Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 23 No. 2-2018
ISSN:1813-1786 (Print) 2313-7770 (Online)

Classified Structures and Comparisons of Cryptanalysis of Wg-7, Wg-8 and Wg-16 Stream Ciphers

A. H. Majid[1], M. Anwar[2], M. W. Ashraf[3]

[1]*Computer Science Department, University of Lahore, Lahore, Pakistan*
[2]*Faculty of Computing, Universiti Teknologi Malaysia, Malaysia*
[3]*Computer Engineering Department, Bahauddin Zakariya University, Multan, Pakistan*
[2]anwer.mirza@gmail.com

Abstract-The family of WG stream cipher is good for the security of resource constrained devices, they have good randomness properties. These ciphers applied efficiently on Microcontrollers, RFID tags and Sensor nodes. Structures of these ciphers are simple and easy to implement. Security of these ciphers against Time/Memory/Data tradeoff attack, algebraic attack, correlation attack, differential attack, distinguishing attack, cube attack and discrete fourier transform attack. Implementation on 4-bit microcontroller ATAM893D, 8-bit microcontroller ATmega128L from Atmel and 16-bit microcontroller MSP430 from Texas instruments offering a good security on these devices. Comparison with the other stream ciphers, series of lightweight WG stream ciphers WG-7, WG-8 and WG-16 better secured for lightweight embedded applications regarding their utilization of energy and the performance.

Keywords-Welch Gong (WG), embedded applications

I. INTRODUCTION

Securing a data and information against the significant risks is an important topic around the world. To achieve the reliable security level of transmission data is the concerned of every owner of the data. Strong security level of the data produces reliable clients for the use of e-banking, business, e-commerce and even in very field of computer science and information technology.

Cryptography deals with problems which are concerned with authenticity, secrecy and integrity. It works like protocols; protocol contains sets of sequence of actions, which are connected to two or more communication channels. Cryptographic algorithm protocols are used to prevent the theft attempts and attack[I].

There are two types of cryptographic algorithm available for ciphering the data. Private Key cryptographic algorithm can be used either in stream cipher or block ciphers. Stream ciphers used memory for the ciphering of data on the other hand block ciphers works with no memory and permute the N bit data to produce the ciphered data like N bits. Stream ciphers are serially generated data with internal states by bitwise XORed data for ciphering. Stream ciphers never suffer due to error propagation but it could happen in Block ciphers. Performance speed of Stream ciphers are comparatively much better than block ciphers and have greater software efficiency[ii]. Here it is the general diagram for the stream cipher in Fig. 1.

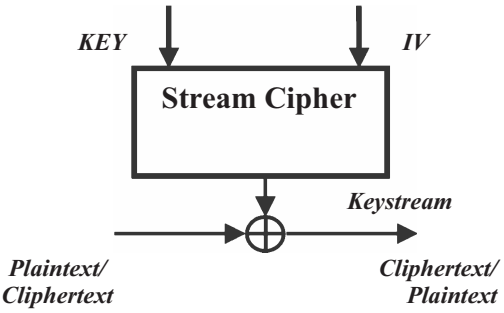

Fig. 1, The Cipher Process

The family of WG stream cipher is reliable for the security because of their randomness property. In this paper we discuss ancestors of WG stream cipher family like WG-7, WG-8 and WG-16. Ubiquitous computing is one of the promising technologies these days. The implementation of WG-7 lightweight stream cipher on Radio Frequency Identification (RFID) and its hardware implementation on 4-bit microcontroller ATAM893D and 8-bit microcontroller ATmega8 from Atmel will be explained. Couple of techniques applied low power usage microcontrollers with WG-8 stream cipher, by applying these modus operandi with 8-bit microcontroller ATmega128L from Atmel and a 16 bit microcontroller MSP430 from Texas instruments[iii]. The experimental results achieved on these microntrollers are 185.5Kbits/s and 95.9Kbit/s throughput and the consumption of power is 458nJ/bit and 125nJ/bit, respectively. When WG-8 is compared with the other existing stream ciphers, throughput is

much more than other stream ciphers which is 2~15times approximately and the energy consumption is much more less than 2~220 times approximately related to other preceding ciphers [iv]. WG-16 implementation provides better security level to RFID devices, Resource Constrained Devices and 4G-LTE networks. This secures the IEEE 802.11 wireless networks, pay TV and Bluetooth. In the implementation phase hardware core of pipelined WG-16 on FPGA achieves the throughput of 124MHz at the cost of 478 slices and ASIC achieves throughput of 552MHz at the cost of 12031 GEs in 65nm. Most recent proposed stream cipher is WG stream cipher, which have high randomness properties and multiplicative auto correlation. This cipher is much resistant for the categories of attacks on stream ciphers (Time/Memory/Data tradeoff, correlation attack, algebraic attack etc). This cipher has variation key lengths of 80, 96, 112 and 128 bit and length of the IV's is 32 or 64 bits [xvii].

Paper is organized as, in section 2, structures of the WG-7, WG-8 and WG-16 has been discussed with their initialization and running phases. In section 3, comparison of the cryptanalysis of the discussed stream ciphers. In section 4, conclusion of all the discussed stream cipher is given.

II. Methodology of WG-7, WG-8 and WG-16 Stream ciphers

WG-7

For WG-7 [v] designed model shown in Fig. 2. The length is 23-words long of the LFSR; every word is 7-bit long. A word (7 Boolean variable) is sieve function of WG non linearity. The primitive polynomial $g(x) = x^7 + x + 1$ over GF(2) produced by F_2^7 and finite field F_2^7 for creation of each word.

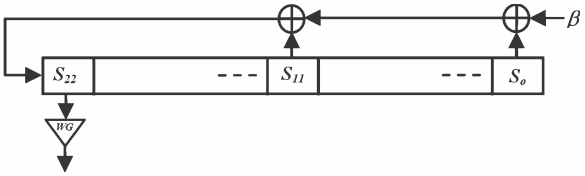

Fig. 2. Processing Phase WG-7

LFSR having characteristic polynomial is primitive over F_2^7 is as:

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

Root of the function f(x) is β. The function WG(x) non-linear sieve showing in Fig and WG transformation is as $F_2^7 \mapsto F_2$ and conversion of transformation from 7 bits to 1 bit is given below.

$$WG7(x) = f(x) = Tr(x^3 + x^9 + x^{21} + x^{57} + x^{87}) \text{ x} \in F_2^7$$

Drawback of WG-7 cipher is it is vulnerable by distinguishing attack. It does not provide security to the optimum level. Less number of tap positions of the LFSR of WG-7, an attacker generates the distinguisher to generate the accurate random key for the characteristics polynomial. Due to the recovery of the key by this type of attack, WG-7 is prohibited for the use of security [iii].

The distinguisher of the WG-8 cipher can construct by the LFSR (8-taps) and characteristics polynomial as given below.

$$F(S_i,.....,S_{i+4}, S_{i+7},....,S_{i+9}) = \text{WGT-8}(\omega \otimes S_i \oplus S_{i+1} \oplus S_{i+2} \oplus S_{i+3} \oplus S_{i+4} \oplus S_{i+7} \oplus S_{i+8} \oplus S_{i+9}) \oplus \text{WGT-8}(S_i) \oplus \text{WGT-8}(S_{i+1}) \oplus \text{WGT-8}(S_{i+2}) \oplus \text{WGT-8}(S_{i+3}) \oplus \text{WGT-8}(S_{i+4}) \oplus \text{WGT-8}(S_{i+7}) \oplus \text{WGT-8}(S_{i+8}) \oplus \text{WGT-8}(S_{i+9}),$$

Probability of the created distinguisher is

$$\Pr(F(x) = 0) = \frac{1}{2} \pm \varepsilon$$

where $x = (a_0,.....a_7)$, $a_i \in F_2^8$ and consist 64 variables Boolean function. Due to enormous number of variables during the distinguishing attack the value of is ε is rather. It is difficult to find the correct value of ε, probable values may be 2^{64} as $\varepsilon = (\Pr(WGT - 8(x^{19}) = f(x)) - 0.5)$[2]. This concluded that WG-8 is much secured than WG-8 in opposition to distinguishing attack. WG-16 works in similar fashion for the recovery of key stream against distinguishing attack [vi].

WG-8

WG-8 [ii] known as lightweight cipher, it contains secret key and initial vector 80 bits each which provide high randomness of the key to get ciphered key stream, this observed on non-linear sieve creator over fixed field F_2^8. This cipher consist structural, mathematical and functional parts. In structural part, LFSR is 20-bit long. In mathematical part it has feedback polynomial and some decimation factor which is d=19 and in functional part it also contains two phases; one is initialization and other is running.

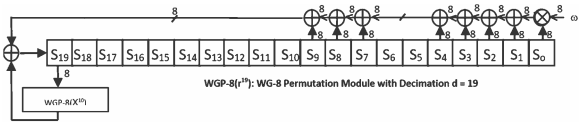

Fig. 3. Initialization Phase of WG-8

Initialization Phase

Functional phase applied by mathematical techniques to produce the 8-bit stream cipher, the initialization part of the cipher discussed below and shown in Fig. 3.

In this phase secret key $K=(K_{79},.....K_0)_2$, and initial vector $IV = (IV_{79},....IV_0)_2$ mixed with the 80 bits each and the LFSR is 20-bits tuple which is $S_0,....S_{19} \in F_2^8$ and $S_i = (S_{i,7},....S_{i,0})_2$ for i= 0, 1, 2, ... 19. The process of developing secret key and initial vector (IV) is as:

$S_{2i} = (K_{8i+3}, K_{8i+2}\ldots,K_{8i}, IV_{8i+3}, IV_{8i+2}\ldots, IV_{8i})_2$ and $S_{2i+1} = (K_{8i+7}, K_{8i+6}\ldots,K_{8i+4}, IV_{8i+7}, IV_{8i+6}\ldots,IV_{8i+4})_2$ for i=0,1,2….9.

In the beginning key and initial vectors loaded simultaneously apparatus of the cipher runs for 40 clock cycles. On the execution of each clock cycle, the internal states of the LFSR S_{19} At the period of every clock cycle, the 8 bits internal situation S_{19} best on permutation of non-linear WG-8, decimation=19 and the output of the feedback is updated due to internal states of the LFSR [vii]. The formulation of recursive relation is shown below.

$$S_{k+20} = (\omega \otimes S_k) \oplus S_{k+1} \oplus S_{k+2} \oplus S_{k+3} \oplus S_{k+4} \oplus S_{k+7} \oplus S_{k+8} \oplus S_{k+9} \oplus WGP\text{-}8(S_{k+19}^{19}), \quad 0 \le k < 40$$

At the completion of every clock cycle the key and initial vector produces the 1 bit key stream of WG-8.

Running Phase

In this phase, running mechanism of WG-8 stream cipher is shown in Fig-4. At the running phase, the 8 bits internal situation S_{19} best on permutation of non-linear WG-8, decimation=19 (WGT-8(x^{19}) and the output of the feedback is updated due to internal states of the LFSR [vii] produces the 1 bit key stream. Recursive relation of the running phase is shown in Fig. 4.

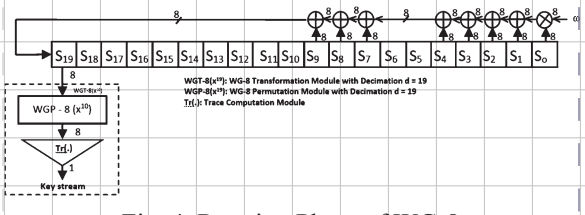

Fig. 4. Running Phase of WG-8

At the running phase WG-8 consists of two sub module; transformation module and permutation module. Transformation module placed at the end after permutation module WGP-8(x^{19}). Transformation module performs trace computation Tr(.). In a permutation module, permutation has done by Welch Gong technique WGP-8(x^{19}) on the 8 bits. After the completion of permutation, trace computation module produces 1 bit key stream.

The length of LFSR for WG-8 is 20-bits stages, shorter length of the LFSR causes the low randomness even having the key and initial vector be the same. Decimation factor exhibits the role to randomize the data, the decimation factor used for to gain the maximum probability of randomize data is d=19. This cipher is used for embedded devices and microcontrollers. The recursive relation performed iteratively and given below:

$$S_{k+20} = (\omega \otimes S_k) \oplus S_{k+1} \oplus S_{k+2} \oplus S_{k+3} \oplus S_{k+4} \oplus S_{k+7} \oplus S_{k+8} \oplus S_{k+9} \oplus WGP\text{-}8(S_{k+19}^{19}), \quad 0 \le k < 40$$

Key stream runs periodically and 2^{160}-1 has length. By increasing the length of LFSR which causes much randomness and mixing of data to create secure keystream, Welch Gong introduces WG-16 technique and the length of the LFSR is 32-bits stages [8] which provide much better randomness property of the key then WG-8. When compared the WG-16 with WG-8, WG-16 has key and initial vector each are 128-bits and decimation factor=1057. Both of decimation factors and the mixing of key and initial vectors are the greater length than previous ciphers. Even its implementation on embedded devices and microcontrollers are excellent. It creates much security for 4G-LTE networks and also for other communication devices. Structural discussion about WG-16[iv] is given below.

WG-16

WG-16[iv] in Fig. 5, known as lightweight stream cipher, it contains secret key and initial vector 128 bits each which provide high randomness of the key to get ciphered key stream, this observed on non-linear sieve creator over fixed field F_2^{16}. This cipher consist structural, mathematical and functional parts. In structural part, LFSR is 32-bit long. In mathematical part it has feedback polynomial and some decimation factor which is d=1057 and in functional part it also contains two phases; one is initialization and other is running[iv].

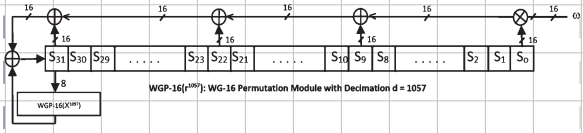

Fig. 5, Initialization Phase of WG-16

Initialization Phase

Functional phase applied by mathematical techniques to produce the 8-bit stream cipher, the initialization part of the cipher discussed below and shown in Fig. 6.

Suppose the 128-bits secret key $K=(K_{127},\ldots..K_0)_2$, the 128 bit initial vector $IV = (IV_{127},\ldots..IV_0)_2$ and the length of LFSR is 32 bits stage and is equivalent to $S_0,\ldots..,S_{31} \in F_2^{16}$ and $S_i = (S_{i,15},\ldots..,S_{i,0})_2$ for i= 0,1,2,….31. The conduction of key and IV initialization process are as:

$$S_i = \begin{cases} (K_{8i+7}, K_{8i+6}\ldots., K_{8i}, IV_{8i+7}, IV_{8i+6}\ldots., IV_{8i})_2 & for\ i = 0,1,2\ldots15 \\ S_{i-16} & for\ i = 16,17,\ldots,31 \end{cases}$$

In the beginning key and initial vectors loaded simultaneously apparatus of the cipher runs for 64 clock cycles. On the execution of each clock cycle, the internal states of the LFSR S_{31} At the period of every clock cycle, the 16 bits internal situation S_{31} best on permutation of non-linear WG-16, decimation=1057 and the output of the feedback is updated due to internal states of the LFSR. [iv]. At the completion of every

clock cycle the key and initial vector produces the secured 1 bit key stream of WG-16.

Running Phase

In this phase, running mechanism of WG-16 stream cipher is shown in Fig-6. At the running phase, the 16 bits internal situation S_{32} best on permutation of non-linear WG-16, decimation=1057 (WGT-16(x^{1057}) and the output of the feedback is updated due to internal states of the LFSR [iv] produces the 1 bit key stream. Recursive relation of the running phase is shown in Fig. 6.

$$S_{k+32} = (\omega^{11} \otimes S_{k+9}) \oplus S_{k+22} \oplus S_{k+31}, \quad k \geq 64$$

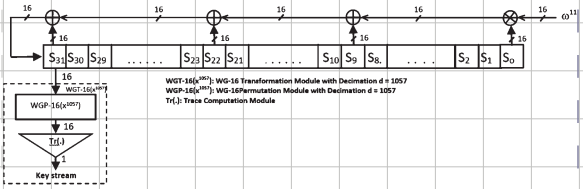

Fig. 6. Running Phase of WG-16

At the running phase WG-16 consists of two sub module; transformation module and permutation module. Transformation module placed at the end after permutation module WGP-16(x^{1057}). Transformation module performs trace computation Tr(.). In a permutation module, permutation has done by Welch Gong technique WGP-16(x^{1057}) on the 16 bits. After the completion of permutation, trace computation module produces 1 bit key stream.

III. Results and Discussions

This section presents the analysis of results and discussion of WG-7, WG-8 and WG-32 against different type of security attacks in the network. The results also presents the comparison of WG-7, WG-8 and WG-32 cyphers in terms of their complexity.

A. Time/Memory/Data Tradeoff Attack

This attack is the one of the most generalized type of attack in stream ciphers. This type of attack is most effective with low sampling resistance.

A tradeoff $TM^2D^2 = N^2$ for $D^2 \leq T \leq N$, was offered in [ix], where

- **T** is the time required for attack
- **M** is the memory required to store data tables
- **D** represents the real time data or key stream required
- **N** is the size of the search space

Search space of the stream cipher is increased to maximize the security level which can achieved by randomization of secret key and increasing the length of LFSR. To keep the keystream much stronger the secret key and the length of the initial vector (IV) should be the same [xvii-xix].

Complexity of the attack is measured in TMD by $O(2^{n/2})$, n represents the number of internal states. Expected complexities and the length of internal states of WG's stream ciphers are given below in Table I.

TABLE I
Time/Memory/Data Complexities

	WG-7	WG-8	WG-16
Internal States	161	160	512
Expected Complexity	$O(2^{80})$	$O(2^{80})$	$O(2^{256})$

Sampling resistance of WG-8 in transformation phase is WGT-8(x^{19}) for the filtering function and in WG-16 the sampling resistance is also WGT-16(x^{1057}) for the filtering functions. Cipher is secure against TMD with these high sampling resistances.

B. Algebraic Attack

Algebraic attack presented by Courtois and Meier [x] this attack is based on filtering sequence generator on the LFSR, the aim of this attack is multiply the low degree multivariate polynomial with the non-linear equation. The development of many key streams produces an over defined system of non-linear equations, this has been done by convalescing the internal states of LFSR.

TABLE II
Linear Function of the LFSR's

	WG-7	WG-8	WG-16
Algebraic Immunity	4	4	8
Time Complexity	$2^{66.1}$	$2^{66.0037}$	$2^{155.764}$
Data Complexity	$2^{24.7}$	$2^{24.65}$	$2^{56.22}$
Multivariate Polynomial (e=1)	6	7	15

Algebraic immunity of the WG-7 and WG-8 is 4, but the WG-8 is better than WG-7 due to their decimation factors. The decimation factor for WG-8 is (d=19) at transformation phase of the data. When compared the WG-8 and WG-16, algebraic immunity for WG-8 is 4 and for WG-16 is 8 so the algebraic immunity of WG-16 is much better than WG-8 and when comparing their decimation factor WG-8 (d=19) and WG-16 (d=1057). This gives huge difference with their data immunity and decimation factor. When applying the algebraic attack, attacker required to search of two multivariate polynomials i.e g and h with the degrees of e and d (e<d), so that f.g=h and e=1 of these stream ciphers. Multivariate polynomial h of WG-7 in h is 6 which is not greater than 7, multivariate polynomial h of WG-8 is not greater than 8 which is 7 and also for WG-16 the multivariate polynomial h is 15 which is not greater than 16. WG-7 has time complexity of $2^{66.1}$ for algebraic attack. WG-8 is $2^{66.0037}$ and WG-16 is $2^{155.764}$ when compared with their data complexity for

recovering the key stream; WG-7 is $2^{24.7}$, WG-8 is $2^{24.6}$ and WG-16 is $2^{56.622}$. Even if the attacker get many of bit key streams and Initial Vector (IV) also the attacker cannot extracts the required results by given constrained of time complexities. So this is secure for algebraic attacks.

C. Correlation Attack

In correlation attack, the attacker finds the relation between key stream and output sequence of LFSR. The key stream is called the earsplitting output of LFSR [xi]. WG stream ciphers are secures the key stream for fast correlation attack due 2-level auto correlation property. In the fast correlation attack, to derive a matrix code linear approximation is used, on convalescing the internal states of the LFSR decoding Maximum Likelihood Decoding (MLD) algorithm has been performed for computation.

TABLE III
LINEAR FUNCTION OF THE LFSR'S

	Linear Function
WG-7	$\Pr[WG7(x)=f(x)]=\frac{2^7-N_{WG7}}{2^7}=0.59375$
WG-8	$\Pr[WGT8(x^{19})=f(x)]=\frac{2^8-N_{WG8}}{2^8}=0.578125$
WG-16	$\Pr[WG716(x^{1057})=f(x)]=\frac{2^{16}-N_{WG16}}{2^{16}}=0.509277$

In Table III, the linear functions of WG-7, WG-8 and WG-16 are with variable length of these LFSR are 7, 8 and 16, respectively. Comparison of the stream ciphers linear functions WG-16 which is 0.509277 and has less value than WG-7 and WG-8. Decimation factors are used with variable length for mixing the values at transformation phase.

TABLE IV
KEY STREAM FOR SUCCESSFUL ATTACK

	Key stream for successful attack
WG-7	$N\approx 1/4(k.12.\ln 2)^{\frac{1}{3}}.\varepsilon^{-2}.2^{\frac{161-k}{3}}$
WG-8	$N\approx (k.12.\ln 2)^{\frac{1}{3}}.\varepsilon^{-2}.2^{\frac{160-k}{3}}$
WG-16	$N\approx (k.12.\ln 2)^{\frac{1}{3}}.\varepsilon^{-2}.2^{\frac{160-k}{3}}$

Key streams generated by these ciphers are different with the calculation for the successful key attacks in Table IV.

TABLE V
DECODING COMPLEXITIES OF THE FUNCTIONS

	Decoding Complexity	ε
WG-7	$C_{dec}=2^k.k.\frac{2\ln 2}{(2\varepsilon)^6}$	0.09375
WG-8		0.078125
WG-16		0.009277

For the comparison of the decoding complexities with these ciphers are calculated by ε for the calculation of amount bit required to the recovery of internal state of bits recovered. Table V helps to support for the calculation of decoding complexities of attack with the given WG stream ciphers.

TABLE VI
COMPLEXITIES OF THE ATTACK

	Number of bits state recovered	Bits required to mount the attack	Decoding complexity of the attack
WG-7	K=3	2^{58}	2^{89}
	K=80	2^{33}	
WG-8	K=7	$2^{60.31}$	$2^{102.68}$
	K=80	$2^{37.15}$	
WG-16	K=7	$2^{66.46}$	$2^{121.31}$
	K=80	$2^{43.3}$	

By given result in table 6, the decoding complexities are going stronger and stronger by enhancing the level of WG stream cipher. As show in Table V, compare the decoding complexities, WG-16 is much secure and provide much stronger security even in exhaustive search. By the comparison of different evaluated tables of the fast correlation attack WG-16 stream cipher gives stronger security against fast correlation attacks.

D. Differential Attack

WG stream cipher is weaker at initialization phase and vulnerable by selected IV attack [xii], an attacker generates the distinguisher to generate the desired output bits by the differential cryptanalysis. This problem is coped by placing permutation module at the end of the LFSR which randomized the serially generated data.

TABLE VII
DIFFERENTIAL ATTACKS COMPARISON

WGP	WG-7	WG-8	WG-16
	WGP-7(x^4)	WGP-8(x^{19})	WGP-16(x^{1057})
LFSR affected after (clock cycles)	34 bits	40 bits	64 bits

Cryptanalysis of the differential attack on LFSR affected after 34 bits, 40 bits and 64 bits is secure against the distinguishing attack. WG-7 not provides enough security on differential attack due to their simple structure. When attacker applied differential attack, WG-8 and WG-16 are much secure rather than WG-7 against this type of attack.

E. Cube Attack

In generally the key recovery attack is applicable

to any cryptosystem. In Cube attack [xiii]; attacker can gain information of the targeted cryptosystem by representing a low degree disintegration of multivariate polynomial in Algebraic Normal Form (ANF) of private and public variables[vi].

Due to low degree of the multivariate polynomial the success possibility of attack in WG-7 increased. After execution of 46 clock cycles the degree grows quickly, which does not provide enough support to break the security against cube attack. WG-8 stream cipher has algebraic degree 7. The ANF representation of 8 components function is 133, 113, 146, 124, 137, 109, 122 and 120 terms, in ANF second component just contains 7 linear terms and other terms have degree greater than or equal to 2. As it completes 40 rounds the degree of the output polynomial increases at the initialization phase. So the vulnerability is difficult for collecting the low degree polynomials[xi]. In WG-16 stream cipher, as it completes 64 rounds in the initialization phase, polynomial degree goes to increasing. This creates much trouble for the attacker in WG-16 to accumulate the low degree polynomial. These ciphers are much secure against the cube attack [xiv].

F. Distinguishing Attack

In the category attacks, distinguishing attack for WG-7[v] proposed recently. On the less number of taps on the LFSR, this cipher is much unsecure due to shorter characteristics polynomial. It is easy for the attacker to make the distinguisher and produce the required stream for the hacking of data. WG-7[vi] is not much secure by distinguishing attack. Less number of tap positions of the LFSR of WG-7, an attacker generates the distinguisher to generate the accurate random key for the characteristics polynomial. Due to the recovery of the key by this type of attack, WG-7 is prohibited for the use of security[xii-xv].

The distinguisher of WG-8 cipher can constructed as LFSR with 8 tap positions and by the characteristics polynomial

$$F(S_i,.....,S_{i+4}, S_{i+7},.....,S_{i+9}) = \text{WGT-8}(\omega \otimes S_i \oplus S_{i+1} \oplus S_{i+2} \oplus S_{i+3} \oplus S_{i+4} \oplus S_{i+7} \oplus S_{i+8} \oplus S_{i+9}) \oplus \text{WGT-8}(S_i) \oplus \text{WGT-8}(S_{i+1}) \oplus \text{WGT-8}(S_{i+2}) \oplus \text{WGT-8}(S_{i+3}) \oplus \text{WGT-8}(S_{i+4}) \oplus \text{WGT-8}(S_{i+7}) \oplus \text{WGT-8}(S_{i+8}) \oplus \text{WGT-8}(S_{i+9}),$$

Probability of the created distinguisher is

$$\Pr(F(x)=0) = \frac{1}{2} \pm \varepsilon$$

where x = $(a_0,.....a_7)$, $a_i \in F_2^8$ and consist 64 variables Boolean function. Due to enormous number of variables during the distinguishing attack the value of is ε is rather. It is difficult to find the correct value of ε, probable values may be 2^{64}as
$\varepsilon = (\Pr(WGT-8(x^{19}) = f(x)) - 0.5)$. This concluded that WG-8 is much secured than WG-8 in opposition to distinguishing attack. WG-16 works in similar fashion for the recovery of key stream against distinguishing attack[v]

G. Discrete Fourier Transform Attack

This is a new type of attack, filtering generator is used to recover the internal state of the filtering function, Ronjom and Helleseth [xvi] proposed first time this type of attack. In this attack, the attacker uses the D keystream bit of filtering generator to recover the internal state of the filtering function. The online and offline complexities are calculated $O(D(\log_2 D)^3)$ [vi] where D is online or offline linear complexity. Computation complexities Table is given below.

TABLE VIII
LINEAR FUNCTION OF THE LFSR'S

	WG-7	WG-8	WG-16
Attacker needs to recover the key stream (bits)	$2^{25.5}$	$2^{33.32}$	$2^{79.046}$
Online complexity	$O(2^{25.5})$	$O(2^{33.32})$	$O(2^{79.049})$
Offline complexity	$O(2^{39.5})$	$O(2^{48.89})$	$O(2^{97.96})$

Discrete Fourier Transform attack is secure against these consecutive key stream bits $2^{25.5}$, $2^{33.32}$ and $2^{79.046}$ for WG-7, WG-8 and WG-16, respectively.

IV. CONCLUSION

By the comparison of these different mechanisms of WG security algorithm every algorithm has its own pros and cons. Short apparatus is used in the family of WG stream cipher. Structure is so simple and implemented efficiently by Welch Gong (WG) technique by their two phases, pre-computation phase and running phase. Cryptanalysis of these stream ciphers provides clarity with category of attacks Time/Memory/Data Tradeoff attack, Algebraic attack, Correlation attack, Distinguishing attack, Discrete Fourier Transform attack, Differential attack and Cube attack with their comparison of attacks. Analysis of all these structures, WG-7 is bit weak for different classes of attacks (i.e. Distinguishing attack, Algebraic attack) and even the structure goes weaker on exhaustive search on discrete fourier transformation attack. WG-8 and WG-16 are much secure for active devices and implemented efficiently on microcontrollers and wireless sensors. Security mechanisms of these ciphers are stronger enough for 8 bit and 16 bit devices. The enhanced structure of these structures is WG stream cipher, which provides high class of randomness of key, stronger security mechanism.

REFERENCES

[i] A. . Fallis, "No Title No Title," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[ii] X. Fan, K. Mandal, and G. Gong, "WG-8 : A Lightweight Stream Cipher for Resource-Constrained Smart Devices."

[iii] L. Ding *et al.*, "Cryptanalysis of WG Family of Stream Ciphers," *Comput. J.*, vol. 58, no. 10, pp. 2677–2685, 2015.

[iv] X. Fan and G. Gong, "Specification of the Stream Cipher WG-16 Based Confidentiality and Integrity Algorithms."

[v] M. A. Orumiehchiha, J. Pieprzyk, and R. Steinfeld, "Cryptanalysis of WG-7 : A Lightweight Stream Cipher."

[vi] S. Rønjom, S. Polynomials, C. Codes, and A. Attacks, "Powers of Subfield Polynomials , Cyclic Codes and Algebraic Attacks with Applications to the WG Stream Ciphers Sondre Rønjom To cite this version :," 2016.

[vii] K. Mandal, G. Gong, X. Fan, and M. Aagaard, "Optimal parameters for the WG stream cipher family," *Cryptogr. Commun.*, vol. 6, no. 2, pp. 117–135, 2014.

[viii] L. Ding, C. Jin, J. Guan, and Q. Wang, "Cryptanalysis of lightweight WG-8 stream cipher," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 4, pp. 645–652, 2014.

[ix] Y. Nawaz and G. Gong, "The WG Stream Cipher," pp. 1–23.

[x] N. T. Courtois and W. Meier, "Algebraic Attacks on Stream Ciphers with Linear Feedback," pp. 9–11, 2003.

[xi] N. T. Courtois, "Higher Order Correlation Attacks , XL Algorithm and Cryptanalysis of Toyocrypt," pp. 36–38.

[xii] H. Wu and B. Preneel, "Chosen IV Attack on Stream Cipher WG," pp. 1–7.

[xiii] I. Dinur and A. Shamir, "Cube Attacks on Tweakable Black Box Polynomials," vol. 2.

[xiv] Kamesh and N. Sakthi Priya, "Security enhancement of authenticated RFID generation," *Int. J. Appl. Eng. Res.*, vol. 9, no. 22, pp. 5968–5974, 2014.

[xv] P. Abina, K. Dhivyakala, L. Suganya, and S. M. Praveena, "Biometric Authentication System for Body Area Network," *Int. J. Adv. Res. Electr.*, vol. 3, no. 3, pp. 7954–7964, 2014.

[xvi] A. Canteaut and Y. Rotella, "Attacks against Filter Generators Exploiting Monomial Mappings," no. April, 2016.

[xvii] 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, Nov. 2002.

[xviii] J. Hong, and P. Sarkar, Rediscovery of Time Memory Tradeoffs, Cryptology ePrint Archive, Report 2005/090, http://eprint.iacr.org/, 2005.

[xix] C. Canniere, J. Lano, and B. Preneel, Comments on the Rediscovery of Time Memory Data Tradeoffs, https://www.cosic.esat.kuleuven.ac.be/ecrypt/stream/TMD.pdf.