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 a unique structure that includes both the Feistel and Substitution-Permutation Network (SPN) structures. Taking the structure of SC2000 into account, we investigate one- and two-round iterative differential and linear characteristics. We present two-round iterative differential characteristics with probability 2^{-58} and two-round iterative linear characteristics with probability 2^{-56}. These characteristics, which we obtained through a search, allowed us to attack four-and-a-half-round SC2000 in the 128-bit user-key case. Our differential attack needs 2^{103} pairs of chosen plaintexts and 2^{20} memory accesses and our linear attack needs $2^{115.17}$ 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 initially introduced by Murphy [10] in an attack on FEAL-4 and was later improved by Biham and Shamir [1, 2] to attack DES. Linear cryptanalysis was first proposed by Matsui and Yamagishi [6] in an attack on FEAL and was extended by Matsui [7] to attack DES. Both methods are well known and often provide very effective means for attacking block ciphers. One of the many steps in establishing a cipher's security is to evaluate its strength against these attacks. The respective degrees of security of a cipher against differential attacks and linear attacks can be estimated from the maximum differential probability and the maximum linear probability. A cipher is considered to be secure against attacks of both types if both probabilities are low enough to make the respective forms of attack impractical.

SC2000 is a block cipher which was submitted to the NESSIE [11] and CRYPTREC [3] projects by Shimoyama et al. [13]. In the *Self-Evaluation Report,* one of 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. The strength of the SC2000 cipher has been evaluated in other published work on attacking SC2000 [3–5, 12, 17].

This paper is based on the work of Yanami and Shimoyama [17] at the 2nd NESSIE workshop, which is a report by the authors on investigation they carried out with both differential and linear attacks on a reduced-round SC2000. We use the same differential characteristics as was used in the above work in the work we describe here. This has a slightly higher probability than the characteristics that have been found by Raddum and Knudsen [12]. The linear cryptanalysis by Yanami and Shimoyama [17] contained some incorrect calculations. We have corrected these and re-examined the linear characteristics. Moreover, in this paper we use a better method of deducing the subkey bits. This new technique reduces the time complexity of the attacks by several orders of magnitude.

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

The paper is organized as follows. We briefly describe the encryption algorithm for SC2000 in Section 2. In Section 3, we illustrate our search method and show our search results. 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 which was submitted to the NESSIE [11] and CRYPTREC [3] projects by Shimoyama et al. [13]. SC2000 has a 128-bit block size and supports 128-/192-/256-bit user keys, and in these ways is the same as the AES.

Before proceeding further, we need to make two remarks: Firstly, we mainly take up the case of 128-bit user keys. 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 The Encryption Algorithm

Three functions are applied in the SC2000 encryption algorithm: the I, R and B functions. Each function has 128-bit input and output. The R functions used are of two types, which only differ in terms of a single constant (`0x55555555` or `0x33333333`). When we need to distinguish between the two types, we use R_5 and R_3 to indicate the respective constants.

The encryption function may be written as:

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

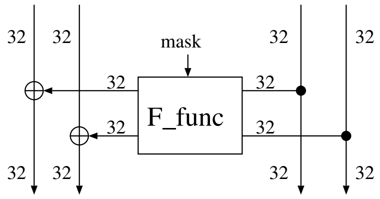

Fig. 1. The R function

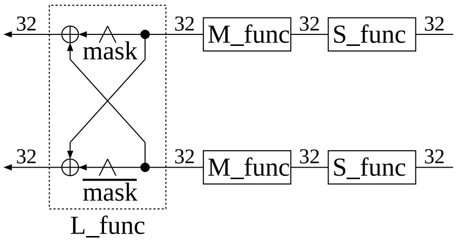

Fig. 2. The F function

where $\times$ stands for the exchange of the left and right 64 bits. We define -I-B-I-$R{\times}R$- as the round in SC2000. The round is iterated six times by the cipher and the final set of operations, -I-B-I, is then applied to obtain symmetry for encryption and decryption. For the sake of simplicity, we refer to the last part -I-B-I as half a round. SC2000 involves six and a half rounds with a 128-bit user key, and seven and a half rounds with a 192-/256-bit user key.

2.2 The *I* Function

The I function XORs a 128-bit input with four 32-bit subkeys. The I function divides the input into four 32-bit words, and then applies an XOR to each of these words and a corresponding 32-bit subkey. These subkeys are only used in the I function.

2.3 The *R* Function

The R function has a conventional Feistel structure, except for the swapping of the left and right 64 bits in its last part (Fig. 1). The F function is applied to the right 64 bits of the input, and the output of the function is XORed with the left 64 bits. The result of the XOR becomes the left half of the output of the R function. The right half of the output of the R function is the same as the right half of the input.

The input and output of the F function in the R function are both 64 bits; the function consists of three subfunctions, the S, M and L functions (Fig. 2).

The F function divides its input into two 32-bit variables and each variable is successively dealt with by the S and M functions. The two outputs become the input value for the L function, the output of which becomes the output of the F function. Note that the F function is bijective. We describe the S, M and L functions below.

The S function is a 32-bit input/output nonlinear function. The 32-bit input is divided into groups, in order, 6, 5, 5, 5, 5 and 6 bits. These groups of bits enter corresponding S-boxes; each of the two 6-bit groups enters S_6, while each of the four 5-bit groups enters S_5. The output of the S function is the concatenation of the outputs of the S-boxes. We refer to Shimoyama et al. [13] for the values in 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 that are elements of $GF(2)$, the Galois field of order two, and a and b are row vectors with entries from $GF(2)$. We refer to Shimoyama et al. [13] for the entries of the matrix M.

The L function has two 32-bit variables as its input and output. We use (a, b) to denote the input and (c, d) to denote the corresponding output. The variables c and d are obtained by applying the following formulae:

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

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

2.4 The B Function

The B function has an SPN structure with 128-bit input/output which contains the thirty-two 4-bit input/output S-boxes. This structure is similar to the one that is used in the Serpent block cipher. We can use a bitslice approach to implement the B function. We represent the input to the B function as (a, b, c, d), where each variable has 32 bits; the i-th bit of a is a_i, and equivalent notation applies to b, c and d. For $i = 0, 1, \ldots, 31$, the i-th bit is taken from each of the variables a, b, c and d, and the resulting four bits (a_i, b_i, c_i, d_i) are replaced by (e_i, f_i, g_i, h_i) according to the S_4 table, where the notation is analogous to that for (a, b, c, d) above, and (e, f, g, h) denotes the four 32-bit words which compose the output of the B function. We refer to Shimoyama et al. [13] for the values in the S_4 table. Note that if the B functions in SC2000 are all replaced by the swapping of the left and right 64 bits, the resulting structure becomes the classical Feistel structure.

3 The Differential and Linear Characteristics of SC2000

In investigating the differential/linear characteristics of a block cipher, it is very hard to compute the probability of every characteristic by applying an exhaustive search to the cipher itself. Roughly speaking, the following strategy is often used to construct a long characteristic that has a high probability. 1) Examine few-round iterative characteristics, i.e., characteristics of the same input and output differences/masks appearing at intervals of a few rounds. 2) Iterate the one with the highest differential/linear probability which was found by the search to make a characteristic for larger numbers of rounds. We will follow this strategy in examining the differential/linear characteristics.

In the SC2000 encryption algorithm, the I functions are merely used for XORing data with subkeys, so we can eliminate them from our examination of differential/linear relationships. Removing these functions leaves the following sequence:

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

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

3.1 Differential Characteristics

We explain our efficient way of searching for an iterative differential characteristic that has a high probability. We start by reviewing the nonlinear functions of SC2000. They are all realized by the S-boxes, S_4, S_5 and S_6. There are thirty-two S_4 boxes in the B function and eight S_5 boxes and four S_6 boxes in the R function. The S function is made up of four S_5 boxes and two S_6 boxes; there are two S functions in the R function. In the differential distribution tables for the S-boxes, we see that given a pair of nonzero input and output differences, the differential probability for S_4 is either 2^{-2} or 2^{-3}, while for S_5 it is 2^{-4} and for S_6 it is either 2^{-4} or 2^{-5}. These facts suggest that the number of nonzero differences for the S_5 and S_6 boxes in the S function will have a stronger effect on the overall differential probability of characteristics than the number for the S_4 boxes in the B function.

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

One-Round Characteristics. We investigate those one-round iterative characteristics that have a nonzero difference in a single one of the four S functions

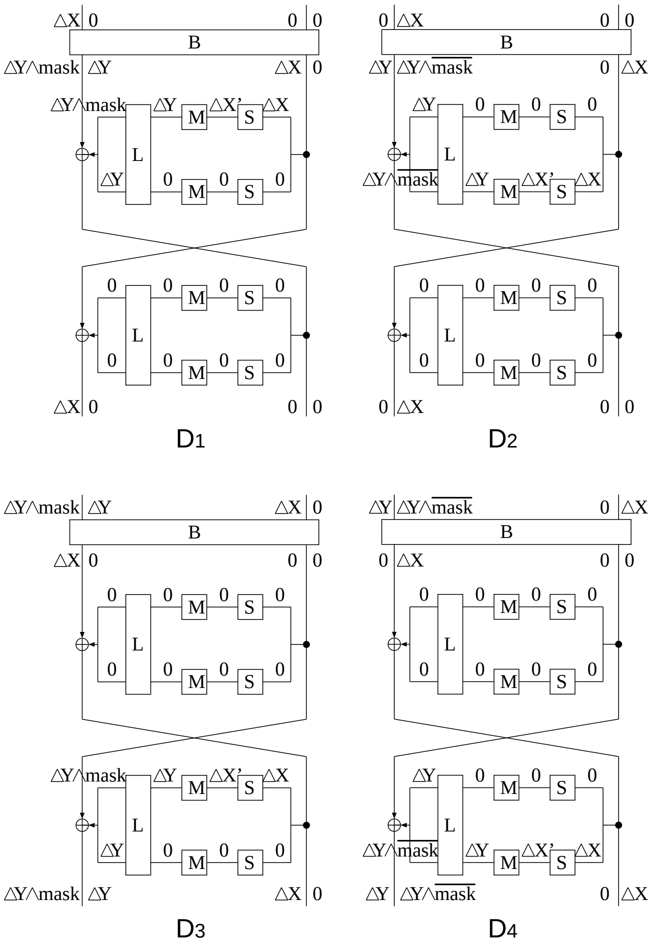

Fig. 3. Patterns of differences

in a -B-R×R- cycle. We illustrate the differential patterns of the characteristics we need to investigate in Fig. 3.

We call the respective types of differential pattern D_1, D_2, D_3 and D_4, according to the position of the S function that has a nonzero difference.

We have investigated differential characteristics that have these patterns for both -B-R_5×R_5- and -B-R_3×R_3-. We have found differential characteristics that have a probability of 2^{-33} in both cycles. This is the highest probability for differential characteristics of the four types mentioned above. These characteristics are of type D_3. We give an example of one such differential characteristic:

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

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

Note that this characteristic has a probability of 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 this characteristic n times.

Two-Round Characteristics. By distinguishing R_5 from R_3, we are also able to treat -B-$R_5{\times}R_5$-B-$R_3{\times}R_3$- as a cycle. Turning our attention to this cycle, we have investigated those two-round iterative characteristics which have a nonzero difference in a single one of the four S functions in each -$R{\times}R$- part. It would appear that we are able to independently choose differential patterns from among D_i $(i = 1, 2, 3, 4)$ for the former -B-$R_5{\times}R_5$- and latter -B-$R_3{\times}R_3$- sequence, but some patterns cannot be concatenated. We can judge whether or not it is possible to concatenate D_i and D_j from the differential distribution table of S_4 (see the Appendix). Below we list the pairs that may be concatenated and thus need to be investigated:

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

Note that differences ΔA's and ΔB's in the above list should be adjusted as required: When, for example, the former pattern is D_1 and the latter is D_2, we think of ΔA as $(0, \Delta X, 0, 0)$ and ΔB as $(\Delta X, 0, 0, 0)$, adopting the respective output differences of the preceding R functions. We have investigated characteristics of the above types 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 a characteristic is given below:

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

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

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

3.2 Linear Characteristics

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

We investigate the linear characteristics in the same way as the iterative differential characteristics, i.e., we examine the linear characteristics with a nonzero mask in a single one of the four S functions in a -B-R×R- cycle.

One-Round Characteristics. We investigate those one-round iterative characteristics whose masks have a nonzero value in a single one of the four S functions in a -B-R×R- cycle. We illustrate the mask patterns of the characteristics we investigate in Fig. 4. We call the respective types of mask pattern L_1, L_2, L_3 and L_4, according to the position of the S function that has a nonzero mask.

We investigated characteristics of these types and found that the linear characteristics with the highest probability have probabilities of $2^{-28.83}$ for -B-R_5×R_5- and of 2^{-28} for -B-R_3×R_3-. All of them are of type L_2. Below, we give examples of such linear characteristics for both -B-R_5×R_5- and -B-R_3×R_3-:

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

$$\begin{array}{lllll}
B & \left\{\begin{array}{l}(\;0\;\;0\;\;\texttt{0x84380080}\;\;\texttt{0x04100000}) \\ \qquad\qquad\downarrow_B \\ (\texttt{0x84380080}\;\;\texttt{0x04100000}\;\;0\;\;\texttt{0x84180000})\end{array}\right\} & & & 2^{-20} \\
R_5 & (\texttt{0x84380080}\;\;\texttt{0x04100000}) & \xleftarrow{F} & (0\;\;\texttt{0x84180000}) & 2^{-8.83} \\
R_5 & (0\;\;0) & \xleftarrow{F} & (0\;\;0) & 1,
\end{array}$$

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

$$\begin{array}{lllll}
B & \left\{\begin{array}{l}(\;0\;\;0\;\;\texttt{0x12020040}\;\;\texttt{0x12020000}) \\ \qquad\qquad\downarrow_B \\ (\texttt{0x12020040}\;\;\texttt{0x12020000}\;\;0\;\;\texttt{0x12020040})\end{array}\right\} & & & 2^{-10} \\
R_3 & (\texttt{0x12020040}\;\;\texttt{0x12020000}) & \xleftarrow{F} & (0\;\;\texttt{0x12020040}) & 2^{-18} \\
R_3 & (0\;\;0) & \xleftarrow{F} & (0\;\;0) & 1.
\end{array}$$

† In Yanami and Shimoyama [17], the authors used 2^{-2} or 2^{-3} for this probability, which turned out to be wrong. We have re-examined linear characteristics with the correct values.

It is not possible for these characteristics to pass through the sequence when the constant is changed into the other one. The highest probability for any linear characteristics which do pass through both constants is $2^{-36.83}$. An example of such a linear characteristic is:

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

$$\begin{array}{lrcll}
B & \left\{\begin{array}{l}(\texttt{0} \quad \texttt{0} \; \texttt{0x11108008} \; \texttt{0x11100000})\\ \qquad\qquad \downarrow_B \\ (\texttt{0x11108008} \; \texttt{0x11100000} \quad \texttt{0} \; \texttt{0x11108008})\end{array}\right\} & & & 2^{-14}\\
R & (\texttt{0x11108008} \; \texttt{0x11100000}) & \xleftarrow{F} & (\texttt{0} \; \texttt{0x11108008}) & 2^{-22.83}\\
R & (\texttt{0} \quad \texttt{0}) & \xleftarrow{F} & (\texttt{0} \quad \texttt{0}) & 1.
\end{array}$$

We are able to construct an n-round linear characteristic with probability $2^{-36.83n}$ by concatenating the above characteristic n times.

Two-Round Characteristics. We can apply the same method as we used for the differential case. We can use the linear distribution table of S_4 to judge whether or not L_i and L_j can be concatenated (see the Appendix). Below, we list those pairs that need to be investigated:

$$\begin{array}{ccc}
\text{-}B\text{-}R_5{\times}R_5\text{-} \quad \text{-}B\text{-}R_3{\times}R_3\text{-} & \qquad & \text{-}B\text{-}R_5{\times}R_5\text{-} \quad \text{-}B\text{-}R_3{\times}R_3\text{-}\\
\Gamma A \to (L_1) \to \Gamma B \to (L_1) \to \Gamma A & & \Gamma A \to (L_1) \to \Gamma B \to (L_2) \to \Gamma A\\
\Gamma A \to (L_2) \to \Gamma B \to (L_2) \to \Gamma A & & \Gamma A \to (L_2) \to \Gamma B \to (L_1) \to \Gamma A\\
\Gamma A \to (L_3) \to \Gamma B \to (L_3) \to \Gamma A & & \Gamma A \to (L_3) \to \Gamma B \to (L_4) \to \Gamma A\\
\Gamma A \to (L_4) \to \Gamma B \to (L_4) \to \Gamma A & & \Gamma A \to (L_4) \to \Gamma B \to (L_3) \to \Gamma A\ .
\end{array}$$

The masks ΓA and ΓB should be considered as the masks output by the immediately preceding R functions, respectively. We have investigated characteristics of the above types and found that the linear characteristics with the highest probability have the pattern

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

The probability of these linear characteristics is 2^{-56}. We list a example of such a characteristic below:

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

$$\begin{array}{lrcll}
B & \left\{\begin{array}{l}(\texttt{0x204000a2} \; \texttt{0x20000022} \quad \texttt{0} \; \texttt{0x20400022})\\ \qquad\qquad \downarrow_B \\ (\texttt{0} \quad \texttt{0} \; \texttt{0x204000a2} \; \texttt{0x00400000})\end{array}\right\} & & & 2^{-12}\\
R_5 & (\texttt{0} \quad \texttt{0}) & \xleftarrow{F} & (\texttt{0} \quad \texttt{0}) & 1\\
R_5 & (\texttt{0x204000a2} \; \texttt{0x00400000}) & \xleftarrow{F} & (\texttt{0} \; \texttt{0x20400022}) & 2^{-16}\\
B & \left\{\begin{array}{l}(\texttt{0x204000a2} \; \texttt{0x00400000} \quad \texttt{0} \; \texttt{0x20400022})\\ \qquad\qquad \downarrow_B \\ (\texttt{0} \quad \texttt{0} \; \texttt{0x204000a2} \; \texttt{0x20000022})\end{array}\right\} & & & 2^{-12}\\
R_3 & (\texttt{0} \quad \texttt{0}) & \xleftarrow{F} & (\texttt{0} \quad \texttt{0}) & 1\\
R_3 & (\texttt{0x204000a2} \; \texttt{0x20000022}) & \xleftarrow{F} & (\texttt{0} \; \texttt{0x20400022}) & 2^{-16}.
\end{array}$$

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

4 A Differential Attack on 4.5-Round SC2000

We now present our attack on a reduced-round SC2000 with 128-bit user key. By using a differential or linear characteristic with the highest probability which we had obtained in our search, we were able to attack the following four-and-a-half-round SC2000:

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

In this section, we illustrate how we use our differential attack to guess some bits in subkeys. Our linear attack will be described in the next section.

Our differential attack utilizes the two-round iterative differential characteristic with probability 2^{-58}, which we mentioned in Section 3.1. By concatenating the two-round differential characteristic we mentioned in Section 3.1 twice (and removing one B function), we obtain a three-and-a-half-round differential characteristic with probability 2^{-101}. We apply the characteristic in the following way:

$$\text{Input-}\underset{K_1}{\oplus}\text{-}\underbrace{B}_{(1)}\text{-}\overbrace{\overset{0}{R}\text{-}\overset{16}{R}\text{-}\overset{11}{B}\text{-}\overset{0}{R}\text{-}\overset{16}{R}\text{-}\overset{15}{B}\text{-}\overset{0}{R}\text{-}\overset{16}{R}\text{-}\overset{11}{B}\text{-}\overset{0}{R}\text{-}\overset{16}{R}}^{101}\text{-}\underbrace{B}_{(2)}\text{-}\underset{K_2}{\oplus}\text{-Output},$$

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

By using this differential characteristic, we are able to deduce 40 bits in the subkeys K_1 and K_2. These subkey bits correspond to the five active S-boxes of the first B function and the five active S-boxes of the last B function. We used the following algorithm to retrieve these 40 bits in the subkeys K_1 and K_2:

- We start by encrypting 2^{84} structures, where each structure contains 2^{20} plaintexts which have the same value in the 108 inactive bits in the first B function, and with the 20 active bits varying across all possible values.
- In each structure we look for collisions in the 108 inactive output bits of the last B function.
- When a collision is detected, we analyze the pair of plaintexts and ciphertexts, and check for the subkey values where the pair satisfied the differential characteristic. For each subkey which satisfies the characteristic, we increment the counter by 1.
- In the end, we go over all of the subkey counters and output the subkey that corresponds to counter with the highest number.

As each structure induces 2^{19} pairs, we have in total 2^{103} pairs which have the same input difference as the input of the characteristic above after the B function. We would expect the right subkey to be suggested about four times. Since in each structure the chance that two of the 2^{20} ciphertexts will agree is about $(2^{20})^2/2 \cdot 2^{-108} = 2^{-69}$, we would also expect $2^{-69} \cdot 2^{84} = 2^{15}$ false hits varying over all the 2^{40} possible subkeys, These false hits have few effects on subkey-counting. Thus, we are assured with a very high probability that the suggested subkey is the correct one.

The time complexity of this attack (aside from the 2^{104} encryptions) is the time taken to hash the ciphertexts in each structure according to the 108 inactive bits, plus the time taken to analyze the 2^{15} suggested pairs. The first term may be neglected as representing part of the encryption, and the analysis can be done in about 2^{20} memory accesses.

5 Linear Attacks on 4.5-Round SC2000

We now present our linear attack on a reduced-round SC2000 with 128-bit user key. By using the linear characteristic with the highest probability which we had obtained in our search, we are able to 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 now illustrate how we use the linear attack to guess subkeys. We use the two-round iterative linear characteristic with probability 2^{-56} from Section 3.2. By concatenating this characteristic twice, we obtain a four-round linear characteristic with probability 2^{-112}. We illustrate two types of attacks; in one, the four-round linear characteristic is used; in the other, the three-and-a-half-round characteristic obtained by eliminating the first B function from the four-round one is used. We illustrate both attacks in due order.

5.1 Attack Using a Four-Round Characteristic

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

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

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

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

– Initialize a 2^{20} array of counters (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 1 (according to the parity of the input subset) to/from the counter related to the given 20 ciphertext bits.
– After counting all occurrences of the given 20 ciphertext bits, for each subkey and for each 20 bit value, calculate the parity of the output subset.
– Rank the subkey candidates according to their respective biases from 1/2.

We expect the right subkey to be highly ranked, and on this basis guess that the top-ranked candidate is the right subkey. The time complexity of the above algorithm 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 improve the success rate without affecting the complexity of the data. We conclude that our linear attack requires $2^{115.17}$ known plaintexts and $2^{42.32}$ S_4 calls.

5.2 Attack Based on a 3.5-Round Characteristic

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

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

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

By making a small change to the above algorithm (taking the 40 plaintext and ciphertext bits into consideration, and trying 40 subkey bits) we obtain the result 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 in which the differences or masks have a nonzero value in only one of the four S functions in each -B-$R{\times}R$- cycle, and found iterative differential characteristics with probability 2^{-58} and iterative linear characteristics with probability 2^{-56}.

We respectively utilized the best differential and best linear characteristic we found. We have presented both differential and linear attacks on the four-and-a-half-round SC2000. 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. Either attack is capable of deducing 40 bits in the subkeys used in the first and last I functions.

We stress that neither our differential nor our linear attack would work on the full-round SC2000, which has six and a half rounds. The equivalent differential and linear characteristics needed to attack 6.5-round SC2000 has respective probabilities of 2^{-159} and 2^{-156}. We conclude that these figures show that these attacks are not applicable to the full-round 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.ipa.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. L. R. Knudsen and H. 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 and A. Yamagishi, *A new method for known plaintext attack of FEAL cipher,* EUROCRYPT '92, LNCS 658, pp.81-91, 1993.
7. M. Matsui, *Linear Cryptanalysis Method for DES Cipher,* EUROCRYPT '93, LNCS 765, pp.386-397, 1994.
8. M. Matsui, *The First Experimental Cryptanalysis of the Data Encryption Standard,* CRYPTO '94, LNCS 839, pp.1-11, 1994.
9. M. Matsui, *On Correlation Between the Order of S-boxes and the Strength of DES,* EUROCRYPT '94, LNCS 950, pp.366-375, 1995.
10. S. Murphy, *The cryptanalysis of FEAL-4 with 20 chosen plaintexts,* Journal of Cryptology 2(3), pp.145-154, 1990.
11. NESSIE - New European Schemes for Signatures, Integrity and Encryption. (`http://www.nessie.eu.org/nessie`)
12. H. Raddum, L. Knudsen, *A Differential Attack on Reduced-Round SC2000* Proceedings of Second Open NESSIE Workshop, September 12-13, 2001.
13. 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.
14. 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.
15. 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.
16. H. Yanami, T. Shimoyama, *Differential/Linear Characteristics of the SC2000 Block Cipher (II),* IEICE Technical Report, ISEC2001-10, pp.63-70, 2001, in Japanese.
17. 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

(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

(Prob$\{In \cdot \Gamma In + Out \cdot \Gamma Out = 0\} - 1/2 = x/16$)

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

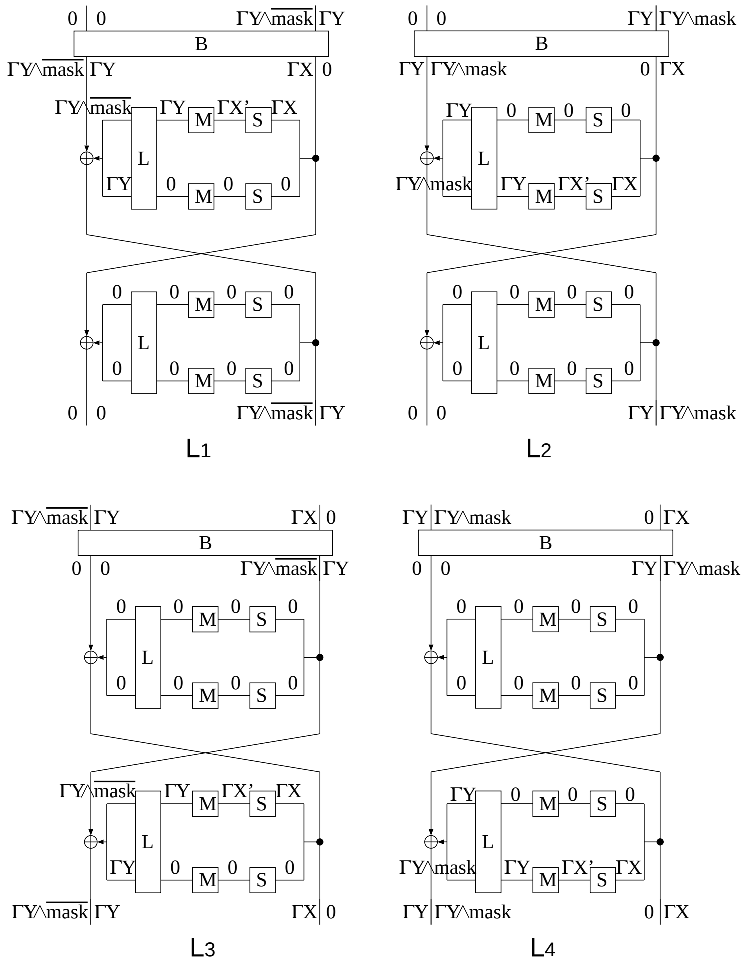

Fig. 4. Patterns of masks