Cryptanalysis of WG-7 A Lightweight Stream Cipher for RFID Encryption (A Draft Paper)

Mohammad Ali Orumiehchiha, Josef Pieprzyk, and Ron Steinfeld

Center for Advanced Computing, Algorithms and Cryptography, Department of Computing,
Faculty of Science, Macquarie University, Sydney, NSW 2109, Australia
(mohammad.orumiehchiha,josef.pieprzyk,ron.steinfeld)@mq.edu.au

Abstract. WG-7 is a stream cipher based on WG Stream Cipher and is designed by Y. Luo, Q. Chai, G. Gong, and X. Lai in 2010. This cipher is designed to implement in low cost and lightweight application such as RFID tags. This paper addresses cryptographic weaknesses of WG-7 Stream Cipher. We point out that the key stream generated by WG-7 can be distinguished from a random sequence with about $2^{13.5}$ keystream bits and negligible error probability. Also, we investigate the security of WG-7 against algebraic attack. A key recovery attack on this cipher is proposed to recover internal state and so secret key with time complexity about $O(2^{27})$.

Keywords: WG-7 Stream cipher, Cryptanalysis, Key Recovery Attack, Distinguishing Attack, WG Stream cipher.

1 Introduction

WG-7 [10] is proposed as a fast, lightweight and secure stream cipher inspired by family of WG stream ciphers [12] design principles. WG is a synchronous stream cipher submitted to ECRYPT call for stream ciphers. WG-7 and WG are hardware-oriented stream ciphers that use a word-oriented Linear Feedback Shift Register (LFSR) and a filter function based on Welch-Gong (WG) transformation [8]. The structure of WG-7 is similar to WG Stream Cipher, both use LFSR and filtering function but WG works in $GF(2^{29})$ and WG-7, $GF(2^7)$. WG-7 uses 80-bit secret key and IV 81-bit. After loading of the LFSR with secret key and IV, it runs for 46 clock cycles with a non-linear feedback function. In our analysis in this paper, we suppose that the initialization part of algorithm is perfect. The internal state of WG-7 is 161 bits and the designers have provided 80-bit security for the cipher. WG-7 is designed for RFID encryption and lightweight security applications. The claimed security analysis of WG-7 [10] indicates that it is secure against time/memory/data trade off attack, differential attack, algebraic attack, correlation attack and Discrete Fourier Transform (DFT) attack.

2 A quick description of WG-7

WG-7 keystream generator is illustrated in the Figure 1. WG-7 consists of a 23 stage linear feedback shift registers (LFSR) over $\mathbb{F}_{2^7}$ and a non-linear transformation called WG. The finite field $\mathbb{F}_{2^7}$ is defined by the primitive polynomial $g(x) = x^7 + x + 1$. The characteristic polynomial of the LFSR is primitive over $\mathbb{F}_{2^7}$ and is given by:

$$f(x) = x^{23} + x^{11} + \beta \tag{1}$$

where β is a root of $g(x)$. The non-linear filter function , WG7(x), is defined as a WG transformation [8] $\mathbb{F}_{2^7} \to \mathbb{F}_2$ as follows:

$$WG7(x) = f(x^3) = Tr(x^3 + x^9 + x^{21} + x^{57} + x^{87}), \quad x \in \mathbb{F}_{2^7}. \tag{2}$$

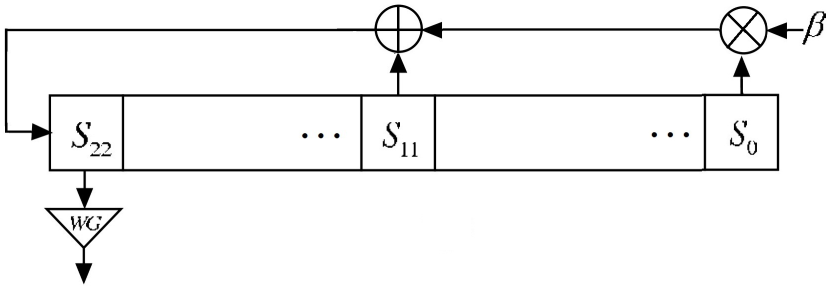

Fig. 1. The WG-7 Stream Cipher Scheme

3 Cryptanalysis of WG-7 Stream Cipher

In this section, we describe our proposed attacks on WG-7. Firstly, we have proposed a distinguishing attack on WG-7. The attack is based on linear approximation attack exploiting a found bias to distinguish the WG-7 outputs from a random binary source.

Secondly, We will describe a key recovery attack based on fast algebraic attack. The attack can recover internal state and secret key in real time.

3.1 Distinguishing Attack on WG-7

The structure of WG-7 Stream Cipher is filter generator which passes the state of a LFSR into a non-linear filtering function to generate one bit keystream output. One idea to analyse the structure is supposing linear approximation of filter function as a linear polynomial with a certain probability. In other words, we are looking for the nearest affine function to WG transformation. By applying Walsh-Hadamard transform to the filter function, the best linear approximation can be achieved. Let $\Gamma.(x_0, ..., x_6) + \alpha$ is the best linear function where x_i is i^{th} bit of word x, ”.” is inner multiplication and $\Gamma(\in \mathbb{F}_{2^7})$ is a constant and α is a bit constant where $\alpha \in \{0, 1\}$. In case of WG-7 Stream Cipher, there are seven affine functions ,like $1 + x_0 + x_1 + x_4$, which are nearest affine functions to WG-7 boolean function. The non-linearity of WG7 is 52. Therefore, we have:

$$Pr(WG(x) = (\Gamma.x + \alpha)) = \frac{2^7 - 52}{2^7} = 0.59375 \tag{3}$$

Let recursive form of Equation (1) as follows:

$$S_{i+23} = S_{i+11} \oplus \beta.S_i \tag{4}$$

By considering linear Equation (1), we need to find the best linear approximation of Equation (5):

$$WG(S_{i+23}) \oplus WG(S_{i+11}) \oplus WG(S_i) = 0 \tag{5}$$

Remark 1: The Piling Up Lemma cannot be used to compute the bias of Equation (5) because the input variables $(S_{i+23}, S_{i+11}, S_i)$ are not independent. In particular, S_{i+23} is correlated with other variables by Equation 1. In addition, $\beta.S_i$ in Equation 4 is linear transformation of S_i. The precise linear relations are given below

$$\beta.S_i = \beta.(s_0^i, s_1^i, s_2^i, s_3^i, s_4^i, s_5^i, s_6^i) = \left|\begin{matrix} s_1^i \oplus s_3^i \oplus s_4^i \\ s_2^i \\ s_2^i \oplus s_5^i \\ s_4^i \\ s_1^i \oplus s_2^i \\ s_6^i \\ s_0^i \oplus s_1^i \oplus s_2^i \oplus s_3^i \oplus s_4^i \oplus s_5^i \oplus s_6^i \end{matrix}\right|^T \tag{6}$$

Now, the target is to determine the exact amount of ϵ in the following probability:

$$Pr(WG(S_{i+23}) \oplus WG(S_{i+11}) \oplus WG(S_i) = 0) = 0.5 + \epsilon \tag{7}$$

One method to compute the bias in Equation 7 is as follows. We consider the bias between three output bits at time (clocks) i, $i+11$, and $i+23$. So we get

$$\begin{aligned} z_{i+23} \oplus z_{i+11} \oplus z_i = & \\ &= WG(S_{i+23}) \oplus WG(S_{i+11}) \oplus WG(S_i) \\ \xRightarrow{From\ Eq.\ 4} &= WG(S_{i+11} \oplus \beta.S_i) \oplus WG(S_{i+11}) \oplus WG(S_i) \end{aligned} \tag{8}$$

Observe that Equation 8 is a boolean function with 14 input variables (instead of 21 variables) and s single bit output. In other words, S_{i+23} depends on S_i and S_{i+11} based on Equations 4 and 6. Let $F : GF(2^{14}) \rightarrow GF(2)$ is a non-linear boolean function in form of

$$F(S_i, S_{i+11}) = WG(S_{i+11} \oplus \beta.S_i) \oplus WG(S_{i+11}) \oplus WG(S_i) \tag{9}$$

Now, we focus on $F(s_0^i, s_1^i, ..., s_6^i, s_0^{i+11}, s_1^{i+11}, ..., s_6^{i+11})$ that is an unbalanced boolean function where

$$Pr(F(s_0^i, s_1^i, ..., s_6^i, s_0^{i+11}, s_1^{i+11}, ..., s_6^{i+11}) = 0) = \frac{1}{2} - 2^{-7.145} \tag{10}$$

The relation given by Equation (9) defines a distinguisher that is able to tell apart the output of the stream cipher from a truly random cipher with the probability expressed by Equation (10). The interesting question is: are there better biases to mount a distinguishing attack? We will discuss the possible answers in the next section.

Better biases In earlier sections we found a linear approximation leading us to a distinguishing attack. It is interesting whether it is possible to find a better linear approximation of output bits so that the bias is closer to the maximal value of 0.5. We explore the following way: Repeated squaring of the characteristic polynomial of the LFSR (Eq. 1) will compute linear recurrence polynomial. Particularly, by exponentiation with 2^7, we have:

$$x^{23 \cdot 2^7} + x^{11 \cdot 2^7} + \beta^{2^7} \tag{11}$$

Since $\beta = \beta^{2^7}$, $\beta \in \mathbb{F}_{2^7}$, the summation of Equations 1 and 11 gives:

$$x^{23 \cdot 2^7} + x^{11 \cdot 2^7} + x^{23} + x^{11} = 0 \tag{12}$$

$$\xRightarrow{divided\ by\ x^{11}} x^{23 \cdot 2^7 - 11} + x^{11 \cdot 2^7 - 11} + x^{12} + 1 = 0 \tag{13}$$

It means that the attacker can derive a bitwise linear equation that is valid for internal state of LFSR. Similar to the previous subsection, function F can be build as follows:

$$\begin{aligned} & z_{i+23 \cdot 2^7 - 11} \oplus z_{i+11 \cdot 2^7 - 11} \oplus z_{i+12} \oplus z_i \\ &= WG(S_{i+23 \cdot 2^7 - 11}) \oplus WG(S_{i+11 \cdot 2^7 - 11}) \oplus WG(S_{i+12}) \oplus WG(S_i) \\ &= WG(S_{i+11 \cdot 2^7 - 11} \oplus S_{i+12} \oplus S_i) \oplus WG(S_{i+11 \cdot 2^7 - 11}) \oplus WG(S_{i+12}) \oplus WG(S_i) \end{aligned} \tag{14}$$

Equation 14 can be considered as a boolean function with 21 input variables (instead of 28 variables) and a single bit output. Let $F : GF(2^{21}) \rightarrow GF(2)$ is an unbalanced boolean function, where

$$Pr(F(S_{i+11 \cdot 2^7 - 11}, S_{i+12}, S_i) = 0) = \frac{1}{2} + 2^{-6.78} \tag{15}$$

The required data Now, we explain the amount of required output sequences to distinguish between keystream generated by WG-7 Stream Cipher and a truly random binary source. The following theorem determines the required samples to detect two distributions which occur with probability $\frac{1}{2}$ (for a random sequence) and $\frac{1}{2}.(1+\epsilon)$ [11].

Theorem 1. *When event E occurs, $O(\frac{1}{\epsilon^2})$ samples are needed to distinguish a binary random sequence which occurs with probability $\frac{1}{2}$ from the distribution of an event which occurs with probability $\frac{1}{2}.(1+\epsilon)$ with a non-negligible success probability.*

In this case, the amount of data required for proposed distinguishing attack is $2^{13.56}$ bits. This amount of data can be collected from consecutive (or non-consecutive) keystream and even from one session key or different session keys in various times.

The result of the implemented distinguishing attack on WG-7 Stream Cipher are shown in Table 1. We have repeated the experiment 1000 times to compute the success rate of distinguishing attack with different length of output sequences.

Table 1. Experimental results for appliying distinguishing attack on WG-7 Stream Cipher

	Used Data (bits)	The success rate
1	2^9	%68
2	$2^{9.8}$	%75
3	$2^{10.3}$	%85
4	$2^{11.5}$	%90
5	$2^{13.5}$	%99.99

3.2 Key Recovery Attack on WG-7

In this section, we apply an algebraic analysis to recover the initial state of the cipher. Note that this attack is as effective as finding the secret key. The proposed attacks can recover internal states of WG-7 and then attacker is able to clock the LFSR backward and find the secret key properly. The designers of WG-7 Stream Cipher has claimed that there is no algebraic attack with complexity lesser than exhaustive search and data complexity 2^{24} consecutive keystream bits. The idea of our attack is as follows. Let $L : GF(2^{161}) \to GF(2^{161})$ be a multivariate linear transformation that corresponds to the linear transformation defined by a single clock. This transformation is done on the whole state of 23 registers each holding 7 bits ($23 \cdot 7 = 161$).

Let z_t, $t = 0, 1, 2, ...$ be the keystream generated by the cipher after running the state initialization algorithm of WG-7. Assume also that f is the non-linear function WG illustrated in Figure 1. We consider f as a non-linear map defined from $GF(2^7) \to GF(2)$. As the output bit is calculated on the contents of the last register or bits from 154 to 160, we denote this by

$$f(T(s_0, ..., s_{160})),$$

where $T(s_0, ..., s_{160})$ extracts the 7-bit content of the last register. So, we can establish the following system of relations for the cipher:

$$\begin{cases} z_0 = f(T(s_0, ..., s_{160})) \\ z_1 = f(T(L(s_0, ..., s_{160}))) \\ ... \\ z_t = f(T(L^t(s_0, ..., s_{160}))) \end{cases} \tag{16}$$

where $f(T(L^t(s_0, ..., s_{160})))$ indicates the output keystream at the clock t, generated by the stream cipher. Now, the cryptanalytic problem turns into solving non-linear systems investigated in [1, 3, 4, 6, 7].

Algebraic attack on WG-7 The simplest scenario to solve System (16) is known as the linearization technique [[5], [7]]. The function f is of degree 5. The number N of monomials of degree smaller or equal to 5 is

$$N = \sum_{i=1}^{5} \binom{161}{i} \approx \binom{161}{5} = 2^{29.65}.$$

Each of these monomials can be considered as a new variable and then attacker can solve the non-linear system with $\approx 2^{29.65}$ equations and time complexity $\approx 2^{29.65 \times log_2^7}$ by the Gaussian elimination method. Consequently, the complexity of attack is larger than the exhaustive key search. Another scenario is

The important idea to improve the efficiency of the above attack is to reduce the degree of the equations. To do this end, attacker tries to find an annihilator function so that $f \cdot g = 0$ and $\deg g < \deg f$. The steps to apply the attack can be described as follows:

1. Finding an annihilator g of f or $f \oplus 1$ with a low degree d.
2. Given multivariate equations of a low degree d on the initial state bits, there are $N = \sum_{i=1}^{d} \binom{n}{i}$ monomials of degree no bigger than d, where n is the length of internal state. Hence by the linearization method, time complexity to solve the non-linear system is $N^{log_2^7}$. Memory complexity of the attack is about N.

The Algebraic Normal Form of f is as follows:

$$\begin{aligned}
&f(x_1,...,x_7) = x_1 + x_1x_3 + x_2x_3 + x_4 + x_1x_4 + x_2x_4 + \\
&x_1x_2x_4 + x_3x_4 + x_1x_3x_4 + x_1x_2x_3x_4 + x_1x_3x_5 + x_4x_5 + x_1x_2x_4x_5 + \\
&x_1x_2x_3x_4x_5 + x_6 + x_2x_6 + x_1x_2x_6 + x_1x_2x_3x_6 + x_1x_2x_4x_6 + x_1x_2x_3x_4x_6 + \\
&x_1x_5x_6 + x_3x_5x_6 + x_1x_4x_5x_6 + x_3x_4x_5x_6 + x_7 + x_2x_7 + x_1x_2x_7 + x_2x_3x_7 + \\
&x_1x_4x_7 + x_1x_2x_4x_7 + x_1x_2x_3x_4x_7 + x_5x_7 + x_1x_5x_7 + x_1x_3x_5x_7 + x_1x_2x_3x_5x_7 + \\
&x_2x_4x_5x_7 + x_2x_3x_4x_5x_7 + x_6x_7 + x_1x_2x_6x_7 + x_1x_3x_6x_7 + x_1x_2x_3x_6x_7 + \\
&x_2x_4x_6x_7 + x_1x_3x_4x_6x_7 + x_2x_3x_4x_6x_7 + x_5x_6x_7 + x_2x_5x_6x_7 + x_1x_2x_5x_6x_7 + \\
&x_2x_3x_5x_6x_7 + x_1x_4x_5x_6x_7 + x_3x_4x_5x_6x_7.
\end{aligned}$$

The best annihilator to reduce degree of f is of the form: $g(x_1,...,x_7) = 1 + x_1 + x_3 + x_1x_2x_3 + x_4 + x_1x_4 + x_2x_4 + x_1x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4 + x_1x_3x_5 + x_4x_5 + x_1x_4x_5 + x_3x_4x_5 + x_6 + x_1x_6 + x_2x_6 + x_1x_2x_6 + x_3x_6 + x_2x_3x_6 + x_7 + x_3x_7 + x_1x_3x_7 + x_2x_3x_7 + x_4x_7 + x_2x_4x_7 + x_3x_4x_7 + x_3x_5x_7 + x_4x_5x_7 + x_6x_7 + x_1x_6x_7 + x_2x_6x_7 + x_3x_6x_7$. It means that the attacker can reduce the degree of the relations to 3 and solve them with time complexity $\approx \binom{161}{3}^{log_2^7} = 2^{54.36}$ and memory complexity $\binom{161}{3} = 2^{19.38}$. It is obvious that the designers of WG-7 Stream Cipher have ignored this attack, which breaks the cipher with mempry complexity lesser than 2^{24}.

Improved Attack on WG-7 Fast algebraic attacks [[7] , [3],[9]] on LFSR-stream ciphers are based on equations of type $z.X^e + X^d$ with $e < d$. This is a shorthand to describe that at least one equation of type

$$z.g(s_0,...,s_{n-1}) + h(s_0,...,s_{n-1}) = 0 \tag{17}$$

exists, where g and h are some multivariate polynomials of degree e and d ($e < d$) respectively, and $z = f(s_0,...,s_{n-1})$. The attack can be summarized as follows:

$$\sum_{i=t}^{t+D} \alpha_{t+i}.z_i.g(T(L^i(s_0,...,s_{160}))) \tag{18}$$

for some linear combination $(\alpha_0,...,\alpha_{D1}) \in GF(2)^D$ where $D = \sum_{i=1}^{d} \binom{n}{i}$. The same equation applies to each window of D consecutive steps and we will write it E times, for E overlapping intervals, with

$E = \sum_{i=1}^{e} \binom{n}{i}$. This is because we need to get the final system of degree e that is solvable by linearisation (with complexity $E^{log_2^7}$). In [, ,], the method to compute α has been described. Briefly, the steps to apply the attack are summarized as follows:

1. Relation step: One searches g and h with small degrees such that $f.g = h$. Worst complexity: solving a linear system with $D + E$ equations, let $O((D + E)^{log_2^7})$. In general one considers $e < d$.
2. Pre-computation step: Computation of linear relations to eliminate the terms of degrees greater than e in the equations. Needs $2.D$ bits of stream with complexity $O(Dlog^2(D))$.
3. Substitution step: One eliminates the monomials of degree greater than e. Complexity is $O(E^2D)$ [2] but by DFT [9] can be reduced to $O(E.D.log(D))$.
4. Solving step: One solves the system with E linear equations in $O(E^{log_2^7})$.

One can consider g and h in equation 17 in the following and apply a systematic fast algebraic attack as mentioned before.

$g(x_1, ..., x_7) = 1 + x_1 + x_3 + x_7$

$h(x_1, ..., x_7) = x_1x_2x_3 + x_4 + x_1x_4 + x_2x_4 + x_1x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4 + x_1x_3x_5 + x_4x_5 + x_1x_4x_5 + x_3x_4x_5 + x_6 + x_1x_6 + x_2x_6 + x_1x_2x_6 + x_3x_6 + x_2x_3x_6 + x_3x_7 + x_1x_3x_7 + x_2x_3x_7 + x_4x_7 + x_2x_4x_7 + x_3x_4x_7 + x_3x_5x_7 + x_4x_5x_7 + x_6x_7 + x_1x_6x_7 + x_2x_6x_7 + x_3x_6x_7$

The data complexity to apply fast algebraic attack on WG-7 is $\binom{161}{d} = \binom{161}{3}$ and time complexity is approximately $\binom{161}{e}^{log_2^7} = \binom{161}{1}^{log_2^7}$. The Table 2 is summarized the results of proposed attacks.

Table 2. Comparison between the different ideas to apply key recovery attack on WG-7 Stream Cipher

	Attack type	n	d	e	Time Complexity	Date Complexity	Memory	Pre-Computation
1	Trivial attack	161	5	-	$2^{83.02}$	$2^{29.65}$	-	-
2	Algebraic attack	161	3	-	$2^{54.36}$	$2^{19.38}$	-	-
3	Fast Algebraic attack	161	1	3	$2^{26.73}$	$2^{19.38}$	$2^{14.66}$	$2^{26.87}$

3.3 Conclusions

In this paper, the security of WG-7 Stream Cipher was investigated. It was shown that distinguishing attack can detect output of the cipher with having about $2^{13.5}$ keystream bits and high success probability. In addition, a key recovery attack on this cipher was proposed that can recover secret key with time complexity about $O(2^{27})$ and data complexity $2^{19.38}$. The presented results proved that WG-7 Stream Cipher has been completely broken and it is not recommended to use in RFID tags as a secure module.

References

1. F. Armknecht. Improving fast algebraic attacks. In *FSE*, pages 65–82, 2004.
2. F. Armknecht and G. Ars. Introducing a new variant of fast algebraic attacks and minimizing their successive data complexity. In *Mycrypt*, pages 16–32, 2005.
3. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - EUROCRYPT 2003,Warsaw, Poland, 2003, Proceedings*, pages 345–359. Springer, 2003.
4. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *ASIACRYPT*, pages 267–287, 2002.
5. N. T. Courtois. Higher order correlation attacks, xl algorithm and cryptanalysis of toyocrypt. In *ICISC 2002*, pages 182–199. Springer-Verlag, 2002.

6. N. T. Courtois. Algebraic attacks on combiners with memory and several outputs. In *Proc. of ICISC04*, pages 3–20, 2004.
7. N. T. Courtois and W. Meier. Fast algebraic attacks on stream ciphers with linear feedback. In *Crypto 2003, LNCS 2729*, pages 177–194. Springer.
8. G. Gong and A. M. Youssef. Cryptographic properties of the welch-gong transformation sequence generators. *IEEE Transactions on Information Theory*, 48(11):2837–2846, 2002.
9. P. Hawkes and G. G. Rose. Rewriting variables: The complexity of fast algebraic attacks on stream ciphers. In *CRYPTO*, pages 390–406, 2004.
10. Y. Luo, Q. Chai, G. Gong, and X. Lai. A lightweight stream cipher wg-7 for rfid encryption and authentication. In *GLOBECOM*, pages 1–6, 2010.
11. I. Mantin, , and A. Shamir. A practical attack on broadcast rc4. In *Proc. of FSE01*, pages 152–164. Springer-Verlag, 2001.
12. Y. Nawaz and G. Gong. Wg: A family of stream ciphers with designed randomness properties. *Inf. Sci.*, 178(7):1903–1916, 2008.