Chosen IV Attack on Stream Cipher WG

Hongjun Wu and Bart Preneel

Katholieke Universiteit Leuven, Dept. ESAT/COSIC
{wu.hongjun,bart.preneel}@esat.kuleuven.be

Abstract. Stream cipher WG [3] is a hardware oriented cipher. In this paper, we point out that the WG stream cipher is vulnerable to the chosen IV attacks. For WG with 80-bit key and 80-bit IV, 48 bits of the secret key could be recovered with about $2^{31.3}$ chosen IVs . For WG with 80-bit key and 64-bit IV, 29-bit information of the secret key could be recovered with probability 2^{-5} and with about $2^{25.1}$ chosen IVs. For each chosen IV, only the first four keystram bits are needed in the attack.

1 Stream Cipher WG [3]

WG is a hardware oriented stream cipher. The main feature of the WG stream cipher is the use of the WG transformation to generate keystream from the LFSR. The WG transformations have excellent cryptographic properties [2].

1.1 Keystream Generation

The keystream generation diagram of WG is given in Fig. 1. WG has a regularly clocked LFSR which is defined by the feedback polynomial

$$p(x) = x^{11} + x^{10} + x^{9} + x^{6} + x^{3} + x + \gamma \tag{1}$$

over $GF(2^{29})$, where $\gamma = \beta^{464730077}$ and β is the primitive root of $g(x)$

$$\begin{aligned} g(x) = x^{29} + x^{28} + x^{24} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + \\ x^{14} + x^{12} + x^{11} + x^{10} + x^{7} + x^{6} + x^{4} + x + 1 \end{aligned} \tag{2}$$

Then the non-linear WG transformation, $GF(2^{29}) \rightarrow GF(2)$, is applied to generate the keystream from the LFSR.

1.2 Key/IV setup

The key/IV setup of WG is given in Fig. 2. After the key and IV being loaded into LFSR, the LFSR is clocked 22 steps. During each of these 22 steps, 29 bits from the middle of the WG transformation are XORed to the feedback of LFSR, as shown in Fig. 2.

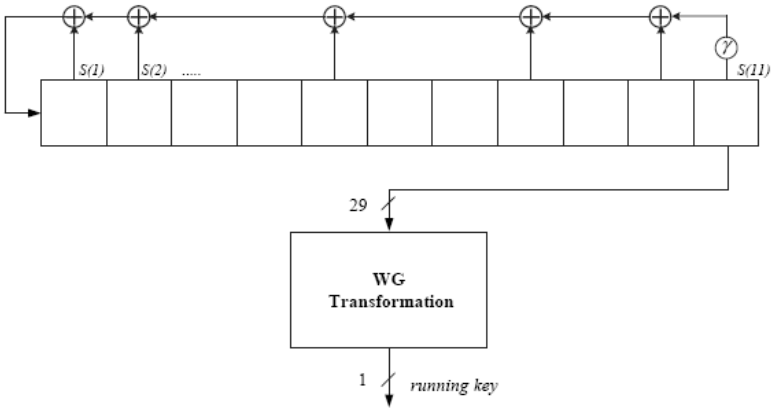

Fig. 1. Keystream Generation Diagram of WG [3]

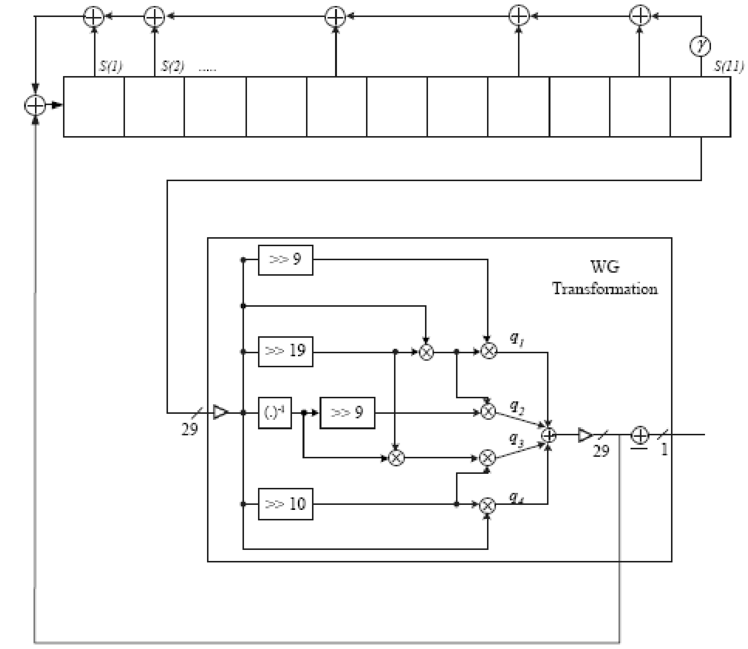

Fig. 2. Key/IV setup of WG [3]

We can express one step of the key/IV setup as follows.

$$T = S(1) \oplus S(2) \oplus S(5) \oplus S(8) \oplus S(10) \oplus (\gamma \times S(11)) \oplus WG'(S(11))$$
$$S(i) = S(i-1) \text{ for } i = 11 \cdots 2;\ S(1) = T$$

where the $WG'(S(11))$ denotes the 29 bits extracted from the WG transformation, as shown in Fig. 2.

The WG cipher supports a number of key and IV sizes. The key size can be 80 bits, 96 bits, 112 bits and 128 bits. The IV sizes can be 32 bits, 64 bits, 80 bits, 96 bits, 112 bits, and 128 bits.

2 Chosen IV Attack on Stream Cipher WG

The key/IV setup of WG could be broken with the chosen IV attack based on the differential cryptanalysis technique [1]. The WG with 32-bit IV size is not vulnerable to the attack given in this section. In Subsection 2.1 the attack is applied to break the WG with 80-bit key and 80-bit IV. The attacks on the WG with IV sizes larger than 80 bits are given in Subsection 2.2. The attack on the WG with 64-bit IV size is given in Subsection 2.3.

2.1 Attack on WG with 80-bit key and 80-bit IV

In this subsection, we will investigate the security of the key/IV setup of WG with 80-bit key and 80-bit IV. For this version of WG, denote the key as $K = k_1, k_2, k_3, \cdots, k_{80}$ and the IV as $IV = IV_1, IV_2, IV_3, \cdots, IV_{80}$. They are loaded into the LFSR as follows.

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

Then the LFSR is clocked 22 steps with the middle value from the WG transformation being used in the feedback.

The chosen IV attack on WG goes as follows. For each secret key K, we choose two IVs, IV' and IV'' so that IV' and IV'' are identical at 6 bytes, but are different at two bytes: $IV'_{17,\dots,24} \neq IV''_{17,\dots,24}$ and $IV'_{49,\dots,56} \neq IV''_{49,\dots,56}$. The differences satisfy $IV'_{17,\dots,24} \oplus IV''_{17,\dots,24} = IV'_{49,\dots,56} \oplus IV''_{49,\dots,56}$.

Denote the $S(i)$ $(1 \leq i \leq 11)$ at the end of the j-th step as $S^j(i)$, and denote loading the key/IV as the 0th step. After loading the key and the chosen IV into LFSR, we know that the difference at $S(2)$ and $S(5)$ are the same, i.e., $S'^0(2) \oplus S''^0(2) = S'^0(5) \oplus S''^0(5)$. We denote this difference as $\triangle_1$, i.e., $\triangle_1 = S'^0(2) \oplus S''^0(2) = S'^0(5) \oplus S''^0(5)$.

We now examine the differential propagation during the 22 steps in the key/IV setup. The complete differential propagation is shown in Table 1, where the differences at the i-th step indicate the differences at the end of the i-th step. The difference $\triangle_2 = (\gamma \times S'^6(11) \oplus WG'(S'^6(11)) \oplus (\gamma \times S''^6(11) \oplus WG'(S''^6(11)) =$

$(\gamma \times S'^0(5) \oplus WG'(S'^0(5)) \oplus (\gamma \times S''^0(5) \oplus WG'(S''^0(5))$. Similarly, we obtain that $\triangle_3 = (\gamma \times S'^0(2) \oplus WG'(S'^0(2)) \oplus (\gamma \times S''^0(2) \oplus WG'(S''^0(2))$.

Table 1. The differential propagation in the key/IV setup of WG

	S(1)	S(2)	S(3)	S(4)	S(5)	S(6)	S(7)	S(8)	S(9)	S(10)	S(11)
step 0	0	$\triangle_1$	0	0	$\triangle_1$	0	0	0	0	0	0
step 1	0	0	$\triangle_1$	0	0	$\triangle_1$	0	0	0	0	0
step 2	0	0	0	$\triangle_1$	0	0	$\triangle_1$	0	0	0	0
step 3	0	0	0	0	$\triangle_1$	0	0	$\triangle_1$	0	0	0
step 4	0	0	0	0	0	$\triangle_1$	0	0	$\triangle_1$	0	0
step 5	0	0	0	0	0	0	$\triangle_1$	0	0	$\triangle_1$	0
step 6	$\triangle_1$	0	0	0	0	0	0	$\triangle_1$	0	0	$\triangle_1$
step 7	$\triangle_2$	$\triangle_1$	0	0	0	0	0	0	$\triangle_1$	0	0
step 8	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0	0	0	0	0	$\triangle_1$	0
step 9	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0	0	0	0	0	$\triangle_1$
step 10	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0	0	0	0	0
step 11	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0	0	0	0
step 12	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0	0	0
step 13	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0	0
step 14	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0	0
step 15	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$	0
step 16	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$	$\triangle_1$
step 17	$\triangle_1\oplus\triangle_4$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$	$\triangle_2$
step 18	$\triangle_3\oplus\triangle_4\oplus\triangle_5$	$\triangle_1\oplus\triangle_4$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0	$\triangle_1\oplus\triangle_2$
step 19	$\triangle_1\oplus\triangle_2\oplus\triangle_3\oplus\triangle_5\oplus\triangle_6$	$\triangle_3\oplus\triangle_4\oplus\triangle_5$	$\triangle_1\oplus\triangle_4$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	0
step 20	$\triangle_4\oplus\triangle_6$	$\triangle_1\oplus\triangle_2\oplus\triangle_3\oplus\triangle_5\oplus\triangle_6$	$\triangle_3\oplus\triangle_4\oplus\triangle_5$	$\triangle_1\oplus\triangle_4$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$
step 21	$\triangle_4\oplus\triangle_5\oplus\triangle_7$	$\triangle_4\oplus\triangle_6$	$\triangle_1\oplus\triangle_2\oplus\triangle_3\oplus\triangle_5\oplus\triangle_6$	$\triangle_3\oplus\triangle_4\oplus\triangle_5$	$\triangle_1\oplus\triangle_4$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$	$\triangle_2\oplus\triangle_3$
step 22	$\triangle_2\oplus\triangle_3\oplus\triangle_4\oplus\triangle_5\oplus\triangle_6\oplus\triangle_7\oplus\triangle_8$	$\triangle_4\oplus\triangle_5\oplus\triangle_7$	$\triangle_4\oplus\triangle_6$	$\triangle_1\oplus\triangle_2\oplus\triangle_3\oplus\triangle_5\oplus\triangle_6$	$\triangle_3\oplus\triangle_4\oplus\triangle_5$	$\triangle_1\oplus\triangle_4$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2\oplus\triangle_3$	$\triangle_3$	$\triangle_2\oplus\triangle_3$	$\triangle_1\oplus\triangle_2$

From Table 1, we notice that at the end of the 22th step, the difference at $S^{22}(10)$ is $\triangle_2 \oplus \triangle_3$. From the above description of $\triangle_2$ and $\triangle_3$, we know that

$$\begin{aligned}\triangle_2 \oplus \triangle_3 = &((\gamma \times S'^0(5) \oplus WG'(S'^0(5)) \oplus (\gamma \times S''^0(5) \oplus WG'(S''^0(5))) \oplus \\ &((\gamma \times S'^0(2) \oplus WG'(S'^0(2)) \oplus (\gamma \times S''^0(2) \oplus WG'(S''^0(2))) \end{aligned} \quad (3)$$

It shows that the value of $\triangle_2 \oplus \triangle_3$ is determined by $k_{17,\ldots,24}$, $k_{49,\ldots,64}$, $IV'_{9,\ldots,24}$, $IV''_{49,\ldots,56}$, $IV''_{9,\ldots,24}$, $IV''_{49,\ldots,56}$.

From the keystream generation of WG, we notice that the first keystream bit is generated from $S^{22}(10)$ (after the key/IV setup, the LFSR is clocked, and the $S^{23}(11)$ is used to generate the first keystream bit). If $\triangle_2 \oplus \triangle_3 = 0$, then the first keystream bits for IV' and IV'' should be the same. This property is applied in the attack to determine whether the value of $\triangle_2 \oplus \triangle_3$ is 0.

Assume that the value of $\triangle_2 \oplus \triangle_3$ is randomly distributed, then $\triangle_2 \oplus \triangle_3 = 0$ with probability 2^{-29}. We thus need to generate about 2^{29} pairs $(\triangle_2, \triangle_3)$ in order to obtain a pair satisfying $\triangle_2 \oplus \triangle_3 = 0$. Note that the key is fixed and that $S'^0(2) \oplus S''^0(2) = S'^0(5) \oplus S''^0(5)$ must be satisfied. There are 3 bytes of IV and one-byte difference can be chosen, so there are about $2^{24} \times 255/2 \approx 2^{31}$ pairs of $(\triangle_2, \triangle_3)$ are available. Thus there is no problem to generate 2^{29} pairs of $(\triangle_2, \triangle_3)$.

Then we proceed to determine which pair $(\triangle_2, \triangle_3)$ satisfies $\triangle_2 \oplus \triangle_3 = 0$. For each pair $(\triangle_2, \triangle_3)$, we modify the values of $IV'_{1,\ldots,8}$ and $IV''_{1,\ldots,8}$, but we ensure that $IV'_{1,\ldots,8} = IV''_{1,\ldots,8}$. This modification does not affect the value of $\triangle_2 \oplus \triangle_3$, but it effects the value of $S^{22}(10)$. We generate keystream and examine the first keystream bits. If the values of the first keystream bits are the same, then the chance that $\triangle_2 \oplus \triangle_3 = 0$ is improved. In that case, we modify the $IV'_{1,\ldots,8}$ and $IV''_{1,\ldots,8}$ again and observe the first keystream bits. This process ends when the first keystream bits are not the same or this process is repeated for 40 times. If one $(\triangle_2, \triangle_3)$ passes the test for 40 times, then we know that $\triangle_2 \oplus \triangle_3 = 0$ with probability extremely close to 1. (Each wrong pair could pass this filtering process with probability 2^{-40}. One pair of 2^{29} wrong pairs could pass this process with probability 2^{-11}.) Thus with about $2 \times 2^{29} \times \sum_{i=1}^{40} \frac{i}{2^i} = 2^{31}$ chosen IVs, we can find a pair $(\triangle_2, \triangle_3)$ satisfying $\triangle_2 \oplus \triangle_3 = 0$. Subsequently according to Eqn. (3) and $\triangle_2 \oplus \triangle_3 = 0$, we recover 24 bits of the secret key, $k_{17,\ldots,24}$ and $k_{49,\ldots,64}$.

The above attack can be improved if we consider the differences at $S^{22}(7)$ and $S^{22}(8)$. The differences there are both $\triangle_1 \oplus \triangle_2 \oplus \triangle_3$. If the value of $\triangle_1 \oplus \triangle_2 \oplus \triangle_3$ is 0, then the third and fourth bits of the two keystreams would be the same. If we only observe the third and fourth keystream bits, the $k_{17,\ldots,24}$ and $k_{49,\ldots,64}$ can be recovered with $2 \times 2^{29} \times \sum_{i=1}^{20} (\frac{1}{2^{i-1}} - \frac{1}{2^i}) \times i = 2^{30.4}$ chosen IVs.

In the attack, we observe the first, third and fourth keystream bits, then recovering $k_{17,\ldots,24}$ and $k_{49,\ldots,64}$ requires about $2 \times 2^{28} \times 2^{1.13} = 2^{30.1}$ chosen IVs (the value $2^{1.13}$ is obtained through numerical computation).

By setting the difference at $S^0(3)$ and $S^0(6)$ and observing the second and third bits of the keystream, we can recover another 24 bits of the secret key, $k_{25,\ldots,40}$ and $k_{65,\ldots,72}$. We need $2^{30.4}$ chosen IVs.

So with about $2^{30.1} + 2^{30.4} = 2^{31.3}$ chosen IVs, we can recover 48 bits of the 80-bit secret key. It shows that the key/IV setup of WG stream cipher is insecure.

2.2 Attacks on WG with key and IV sizes larger than 80 bits

The WG ciphers with the key and IV sizes larger than 80 bits are all vulnerable to the chosen IV attack. The attacks are very similar to the above attack. We omit the details of the attacks here. The results are given below.

1. For WG with 96-bit key and 96-bit IV, 48 bits of the key can be recovered.
2. For WG with 112-bit key and 112-bit IV, 72 bits of the key can be recovered.
3. For WG with 128-bit key and 128-bit IV, 72 bits or 96 bits of the key can be recovered.

2.3 Attacks on WG with 64-bit IV size

We use the WG with 80-bit key and 64-bit IV as an example to illustrate the attack. For the WG cipher with 80-bit key and 64-bit IV, the key and IV are loaded into the LFSR as follows:

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

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

In the attack, we set the differences at $S(2)$ and $S(5)$, we can only generate about 2^{23} pairs of $(\triangle_2, \triangle_3)$ since we can only modify $IV_{9,\ldots,16}$ and $IV_{33,\ldots,40}$. Thus we can obtain a pair $(\triangle_2, \triangle_3)$ satisfying $\triangle_2 \oplus \triangle_3 = 0$ or $\triangle_1 \oplus \triangle_2 \oplus \triangle_3 = 0$ with probability 2^{-5}. Once we know $\triangle_2 \oplus \triangle_3 = 0$ or $\triangle_1 \oplus \triangle_2 \oplus \triangle_3 = 0$, we can recover 29-bit information of $k_{17,\ldots,32}$ and $k_{65,\ldots,80}$. It shows that 29-bit information of the secret key could be recovered with probability 2^{-5}. This attack requires about $2^{25.1}$ chosen IVs.

The attack on WG with 96-bit key and 64-bit IV is similar to the above attack. We can set the differences at $S(2)$ and $S(5)$ or at $S(3)$ and $S(6)$. In the attack 29-bit information of $k_{17,\ldots,32}$ and $k_{65,\ldots,80}$ can be recovered with probability 2^{-5}, and another 29-bit information of $k_{33,\ldots,48}$ and $k_{81,\ldots,96}$ can be recovered with probability 2^{-5}.

The attack on WG with 112-bit key and 64-bit IV is also similar. The result is that 29-bit information of $k_{17,\ldots,32}$ and $k_{65,\ldots,80}$ can be recovered with probability 2^{-5}, 29-bit information of $k_{33,\ldots,48}$ and $k_{81,\ldots,96}$ can be recovered with probability 2^{-5}, and 29-bit information of $k_{49,\ldots,64}$ and $k_{97,\ldots,112}$ can be recovered with probability 2^{-5}.

The attack on WG with 128-bit key and 64-bit IV is also similar. The result is that 29-bit information of $k_{17,\ldots,32}$ and $k_{65,\ldots,80}$ can be recovered with probability 2^{-5}, 29-bit information of $k_{33,\ldots,48}$ and $k_{81,\ldots,96}$ can be recovered with probability 2^{-5}, 29-bit information of $k_{49,\ldots,64}$ and $k_{97,\ldots,112}$ can be recovered with probability 2^{-5}, and 29-bit information of $k_{64,\ldots,80}$ and $k_{113,\ldots,128}$ can be recovered with probability 2^{-5}.

3 Conclusion

It was shown in this paper that the key/IV setup of stream cipher WG is vulnerable to the chosen IV attack. The only exception is the WG cipher with 32-bit IV.

References

1. E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", in *Advances in Cryptology – Crypto'90*, LNCS 537, pp. 2-21, Springer-Verlag, 1991.
2. 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.
3. Yassir Nawaz, Guang Gong. "The WG Stream Cipher". *ECRYPT Stream Cipher Project Report 2005/033.* Available at http://www.ecrypt.eu.org/stream/