Some Observations on TWIS Block Cipher

Bozhan Su, Wenling Wu, Lei Zhang, Yanjun Li

State Key Laboratory of Information Security,
Institute of Software, Chinese Academy of Sciences, Beijing 100190, P. R. China
{*subozhan, wwl, zhanglei1015, liyanjun*}*@is.iscas.ac.cn*

Abstract. The 128-bit block cipher TWIS was proposed by Ojha et al in 2009. It is a lightweight block cipher and its design is inspired from CLEFIA. In this paper, we first study the properties of TWIS structure, and as an extension we also considered the generalized TWIS-type structure which can be called G-TWIS cipher, where the block size and round number can be arbitrary values. Then we present a series of 10-round differential distinguishers for TWIS and a n-round differential distinguisher for G-TWIS whose probabilities are all equal to 1. Therefore, by utilizing these kinds of differential distinguishers, we can break the full 10-round TWIS cipher and n-round G-TWIS cipher.

Key words: Block Cipher, TWIS, G-TWIS, Differential Distinguisher, Differential Cryptanalysis.

1 Introduction

Recently, researches on the design of lightweight cryptography have received lots of attention. Lightweight cryptography mainly deals with designing ciphers for extremely resource constrained environments, such as applications of RFID tags and sensor networks. Considering that conventional algorithms such as AES although quite secure, are not suitable for such environments, hence a number of new symmetric lightweight block ciphers have been proposed in the open literature, such as DESL [6], PRESENT [2], HIGHT [5], LCASE [10], Cobra [9] and TWIS [7] et al.

TWIS is a lightweight block cipher designed by Ojha et al in 2009. Both of its block size and key size are 128-bit and the total number of rounds is 10. The overall structure of TWIS is a 2-branch generalized Feistel structure which employs key whitening at the beginning and at the end of the cipher.

In this paper, we first study the properties of TWIS structure, and as an extension we also considered the generalized TWIS-type structure which can be called G-TWIS cipher, whose block size is 4m-bits and consists of n rounds encryption in all, where n and m are arbitrary positive integers. Then we evaluate the security of TWIS and G-TWIS against differential cryptanalysis respectively. Our main results include: we present $(2^3 - 1)$ differential distinguishers for 10-round TWIS cipher and a differential distinguisher for n-round G-TWIS cipher whose probabilities are both equal to 1. Based on these distinguishers, we can break the full 10-round TWIS cipher and the full n-round G-TWIS cipher. Since

our analysis does not depend on any weak-key or weak-subkey assumptions, these attacks can both be independent of the key schedule algorithm.

The rest of this paper is organized as follows. Section 2 gives a brief description of TWIS first and then gives the specification of the proposed cipher G-TWIS. Section 3 and Section 4 present the differential attack on the full TWIS cipher and on the full G-TWIS cipher respectively. Finally, Section 5 summarizes the paper.

2 Descriptions of TWIS and G-TWIS

TWIS is a 128-bit block cipher which uses key of size 128-bit. It employs a 2-branch Generalized Feistel structure and consists of 10 rounds. Each round of TWIS uses two rounds of Feistel network which involves a 64-bit round function called G-function. Furthermore, key whitening layers are employed both at the beginning and at the end of the encryption procedure. Since the key scheduling is not involved in out attack, we will omit the description of key schedule algorithm here and interested readers can refer to [7] for more details.

As an extension of TWIS, we construct a generalized TWIS-type cipher called G-TWIS. Its block size can be 4m-bit and consists of n rounds, where m and n are arbitrary positive integers. Similar to the round function of TWIS, in each round of G-TWIS we also use two rounds of Feistel network which involves a 2m-bit round function called G'-function. In the following, we will give detailed descriptions of the encryption procedures of TWIS and G-TWIS.

2.1 Notation

In this subsection, we first introduce the following notations which are used throughout this paper.
- Z_2^m: the set of m-bit words.
- $a \oplus b$: bitwise XOR of a and b.
- $a \wedge b$: bitwise AND of a and b.
- $a|b$: concatenation of a and b.
- $\lll i$: left rotation by i bits.
- $\ggg i$: right rotation by i bits.

2.2 Encryption Procedure of TWIS

For the encryption procedure of TWIS, let $P = (P_0, P_1, P_2, P_3) \in (Z_2^{32})^4$ denote a 128-bit plaintext, and $C = (C_0, C_1, C_2, C_3) \in (Z_2^{32})^4$ denote the corresponding ciphertext. Let $RK_i \in Z_2^{32}$ $(i = 0, 1, \ldots, 10)$ denote the round subkeys provided by the key scheduling part. First of all, two 32-bit whitening subkeys RK_0 and RK_1 are XORed to P_0 and P_3 respectively, and the resulted intermediate value is denoted as (T_0, T_1, T_2, T_3). Then the same round transformation is iterated for 10 times, and the operations in each round is defined as follows.

For the $i-$th round, $1 \leq i \leq 10$

a) $X_0|X_1 \leftarrow G\_function(RK_{i-1}, T_0|T_1)$
b) $T_2 \leftarrow X_0 \oplus T_2, \quad T_3 \leftarrow X_1 \oplus T_3$
c) $T_1 \leftarrow T_1 \lll 8, \quad T_3 \leftarrow T_3 \ggg 1$
d) $T_0|T_1|T_2|T_3 \leftarrow T_2|T_3|T_0|T_1$
e) $X_0|X_1 \leftarrow G\_function(RK_i, T_0|T_3)$
f) $T_1 \leftarrow X_0 \oplus T_1, \quad T_2 \leftarrow X_1 \oplus T_2$
g) $T_2 \leftarrow T_2 \ggg 1, \quad T_3 \leftarrow T_3 \lll 8$

In the end, two whitening subkeys RK_2 and RK_3 are XORed to T_0 and T_3 respectively, and the result is just the ciphertext $C = (C_0, C_1, C_2, C_3)$. The detailed encryption procedure of TWIS is also illustrated in Fig. 1.

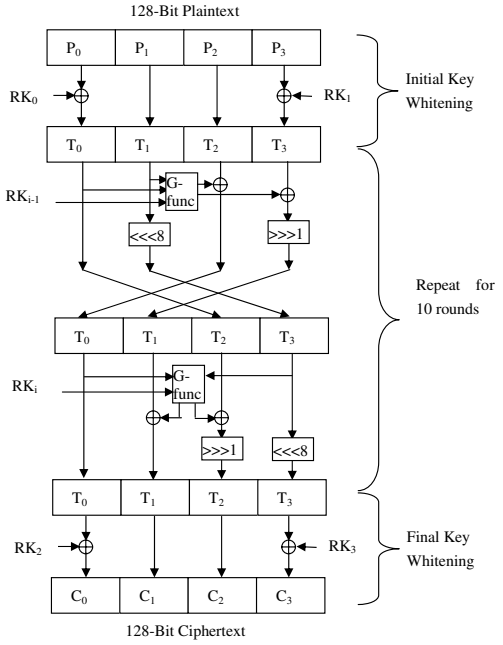

Fig. 1. The Encryption Process of TWIS

For the G-function used in each round, it is defined as follows. It takes 64-bit data and 32-bit round subkey as inputs and produces 64-bit output, and this transformation can be written as the following expressions.

1. $T_0|T_1 \leftarrow X_0|X_1$
2. $T_0 \leftarrow T_1 \oplus$ F_function(RK, T_0)

3. $Y_0|Y_1 \leftarrow T_1|T_0$

Here it calls another transformation named $F\_function$ which takes 32-bit intermediate state X and 32-bit round subkey RK as inputs, and produces 32-bit output Y. The transformation of $F\_function$ is defined as follows:

1. $T_0|T_1|T_2|T_3 \leftarrow RK \oplus X$
2. $T_0 \leftarrow Sbox(T_0 \wedge 0x3f)$
   $T_1 \leftarrow Sbox(T_1 \wedge 0x3f)$
   $T_2 \leftarrow Sbox(T_2 \wedge 0x3f)$
   $T_3 \leftarrow Sbox(T_3 \wedge 0x3f)$
3. $Y_0|Y_1|Y_2|Y_3 \leftarrow T_2|T_3|T_0|T_1$

Note that the Sbox used in $F\_function$ takes 6-bit input and yields 8-bit output, and the specific Sbox table can be obtained in [7].

2.3 Encryption Procedure of G-TWIS

As an extension of TWIS, we construct a generalized TWIS-type cipher called G-TWIS. Its block size can be 4m-bit and consists of n rounds, where m and n are arbitrary values. Let $P = (P_0, P_1, P_2, P_3) \in (Z_2^m)^4$ and $C = (C_0, C_1, C_2, C_3) \in (Z_2^m)^4$ denote the plaintext and its corresponding ciphertext respectively. Let $RK_i \in Z_2^m$ $(i = 0, \ldots, n-1)$ denote the round subkeys provided by the key scheduling part. The key whitening layers at the beginning and at the end of G-TWIS are exactly the same with TWIS, and the round transformation used in each round is defined as follows. The encryption procedure of G-TWIS is also illustrated in Fig. 2.

For the $i-$th round, $1 \le i \le n$
a) $X_0|X_1 \leftarrow G'\_function(RK_{i-1}, T_0|T_1)$
b) $T_2 \leftarrow X_0 \oplus T_2, \quad T_3 \leftarrow X_1 \oplus T_3$
c) $T_1 \leftarrow T_1 \lll r_0, \quad T_3 \leftarrow T_3 \ggg r_1$
d) $T_0|T_1|T_2|T_3 \leftarrow T_2|T_3|T_0|T_1$
e) $X_0|X_1 \leftarrow G'\_function(RK_i, T_0|T_3)$
f) $T_1 \leftarrow X_0 \oplus T_1, \quad T_2 \leftarrow X_1 \oplus T_2$
g) $T_2 \leftarrow T_2 \ggg r_2, \quad T_3 \leftarrow T_3 \lll r_3$

For the G'-function used in each round, it takes 2m-bit data and m-bit round subkey as inputs and produces 2m-bit output. Similar to the G-function in TWIS, G'-function can be written as the following expressions.

1. $T_0|T_1 \leftarrow X_0|X_1$
2. $T_0 \leftarrow T_1 \oplus F'\_function(RK, T_0)$
3. $Y_0|Y_1 \leftarrow T_1|T_0$

Here it calls $F'\_function$ which takes m-bit intermediate state X and m-bit round subkey RK as inputs, and produces m-bit output Y.

$$F'\_function = \begin{cases} \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}^m, \\ (RK, X) \mapsto Y \end{cases}$$

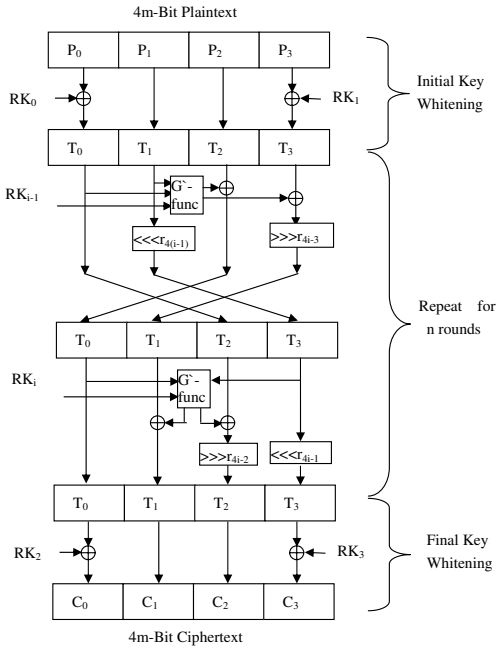

Fig. 2. The Encryption Process of G-TWIS

3 10-Round Differential Distinguishers for TWIS

In this section, we present $(2^3 - 1)$ 10-round differential distinguishers for TWIS whose probabilities are all equal to 1. These differential distinguishers are mainly based on the following one-round iterative differential characteristic with probability 1.

Fig. 3 illustrates this kind of one-round iterative differential characteristic in detail. Note here we choose both the input and output differences of the i-th round as $\Delta X = (\Delta X_0, \Delta X_1, \Delta X_2, \Delta X_3) \in (Z_2^{32})^4$ which denotes a 128-bit nonzero difference. Then the input and output differences of $F_0\_function$ are equal to ΔX_0 and $\Delta X_1 \oplus (\Delta X_1 \oplus (\Delta X_1 \lll 8)) \lll 1 \oplus \Delta X_3$ respectively. Similarly, the input and output differences of $F_1\_function$ are equal to ΔX_0 and $\Delta X_0 \oplus (\Delta X_2 \lll 1) \oplus (\Delta X_1 \lll 8)$ respectively. Furthermore, we can obtain the following equations.

$$\Delta X_1 \lll 16 = \Delta X_3 \tag{1}$$

$$\Delta X_1 \oplus \Delta X_2 = \Delta X_0 \tag{2}$$

If we set the input and output differences of $F_0\_function$ and $F_1\_function$ be zero, then we can obtain the following three equations.

$$\Delta X_0 \wedge 0x3f3f3f3f = 0 \tag{3}$$

$$\Delta X_1 \oplus (\Delta X_1 \oplus (\Delta X_1 \lll 8)) \lll 1 \oplus \Delta X_3 = 0 \tag{4}$$

$$\Delta X_0 \oplus (\Delta X_2 \lll 1) \oplus (\Delta X_1 \lll 8) = 0 \tag{5}$$

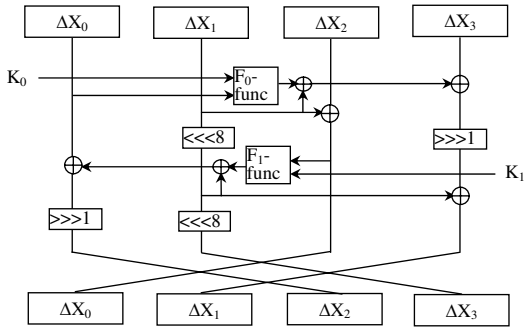

Fig. 3. one-round iterative differential characteristic of TWIS

By solving the above system of equations (1)-(5), we find that there are $(2^3 - 1)$ non-zero solutions in all. Since all these solutions satisfy that the input and output differences of $F_0\_function$ and $F_1\_function$ equal to zero, we can construct $(2^3 - 1)$ one-round iterative differential characteristics which all hold with probability 1. Then by iterating this kind of one-round differential characteristic 10 times, we can obtain $(2^3 - 1)$ 10-round differential distinguishers for TWIS whose probabilities are all equal to 1. Table 1 contains all the $(2^3 - 1) = 7$ one-round iterative differential characteristics.

Table 1. one-round iterative differential characteristics for TWIS

No.	$\Delta X = \Delta X_0, \Delta X_1, \Delta X_2, \Delta X_3$	$\Pr(\Delta X \rightarrow \Delta X)$
1	$(0xc0c0c0c0,\ 0xc0c0c0c0,\ 0x00000000,\ 0xc0c0c0c0)$	1
2	$(0x80808080,\ 0x80808080,\ 0x00000000,\ 0x80808080)$	1
3	$(0x40404040,\ 0x40404040,\ 0x00000000,\ 0x40404040)$	1
4	$(0x40404040,\ 0xbfbfbfbf,\ 0xffffffff,\ 0xbfbfbfbf)$	1
5	$(0x80808080,\ 0x7f7f7f7f,\ 0xffffffff,\ 0x7f7f7f7f)$	1
6	$(0xc0c0c0c0,\ 0x3f3f3f3f,\ 0xffffffff,\ 0x3f3f3f3f)$	1
7	$(0x00000000,\ 0xffffffff,\ 0xffffffff,\ 0xffffffff)$	1

4 n-Round Differential Distinguisher for G-TWIS

In this section, we present an n-round differential distinguisher for G-TWIS whose probability is also equal to 1. This n-round differential distinguisher is based on the following one-round iterative differential characteristic with probability 1.

Similar to the analysis in Sect. 3, we also choose the input and output differences of the i-th round as $\Delta X = (\Delta X_0, \Delta X_1, \Delta X_2, \Delta X_3) \in (Z_2^m)^4$, which denotes a 4m-bit nonzero difference. Then the input and output differences of F_0'-$function$ are equal to $(\Delta X_0,\ \Delta X_1 \oplus (\Delta X_1 \oplus (\Delta X_1 \lll r_0)) \lll r_1 \oplus \Delta X_3)$, and the input and output differences of F_1'-$function$ are equal to $(\Delta X_0,\ \Delta X_0 \oplus (\Delta X_2 \lll r_2) \oplus (\Delta X_1 \lll r_0))$ respectively. Similarly, we can obtain the following equations.

$$\Delta X_1 \lll (r_0 + r_3) = \Delta X_3 \tag{6}$$

$$\Delta X_1 \oplus \Delta X_2 = \Delta X_0 \tag{7}$$

Then by setting the input and output differences of F_0'-$function$ and F_1'-$function$ as zero, we can obtain the following equations.

$$\Delta X_0 = 0 \tag{8}$$

$$\Delta X_1 \oplus (\Delta X_1 \oplus (\Delta X_1 \lll r_0)) \lll r_1 \oplus \Delta X_3 = 0 \tag{9}$$

$$\Delta X_0 \oplus (\Delta X_2 \lll r_2) \oplus (\Delta X_1 \lll r_0) = 0 \tag{10}$$

Considering the above system of equations (6)-(10), it is easy to see that $(0, \alpha, \alpha, \alpha)$ is a solution of the system, where $\alpha = 2^m - 1$. Hence we can construct an iterative differential characteristic $(0, \alpha, \alpha, \alpha) \rightarrow (0, \alpha, \alpha, \alpha)$ where $\alpha = 2^m - 1$, and it holds with probability 1. Then by iterating this differential characteristic n times, we can obtain the following n-round differential distinguisher for G-TWIS whose probability is equal to 1.

$$(0, \alpha, \alpha, \alpha) \xrightarrow{n\ R} (0, \alpha, \alpha, \alpha). \quad \alpha = 2^m - 1$$

The following Fig. 4 illustrates this one-round iterative differential characteristic of G-TWIS in detail.

5 Summary

In this paper, we first study the properties of TWIS structure, and as an extension we also considered the generalized TWIS-type structure which can be called G-TWIS cipher, where the block size and round number can be arbitrary values. Then we present $(2^3 - 1)$ 10-round differential distinguishers for TWIS and an n-round differential distinguisher for G-TWIS whose probabilities are all equal to 1. Therefore, by utilizing these kinds of differential distinguishers, the full-round TWIS and G-TWIS are distinguishable from an ideal cipher, and

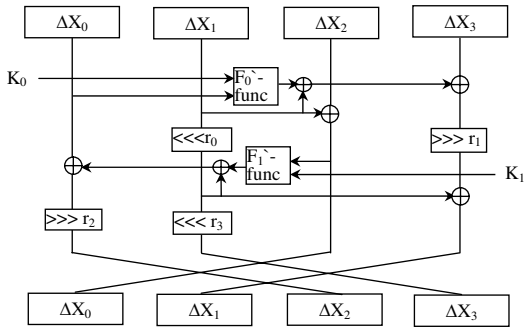

Fig. 4. one-round iterative differential characteristic of G-TWIS

hence we can break the full 10-round TWIS cipher and n-round G-TWIS cipher very efficiently.

Our results demonstrate that the design of TWIS-type structure has fatal weakness, and no matter how security the internal building blocks such as Sbox and diffusion matrix are used and even how many rounds are used, the overall cipher is still vulnerable to differential attack. Furthermore, the reuse of whitening subkeys as round subkeys may endanger the cipher, too. Therefore, we suggest that this kind of TWIS-type cipher should be carefully used in a cryptographic system.

Acknowledgment

We would like to thank anonymous referees for their helpful comments and suggestions. The research presented in this paper is supported by the National Natural Science Foundation of China (No.60873259); the National Natural Science Foundation of China (No.60903212); the National High-Tech Research and Development 863 Plan of China (No.2007AA01Z470).

References

1. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, Vol.4, No.1, pp. 3-72, 1991.
2. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450C466. Springer, Heidelberg (2007).
3. Daemen, J.: Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis. Doctoral Dissertation, March 1995, K.U.Leuven.
4. Daemen, J., Rijmen, V.: The Design of Rijndael- AES, the Advanced Encryption Standard. Springer, 2002.

5. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46C59. Springer, Heidelberg (2006).
6. Leander, G., Paar, C., Poschmann, A., Schramm, K.: New Lightweight DES Variants. FSE 2007. LNCS, vol. 4539, pp. 196-210. Springer, Heidelberg (2007).
7. Ojha, S., Kumar, N., Jain, K., Lal, S.: TWIS - A Lightweight Block Cipher. ICISS 2009. LNCS, vol. 5905, pp. 280-291. Springer, 2009.
8. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit block cipher CLEFIA. FSE 2007. LNCS, vol 4593, pp. 181-195. Springer, 2007.
9. Sklavos, N., Moldovyan, N.A., Koufopavlou, O.: High Speed Networking Security: Design and Implementation of Two New DDP-Based Ciphers. Mobile Networks and Applications 10, pp. 219C231. Springer, Heidelberg (2005).
10. Tripathy, S., Nandi, S.: LCASE: Lightweight Cellular Automata-based Symmetrickey Encryption. International Journal of Network Security 8(2), 243C252 (2009).