An Improved Attack on WG Stream Cipher

Arash Mirzaei†, Mohammad Dakhilalian† and Mahmoud Modarres-Hashemi†

†Cryptography and System Security Research Laboratory
Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran

Summary
WG is a synchronous stream cipher submitted to the hardware profile of eSTREAM project. The main feature of this stream cipher is the use of WG transformation. WG uses keys and initial vectors (IVs) of the same lengths 80, 96, 112 and 128 bits. Moreover, IVs of the length 32 and 64 bits are admitted. The most important key recovery attack on WG was presented by Wu and Preneel and uses the weakness of the initialization step of the algorithm. The attack is a chosen IV one which its success probability for WG with 80 bit (or more) and 64 bit IVs is close to 1 and 2^{-5}, respectively. The attack cannot be performed on WG with IVs of the length 32 bits. In this paper Wu and Preneel's attack is improved in such a way that the success probability increases nearly to 1 for IVs of length 64 and 32 bits.

Key words:
WG Stream Cipher, Key Recovery,Chosen IV

1. Introduction

WG is a hardware oriented stream cipher submitted to the eSTREAM project by Nawaz and Gong [1] but was not accepted for the final phase of this competition [2]. The main feature of the WG stream cipher is the use of WG transformation and up to now no attack has been introduced on this part of the cipher. WG uses 11 stage LFSR with primitive polynomial over $F_{2^{29}}$ and its output is filtered by a nonlinear WG transformation $F_{2^{29}} \to F_2$ to produce the keystream.

WG supports a number of key and IV sizes. The keys of length 80, 96, 112 and 128 bits and IVs of the same size as the key and also 64 bits and 32 bits can be used to initialize the algorithm. The key and IV are simply loaded into the LFSR and then the keystream generator is run for 22 clock cycles. During this phase without producing any keystream, 29 bits from the middle of the WG transformation are XORed to the feedback of the LFSR.

Wu and Preneel in [3,4] presented a key recovery attack on WG using chosen IVs with specified differences and weak propagation of these differences during 22 clocks in the initialization step. The attack is practical for WG with IVs of the same length as the key (80 bits or more) with probability close to 1 but this probability is reduced nearly to 2^{-5} and 0 for IVs of the length 64 and 32 bits, respectively.

In this paper, by using some other patterns of difference, Wu and Preneel's attack is going to be improved in such a way that the key recovery attack on WG with IVs of length 64 and 32 bits would be practical with probability close to 1. The presented attacks in this paper are chosen IV ones, like Wu and Preneel's attack.

The rest of the paper is organized as follows. In Section 2 the WG stream cipher is described briefly. Wu and Preneel's attack is explained in Section 3 and then in Section 4 the limitations of this attack are discussed as well as the way of breaking up these limitations. In Sections 5 and 6 by using the presented solution in Section 4, Wu and Preneel's attack is improved and shown that the attack can be performed on WG with IVs of the length 32 and 64 bits, respectively. Section 7 presents a summary of the paper.

2. Description of the WG Stream Cipher

The keystream generator of WG is shown in Fig 1. WG has a regularly clocked LFSR which consists of eleven, 29-bit registers and its feedback polynomial over $GF(2^{29})$ is as follows:

$$p(x) = x^{11} + x^{10} + x^9 + x^6 + x^3 + x + \gamma$$

where $\gamma = \beta^{464730077}$ and β is the primitive root of g(x)

$$g(x) = x^{29} + x^{28} + x^{24} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^6 + x^4 + x + 1$$

Then the first word of the LFSR (S(11)) is filtered by a nonlinear WG transformation $GF(2^{29}) \to GF(2)$ to produce the keystream.

To initialize WG, the key and IV are loaded into the LFSR, then LFSR is clocked 22 times. During each of these 22 clocks, 29 bits from the middle of the WG transformation are XORed to the feedback of the LFSR, without producing any keystream. $WG'(S(11))$ denotes this 29-bit extracted from the WG transformation. So the feedback word in the initialization step is as follows:

$$T = S(1) \oplus S(2) \oplus S(5) \oplus S(8) \oplus S(10) \oplus WG'(S(11))$$

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

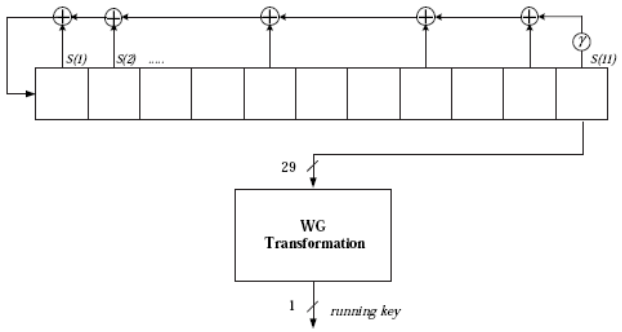

Fig 1. Keystream Generator of WG

Now the way of loading the key and IV into the LFSR is being described. When IV size is 32 or 64 bits, 80-bit key is loaded as:

$S_{1,\ldots,16}(1)=k_{1,\ldots,16}$ $S_{1,\ldots,16}(2)=k_{17,\ldots,32}$ $S_{1,\ldots,16}(3)=k_{33,\ldots,48}$
$S_{1,\ldots,16}(4)=k_{49,\ldots,64}$ $S_{1,\ldots,16}(5)=k_{65,\ldots,80}$ $S_{1,\ldots,16}(9)=k_{1,\ldots,16}$
$S_{1,\ldots,16}(10)=k_{17,\ldots,32}\oplus 1$ $S_{1,\ldots,16}(11)=k_{33,\ldots,48}$

and 96-bit key is loaded as:

$S_{1,\ldots,16}(1)=k_{1,\ldots,16}$ $S_{1,\ldots,16}(2)=k_{17,\ldots,32}$ $S_{1,\ldots,16}(3)=k_{33,\ldots,48}$
$S_{1,\ldots,16}(4)=k_{49,\ldots,64}$ $S_{1,\ldots,16}(5)=k_{65,\ldots,80}$ $S_{1,\ldots,16}(6)=k_{81,\ldots,96}$
$S_{1,\ldots,16}(9)=k_{1,\ldots,16}$ $S_{1,\ldots,16}(10)=k_{17,\ldots,32}\oplus 1$ $S_{1,\ldots,16}(11)=k_{33,\ldots,48}$

and 112-bit key is loaded as:

$S_{1,\ldots,16}(1)=k_{1,\ldots,16}$ $S_{1,\ldots,16}(2)=k_{17,\ldots,32}$ $S_{1,\ldots,16}(3)=k_{33,\ldots,48}$
$S_{1,\ldots,16}(4)=k_{49,\ldots,64}$ $S_{1,\ldots,16}(5)=k_{65,\ldots,80}$ $S_{1,\ldots,16}(6)=k_{81,\ldots,96}$
$S_{1,\ldots,16}(7)=k_{97,\ldots,112}$ $S_{1,\ldots,16}(9)=k_{1,\ldots,16}$ $S_{1,\ldots,16}(10)=k_{17,\ldots,32}\oplus 1$
$S_{1,\ldots,16}(11)=k_{33,\ldots,48}$

and finally 128-bit key is loaded as:

$S_{1,\ldots,16}(1)=k_{1,\ldots,16}$ $S_{1,\ldots,16}(2)=k_{17,\ldots,32}$ $S_{1,\ldots,16}(3)=k_{33,\ldots,48}$
$S_{1,\ldots,16}(4)=k_{49,\ldots,64}$ $S_{1,\ldots,16}(5)=k_{65,\ldots,80}$ $S_{1,\ldots,16}(6)=k_{81,\ldots,96}$
$S_{1,\ldots,16}(7)=k_{97,\ldots,112}$ $S_{1,\ldots,16}(8)=k_{113,\ldots,128}$ $S_{1,\ldots,16}(9)=k_{1,\ldots,16}$
$S_{1,\ldots,16}(10)=k_{17,\ldots,32}\oplus 1$ $S_{1,\ldots,16}(11)=k_{33,\ldots,48}$

Then IV bits are divided into blocks of 8 bits and each block is loaded into the LFSR. 32-bit IV is loaded as:

$S_{17,\ldots,24}(1)=IV_{1,\ldots,8}$ $S_{17,\ldots,24}(2)=IV_{9,\ldots,16}$ $S_{17,\ldots,24}(3)=IV_{17,\ldots,24}$
$S_{17,\ldots,24}(4)=IV_{25,\ldots,32}$

and 64-bit IV is loaded as:

$S_{17,\ldots,24}(1)=IV_{1,\ldots,8}$ $S_{17,\ldots,24}(2)=IV_{9,\ldots,16}$ $S_{17,\ldots,24}(3)=IV_{17,\ldots,24}$
$S_{17,\ldots,24}(4)=IV_{25,\ldots,32}$ $S_{17,\ldots,24}(5)=IV_{33,\ldots,40}$ $S_{17,\ldots,24}(6)=IV_{41,\ldots,48}$
$S_{17,\ldots,24}(7)=IV_{49,\ldots,56}$ $S_{17,\ldots,24}(8)=IV_{57,\ldots,64}$

When both the key and IV are 80 bits, completion of the LFSR is as follows:

$S_{1,\ldots,16}(1)=k_{1,\ldots,16}$ $S_{17,\ldots,24}(1)=IV_{1,\ldots,8}$ $S_{1,\ldots,8}(2)=k_{17,\ldots,24}$
$S_{9,\ldots,24}(2)=IV_{9,\ldots,24}$ $S_{1,\ldots,16}(3)=k_{25,\ldots,40}$ $S_{17,\ldots,24}(3)=IV_{25,\ldots,32}$
$S_{1,\ldots,8}(4)=k_{41,\ldots,48}$ $S_{9,\ldots,24}(4)=IV_{33,\ldots,48}$ $S_{1,\ldots,16}(5)=k_{49,\ldots,64}$
$S_{17,\ldots,24}(5)=IV_{49,\ldots,56}$ $S_{1,\ldots,8}(6)=k_{65,\ldots,72}$ $S_{9,\ldots,24}(6)=IV_{57,\ldots,72}$
$S_{1,\ldots,8}(7)=k_{73,\ldots,80}$ $S_{17,\ldots,24}(7)=IV_{73,\ldots,80}$

All of the remaining bits of the LFSR are set to zero. Loading the key and IV of the same lengths 96, 112 and 128 bits are not mentioned here.

3. Wu and Preneel's attack on WG[3,4]

Wu and Preneel's attack on WG with 80-bit key and 80-bit IV is as follows. For each key K, two IVs, IV′ and IV″ are chosen which are identical at 8 bytes but are different at two bytes : $IV'_{17,\ldots,24}\neq IV''_{17,\ldots,24}$ and $IV'_{49,\ldots,56}\neq IV''_{49,\ldots,56}$. The differences satisfy

$IV'_{17,\ldots,24}\oplus IV''_{17,\ldots,24}=IV'_{49,\ldots,56}\oplus IV''_{49,\ldots,56}$

$IV'_{17,\ldots,24}\oplus IV''_{17,\ldots,24}$ is denoted by Δ_1. S(i) $(1\le i\le 11)$ at the end of the j-th step of the initialization is denoted by $S^j(i)$ and after loading the key and IV is denoted by $S^0(i)$. The whole differential propagation is given in Table 1 where the differences at the i-th step indicate the differences at the end of the i-th step. In all the tables of this paper, $\Delta_{i,j}$ indicates $\Delta_i\oplus\Delta_j$. There are similar notations for functions with more than two variables, like $\Delta_{i,j,k}$.

Δ_2 and Δ_3 are as follows:

$$\Delta_2=(\gamma\times S'^0(11))\oplus WG'(S'^6(11))\oplus(\gamma\times S''^6(11))\oplus WG'(S''^6(11))=$$
$$=(\gamma\times S'^0(5))\oplus WG'(S'^0(5))\oplus(\gamma\times S''^0(5))\oplus WG'(S''^0(5))$$

and

$$\Delta_3=(\gamma\times S'^0(2))\oplus WG'(S'^0(2))\oplus(\gamma\times S''^0(2))\oplus WG'(S''^0(2))$$

So $\Delta_2\oplus\Delta_3$ is determined by:

$$\Delta_2\oplus\Delta_3=$$
$$(\gamma\times S'^0(5))\oplus WG'(S'^0(5))\oplus(\gamma\times S''^0(5))\oplus WG'(S''^0(5))\oplus \quad (1)$$
$$(\gamma\times S'^0(2))\oplus WG'(S'^0(2))\oplus(\gamma\times S''^0(2))\oplus WG'(S''^0(2))$$

The first keystream bit is resulted from $S^{22}(10)$. If $\Delta_2\oplus\Delta_3=0$, then the first keystream bits for IV' and IV'' should be the same. Assuming $\Delta_2\oplus\Delta_3$ is randomly distributed, we have $\Delta_2\oplus\Delta_3=0$ with probability 2^{-29}. Therefore, about 2^{29} pairs of (Δ_2,Δ_3) are required to obtain a pair satisfying $\Delta_2\oplus\Delta_3=0$. If there are 2^{29} pairs of (Δ_2,Δ_3), probability of finding a pair satisfying $\Delta_2\oplus\Delta_3=0$ will be $1-(1-2^{-29})^{2^{29}}\approx 0.63$. There are 3 bytes of IV loaded in S(2) and S(5) and one byte difference (Δ_1) can be chosen between two IVs, so there are $2^{24}\times\frac{255}{2}\approx 2^{31}$ pairs of IVs with mentioned difference and so 2^{31} pairs of (Δ_2,Δ_3). Having these pairs of

(Δ_2,Δ_3), the probability of finding a pair satisfying $\Delta_2 \oplus \Delta_3 = 0$ will be $1-(1-2^{-29})^{2^{31}} \approx 1$.

Then for recognizing the pair of (Δ_2,Δ_3) that satisfies $\Delta_2 \oplus \Delta_3 = 0$, the values of the first bytes of two IVs are modified so that $IV'_{1,\ldots,8} = IV''_{1,\ldots,8}$. This modification does not affect the value of $\Delta_2 \oplus \Delta_3$ but it affects the value of $S^{22}(10)$ and so the first keystream bits. Therefore, for each pair of (Δ_2,Δ_3), first the keystream bits are generated and compared, if these bits are different, it will be known that $\Delta_2 \oplus \Delta_3 \neq 0$ and a new pair of (Δ_2,Δ_3) should be generated. Otherwise, the first bytes of the two IVs are modified and the first keystream bits are compared again. If one pair of (Δ_2,Δ_3) passes the test for 40 times (40 modifications of the first bytes of IVs and equality of the first keystream bits resulted from them) then $\Delta_2 \oplus \Delta_3 = 0$ with probability of $1-2^{-40}$. Therefore with first output bits of about $2\times 2^{29}\times\sum_{i=1}^{40}\frac{i}{2^i} \approx 2^{31}$ chosen IVs, a pair (Δ_2,Δ_3) is found satisfying $\Delta_2 \oplus \Delta_3 = 0$ (if we assume that 2^{31} pairs of (Δ_2,Δ_3) are required in order to find a pair satisfying $\Delta_2 \oplus \Delta_3 = 0$, the number of required chosen IVs will be 2^{33}). The factor $\sum_{i=1}^{40}\frac{i}{2^i}$ is added to count the average number of modification of the first byte of IVs. Then according to equation (1) and $\Delta_2 \oplus \Delta_3 = 0$, 24 bits of the key $K_{17,\ldots,24}$ and $K_{49,\ldots,64}$ can be recovered.

In the similar way, using differences at $S^0(3)$ and $S^0(6)$ and observing the 2-th and 3-th of two keystreams (for finding a pair of (Δ_2,Δ_3) satisfying $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 = 0$) another 24 bits of the key $K_{25,\ldots,40}$ and $K_{65,\ldots,72}$ can be recovered[3,4].

The Wu and Preneel's attack on WG with 64-bit IVs is not as powerful as the 80-bit (or more) IV cases because by changing the loaded IV bits into S(2) and S(5) it is possible to generate just 2^{23} pairs of (Δ_2,Δ_3). Thus a pair satisfying $\Delta_2 \oplus \Delta_3 = 0$ or $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 = 0$ is obtained with probability of $1-(1-2^{-29})^{2^{23}}.(1-2^{-29})^{2^{23}} \approx 2^{-5}$. If we find the desired pair it might be possible to obtain 29-bit information about $K_{17,\ldots,32}$ and $K_{65,\ldots,80}$. The attack requires about $2^{25.1}$ chosen IVs.

The attack on WG with the 96, 112 and 128 bit key and the 64 bit IV are similar to the previous one and 2,3 and 4, 29-bit information can be obtained about the key, for each one, respectively. The probability of obtaining each 29 bit information is close to 2^{-5}.

Wu and Preneel claimed that their chosen IV attack cannot be performed on WG with 32 bit IVs [3,4].

Later, Nawaz and Gong increased the number of initialization steps from 22 to 44 to prevent the mentioned attack[5]. Applying this modification, Wu and Preneel's attack cannot be performed on WG, as well as our attacks presented in Sections 5 and 6.

4. Limitations of Wu and Preneel's Attack

As it was presented in Section 3, the Wu and Preneel's attack only uses the weak differential propagation of existing differences at $S^0(2)$ and $S^0(5)$ as well as $S^0(3)$ and $S^0(6)$ or $S^0(4)$ and $S^0(7)$ or $S^0(5)$ and $S^0(8)$. Therefore when in the loading step, key or IV bits are not loaded into each register of these pairs of registers, the corresponding attack will not be as efficient as the attack described in section 4 on WG with 80-bit (or more) IV which many bits of the key could be obtained with probability close to 1.

For instance for 80-bit key and 64-bit IV case, key bits are not loaded in S(6), S(7) and S(8) so the attacker can only use the corresponding attack of differences at $S^0(2)$ and $S^0(5)$ of two IVs. In this case just two bytes of IV are loaded into these registers. Therefore the number of possible pairs of (Δ_2,Δ_3) is about 2^{23} and 29 bit information is obtained about 32 bits of the key with too lower probability than 1. Using the pair of $S^0(3)$ and $S^0(6)$, 16 bits of the key can be recovered with too lower probability than 1. So the attack is not too powerful.

For WG with 80-bit key and 32-bit IV, all of the IV bits are loaded into S(1), S(2), S(3) and S(4), so it is inefficient to use every pair of the mentioned pairs, e.g. using the pair of $S^0(2)$ and $S^0(5)$ and with changing the loaded IV bits into $S^0(2)$, it is possible to generate $2^8\times\frac{255}{2} \approx 2^{15}$ pairs of (Δ_2,Δ_3) and 29-bit information is obtained about 32 bits of the key with probability of $(1-(1-2^{-29})^{2^{15}}\cdot(1-2^{-29})^{2^{15}}) \approx 0$.

To improve the Wu and Preneel's attack we try to find 3 register combinations which have weak difference propagation property. Finding these combinations, we are able to attack on WG with 64-bit IV with probability close to 1. If we find combinations of differences at $S^0(1)$, $S^0(2)$, $S^0(3)$ and $S^0(4)$ with desired differential propagation property then we may also attack on WG with 32 bit IVs.

5. Attack on WG with 32-bit IV

Two IVs are chosen which are identical at 3-th byte but have similar difference Δ_1 at 1-th, 2-th and 4-th bytes. Therefore after completion of registers with the key and IV, these 3 registers are different as follows:

$S'^0(1) \oplus S''^0(1) = S'^0(2) \oplus S''^0(2) = S'^0(4) \oplus S''^0(4)$

Table 2 gives the propagation of this difference during 22 clocks in the initialization step.

In the table, each '-' represents a value that depends on about all of the initial values of registers and because of that, non of them is used in the attack. It is obvious that if $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$, then the second output bits of two IVs should be equal. It is concluded that

$$\begin{aligned}\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = \Delta_1 &\oplus (\gamma \times S'^0(4)) \oplus WG'(S'^0(4)) \\ &\oplus (\gamma \times S''^0(4)) \oplus WG'(S''^0(4)) \\ &\oplus (\gamma \times S'^0(2)) \oplus WG'(S'^0(2)) \\ &\oplus (\gamma \times S''^0(2)) \oplus WG'(S''^0(2)) \\ &\oplus (\gamma \times S'^0(1)) \oplus WG'(S'^0(1)) \\ &\oplus (\gamma \times S''^0(1)) \oplus WG'(S''^0(1))\end{aligned}$$

The above relation represents that $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4$ depends on the initial values of S(1), S(2) and S(4) of two IVs. So changing corresponding bytes of two IVs we can change the value of $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4$ and about 2^{29} pairs of IVs with the above differences are required to find a pair that satisfies $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$. Changing 1-th, 2-th and 4-th bytes of IVs, we can generate around 2^{31} combinations of $(\Delta_1, \Delta_2, \Delta_3, \Delta_4)$ so there is no problem to find a pair with the relation of $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$. Like Wu and Preneel's attack, the 3-th bytes of two IVs are changed similarly 40 times in order to recognize the case $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$.

Therefore $2 \times 2^{29} \times \sum_{i=1}^{40} \frac{i}{2^i} \approx 2^{31}$ chosen IVs are needed and by using the first 2 bits of the keystream of these IVs we can obtain 29-bit information about 48 bits of key $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$ and the success probability of the attack is 0.63. As it was presented in Section 3, using 2^{33} chosen IVs the success probability reaches nearly to 1. To obtain more information about the key, we can use the first keystream bit of each IV. For a pair with the mentioned difference, if $\Delta_2 \oplus \Delta_3 = 0$ then the first keystream bits of these two IVs should be equal but just the initial value of S(2) and S(4) affect the value of $\Delta_2 \oplus \Delta_3$. Changing 2-th and 4-th bytes of two IVs, we can almost have $\frac{(2^8)^2 \times 255}{2} \approx 2^{23}$ pairs of IVs with desired differences.

So the probability of finding a pair satisfying $\Delta_2 \oplus \Delta_3 = 0$ is $1-(1-2^{-29})^{2^{23}} \approx 2^{-6}$. If this property is found for a pair, we can obtain 29-bit information about $K_{17,\ldots,32}$ and $K_{49,\ldots,64}$. Thus about $2^{32-29} = 8$ cases are founded for these 32 bits of the key. Then using these cases and putting them into the 29-bit information that is related to $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$, we can find all of the 48 bits $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$ because there are about 8 cases for $K_{17,\ldots,32}$ and $K_{49,\ldots,64}$ and 2^{16} values for $K_{1,\ldots,16}$ and we know that each wrong value for $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$ satisfies $\Delta_1 \oplus \Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$ with probability of 2^{-29} so totally about $8 \times 2^{16} \times 2^{-29} = 2^{-10}$ wrong keys is obtained. This value is less than 1 so finally just the correct value for $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$ is concluded. For finding a pair of IVs satisfying $\Delta_2 \oplus \Delta_3 = 0$, $2 \times 2^{23} \times \sum_{i=1}^{40} \frac{i}{2^i} \approx 2^{25}$ chosen IVs are required. Therefore the total number of chosen IVs, needed for performing the attack is $2^{33} + 2^{25}$ and with knowing the first 2 bits of these IVs 29-bit and 48-bit information is obtained about $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$ with the probability close to 1 and 2^{-6}, respectively.

6. Attacks on WG with 64-bit IV

The main problem of performing the Wu and Preneel's attack on WG with the 64-bit IV is that the number of pairs of IVs with chosen differences is low, so the attack will be successful with too lower probability than 1. In this section we try to find pairs of IVs which lead to differences of 3 registers in the loading step and these differences have desired propagation property during 22 clocks in the initialization step in order to give information about the key with probability close to 1.

Suppose that we want to obtain m-bit information about n bits of the key. In all attacks that will be discussed in this section we try to make m and n close together because in this way the complexity of finding the whole key is less. For instance suppose the key is 64 bit long and 29-bit information is available about 48 bits of the key, so we should check all of the 2^{48} values of these 48 bits of the key to find about $2^{48-29} = 2^{19}$ possible values for them. Then an exhaustive search is done on these 2^{19} values and all of the possible cases for remaining 16 bits of the key

which needs $2^{16} \times 2^{19} = 2^{35}$ searches. Therefore obtaining the whole key needs $2^{48} + 2^{35}$ searches.

Now suppose that we have 29 bit information about 32 bits of the key, so we should search all of the 2^{32} values for these 32 bits of the key to find about 2^3 possible values. Then for finding the key we should search on these 2^3 possible values and remaining 32 bits of the key which needs $2^{32} \times 2^3 = 2^{35}$ searches. Therefore, finding the whole key needs $2^{32} + 2^{35}$ searches which is less than the corresponding value in the previous case.

First the attack on WG with 64-bit IV and 80-bit or 96-bit key is presented. As discussed in Section 2, 8-bit blocks of IV are loaded in S(1) ,…, S(8). We can use two IVs which are different at 1-th, 2-th and 4-th bytes (as discussed in Section 5) and similar at the other bytes and obtain 29-bit information about 48 bits of the key $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$.

For concluding 29-bit information about 32 bits of the key and improving the attack we use this point that in the 80-bit or 96-bit key cases, S(7) and S(8) are completed just with IV bits and independent from the key bits. Thus if we find any pair of IVs with difference Δ_1 at 3 bytes and one of these 3 bytes is 7-th (8-th) byte, it will result in difference Δ_1 at $S^0(7)$ ($S^0(8)$) and 2 other registers from $S^0(1)$,…, $S^0(6)$ of two IVs denoted by $S^0(i)$ and $S^0(j)$. Finally if this pattern of difference has desired propagation property, 29-bit information will be concluded about 32 bits of the key loaded into $S^0(i)$ and $S^0(j)$.

Now, by using these results, we introduce our attacks. For each key K, two IVs, IV' and IV'' are chosen which are identical at 5 bytes but have the same difference of Δ_1 at the 1-th, 2-th and 7-th bytes. Table 3 gives the corresponding differential propagation during the 22 clocks in the initialization step.

It is clear that if $\Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$, then the second output bits of two IVs should be equal. The value of $\Delta_2 \oplus \Delta_3 \oplus \Delta_4$ depends on initial value of the 1-th, 2-th and 7-th registers and so the 1-th, 2-th and 7-th bytes of IVs. For recognizing the case $\Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$, we can change for example 3-th bytes of two IVs at most 40 times and compare the second output bits of two IVs. Therefore, as discussed in Sections 3 and 4 we need the first 2 output bits of 2^{33} chosen IVs and there is no problem to generate this number of chosen IVs. Thus the attack will be practical with the probability close to 1.

In a similar way we can use pairs of chosen IVs which have the same difference of Δ_1 in the 3-th, 5-th and 8-th bytes and are similar in other bytes. Table 4 gives the corresponding propagation during the first 22 clocks in the initialization step.

Table 4 represents that if $\Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$, then the first output bits of two IVs should be the same. Recognizing $\Delta_2 \oplus \Delta_3 \oplus \Delta_4 = 0$ we can obtain 29-bit information about 32 bits of the key $K_{33,\ldots,48}$ and $K_{65,\ldots,80}$.

Therefore, having the first 2 output bits of $2^{33} + 2^{33} = 2^{34}$ chosen IVs, 29-bit information about $K_{1,\ldots,32}$ and 29-bit information about $K_{33,\ldots,48}$ and $K_{65,\ldots,80}$ are obtained with probability close to 1.

When the key size is 112 bits, S(7) is completed with 16 bits of the key in the loading step. So we cannot perform the attack exactly the same as WG with 80-bit or 96-bit key. In this case we compare the first keystream bits of WG, loaded by two IVs which have the same difference at the 2-th, 3-th and 8-th bytes but are similar at the other bytes. Then we can obtain 29-bit information about 32 bits of the key $K_{17,\ldots,48}$. Thus about 2^3 values are concluded for these bits of the key. Table 5 gives the corresponding differential propagation.

Then using the second output bits of two IVs which have the same difference of Δ_1 at the 1-th, 2-th and 4-th bytes and are similar at the other bytes, 29-bit information is obtained about 48 bits of the key $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$. We know that 16 bits of these 48 bits $K_{17,\ldots,32}$ have about 2^3 possible values (from the first step of the attack). Thus determining the possible values of these 48 bits can be done by exhaustive search on these 2^3 possible values and 2^{32} possible values for $K_{1,\ldots,17}$ and $K_{49,\ldots,64}$. Therefore, about $2^{32} \times 2^3 / 2^{29} = 2^6$ values are concluded for 64 bits of the key $K_{1,\ldots,64}$.

Therefore to perform the attack we need the first 2 keystream bits of 2^{33} chosen IVs and also the first keystream bits of another 2^{33} chosen IVs. Determining the exact value of these 64 bits and remaining 32 bits of the key can be done by exhaustive search.

Consider the case that key size is 128 bits. In this case registers S(1) ,…, S(8) are completed with both the key bits and IV bits. Thus concluding 29-bit information about 32 bits of the key with success probability of close to 1 is impossible. Therefore in order to perform a fairly better attack, we obtain two 29 bit information about two 48 bits of the key which are common in some bits. Then we can use the possible cases of the first 48 bits of the key to obtain the possible cases of the second 48 bits of the key. Following attack shows this method better.

At first, consider two IVs which have the same difference at the 3-th, 5-th and 8-th bytes and are similar at the other bytes. Comparing the first keystream bits of these IVs we

can conclude 29-bit information about 48 bits of the key $K_{33,\ldots,48}$, $K_{65,\ldots,80}$ and $K_{113,\ldots,128}$. Thus about $2^{48-29}=2^{19}$ values are concluded for these bits of the key. Then in the second step of the attack, the first keystream bits of pairs of IVs which are different at the 2-th, 3-th and 8-th bytes but are similar at the other bytes are used in order to obtain 29-bit information about 48 bits of the key $K_{17,\ldots,48}$ and $K_{113,\ldots,128}$. 32 bits $K_{33,\ldots,48}$ and $K_{113,\ldots,128}$ are common in these two steps of the attack and we know that about 2^{19} values are possible for these 32 bits (from the first step of the attack). Searching on these 2^{19} values and 2^{16} possible values for 16 bits of the key $K_{17,\ldots,32}$ and having 29-bit information concluded in the second step of the attack we can find about $2^{16}\times 2^{19}/2^{29}=2^{6}$ possible values for 64 bits of the key $K_{17,\ldots,48}$, $K_{65,\ldots,80}$ and $K_{113,\ldots,128}$ (totally 58-bit information is available about 64 bits of the key so $2^{64-58}=2^{6}$ values are possible for these 64 bits).

Finally using the first 2 output bits of IVs which are different at the 1-th, 2-th and 4-th bytes but are similar at the other bytes, we can conclude 29-bit information about $K_{1,\ldots,32}$ and $K_{49,\ldots,64}$ which we found about 2^{6} possible values for 16 bits of these 48 bits $K_{17,\ldots,32}$. Thus searching on these 2^{6} values and 2^{32} values for $K_{1,\ldots,16}$ and $K_{49,\ldots,64}$ we obtain about $2^{6}\times 2^{32}/2^{29}=2^{9}$ possible values for 96 bits of the key $K_{1,\ldots,80}$ and $K_{113,\ldots,128}$ (totally 87-bit information is obtained about 96 bits of the key so about $2^{96}/2^{87}=2^{9}$ values are possible for these 96 bits of the key).

We can do an exhaustive search over these 2^{9} values and remaining 32 bits of the key to determine the whole key. Therefore, totally we need the first keystream bits of $2^{33}+2^{33}=2^{34}$ chosen IVs and also the first 2 keystream bits of another 2^{33} chosen IVs.

7. Conclusion

In this paper the previous attack on the WG stream cipher is improved. The previous attack can be performed on WG with 64 bit IVs with the probability close to 2^{-5} and is impractical for WG with 32 bit IVs. Improved attack can be performed on WG with 32 and 64 bit IVs with the probability close to 1. For WG with 64 bit IVs and 80, 96 or 112 bit keys 2^{34} chosen IVs are required in order to 58 bit information is obtained about the key with the probability close to 1. Also for 64 bit IVs and 128 bit keys using 3×2^{33} chosen IVs, 87 bit information is obtained about the key with the probability close to 1. For WG with 32 bit IVs using $2^{33}+2^{25}$ chosen IVs 29 bit and 48 bit information is concluded about 48 bits of the key with the probability close to 1 and 2^{-6}, respectively. For all the attacks, maximum the first 2 bits of the keystream of WG with chosen IVs are needed.

References

[1] Nawaz, Y., Gong, G. : The WG Stream Cipher". ECRYPT Stream Cipher Project Report 2005/033. Available at http://www.ecrypt.eu.org/stream/

[2] ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream/

[3] Wu, H., Preneel, B. : Resynchronization attacks on WG and LEX. In : Robshaw, M. (eds), Fast Software Encryption 2006. LNCS, vol. 4047, pp 422-432. Springer-Verlag (2006).

[4] Wu, H., Preneel, B. : Chosen IV Attack on Stream Cipher WG, ECRYPT Stream Cipher Project Report 2005/045. Available at http://www.ecrypt.eu.org/stream/

[5] Nawaz, Y., Gong, G. : Preventing Chosen IV Attack on WG Cipher by Increasing the Length of Key/IV Setup In: ECRYPT Stream Cipher Project Report 2005/047. Available at http://www.ecrypt.eu.org/stream/

Table 1. Propagation of Differen ces at Registers S(2) and S(5) of Two IVs During the First 22 Clocks in the Initialization Step

	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)	S(9)	S(10)	S(11)
0	0	Δ_1	0	0	Δ_1	0	0	0	0	0	0
1	0	0	Δ_1	0	0	Δ_1	0	0	0	0	0
2	0	0	0	Δ_1	0	0	Δ_1	0	0	0	0
3	0	0	0	0	Δ_1	0	0	Δ_1	0	0	0
4	0	0	0	0	0	Δ_1	0	0	Δ_1	0	0
5	0	0	0	0	0	0	Δ_1	0	0	Δ_1	0
6	Δ_1	0	0	0	0	0	0	Δ_1	0	0	Δ_1
7	Δ_2	Δ_1	0	0	0	0	0	0	Δ_1	0	0
8	$\Delta_{1,2}$	Δ_2	Δ_1	0	0	0	0	0	0	Δ_1	0
9	0	$\Delta_{1,2}$	Δ_2	Δ_1	0	0	0	0	0	0	Δ_1
10	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1	0	0	0	0	0	0
11	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1	0	0	0	0	0
12	$\Delta_{1,2}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1	0	0	0	0
13	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1	0	0	0
14	Δ_3	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1	0	0
15	$\Delta_{1,2,3}$	Δ_3	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1	0
16	$\Delta_{1,2,3}$	$\Delta_{1,2,3}$	Δ_3	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	Δ_2	Δ_1
22	$\Delta_{2,3,4,5,6,7,8}$	$\Delta_{4,5,7}$	$\Delta_{4,6}$	$\Delta_{1,2,3,5,6}$	$\Delta_{3,4,5}$	$\Delta_{1,4}$	$\Delta_{1,2,3}$	$\Delta_{1,2,3}$	Δ_3	$\Delta_{2,3}$	$\Delta_{1,2}$

Table 2. Propagation of Differences at Registers S(1), S(2) and S(4) of Two IVs During First 22 Clocks in the Initialization Step

	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)	S(9)	S(10)	S(11)
0	Δ_1	Δ_1	0	Δ_1	0	0	0	0	0	0	0
1	0	Δ_1	Δ_1	0	Δ_1	0	0	0	0	0	0
2	0	0	Δ_1	Δ_1	0	Δ_1	0	0	0	0	0
3	0	0	0	Δ_1	Δ_1	0	Δ_1	0	0	0	0
4	Δ_1	0	0	0	Δ_1	Δ_1	0	Δ_1	0	0	0
5	Δ_1	Δ_1	0	0	0	Δ_1	Δ_1	0	Δ_1	0	0
6	0	Δ_1	Δ_1	0	0	0	Δ_1	Δ_1	0	Δ_1	0
7	Δ_1	0	Δ_1	Δ_1	0	0	0	Δ_1	Δ_1	0	Δ_1
8	Δ_2	Δ_1	0	Δ_1	Δ_1	0	0	0	Δ_1	Δ_1	0
9	$\Delta_{1,2}$	Δ_2	Δ_1	0	Δ_1	Δ_1	0	0	0	Δ_1	Δ_1
10	$\Delta_{1,3}$	$\Delta_{1,2}$	Δ_2	Δ_1	0	Δ_1	Δ_1	0	0	0	Δ_1
11	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2}$	Δ_2	Δ_1	0	Δ_1	Δ_1	0	0	0
12	$\Delta_{1,2,4}$	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2}$	Δ_2	Δ_1	0	Δ_1	Δ_1	0	0
13	$\Delta_{2,3}$	$\Delta_{1,2,4}$	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2}$	Δ_2	Δ_1	0	Δ_1	Δ_1	0
14	$\Delta_{1,2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2,4}$	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2}$	Δ_2	Δ_1	0	Δ_1	Δ_1
22	-	-	-	-	-	-	-	-	$\Delta_{1,2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2,4}$

Table 3. Propagation of Difference at Registers S(1), S(2) and S(7) of Two IVs During the First 22 Clocks in the Initialization Step

	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)	S(9)	S(10)	S(11)
0	Δ_1	Δ_1	0	0	0	0	Δ_1	0	0	0	0
1	0	Δ_1	Δ_1	0	0	0	0	Δ_1	0	0	0
2	0	0	Δ_1	Δ_1	0	0	0	0	Δ_1	0	0
3	0	0	0	Δ_1	Δ_1	0	0	0	0	Δ_1	0
4	0	0	0	0	Δ_1	Δ_1	0	0	0	0	Δ_1
5	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0	0	0	0
6	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0	0	0
7	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0	0
8	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0
9	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1
10	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1
11	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0
12	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0
13	$\Delta_{1,2,3}$	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0
14	$\Delta_{2,3,4}$	$\Delta_{1,2,3}$	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0
15	$\Delta_{1,3,4}$	$\Delta_{2,3,4}$	$\Delta_{1,2,3}$	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$
22	-	-	-	-	-	-	-	$\Delta_{1,3,4}$	$\Delta_{2,3,4}$	$\Delta_{1,2,3}$	$\Delta_{1,4}$

Table 4. Propagation of Difference at Registers S(3), S(5) and S(8) of Two IVs During the First 22 Clocks in the Initialization Step

	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)	S(9)	S(10)	S(11)
0	0	0	Δ_1	0	Δ_1	0	0	Δ_1	0	0	0
1	0	0	0	Δ_1	0	Δ_1	0	0	Δ_1	0	0
2	0	0	0	0	Δ_1	0	Δ_1	0	0	Δ_1	0
3	0	0	0	0	0	Δ_1	0	Δ_1	0	0	Δ_1
4	$\Delta_{1,2}$	0	0	0	0	0	Δ_1	0	Δ_1	0	0
5	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	0	Δ_1	0	Δ_1	0
6	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	0	Δ_1	0	Δ_1
7	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	0	Δ_1	0
8	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	0	Δ_1
9	$\Delta_{2,4}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	0
10	$\Delta_{1,2,3,4}$	$\Delta_{2,4}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0
11	$\Delta_{1,3}$	$\Delta_{1,2,3,4}$	$\Delta_{2,4}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0
12	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2,3,4}$	$\Delta_{2,4}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0
13	$\Delta_{2,3,4}$	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2,3,4}$	$\Delta_{2,4}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$	0
14	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3,4}$	$\Delta_{1,3}$	$\Delta_{1,2,3,4}$	$\Delta_{2,4}$	$\Delta_{2,3}$	$\Delta_{1,2,3}$	0	$\Delta_{1,2}$	$\Delta_{1,2}$
22	-	-	-	-	-	-	-	-	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3,4}$

Table 5. Propagation of Difference at Registers S(2), S(3) and S(8) of Two IVs During the First 22 Clocks in the Initialization Step

	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)	S(9)	S(10)	S(11)
0	0	Δ_1	Δ_1	0	0	0	0	Δ_1	0	0	0
1	0	0	Δ_1	Δ_1	0	0	0	0	Δ_1	0	0
2	0	0	0	Δ_1	Δ_1	0	0	0	0	Δ_1	0
3	0	0	0	0	Δ_1	Δ_1	0	0	0	0	Δ_1
4	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0	0	0	0
5	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0	0	0
6	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0	0
7	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1	0
8	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1	Δ_1
9	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0	Δ_1
10	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0	0
11	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0	0
12	$\Delta_{1,2,3}$	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0	0
13	$\Delta_{2,3,4}$	$\Delta_{1,2,3}$	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$	0
14	$\Delta_{1,3,4}$	$\Delta_{2,3,4}$	$\Delta_{1,2,3}$	$\Delta_{1,4}$	$\Delta_{2,3,4}$	$\Delta_{2,3}$	$\Delta_{1,2}$	$\Delta_{1,2}$	Δ_1	$\Delta_{1,2}$	$\Delta_{1,2}$
22	-	-	-	-	-	-	-	-	$\Delta_{1,3,4}$	$\Delta_{2,3,4}$	$\Delta_{1,2,3}$

Arash Mirzaei received the B.Sc. and M.Sc. degrees in Control and Communication Engineering from Isfahan University of Technology (IUT), Isfahan, Iran, in 2007 and 2009, respectively. Since 2007, he was a member of Cryptography & System Security Research Group at IUT. His research interests include Cryptography and Data Security.

Mohammad Dakhilalian received the B.Sc. and Ph.D. degrees in Electrical Engineering from Isfahan University of Technology (IUT) in 1989 and 1998 respectively and M.Sc. degree in Electrical Engineering from Tarbiat Modarres University in 1993. He was an Assistant Professor of Faculty of Information & Communication Technology, Ministry of ICT, Tehran, Iran in 1999-2001. He joined IUT in 2001 and is an Assistant Professor in Electrical and Computer Engineering Department. His current research interests are Cryptography and Data Security.

Mahmoud Modarres-Hashemi Received his B.Sc. and M.Sc. degrees in electrical engineering in 1990 and 1992 from the Electrical and Computer Engineering department of Isfahan University of Technology (IUT), Isfahan, Iran. He pursued his studies at the department of Electrical Engineering of Sharif University of Technology, Tehran, Iran, where he received his PhD in 2000. Dr. Modarres-Hashemi was an assistant professor at the ECE department of IUT up to 2008 and he is currently an associate professor there. His research interests are Detection Theory, Radar Signal Processing, Electronic Warfare, Cryptography, and Channel Coding.