha^8x^2 + \alpha^{21}x^3 + \alpha^{13}x^4 + x^5$	N	31959770, 1594335, 112, 173, 7, 17, 9, 1
25	$\alpha + x + \alpha^2x^2 + \alpha^{12}x^3 + \alpha^{20}x^4 + x^5$	N	14631594, 17557700, 1270630, 23428, 50395, 20669, 11, 2
26	$\alpha + x + \alpha^3x^2 + \alpha^{10}x^3 + \alpha^{10}x^4 + x^5$	N	8613690, 17190010, 7681297, 17715, 34521, 17155, 41, 1
27	$\alpha + x + \alpha^{17}x^2 + \alpha^{10}x^3 + \alpha^9x^4 + x^5$	N	31934521, 1487357, 11327, 64353, 56840, 28, 3, 1
28	$\alpha + x + \alpha^{21}x^2 + \alpha^{16}x^3 + \alpha^{29}x^4 + x^5$	Y	11545515, 21015426, 720059, 240858, 32564, 3, 2, 1
29	$\alpha + \alpha x + \alpha^3x^2 + x^3 + \alpha^{12}x^4 + x^5$	N	20341385, 6807881, 4023518, 1776187, 598917, 6539, 2, 1

we want to compute what the success probability is that for any initial state of the recurrence relation, the WG-NLFSR can generate a sequence with period lower bounded by $\sqrt{N}$. The main goal of performing this empirical study is that it can convey a general behavior of this type of recurrence relations.

Procedure for Computing the Success Probability for the Period $\geq \sqrt{N}$. We calculate the probability distribution of period as follows. For a WG-NLFSR recurrence relation, we perform the complete cycle decomposition by computer simulations. We first compute the complete cycle decompositions for different characteristic polynomials with the same WG permutation, where different characteristic polynomials are chosen randomly. Then, using the cycle decomposition we calculate the expected success probability and the standard

Table 4. Complete cycle decompositions of the WG-NLFSR for $n = 3$ over $\mathbb{F}_{2^7}$

Index	Characteristic Polynomial	Irreducible	Cycle decomposition, Ω
1	$\beta + \beta x + \beta^{116}x^2 + x^3$	Y	1972915, 124227, 9
2	$\beta + \beta^4 x + \beta^2 x^2 + x^3$	N	281885, 213421, 858081, 306286, 24446, 327239, 11564, 58233, 15994, 1
3	$\beta + \beta^4 x + \beta^{111}x^2 + x^3$	N	1862053, 21922, 161976, 38595, 12601, 2
4	$\beta + \beta^7 x + \beta^{43}x^2 + x^3$	Y	1548601, 335992, 200230, 12315, 3, 1
*5	$\beta + \beta^{21}x + \beta^{121}x^2 + x^3$	Y	1482387, 331576, 283188
6	$\beta + \beta^{55}x + \beta^{45}x^2 + x^3$	N	2079604, 17535, 5, 3, 4
7	$\beta + \beta^{80}x + \beta^{84}x^2 + x^3$	Y	2097095, 52, 2, 1
8	$\beta + \beta^{81}x + \beta^8 x^2 + x^3$	Y	245680,143280,675851,1003363, 20428,8546,1
9	$\beta + \beta^{91}x + \beta^7 x^2 + x^3$	N	1980490, 75492, 41167, 1
10	$\beta^3 + \beta^2 x + x^3$	Y	1923727, 173414, 7, 2, 1
*11	$\beta^3 + \beta^4 x + \beta^{83}x^2 + x^3$	N	2043475, 38142, 15534
12	$\beta^3 + \beta^{54}x + \beta^{84}x^2 + x^3$	Y	1892847, 184935, 19367, 1
13	$\beta^3 + \beta^{87}x + \beta^{38}x^2 + x^3$	N	2082246, 14900, 3, 1
14	$\beta^9 + \beta^{69}x + \beta^{69}x^2 + x^3$	N	1956446, 140682, 16, 6, 1
15	$\beta^9 + \beta^{70}x + \beta^{21}x^2 + x^3$	Y	1918311, 174964, 3872, 3, 1
16	$\beta^9 + \beta^{101}x + \beta^{84}x^2 + x^3$	Y	1955962, 141168, 14, 4, 3
17	$\beta^9 + \beta^{115}x + \beta^{29}x^2 + x^3$	Y	1610286, 486846, 16, 2, 1
18	$\beta^5 + \beta^{78}x + \beta^{118}x^2 + x^3$	N	1780061, 274339, 42749, 1
19	$\beta^9 + \beta^{20}x + \beta^{121}x^2 + x^3$	N	678904, 1418237, 4, 3
20	$\beta^{11} + \beta^{30}x + \beta^4 x^2 + x^3$	Y	624809, 1446046, 26294, 1
21	$\beta^{21} + \beta^{99}x + \beta^{59}x^2 + x^3$	N	2038686, 58448, 9, 4
22	$\beta + \beta^{25}x + \beta^{81}x^2 + x^3$	N	191464, 1328016, 460109, 117558, 4
23	$\beta^3 + \beta^{17}x + \beta x^2 + x^3$	Y	1576062, 356525, 140941, 23621, 2
*24	$\beta^3 + \beta^{112}x + \beta^{44}x^2 + x^3$	Y	93674, 1203620, 395834, 392354, 11669
25	$\beta^7 + \beta^{46}x + \beta^{84}x^2 + x^3$	N	1023858, 706836, 334068, 32387, 2
*26	$\beta^{11} + \beta^{53}x + \beta^{13}x^2 + x^3$	N	162697, 1628279, 72007, 114484, 119684
*27	$\beta^{27} + \beta^{28}x + \beta^{90}x^2 + x^3$	N	1393588, 534559, 116786, 34123, 18095
28	$\beta^{27} + \beta^{48}x + \beta^{91}x^2 + x^3$	Y	658722, 1230400, 176058, 31965, 6
29	$\beta + \beta^4 x + \beta^{111}x^2 + x^3$	N	1862053, 21922, 161976, 38595, 12601, 2
*30	$\beta^{23} + \beta^{62}x + \beta^{46}x^2 + x^3$	N	450219, 149546, 530547, 287938, 648238, 13859, 16804
*31	$\beta^{21} + \beta^5 x + \beta^{75}x^2 + x^3$	Y	668870, 643111, 86400, 73493, 343991, 277419, 3867
*32	$\beta^{19} + \beta^{118}x + \beta^{15}x^2 + x^3$	N	283412, 1296087, 431294, 23925, 25440, 24900, 12093

deviation (SD) of the period greater than or equal to $\sqrt{N}$. We note that the success probability is equal to one when the lengths of all the cycles are greater than or equal to $\sqrt{N}$. The details of the success probability calculation is described in the following procedure.

Let D be a random variable which represents the number of distinct characteristic polynomials of the same degree. For each characteristic polynomial, the success probability of the period greater than or equal to $\sqrt{N}$ is computed as follows:

Procedure 1.

1. Compute $\{C_1, C_2, ..., C_r\}$, which is the cycle decomposition of the characteristic polynomial with $L_i = |C_i|,\ i = 1, 2, ..., r$.
2. Add all L_j's which are less than $\sqrt{N}$ and let the sum be L_{sum}.
3. The success probability of the period bounded below by $\sqrt{N}$ for any initial state is $1 - \frac{L_{sum}}{N}$.

We then compute the expectation and standard deviation (SD) for the period of D success probabilities. Let D_{mean} and D_{SD} be the expectation and standard deviation, respectively. Then, we use the histogram with (D_{mean}, D_{SD}) to represent the probability distribution of the period. In the following subsection, we present the experimental results by the above procedure.

Period Distribution of the WG-NLFSR over the Field $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$. In this subsection, we compute the expected success probability of period by the above Procedure 1 for the recurrence relation of length $n = 3, 4$ and 5 over the field $\mathbb{F}_{2^5}$ and for the recurrence relation of length $n = 3, 4$ over the field $\mathbb{F}_{2^7}$. In Table 5, the WG permutations over fields $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$ are defined.

Table 5. Parameter descriptions

t	Primitive element of $\mathbb{F}_{2^t}$	Primitive Polynomial	WG permutations
5	α	$\alpha^5 + \alpha^3 + 1 = 0$	$\mathrm{WGP5}(x) = x + (x+1)^5 + (x+1)^{13} + (x+1)^{19} + (x+1)^{21}$
7	β	$\beta^7 + \beta + 1 = 0$	$\mathrm{WGP7}(x) = x + (x+1)^{33} + (x+1)^{39} + (x+1)^{41} + (x+1)^{104}$

We consider the n-stage recurrence relation (3) with WGP5(x) and WGP7(x) as the WG permutation over the field $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$, respectively. Our simulation results for $n = 3, 4$ and 5 over the field $\mathbb{F}_{2^5}$ are given in Table 6. Similarly, the simulation results for $n = 3$ and 4 over $\mathbb{F}_{2^7}$ are given in Table 7. In Tables 6 and 7, we provide the number of characteristic polynomials (D), the expected success probability (D_{mean}), the standard deviation (D_{SD}), and the maximum value of the sum of all smaller length cycles which are less than $\sqrt{N}$ (L_{sum}). In addition, the average number of cycles in the cycle decomposition of the WG-NLFSR recurrence relation is presented. Our experimental results show that the numerical value for the average number of cycles is very close to the average number of cycles generated by the random sampling (let $\overline{r}_s$ denote the expected number of cycles generated by the random sampling, then $\overline{r}_s \approx \ln N$, see [5]).

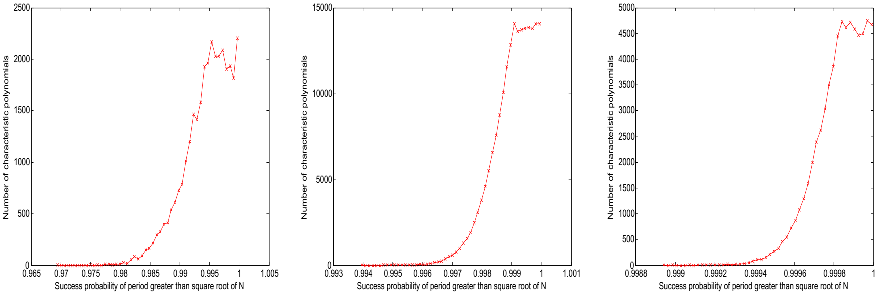
Table 6. The summary of simulation results over $\mathbb{F}_{2^5}$

Length, n	Max period, N	D	D_{mean}	D_{SD}	L_{sum}	Avg.#of cycles	$\overline{r}_s$
3	$2^{15} - 1$	31744	0.9945	0.0039	1011	10.51	10.38
4	$2^{20} - 1$	197296	0.9990	0.00069	6394	13.95	13.86
5	$2^{25} - 1$	66888	0.9998	0.00012	35828	17.44	17.32

For $n = 3$, the success probability of period lower bounded by $\sqrt{N}$ is depicted in Fig. 3a in the form of a histogram. In figures, the x-axis represents the success probability values and the y-axis represents the number of characteristic polynomials that have been taken. In the histogram, it can be observed that for most characteristic polynomials the recurrence relation produces sequences with period of at least $\sqrt{N}$ when the success probability is greater than 0.985. The empirical result for $n = 3$ in Table 6 says that if an arbitrary characteristic polynomial is chosen in the WG-NLFSR recurrence relation with WGP5(x),

Table 7. The summary of simulation results over $\mathbb{F}_{2^7}$

Length, n	Max period, N	D	D_{mean}	SD	L_{sum}	Avg.#of cycle	$\overline{r}_s$
3	$2^{21}-1$	294912	0.9993	0.00049	35828	14.49	14.55
4	$2^{28}-1$	7337	0.9999	0.00004	82216	19.38	19.41



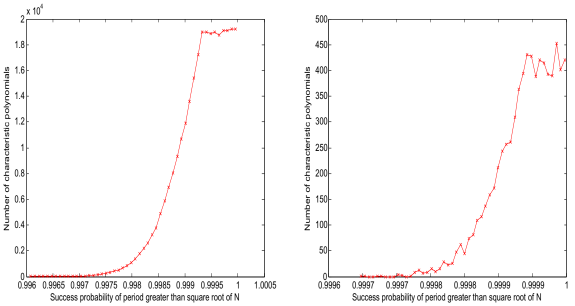
(a) $n = 3$ (b) $n = 4$ (c) $n = 5$

Fig. 3. Distribution of the period $\geq \sqrt{N}$ for $t = 5$, (a) $n = 3$, (b) $n = 4$ and (c) $n = 5$

then, with expected probability 0.9945, the recurrence relation can generate a sequence with period lower bounded by $\sqrt{N}$.

In a similar fashion, the probability distributions of period for $n = 4$ and 5 over $\mathbb{F}_{2^5}$ in Figs. 3b and 3c, and $n = 3$ and 4 over $\mathbb{F}_{2^7}$ in Figs. 4a and 4b are depicted in the form of a histogram along with the expected success probability. For $n = 4$ and 5, the expected success probabilities of the period are given by 0.990 and 0.9998, respectively, which are greater than the expected success probability for $n = 3$.

The empirical analysis shows that with a high probability the WG-NLFSR can generate a sequence with period at least $\sqrt{N}$ for a large length of the NLFSR. In



(a) $n = 3$ (b) $n = 4$

Fig. 4. Distribution of the period $\geq \sqrt{N}$ for $t = 7$, (a) $n = 3$, (b) $n = 4$

particular, with very high probability, the filtering WG7-NLFSR can generate a sequence with period at least $2^{80.5}$.

5 Conclusions

In this paper, we presented a family of pseudorandom number generators named the filtering WG-NLFSR and the filtering WG7-NLFSR for EPC C1 Gen2 RFID tags. Due to the nonlinear feedback for the state update, the filtering WG-NLFSR and filtering WG7-NLFSR will be resistant to the powerful cryptanalytic attacks. In order to investigate the periodicity of the filtering WG7-NLFSR sequence, we introduced the WG-NLFSR, which generates sequences over the finite field. The periodicity of WG-NLFSR sequences is investigated 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 the cycle decomposition, we observed that there are many characteristic polynomials in which the cycle lengths are close to the maximum period or bounded below by $\sqrt{N}$ and we listed some characteristic polynomials over the fields $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$. In the empirical study, the period distribution of the WG-NLFSR sequences over the field $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$ for different lengths of the shift registers are conducted. Moreover, the empirical study reveals that, with high probability, the filtering WG7-NLFSR can generate sequences with periods bounded below by $2^{80.5}$. To the best of our knowledge, this is the first study in the literature on the cycle decomposition and the distribution of a period of a sequence generated by the nonlinear feedback shift register over an extension field.

References

1. Che, W., Deng, H., Tan, X., Wang, J.: A Random Number Generator for Application in RFID Tags. In: Networked RFID Systems and Lightweight Cryptography, ch. 16, pp. 279–287. Springer (2008)
2. Dinur, I., Shamir, A.: Cube Attacks on Tweakable Black Box Polynomials. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 278–299. Springer, Heidelberg (2009)
3. EPCglobal. EPC Radio-Frequency Identification Protocol Class-1 Generation-2 UHF RFID for Communication at 860-960 MHz (2008), http://www.epcglobalinc.org/
4. The eStream Project, http://www.ecrypt.eu.org/stream/
5. Golomb, S.W.: Shift Register Sequences. Aegean Park Press, Laguna Hills (1981)
6. Golomb, S.W., Gong, G.: Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar. Cambridge University Press, New York (2004)
7. Gong, G., Rønjom, S., Helleseth, T., Hu, H.: Fast Discrete Fourier Spectra Attacks on Stream Ciphers. IEEE Transactions on Information Theory 57(8), 5555–5565 (2011)

8. Gong, G., Youssef, A.: Cryptographic Properties of the Welch-Gong Transformation Sequence Generators. IEEE Transactions on Information Theory 48(11), 2837–2846 (2002)
9. Juels, A.: RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications (J-SAC) 24(2), 381–394 (2006)
10. Lam, C., Aagaard, M., Gong, G.: Hardware Implementations of Multi-output Welch-Gong Ciphers, CACR Technical Report (2011), http://www.cacr.math.uwaterloo.ca/
11. Luo, Y., Chai, Q., Gong, G., Lai, X.: WG-7: A Lightweight Stream Cipher with Good Cryptographic Properties. In: IEEE Global Communications Conference – GLOBECOM 2010, pp. 1–6 (2010)
12. Mandal, K., Fan, X., Gong, G.: Warbler: A Lightweight Pseudorandom Number Generator for EPC Class 1 Gen 2 RFID Tags. In: Radio Frequency Identification System Security: RFIDsec 2011 Asia Workshop Proceedings (Cryptology and Information Security), November 7-8 (2012)
13. Melia-Segui, J., Garcia-Alfaro, J., Herrera-Joancomarti, J.: Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 34–46. Springer, Heidelberg (2010)
14. Meier, W., Staffelbach, O.: Fast Correlation Attacks on Certain Stream Ciphers. Journal of Cryptology, 159–176 (1989)
15. Nawaz, Y., Gong, G.: WG: A Family of Stream Ciphers with Designed Randomness Properties. Information Science 178(7), 1903–1916 (2008)
16. Courtois, N., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345–359. Springer, Heidelberg (2003)
17. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: LAMED - A PRNG for EPC Class-1 Generation-2 RFID Specification. Computer Standard Interfaces 31, 88–97 (2009)
18. Ranasinghe, D.C., Cole, P.H.: An Evaluation Framework. In: Networked RFID Systems and Lightweight Cryptography, pp. 157–167. Springer (2008)

Appendix A.

We here present the performance comparison table for the WG-7 stream cipher from [11]. Another implementation of WG-7 stream cipher can be seen in [10].

Table 8. Comparison of WG-7 and other lightweight ciphers [11]

a	Cipher	Cost of Resources		Init. [cycles]	Thru.put [bits/sec]
		Code	EXP/RET		
	PRESENT@2MHz PRESENT@0.5MHz	841	25/4	230	2,297 574
	HB@2MHz HB@0.5MHz	1,532	9/7	22,949	5543 1,386
	WG-7@2MHz **WG-7**@0.5MHz	1,097	7/4	10,084	9,852 2,463
b		Flash	SRAM		
	AES@8MHz	6,664	88	7,149	81,432
	Salsa20@8MHz	3,842	258	318	83,688
	XTEA@8MHz	820	0	–	51655
	PRESENT@8MHz	2,398	528	–	53,361
	Size+HB@8MHz	1,308	0	14,735	34,934
	Speed+HB@8MHz	10,918	0	8,182	91,494
	GRAIN@8MHz	778	20	107,366	12,966
	TRIVIUM@8MHz	424	36	775,726	12,030
	WG-7@8MHz	1,100	0	10074	280,087