Differential and Linear Cryptanalysis of a Reduced-Round SC2000

Hitoshi Yanami[1], Takeshi Shimoyama[1], and Orr Dunkelman[2]

[1]FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-Chome, Nakahara-ku, Kawasaki, 211-8588, Japan
{yanami, shimo}@flab.fujitsu.co.jp
[2]COMPUTER SCIENCE DEPARTMENT, TECHNION.
Haifa 32000, Israel
orrd@cs.technion.ac.il

Abstract. We analyze the security of the SC2000 block cipher against both differential and linear attacks. SC2000 is a six-and-a-half-round block cipher, which has unique structure containing both Feistel and SPN structure. Taking into account the structure of SC2000, we investigate one- and two-round iterative differential and linear characteristics. We present two-round iterative differential characteristics with probability 2^{-58} and a two-round linear characteristic with probability 2^{-56}. By using these characteristics obtained by our search, we can attack four-and-a-half-round SC2000 for 128-bit user key. Our differential attack needs 2^{103} pairs of chosen plaintexts and 2^{20} memory accesses, and linear attack $2^{115.17}$ known plaintexts and $2^{42.32}$ memory accesses, or $2^{104.32}$ known plaintexts and $2^{83.32}$ memory accesses.

Keywords: symmetric block cipher, SC2000, differential attack, linear attack, characteristic, probability

1 Introduction

Differential cryptanalysis was proposed by Biham and Shamir [1]. Linear cryptanalysis was introduced by Matsui [6]. Both methods are well known and are often very effective means to attack a block cipher. One of the many steps in establishing cipher's security is to evaluate its strength against these attacks. The security of a cipher against differential attacks can be estimated according to the maximum differential probability and against linear attacks according to the maximum linear probability. A cipher is considered to be secure against these attacks if these two probabilities are small enough to make these attacks impractical.

SC2000 is a block cipher submitted to the NESSIE [9] and the CRYPTREC [3] projects by Shimoyama et al. [11]. In *Self-Evaluation Report* in the submitted documents, the security against differential and linear cryptanalysis was evaluated by estimating the number of active S-boxes in differential and linear characteristics. Other studies on SC2000 can be seen in several papers [3, 4, 5, 10, 15].

This paper is based on [15] presented by Yanami and Shimoyama in the 2nd NESSIE workshop, in which the authors made both differential and linear attacks on a reduced-round SC2000. Our differential characteristics used here is the same as in [15], which is slightly better than the ones found by Raddum and Knudsen [10]. The linear cryptanalysis in [15] contained some wrong calculations, so we correct them and re-examine linear characteristics. Moreover, Dunkelman, one of the authors, improve the computational complexity of deducing subkey bits.

In this paper we investigate one- and two-round iterative differential/linear characteristics. By iterating a differential/linear characteristic obtained by our search, we construct a longer characteristic and utilize it for attacking a four-and-a-half-round SC2000.

The paper is organized as follows: We briefly describe the encryption algorithm of SC2000 in Section 2. In Section 3 we illustrate our search method and show our search result. We present our differential and linear attacks on four-and-a-half-round SC2000 in Sections 4 and 5, respectively. We summarize our paper in Section 6.

2 Description of SC2000

SC2000 is a block cipher submitted to the NESSIE[9] and the CRYPTREC[3] projects by Shimoyama et al. [11]. SC2000 has 128-bit block size and supports 128-/192-/256-bit user keys, the same as the AES.

Before proceeding further, we remark two things: Firstly, we mainly take up the case of 128-bit user key. Secondly, we omit the description of the SC2000 key schedule as it has no relevance to the attacks presented in this paper. The key schedule generates sixty-four 32-bit subkeys from a 128-bit user key.

2.1 Encryption Algorithm

The SC2000 encryption procedure consists of three functions: the I, the R and the B functions. Each function has a 128-bit input/output. There are two kinds of R functions which differ only in a constant used in them (`0x55555555` or `0x33333333`). When we need to distinguish these two types of R function, we denote them R_5 or R_3 by the constant, respectively.

The encryption function can be written as:

$$\begin{aligned} &I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}\\ &\quad I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I, \end{aligned}$$

where $\times$ stands for exchanging the left and right 64 bits. We define -I-B-I-$R{\times}R$- as a round of SC2000. The cipher iterates it six times and finally operates -I-B-I for encryption-decryption symmetry. For the sake of simplicity we call the last -I-B-I part half a round. SC2000 has six and a half rounds for a 128-bit user key, and seven and a half rounds for a 192-/256-bit user key.

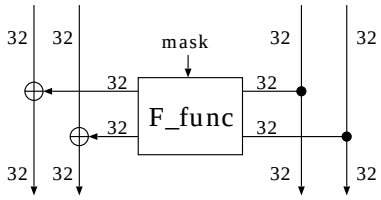

Fig. 1. R function

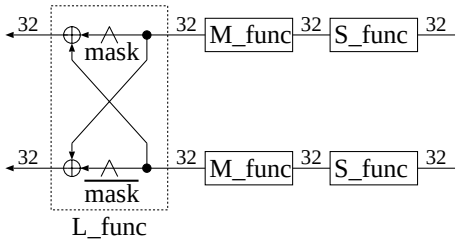

Fig. 2. F function

2.2 *I* Function

The I function XORs a 128-bit input with four subkeys. The I function divides an input into four 32 bits, each of which is XORed with a corresponding 32-bit subkey. The subkeys are used only in the I functions.

2.3 *R* Function

The R function has a conventional Feistel structure, except for the swap of the left and right 64 bits in the last part (Fig.1). The right 64 bits of the input enter the F function, and the output is XORed with the left 64 bits. The XORed value becomes the left half of the output of the R function. The right half of the output of the R function equals that of the input.

The F function in the R function has a 64-bit input/output and consists of three subfunctions, S, M, and L functions (Fig.2). The F function divides its input into two 32-bit variables and each variable is dealt with the S and M functions successively. The two outputs become the input of the L function, the output of which becomes that of the F function. Note that the F function is bijective. We describe the S, M, and L functions in the following:

The S function is a 32-bit input/output nonlinear function. A 32-bit input is divided into 6, 5, 5, 5, 5 and 6 bits. These groups of bits enter S-boxes; the 6-bit groups enter S_6, while the 5-bit groups enter S_5. The output of the S

function is the concatenated outputs of the S-boxes. We refer to [11] for the values of the S_5 and S_6 tables.

The M function is a 32-bit input/output linear function. The output b for an input a is the product of a and a matrix M,

$$b = a \cdot M,$$

where M is a square matrix of order 32 with entries in $GF(2)$, the Galois field of order two, and a and b are considered as row vectors with entries in $GF(2)$. For the entries of the matrix M, we refer to [11].

The L function has two 32-bit variables as an input/output. We denote the input by (a, b) and the corresponding output by (c, d). The variables c and d are obtained by the following formula:

$$c = (a \wedge mask) \oplus b, \quad d = (b \wedge \overline{mask}) \oplus a,$$

where $mask$ is a constant we have mentioned, `0x55555555` or `0x33333333`, $\overline{mask}$ is the bitwise-NOT of $mask$, and the symbol $\wedge$ represents bitwise-AND operation.

2.4 *B* Function

The B function has an SPN structure with 128-bit input/output which resembles the S-boxes in the Serpent block cipher, i.e., 4-bit to 4-bit S-boxes. We can apply bitslice implementation to the B function. We denote the input of the B function by (a, b, c, d) with each variable 32 bits and the i-th bit of a by a_i, and so similarly for b, c and d. For $i = 0, 1, \ldots, 31$, the B function picks the i-th bit from each of the variables a, b, c and d, and replaces the four bits of (a_i, b_i, c_i, d_i) into (e_i, f_i, g_i, h_i) according to the S_4 table, where (e, f, g, h) denotes the four 32-bit words which compose the output of the B function. We refer to [11] for the values of the S_4 table. Note that if the B functions in SC2000 are all replaced by the swap of the left and right 64 bits, the resulting structure becomes a classical Feistel one.

3 Differential and Linear Characteristics of SC2000

When differential/linear characteristics of a block cipher are investigated, it is almost impossible to compute the probability of every characteristic by exhaustive search for the cipher itself. Roughly speaking, the following strategy is often used to construct a long characteristic with high probability: 1)Examine short iterative characteristics, i.e., characteristics with small number of rounds whose input and output differences/masks are the same; 2)Iterate one with the highest differential/linear probability found by the search to make a characteristic with more rounds. We will follow the strategy when we examine differential/linear characteristics.

In SC2000 encryption algorithm, the I functions are merely used for XORing data with subkeys, so we can eliminate them when we examine differential/linear relationships. By removing them, we obtain the following:

$$B\text{-}R_5{\times}R_5\text{-}B\text{-}R_3{\times}R_3\text{-}B\text{-}R_5{\times}R_5\text{-}B\text{-}R_3{\times}R_3\text{-}B\text{-}R_5{\times}R_5\text{-}B\text{-}R_3{\times}R_3\text{-}B\,.$$

It can be seen that -B-$R{\times}R$- is a period. It is repeated six times and finally B function is added for preserving symmetry in encryption-decryption procedure. Taking the period into consideration, we investigate one- and two-round differential/linear characteristics with certain patterns of differences/masks.

3.1 Differential Characteristics

We explain our efficient search method for an iterative differential characteristic with high probability. We start by reviewing the nonlinear functions in SC2000. They are all realized by the S-boxes, S_4, S_5, and S_6. There are thirty-two S_4's in the B function and eight S_5's and four S_6's in the R function. Four S_5's and two S_6's constitute the S function; two S functions exist in the R function. From the differential distribution tables of the S-boxes, we see differential probability for a pair of nonzero input and output differences in S_4 is either 2^{-2} or 2^{-3}, in S_5 it is 2^{-4}, in S_6 either 2^{-4} or 2^{-5}. These facts suggest that the number of nonzero differences in S_5 and S_6 in the S function have more effect on total differential probability of characteristics than that of S_4 in the B function.

Taking this into consideration, we decide to investigate the differential characteristics with a nonzero difference in only one of the four S functions in a -B-$R{\times}R$- cycle, which enables us to efficiently find a differential characteristic with high probability.

One-Round Characteristics. We investigate the one-round iterative characteristics with a nonzero difference in only one of the four S functions in a -B-$R{\times}R$- cycle. We illustrate the differential patterns of the characteristics we need to investigate in Fig.3. We call each type of these differential patterns D_1, D_2, D_3, or D_4, respectively, according to the position of the S function with the nonzero difference.

We have investigated differential characteristics with these patterns for both -B-$R_5{\times}R_5$- and -B-$R_3{\times}R_3$-. We have found differential characteristics that have probability 2^{-33} for both cycles, which is the highest probability for differential characteristics of this kind. These characteristics are of type D_3. We show an example of such differential characteristics:

-B-$R{\times}R$-

$$\begin{array}{ll}
 & \left\{\begin{array}{c}(\quad 0\ \texttt{0x00080008}\ \texttt{0x08090088}\quad 0)\\ \downarrow B\\ (\texttt{0x08090088}\quad 0\quad 0\quad 0)\end{array}\right\}\ 2^{-15}\\
R & (\quad 0\quad 0) \xleftarrow{F} (\quad 0\quad 0)\ 1\\
R & (\quad 0\ \texttt{0x00080008}) \xleftarrow{F} (\texttt{0x08090088}\quad 0)\ 2^{-18}.
\end{array}$$

Note that this characteristic has probability 2^{-33} regardless of the constant in the R function, and that we can construct an n-round differential characteristic with probability 2^{-33n} by concatenating it n times.

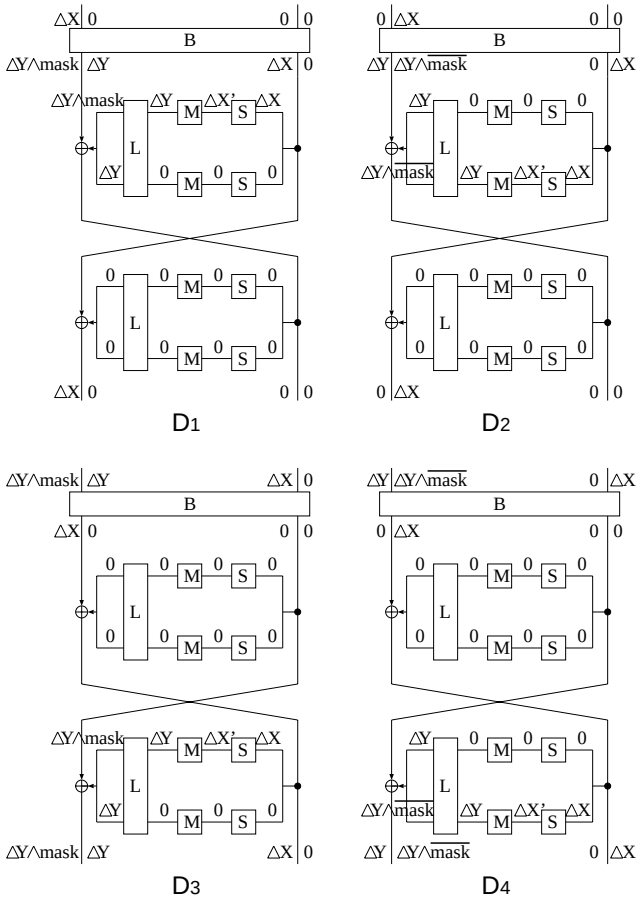

Fig. 3. Patterns of differences

Two-Round Characteristics. By distinguishing R_5 and R_3, we can also treat -B-R_5×R_5-B-R_3×R_3- as a cycle. Turning our attention to the cycle, we have investigated two-round iterative characteristics which have a nonzero difference in only one of four S functions in each -R×R- part. It seems that we could independently choose differential patterns among D_i's for the former -B-R_5×R_5- and the latter -B-R_3×R_3-, but some pairs cannot be concatenated at the B function. We can judge whether a pair can be concatenated or not from the differential distribution table of S_4. (See Appendix.) We list the pairs that need to be investigated:

$$
\begin{array}{cc}
\text{-}B\text{-}R_5{\times}R_5\text{-} \quad \text{-}B\text{-}R_3{\times}R_3\text{-} & \text{-}B\text{-}R_5{\times}R_5\text{-} \quad \text{-}B\text{-}R_3{\times}R_3\text{-} \\
\Delta A \to (D_1) \to \Delta B \to (D_1) \to \Delta A & \Delta A \to (D_1) \to \Delta B \to (D_2) \to \Delta A \\
\Delta A \to (D_2) \to \Delta B \to (D_2) \to \Delta A & \Delta A \to (D_2) \to \Delta B \to (D_1) \to \Delta A \\
\Delta A \to (D_3) \to \Delta B \to (D_3) \to \Delta A & \Delta A \to (D_3) \to \Delta B \to (D_4) \to \Delta A \\
\Delta A \to (D_4) \to \Delta B \to (D_4) \to \Delta A & \Delta A \to (D_4) \to \Delta B \to (D_3) \to \Delta A\,.
\end{array}
$$

Note that differences ΔA's and ΔB's in the above list should be adjusted in need: When, for example, the former pattern is D_1 and the latter D_2, we think ΔA as $(0, \Delta X, 0, 0)$ and ΔB as $(\Delta X, 0, 0, 0)$, having a preference for the output difference of the preceding R function. We have investigated these types of characteristics and found that the differential characteristics with the highest probability have the pattern

$$\Delta A \to (D_4) \to \Delta B \to (D_3) \to \Delta A$$

with probability 2^{-58}. An example of such characteristics is as follows:

$$
\begin{array}{lll}
 & \text{-}B\text{-}R_5{\times}R_5\text{-}B\text{-}R_3{\times}R_3\text{-} & \\
B & \left\{ \begin{array}{l} (\texttt{0x01120000}\ \texttt{0x01124400}\ \texttt{0x01124400}\ \ \ 0) \\ \qquad\qquad\qquad\qquad \downarrow B \\ (\ \ \ 0\ \texttt{0x01124400}\ \ \ 0\ \ \ 0) \end{array} \right\} & 2^{-15} \\
R_5 & (\ \ \ 0\ \ \ 0) \xleftarrow{F} (\ \ \ 0\ \ \ 0) & 1 \\
R_5 & (\texttt{0x01124400}\ \ \texttt{0x00020000}) \xleftarrow{F} (\ \ \ 0\ \ \texttt{0x01124400}) & 2^{-16} \\
B & \left\{ \begin{array}{l} (\texttt{0x01124400}\ \texttt{0x00020000}\ \ \ 0\ \texttt{0x01124400}) \\ \qquad\qquad\qquad\qquad \downarrow B \\ (\texttt{0x01124400}\ \ \ 0\ \ \ 0\ \ \ 0) \end{array} \right\} & 2^{-11} \\
R_3 & (\ \ \ 0\ \ \ 0) \xleftarrow{F} (\ \ \ 0\ \ \ 0) & 1 \\
R_3 & (\texttt{0x01120000}\ \ \texttt{0x01124400}) \xleftarrow{F} (\texttt{0x01124400}\ \ \ 0) & 2^{-16}.
\end{array}
$$

The probability 2^{-58} of the characteristic is higher than 2^{-66}, the probability of the two-round differential characteristic obtained from a one-round iterative one with the highest probability we have found. The characteristic will be used later for our differential attack on a reduced-round SC2000.

3.2 Linear Characteristics

As in the differential probability, the linear distribution tables also tell us that the number of nonzero masks of S_5 and S_6 in the S function have more effect on the total linear probability than that of S_4 in the B function; the linear probability for a pair of nonzero input/output masks in S_4[†] is either 2^{-2} or 2^{-4}, in S_5 it is 2^{-4}, and in S_6 it is between 2^{-4} and 2^{-8}.

We investigate linear characteristics in the same way as for iterative differential characteristics, i.e., we examine the linear characteristics with a nonzero mask in only one of the four S functions in a -B-$R{\times}R$- cycle.

[†] In [15], the authors used 2^{-2} or 2^{-3} for the probability in S_4, which was wrong. We re-examined linear characteristics with the right values.

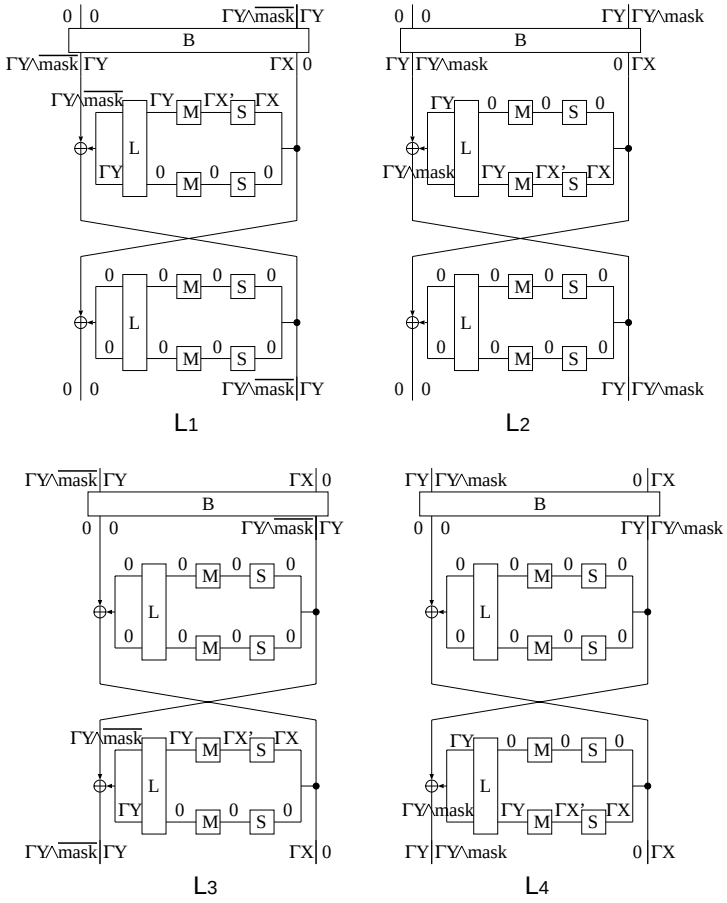

Fig. 4. Patterns of masks

One-Round Characteristics. We investigate those one-round iterative characteristics whose masks have a nonzero value in only one of the four S functions in a -B-R×R- cycle. We illustrate the mask patterns of these characteristics we investigate in Fig.4. We call each type of mask patterns L_1, L_2, L_3, or L_4, respectively, according to the position of the S function with the nonzero mask.

We have investigated these types of characteristics and found that the linear characteristics with the highest probability have probability $2^{-28.83}$ for -B-R_5×R_5- and 2^{-28} for -B-R_3×R_3-. All of them are of type L_2. We give an example of such linear characteristics in each case:

$$
\begin{array}{lll}
 & \text{-}B\text{-}R_5{\times}R_5\text{-} & \\
B & \left\{\begin{array}{c}(\quad 0 \qquad 0\ \texttt{0x84380080}\ \texttt{0x04100000}) \\ \downarrow B \\ (\texttt{0x84380080}\ \texttt{0x04100000} \qquad 0\ \texttt{0x84180000})\end{array}\right\} & 2^{-16} \\
R_5 & (\texttt{0x84380080}\ \ \texttt{0x04100000}) \xleftarrow{F} (\qquad 0\ \ \texttt{0x84180000}) & 2^{-8.83} \\
R_5 & (\quad 0 \qquad 0) \xleftarrow{F} (\quad 0 \qquad 0) & 1,
\end{array}
$$

$$
\begin{array}{lll}
 & \text{-}B\text{-}R_3{\times}R_3\text{-} & \\
B & \left\{\begin{array}{c}(\quad 0 \qquad 0\ \texttt{0x12020040}\ \texttt{0x12020000}) \\ \downarrow B \\ (\texttt{0x12020040}\ \texttt{0x12020000} \qquad 0\ \texttt{0x12020040})\end{array}\right\} & 2^{-12} \\
R_3 & (\texttt{0x12020040}\ \ \texttt{0x12020000}) \xleftarrow{F} (\qquad 0\ \ \texttt{0x12020040}) & 2^{-16} \\
R_3 & (\quad 0 \qquad 0) \xleftarrow{F} (\quad 0 \qquad 0) & 1.
\end{array}
$$

They cannot pass through if the constant is changed into the other. The linear characteristics which pass through both constants have the best probability $2^{-34.83}$. An example for such a linear characteristic is:

$$
\begin{array}{lll}
 & \text{-}B\text{-}R{\times}R\text{-} & \\
B & \left\{\begin{array}{c}(\quad 0 \qquad 0\ \texttt{0x11108008}\ \texttt{0x11100000}) \\ \downarrow B \\ (\texttt{0x11108008}\ \texttt{0x11100000} \qquad 0\ \texttt{0x11108008})\end{array}\right\} & 2^{-14} \\
R & (\texttt{0x11108008}\ \ \texttt{0x11100000}) \xleftarrow{F} (\qquad 0\ \ \texttt{0x11108008}) & 2^{-22.83} \\
R & (\quad 0 \qquad 0) \xleftarrow{F} (\quad 0 \qquad 0) & 1.
\end{array}
$$

We can construct an n-round linear characteristic with probability $2^{-36.83n}$ by concatenating it n times.

Two-Round Characteristics. We can also apply the same method as in the differential case. We can judge whether L_i and L_j can be concatenated or not from the linear distribution table of S_4. (See Appendix.) We list the pairs that need to be investigated:

$$
\begin{array}{cc}
\begin{array}{cc}
\text{-}B\text{-}R_5{\times}R_5\text{-} & \text{-}B\text{-}R_3{\times}R_3\text{-} \\
\Gamma A \rightarrow (L_1) \rightarrow \Gamma B \rightarrow (L_1) \rightarrow \Gamma A & \\
\Gamma A \rightarrow (L_2) \rightarrow \Gamma B \rightarrow (L_2) \rightarrow \Gamma A & \\
\Gamma A \rightarrow (L_3) \rightarrow \Gamma B \rightarrow (L_3) \rightarrow \Gamma A & \\
\Gamma A \rightarrow (L_4) \rightarrow \Gamma B \rightarrow (L_4) \rightarrow \Gamma A &
\end{array}
&
\begin{array}{cc}
\text{-}B\text{-}R_5{\times}R_5\text{-} & \text{-}B\text{-}R_3{\times}R_3\text{-} \\
\Gamma A \rightarrow (L_1) \rightarrow \Gamma B \rightarrow (L_2) \rightarrow \Gamma A & \\
\Gamma A \rightarrow (L_2) \rightarrow \Gamma B \rightarrow (L_1) \rightarrow \Gamma A & \\
\Gamma A \rightarrow (L_3) \rightarrow \Gamma B \rightarrow (L_4) \rightarrow \Gamma A & \\
\Gamma A \rightarrow (L_4) \rightarrow \Gamma B \rightarrow (L_3) \rightarrow \Gamma A\,. &
\end{array}
\end{array}
$$

The masks ΓA and ΓB should be considered as the output mask of the immediately preceding R function. We have investigated these types of characteristics and found that the linear characteristic with the highest probability has the pattern

$$\Gamma A \rightarrow (L_4) \rightarrow \Gamma B \rightarrow (L_4) \rightarrow \Gamma A.$$

Its probability is 2^{-56} and we have found only one with that probability. We list it below:

$$\text{-}B\text{-}R_5{\times}R_5\text{-}B\text{-}R_3{\times}R_3\text{-}$$

$$\begin{array}{lll}
B & \left\{\begin{array}{c}(\texttt{0x204000a2 0x20000022 0 0x20400022})\\ \downarrow B\\ (\texttt{0 0 0 0x204000a2 0x00400000})\end{array}\right\} & 2^{-12}\\
R_5 & (\texttt{0 0}) \xleftarrow{F} (\texttt{0 0}) & 1\\
R_5 & (\texttt{0x204000a2 0x00040000}) \xleftarrow{F} (\texttt{0 0 0x20400022}) & 2^{-16}\\
B & \left\{\begin{array}{c}(\texttt{0 0 0x00040000 0 0x20400022})\\ \downarrow B\\ (\texttt{0 0 0 0x204000a2 0x20000022})\end{array}\right\} & 2^{-12}\\
R_3 & (\texttt{0 0}) \xleftarrow{F} (\texttt{0 0}) & 1\\
R_3 & (\texttt{0x204000a2 0x20000022}) \xleftarrow{F} (\texttt{0 0 0x20400022}) & 2^{-16}.
\end{array}$$

The probability 2^{-56} of the characteristic is much higher than $2^{-73.66}$, the probability of the two-round linear characteristic obtained from a one-round iterative one with the highest probability we have previously found. We use this characteristic in our linear attack on a reduced-round SC2000.

4 Differential Attack on 4.5-Round SC2000

We present an attack on a reduced-round SC2000 for 128-bit user key. By using a differential or linear characteristic with the highest probability obtained by our search, we can attack the following four-and-a-half-round SC2000:

$$I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I.$$

We illustrate in this section how we guess bits in subkeys by our differential attack. Our linear attack will be given in the next section.

Our differential attack utilizes the two-round iterative differential characteristic with probability 2^{-58} in Section 3.1.

By concatenating it twice (and removing one B round), we obtain a 3.5-round differential characteristic with probability 2^{-101}. We apply the characteristic as follows:

$$\text{Input-}\underbrace{B}_{(1)}\overbrace{\overset{0}{R}\text{-}\overset{16}{R}\text{-}\overset{11}{B}\text{-}\overset{0}{R}\text{-}\overset{16}{R}\text{-}\overset{15}{B}\text{-}\overset{0}{R}\text{-}\overset{16}{R}\text{-}\overset{11}{B}\text{-}\overset{0}{R}\text{-}\overset{16}{R}}^{101}\text{-}\underbrace{B}_{(2)}\text{-}\underset{K_1}{\oplus}\text{-Output},$$

where the numeral 15 above B should be read as "the differential probability through the B function is 2^{-15}." We present a list of the total differential probability according to the number of functions in the Appendix.

Using this differential characteristic, we can deduce 40 subkey bits in K_1, K_2. These subkey bits correspond to the 5 active S-boxes in the first B function and the 5 active S-boxes in the last B function.

We use the following algorithm to retrieve these 40 subkey bits:

- We encrypt 2^{84} structures, when each structure contains 2^{20} plaintexts which have the same value in the 108 in-active bits in the first B function, and vary over all possible values of the 20 active bits.
- In each structure we look for collisions in the 108 in-active output bits of the last B function.
- In case of a collision we analyze the pair of plaintexts and ciphertexts, and check for which subkey values the pair satisfy the differential characteristic. For each subkey which satisfy the characteristic we increment its counter by 1.
- In the end we go over all the subkey counters and output the subkey corresponding the the highest counter.

As each structure induce 2^{19} pairs after the B function which have the characteristic's input difference, thus, we have a total of 2^{103} pairs. The right subkey is expected to be suggested about 4 times. As in each structure the chance that two of the 2^{20} ciphertexts agree on the 108 in-active bits is about $(2^{20})^2/2 \cdot 2^{-108} = 2^{-69}$. The $2^{-69} \cdot 2^{84} = 2^{15}$ false hits vary over the $2^{40} - 1$ wrong subkeys, and we assured that with very high probability the suggested subkey is the correct one.

The time complexity of this attack (besides 2^{104} encryptions), is the time of hashing in each structure the ciphertexts according the 108 in-active bits, plus the time of analyzing the 2^{15} suggested pairs. The first term can be neglected as part of the encryptions, and the analysis time can be done in about 2^{20} memory accesses.

5 Linear Attack on 4.5-Round SC2000

We now present a linear attack on a reduced-round SC2000 for 128-bit user key. By using the linear characteristic with the highest probability obtained by our search, we can attack the following four-and-a-half-round SC2000:

$$I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I\text{-}R_5{\times}R_5\text{-}I\text{-}B\text{-}I\text{-}R_3{\times}R_3\text{-}I\text{-}B\text{-}I.$$

We illustrate how we can guess subkeys by our linear attack. We use the two-round iterative linear characteristic with probability 2^{-56} from Section 3.2. By concatenating it twice, we obtain a four-round linear characteristic with probability 2^{-112}. We illustrate two types of attacks; one utilizes the four-round linear characteristic, the other uses a three-and-a-half-round one obtained by eliminating the first B function from the four-round one. We illustrate both of them in due order.

5.1 Attack Using a Four-Round Characteristic

We use the following four-round linear characteristic with probability 2^{-112}:

$$\text{Input-}\overbrace{\underset{12}{B}\text{-}\underset{16}{R}\text{-}\underset{0}{R}\text{-}\underset{12}{B}\text{-}\underset{16}{R}\text{-}\underset{0}{R}\text{-}\underset{12}{B}\text{-}\underset{16}{R}\text{-}\underset{0}{R}\text{-}\underset{12}{B}\text{-}\underset{16}{R}\text{-}\underset{0}{R}}^{112}\text{-}\underbrace{B}_{(1)}\text{-}\underset{K_1}{\oplus}\text{-Output},$$

where the numeral 12 above B should be read as "the linear probability through the B function is 2^{-12}". We present a list of total linear probability according to the number of functions in the Appendix.

We can deduce 20 bits of subkeys in K_1, which consists of four 32-bit subkeys. In the last B function (1), output mask relates to only five S_4 S-boxes. As there are only 20 ciphertext bits which interest us, we can count the number of occurrences of each case, and do the analysis once for each 20-bit ciphertext value. The following algorithm can extract the 20 subkey bits:

- Initialize a 2^{20} counters array (corresponding to the 20 ciphertext bits which are related to the characteristic).
- Encrypt $2^{112} \cdot 9 = 2^{115.17}$ plaintexts.
- For each plaintext and its corresponding ciphertext add or subtract (according to the parity of the input subset) to/from the counter related to the 20 ciphertext bits.
- After counting all the occurrences of the 20 ciphertext bits, For each subkey and for each 20 bit value, calculate the parity of the output subset.
- Rank the subkey candidates according as its bias from 1/2.

The right subkey is expected to be highly ranked. The above algorithm reduce the subkey candidates by half and its time complexity is at most $2^{40} \cdot 5 = 2^{42.32}$ S_4 calls. The success rate for the above algorithm is at least 62.3%. We can use key ranking to enlarge the success rate without affecting the data complexity. We conclude that our linear attack requires $2^{115.17}$ known plaintexts and $2^{42.32}$ S_4 calls.

5.2 Attack Using a 3.5-Round Characteristic

We use the following linear characteristic with probability 2^{-100}:

$$\text{Input-}\underset{K_1}{\oplus}\text{-}\underbrace{B}_{(1)}\overbrace{\text{-}R\overset{16}{\text{-}}R\overset{0}{\text{-}}B\overset{12}{\text{-}}R\overset{16}{\text{-}}R\overset{0}{\text{-}}B\overset{12}{\text{-}}R\overset{16}{\text{-}}R\overset{0}{\text{-}}B\overset{12}{\text{-}}R\overset{16}{\text{-}}R}^{100}\text{-}\underbrace{B}_{(2)}\text{-}\underset{K_2}{\oplus}\text{-Output.}$$

We need to infer 20 bits each in K_1 and K_2.

By changing a little bit the above algorithm (taking into consideration 40 plaintext and ciphertext bits, and trying 40 subkey bits) we get that given $2^{104.32}$ known plaintexts the attack requires $2^{83.32}$ S_4 calls.

6 Conclusions

We have studied the security of SC2000 against differential and linear cryptanalysis. Taking the periodic structure of SC2000 into consideration, we have investigated two-round iterative characteristics whose differences/masks have a nonzero value in only one of the four S functions in each -B-R×R- cycle, and

found iterative differential characteristics with probability 2^{-58} and an iterative linear characteristic with probability 2^{-56}.

By utilizing the best differential or the best linear characteristic we have found, we presented differential and linear attack on four-and-a-half-round SC2000, respectively. Our differential attack needs 2^{104} pairs of chosen plaintexts and 2^{20} memory accesses, and our linear attack requires $2^{115.17}$ known plaintexts and $2^{42.32}$ S_4 calls, or $2^{104.32}$ known plaintexts and $2^{83.32}$ S_4 calls. Both differential and linear attacks can deduce 40 bits in the subkeys used in the first and last I function.

We stress that neither our differential nor our linear attack would work on full-round SC2000 which has six and a half rounds. The equivalent characteristics needed for attacking 6.5-round SC2000 has probability of 2^{-159} for the differential characteristic and 2^{-156} for the linear characteristic. We conclude that these figures show that these attacks cannot be applied to the full SC2000.

References

1. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems,* CRYPTO '90, LNCS 537, pp.2-21, 1991.
2. E. Biham and A. Shamir, *Differential Cryptanalysis of the Full 16-round DES,* CRYPTO '92, LNCS 740, pp.487-496, 1993.
3. CRYPTREC project - Evaluation of Cryptographic Techniques, *http://www.jpg.go.jp/security/enc/CRYPTREC/index-e.html*
4. O. Dunkelman and N. Keller, *Boomerang and Rectangle Attack on SC2000*, Proceedings of Second Open NESSIE Workshop, September 12-13, 2001.
5. Lars R. Knudsen and Håvard Raddum, *A first report on Whirlpool, NUSH, SC2000, Noekeon, Two-Track-Mac and RC6,* 2001. (`http://www.cosic.esat.kuleuven.ac.be/nessie/reports/`)
6. M. Matsui, *Linear Cryptanalysis Method for DES Cipher,* EUROCRYPT '93, LNCS 765, pp.386-397, 1994.
7. M. Matsui, *The First Experimental Cryptanalysis of the Data Encryption Standard,* CRYPTO '94, LNCS 839, pp.1-11, 1994.
8. M. Matsui, *On Correlation Between the Order of S-boxes and the Strength of DES,* EUROCRYPT '94, LNCS 950, pp.366-375, 1995.
9. NESSIE - New European Schemes for Signatures, Integrity and Encryption. *http://www.nessie.eu.org/nessie.*
10. H. Raddum, L. Knudsen, *A Differential Attack on Reduced-Round SC2000* Proceedings of Second Open NESSIE Workshop, September 12-13, 2001.
11. T. Shimoyama, H. Yanami, K. Yokoyama, M. Takenaka, K. Itoh, J. Yajima, N. Torii, H. Tanaka, *The SC2000 Block Cipher,* Proceedings of First Open NESSIE Workshop, November 13-14, 2000.
12. T. Shimoyama, H. Yanami, K. Yokoyama, M. Takenaka, K. Itoh, J. Yajima, N. Torii, H. Tanaka, *The Block Cipher SC2000,* Preproceedings of 8th Fast Software Encryption Workshop, April 2-4, 2001.
13. H. Yanami, T. Shimoyama, *Differential/Linear Characteristics of the SC2000 Block Cipher,* Proceedings of the 2001 Symposium on Cryptography and Information Security, SCIS2001-12A-2, pp.653-658, 2001, in Japanese.

14. H. Yanami, T. Shimoyama, *Differential/Linear Characteristics of the SC2000 Block Cipher (II),* IEICE Technical Report, ISEC2001-10, pp.63-70, 2001, in Japanese.
15. H. Yanami, T. Shimoyama, *Differential and Linear Cryptanalysis of Reduced-Round SC2000,* Proceedings of Second Open NESSIE Workshop, September 12-13, 2001.

Appendix

Differential distribution table of S_4

	ΔOut															
ΔIn	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	0	0	2	2	2	2	2	2	2	2	0	0
0x2	0	0	0	0	2	0	4	2	2	2	0	0	0	2	0	2
0x3	0	0	0	0	2	0	2	0	0	0	2	2	2	0	4	2
0x4	0	0	0	2	0	2	0	4	0	2	2	2	0	0	2	0
0x5	0	2	4	0	0	2	0	0	0	0	2	0	0	4	2	0
0x6	0	2	0	4	2	0	0	0	2	0	0	0	0	2	4	0
0x7	0	0	0	2	2	4	0	0	2	2	0	2	0	2	0	0
0x8	0	0	2	4	0	4	0	2	0	0	2	0	0	0	0	2
0x9	0	0	0	2	2	0	0	0	4	0	0	2	2	0	0	4
0xa	0	2	2	2	2	2	0	2	0	0	2	0	2	0	0	0
0xb	0	2	0	0	0	2	0	0	0	4	0	2	4	0	0	2
0xc	0	2	4	0	0	0	2	0	0	4	2	0	0	2	0	0
0xd	0	4	2	0	2	0	0	0	2	0	2	2	0	0	0	2
0xe	0	2	0	0	2	0	2	2	0	0	0	2	2	2	2	0
0xf	0	0	2	0	0	0	4	2	2	0	0	0	2	0	2	2

$(\mathrm{Prob} = \{\Delta In \rightarrow \Delta Out\} = x/16)$

Linear distribution table of S_4

	ΓOut															
ΓIn	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	2	2	-2	-2	4	0	0	4	2	-2	2	-2
0x2	0	0	0	0	-4	4	0	0	2	2	-2	-2	-2	-2	-2	-2
0x3	0	0	0	0	-2	-2	-2	-2	-2	2	-2	2	0	4	0	-4
0x4	0	2	2	-4	0	2	-2	0	0	2	-2	0	0	2	2	4
0x5	0	2	-2	0	2	4	0	2	-4	2	2	0	2	0	0	-2
0x6	0	-2	-2	-4	0	-2	-2	4	2	0	0	-2	2	0	0	-2
0x7	0	-2	2	0	2	0	0	-2	-2	0	-4	-2	4	-2	-2	0
0x8	0	-2	-2	0	0	2	-2	-4	0	-2	2	-4	0	2	2	0
0x9	0	2	-2	-4	2	0	4	-2	0	-2	-2	0	-2	0	0	-2
0xa	0	-2	-2	0	0	2	2	0	2	0	0	2	2	4	-4	2
0xb	0	2	-2	4	2	0	0	2	2	0	-4	-2	0	2	2	0
0xc	0	4	0	0	0	0	-4	0	0	-4	0	0	0	0	-4	0
0xd	0	0	-4	0	2	-2	-2	-2	0	4	0	0	-2	-2	-2	2
0xe	0	0	4	0	4	0	0	0	2	2	2	-2	-2	2	-2	-2
0xf	0	4	0	0	-2	-2	2	-2	2	2	2	-2	4	0	0	0

$(\mathrm{Prob}\{In \cdot \Gamma In + Out \cdot \Gamma Out = 0\} = x/16)$

Probability list obtained from our best differential characteristic

Number of functions	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Function name	B	R_5	R_5	B	R_3	R_3	B	R_5	R_5	B	R_3	R_3	B	R_5	R_5	B	R_3
Probability	15	0	16	11	0	16	15	0	16	11	0	16	15	0	16	11	0
Total probability	15	15	31	42	42	58	73	73	89	100	100	116	131	131	147	158	158

Probability list obtained from our best linear characteristic

Number of functions	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Function name	B	R_5	R_5	B	R_3	R_3	B	R_5	R_5	B	R_3	R_3	B	R_5	R_5	B	R_3
Probability	12	0	16	12	0	16	12	0	16	12	0	16	12	0	16	12	0
Total probability	12	12	28	40	40	56	68	68	84	96	96	112	124	124	140	152	152

This article was processed using the LaTeX macro package with LLNCS style