Improved Truncated Differential Attacks on SAFER

Hongjun Wu[*] Feng Bao[**] Robert H. Deng[**] Qin-Zhong Ye[*]

[*]Department of Electrical Engineering
National University of Singapore
Singapore 1 19260

[**]Information Security Group
Kent Ridge Digital Labs
Singapore 119613

Abstract. Knudsen and Berson have applied truncated differential attack on 5 round SAFER K-64 successfully. However, their attack is not efficient when applied on 5 round SAFER SK-64 (with the modified key schedule) and can not be applied on 6 round SAFER.

In this paper, we improve the truncated differential attack on SAFER by using better truncated differential and additional filtering method. Our attack on 5 round SAFER (both SAFER K-64 and SAFER SK-64) can find the secret key much faster than by exhaustive search. Also, the number of chosen plaintexts required are less than those needed in Knudsen and Bersonís attack. Our attack on 6 round SAFER (both SAFER K-64 and SAFER SK-64) can find the secret key faster than by exhaustive search.

1 Introduction

In [6], Massey proposed an encryption algorithm, SAFER K-64. It is an iterated block cipher with 64-bit block size. The suggested number of rounds is minimum 6 and maximum 10 [6,7]. Knudsen discovered a weakness in the key schedule of SAFER and suggested a modified version [3]. Later, this new key schedule was adopted by Massey which resulted in SAFER SK-64 [8]. Also, Massey suggested 8 rounds to be used for SAFER with 64-bit key. The other variants of SAFER with 128-bit key are SAFER K-128 and SAFER SK-128 corresponding to SAFER K-64 and SAFER SK-64, respectively.

Evidence was given in [7] that SAFER is secure against differential cryptanalysis [1] after 5 rounds. In [2], SAFER is shown to be secure against linear cryptanalysis [9] after 2 rounds. In [5], Knudsen and Berson applied truncated differential cryptanalysis [6] on 5 round SAFER K-64 successfully. Their result showed that the secret key of 5 round SAFER K-64 can be found much faster than by exhaustive search. However, their attack is not efficient when applied on 5 round SAFER SK-64. Also, their attack cannot be extended to attack 6 round SAFER since too many wrong pairs are not filtered out.

In this paper, we improve the truncated differential cryptanalysis and apply it on 5 round and 6 round SAFER. We propose better truncated differential and additional filtering method in our attacks. For 5 round SAFER (both SAFER K-64 and SAFER SK-64), our truncated differential is with probability of about 2^{-69} in average and about 2^{38} chosen plaintexts (a large reduction in the amount of chosen plaintexts) are needed to find the secret key. This attack runs in time similar to 2^{46} encryptions of 5-round SAFER. For 6 round SAFER, our truncated differential has a probability of about 2^{-84}

K. Ohta and D. Pei (Eds.): ASIACRYPTí98, LNCS 1514, pp. 133-147, 1998.

and about 2^{53} chosen plaintexts are needed. This attack runs in time similar to 2^{61} encryptions of 6-round SAFER.

The paper is organised as follows. Section 2 briefly reviews the SAFER algorithms. Section 3 introduces Knudsen and Bersonís truncated differential attack on 5 round SAFER K-64. In Section 4, we present our attack on 5 round SAFER. Our attacks on 6 round SAFER are given in Section 5. Section 6 discusses the strength of 7 round SAFER and Section 7 concludes the paper.

2 Description of SAFER

SAFER K-64 is an iterated block cipher with both block and key sizes of 64 bits and with all the operations done on bytes. The key is expanded to $2r + 1$ round keys each of 8 bytes, where the round number r was suggested to be 6 [6] and then 8 [8], respectively. Each round takes 8 bytes of text input and two round keys each of 8 bytes. Each round consists of 4 layers as shown in Fig. 1.

The first layer consists of xoríing or adding modulo 256 with the first round key. In the second layer, the 8 bytes pass through two permutations or S-boxes: $X(a) = (45^a \bmod 257) \bmod 256$, and the inverse of X, $L(a) = \log_{45}(a) \bmod 257$ for $a \neq 0$ and $L(0) = 128$. The third layer consists of adding modulo 256 or xoríing with the second round key. The final layer is the *Pseudo-Hadamard Transformation (PHT)*. It is defined by three layers of the 2-*PHT*:

$$2\text{-}PHT(x, y) = (2x + y, x + y)$$

where each coordinate is taken modulo 256. After the last round, an output transformation is applied, which consists of xoríing or adding modulo 256 with the last round key and is the same as the first layer of the round operation. We call this the last half round in the rest of the paper.

The PHT-transformation is simply described by a matrix M [6]. Let the input be a vector $v = [v_1, v_2, \ldots v_8]$, then the output is obtained by $v \cdot M$. M and its inverse M^{-1} are given, respectively, by

$$M = \begin{pmatrix} 8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \\ 4 & 2 & 4 & 2 & 2 & 1 & 2 & 1 \\ 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 4 & 4 & 2 & 2 & 2 & 2 & 1 & 1 \\ 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad M^{-1} = \begin{pmatrix} +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \\ -1 & +1 & +1 & -1 & +2 & -2 & -2 & +2 \\ -1 & +2 & +1 & -2 & +1 & -2 & -1 & +2 \\ +1 & -2 & -1 & +2 & -2 & +4 & +2 & -4 \\ -1 & +1 & +2 & -2 & +1 & -1 & -2 & +2 \\ +1 & -1 & -2 & +2 & -2 & +2 & +4 & -4 \\ +1 & -2 & -2 & +4 & -1 & +2 & +2 & -4 \\ -1 & +2 & +2 & -4 & +2 & -4 & -4 & +8 \end{pmatrix} \qquad (1)$$

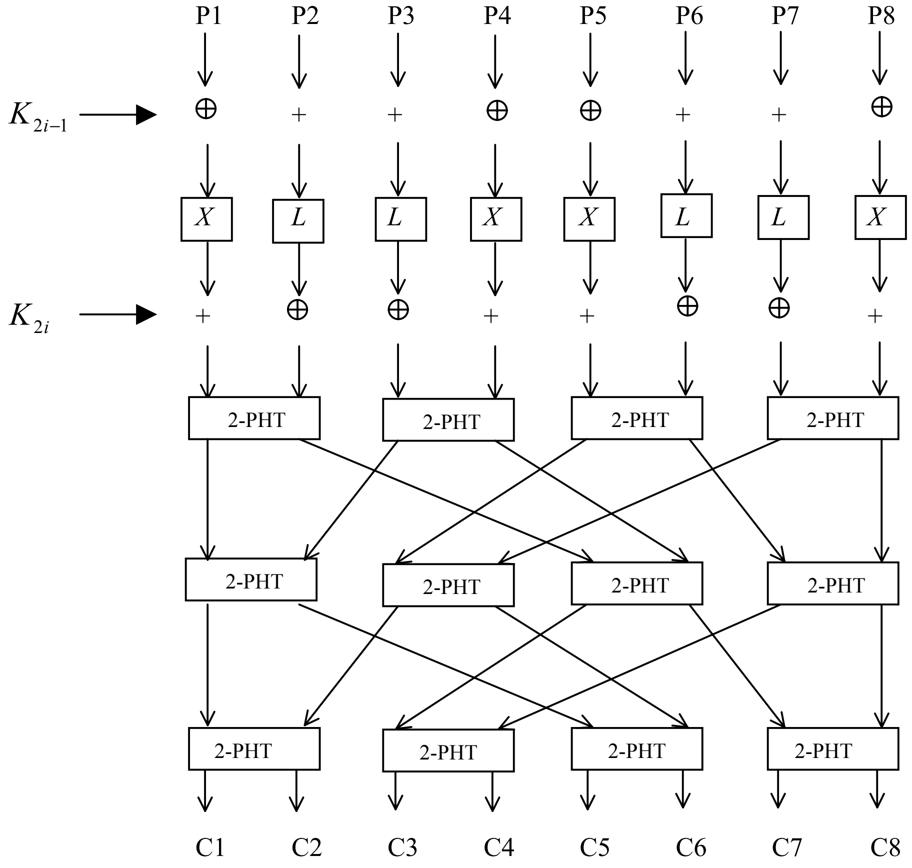

Fig. 1. One round of SAFER

The 8-byte key is expanded to $2r+1$ round keys each of 8 bytes. The original key schedule works as follows. Let $K=(k_1,\ldots,k_8)$ be an 8-byte key. The round key byte *j* in round *i* is denoted as $K_{i,j}$. The round key bytes are derived as follows:

```
for $j$ = 1,2,...8: $K_{1,j} = t_{1,j} = k_j$
for $i$ = 2,...,2$r$ + 1,
    for $j$ = 1,2,...8: $t_{i,j} = t_{i-1,j} << 3$
    for $j$ = 1,2,...8: $K_{i,j} = (t_{i,j} + bias[i,j]) \bmod 256$
```

where ë<<3í is a bitwise rotation 3 positions to the left and $bias[i,j] = X[X[9i+j]]$, where X is the exponentiation permutation.

Knudsen suggested a modified key schedule for SAFER to eliminate the key schedule weakness found by him [3]. Later, this key schedule was adopted for SAFER by Massey in [8]. The original SAFER is now called SAFER K-64 and the one with the modified key schedule is called SAFER SK-64. The new key schedule is given below.

```
$k_9 = \oplus_{i=1}^{8} k_i$
for $j$ = 1,2,...9: $t_{1,j} = k_j$
for $j$ = 1,2,...8: $K_{1,j} = t_{1,j}$
for $i$ = 2,..., 2r + 1:
        for $j$ = 1,2,...9: $t_{i,j} = t_{i-1,j} << 3$
        for $j$ = 1,2,...8:
$K_{i,j} = (t_{i,(i+j-2 \bmod 9)+1} + bias[i,j]) \bmod 256$
```

The 128-bit version of SAFER differs from the 64-bit version SAFER in the suggested number of rounds which is 10 and in the key schedule [7]. The key schedule consists of two sub-schedules each dealing with 64-bit key separately. The odd number round keys are taken from the first sub-schedule and the even number round keys from the second. A 128-bit schedule is compatible with its 64-bit version if the two 64-bit key halves input to the key schedule are equal.

3 Knudsen and Berson's Truncated Differential Attack on SAFER

Knudsen introduced the concept of truncated differential attack in [4]. Truncated differential is a differential that predicts only parts of an *n*-bit value. Knudsen and Berson applied truncated differential attack on 5 round SAFER K-64 successfully [5]. Their attack can find the key in time much faster than by exhaustive search. One version of their attack needs about 2^{45} chosen plaintexts and runs in time similar to 2^{46} encryptions of 5-round SAFER. Another version of their attack needs about 2^{46} chosen plaintexts and runs in time similar to 2^{35} encryptions of 5-round SAFER. We introduce their truncated differential attack on SAFER below.

3.1 Truncated Differential of SAFER

The notation of ìexpanded viewî from [7] is used to denote a one round differential by three tuples of each 8 entries. The first tuple indicates the difference in the 8 bytes of the inputs to the round, the second tuple indicates the difference of the bytes before the PHT-transformation and the third tuple indicates the difference of the bytes after the PHT-transformation, i.e. the difference of the outputs of the round (it is also the difference of the inputs of the next round). A difference of two bytes (a,b) is defined as

$$(a-b) \bmod 256 .$$

The one round truncated differential is obtained from the properties of the PHT-transformation and *S* boxes $(X \text{ and } L)$. The properties of the PHT-transformation is obtained from the matrix *M*. These properties are also listed in the six tables (table 4 to table 10) of [7]. The properties of the *S* boxes $(X \text{ and } L)$ used in obtaining the round differential are listed in table 3 of [6]. Knudsen and Berson listed the one round truncated differentials (together with the probability) for SAFER with inputs different in less than or equal to four bytes in table 2 and table 3 of [5]. For example, the following one round truncated differential is with probability 2^{-24}:

[0, 0, a, b, 0, 0, c, d], [0, 0, e, -e, 0, 0, -e, e], [e, 0, 0, 0, e, 0, 0, 0]

It is denoted simply as

$$3478 \rightarrow 15, \quad p = 2^{-24}$$

where 3478 denotes that the inputs are different at the bytes 3, 4, 7 and 8 and where 15 denotes that the outputs are different at the bytes 1 and 5.

One round truncated differentials can be concatenated to get truncated differentials of more than one round. For examples, the following one round truncated differentials

$$3478 \rightarrow 15, \quad p = 2^{-24} \qquad \text{and} \qquad 15 \rightarrow 1357, \qquad p = 2^{-8}$$

are concatenated to get a two round truncated differential

$$3478 \rightarrow 15 \rightarrow 1357, \quad p = 2^{-32}$$

However, when the one round truncated differentials are concatenated, its feasibility need be considered. This problem has been mentioned in [7]. Specifically, we note that the input difference of 128 to the S boxes cannot result in output difference of 128. Thus some one round truncated differential like 24→24 cannot be concatenated with itself. It is also noted that the input difference of 128 to the exponential permutation X results in odd output difference. Thus some one round differentials like 5→78 and 78→3478 cannot be concatenated.

3.2 Knudsen and Berson's Truncated Differential Attack on 5 Round SAFER K-64

Before introducing Knudsen and Bersonís truncated differential attack on 5 round SAFER, the proposition 4 in [7] is given below:

Proposition 1. *For byte differences* $\Delta V = V \oplus V^*$ *and* $\widetilde{\Delta} V = V - V^*$,

a) $\widetilde{\Delta} V$ *= 0 if and only if* ΔV *= 0;*

b) $\widetilde{\Delta} V$ *= 128 if and only if* ΔV *= 128;*

c) $\widetilde{\Delta} V$ *is odd if and only if* ΔV *is odd.*

Knudsen and Bersonís attack on 5 round SAFER K-64 uses the following 4-round truncated differential with input difference

$$[a, 0, 0, b, c, 0, 0, d]$$

and output difference [0, 0, 0, 128, 0, 0, 0, 0]. There are four differentials in this truncated differential which are listed below. The first two differentials are with probability of $2^{-71.68}$. The last two differentials are each of probability $2^{-72.19}$, not $2^{-71.7}$ as stated in [5]. However, this small error does not affect Knudsen and Bersonís attack too much.

$$1458 \rightarrow 1357 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \qquad (2)$$
$$1458 \rightarrow 2468 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \qquad (3)$$
$$1458 \rightarrow 1357 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \qquad (4)$$
$$1458 \rightarrow 2468 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \qquad (5)$$

The probabilities in the first two rounds are each of 2^{-16} and the probability in the third round is 2^{-24}. Now we look at the differential in the fourth round. For the first two differentials, the differential in the fourth round is

$$[2v, 0, v, 0, 0, 0, 0, 0],\ [128, 0, 128, 0, 0, 0, 0, 0],\ [0, 0, 0, 128, 0, 0, 0, 0]$$

This round has probability $2^{-15.68}$, which can be found by direct calculation. However, for the last two differentials, the differential in the forth round is

$$[v, 0, v, 0, 0, 0, 0, 0],\ [128, 0, 128, 0, 0, 0, 0, 0],\ [0, 0, 0, 128, 0, 0, 0, 0]$$

This round has a probability of $2^{-16.19}$, which is also found by direct calculation. So the probabilities are each of $2^{-71.68}$ for the first two differentials and $2^{-72.19}$ for the last two differentials. The probability for the 4-round differential is thus $2^{-69.9}$, not $2^{-69.7}$ as stated in [5]. This 4-round differential is concatenated with the fifth round differential

$$[0, 0, 0, 128, 0, 0, 0, 0],\ [0, 0, 0, x, 0, 0, 0, 0],\ [2x, x, 2x, x, 2x, x, 2x, x]$$

where the value of x is odd. This differential has probability 1 since the input difference 128 to the exponential permutation table always yields an odd output difference.

After the final output transformation consisting of byte wise xoríing and addíing with the last round key, the output difference is:

$$[z_1, x, 2x, z_2, z_3, x, 2x, z_4] \qquad (6)$$

where x is odd, z_1 and z_3 are even number while z_2 and z_4 are odd number according to c) of proposition 1.

The probability for this truncated differential is $2^{-69.9}$. About 2^{70} pairs are needed to get one right pair. Every structure consisting of 2^{32} chosen plaintexts yields about $(2^{32} \times (2^{32} - 1))/2 \approx 2^{63}$ pairs with the desired input difference. 128 such structures are required to get one right pair, a total of 2^{39} plaintexts. This analysis can be performed on each structure and thus the memory requirements are 2^{32} 64-bits quantities.

The filtering processes are carried out at the last half round and the first round. The filtering at the last half round is carried out firstly. Note that the difference at the second byte of the ciphertexts (denoted as x) should be odd. The differences in bytes 3, 6 and 7 have values 2x, x and 2x, respectively. The differences at the first and fifth bytes are even and the difference at the forth and eighth bytes are odd. After considering these, all but one out of 2^{29} pairs are discarded. 2^{41} pairs are left and each of the pair suggests 16 values of the bytes 1, 4, 5 and 8 of the last round key. Next, the filtering process is carried out at the first round. After checking whether the suggested key yields the desired difference at the output of the first round, every pair suggests about $16\times2^{-15} = 2^{-11}$ values of 4 key bytes 1, 4, 5 and 8. Totally, 2^{41} pairs suggest 2^{30} values of the four bytes of the key. An exhaustive key search at this point can be done in time about $1/2\times2^{30}\times2^{32} = 2^{61}$. By repeating the attack 64 times (using 2^{45} chosen plaintexts), the complexity is reduced to 2^{46}. The complexity is reduced further to 2^{35} if the attack is repeated 128 times by using 2^{46} chosen plaintexts.

In the filtering process at the last half round, sorting *n* items requires about $n \log n$ simple operations. A method is given in [5] to reduce the time requirements for the first filtering process. Let a ciphertext be denoted $(c_1,...,c_8)$ which is hashed to $(c_3 - 2c_2,\ c_6 - c_2,\ c_7 - 2c_2)$. The ciphertexts with the same hash value are candidates for a right pair after the first filtering process. Thus, the complexity is reduced to *n* simple operations.

4 Improved Attack on 5 Round SAFER

Knudsen and Bersonís attack is able to find out the secret key of 5 round SAFER K-64 much faster than by exhaustive search. However, when it is used to attack 5 round SAFER SK-64, the suggested key by each pair is 56 bits and it is infeasible to keep a counter for each 56-bit key and repeat the attack. Knudsen and Berson left their attack on 5 round SAFER SK-64 as an open problem [5]. In the following, we improve Knudsen and Bersonís attack on 5 round SAFER SK-64 by using better truncated differential and additional filtering process. Our truncated differential attack on 5 round SAFER SK-64 needs about 2^{38} chosen plaintexts and runs in time similar to 2^{46} encryptions of 5-round SAFER. A similar attack can be applied to 5 round SAFER K-64 and the same result can be obtained. Compared with one version of Knudsen and Bersonís attack on 5 round SAFER K-64 that requires about 2^{45} chosen plaintexts and runs in time similar to 2^{46} encryptions of 5 round SAFER, our attack uses much less chosen plaintexts (reduced by a factor of about 2^7) and runs in about the same time (if the filtering time is not considered).

4.1 Attack on 5 Round SAFER SK-64

Our attack on 5 round SAFER SK-64 uses the following 4-round truncated differential with input difference

$$[0, 0, 0, 0, a, b, c, d]$$

and output difference [0, 0, 0, 0, 0, 0, 128, 0]. There are 8 differentials (see (7)-(14)) in this 5-round truncated differential. The probabilities are about $2^{-71.7}$ for half of the differentials, and are about 2^{-72} for another half of the differentials.

$$5678 \to 12 \to 1256 \to 15 \to 7 \tag{7}$$
$$5678 \to 12 \to 3478 \to 15 \to 7 \tag{8}$$
$$5678 \to 34 \to 1256 \to 15 \to 7 \tag{9}$$
$$5678 \to 34 \to 3478 \to 15 \to 7 \tag{10}$$
$$5678 \to 56 \to 1256 \to 15 \to 7 \tag{11}$$
$$5678 \to 56 \to 3478 \to 15 \to 7 \tag{12}$$
$$5678 \to 78 \to 1256 \to 15 \to 7 \tag{13}$$
$$5678 \to 78 \to 3478 \to 15 \to 7 \tag{14}$$

The probabilities in the first round and the third round are each of 2^{-24} and the probability in the second round is 2^{-8}. Now we look at the differential in the fourth round. For those differentials with 1256 → 15 at the third round, the differential in the fourth round is

$$[2v, 0, 0, 0, v, 0, 0, 0],\; [128, 0, 0, 0, 128, 0, 0, 0],\; [0, 0, 0, 0, 0, 0, 128, 0]$$

The probability for this round differential varies slightly with values of key and is about 2^{-16} on average. For those differentials with 3478 → 15 at the third round, the differential in the forth round is

$$[v, 0, 0, 0, v, 0, 0, 0],\; [128, 0, 0, 0, 128, 0, 0, 0],\; [0, 0, 0, 0, 0, 0, 128, 0]$$

The probability for this round differential also varies with values of the key and is larger than $2^{-15.7}$ on average. So the probabilities are each of 2^{-72} for half of the differentials and $2^{-71.7}$ for another half of the differentials. The probability for the 4-round differential is thus larger than $2^{-68.9}$ on average. This 4-round differential is concatenated with the fifth round differential

$$[0, 0, 0, 0, 0, 0, 128, 0],\; [0, 0, 0, 0, 0, 0, x, 0],\; [2x, 2x, x, x, 2x, 2x, x, x]$$

This differential has probability 1.

After the final output transformation consisting of byte wise xoríing and addíing with the last round key, the output difference is:

$$[z_1, 2x, x, z_2, z_3, 2x, x, z_4] \tag{15}$$

where z_1 and z_3 are even numbers while the least significant bits of z_2 and z_4 are the same as that of x according to c) of Proposition 1.

The probability for this differential is about $2^{-68.9}$. About 2^{69} pairs are needed to get one right pair. Every structure consisting of 2^{32} chosen plaintexts yields about 2^{63} pairs with the desired input difference. 64 such structures are required to get one right pair, a total of 2^{38} plaintexts. The analysis can be performed on each structure and thus the memory requirements are 2^{32} 64-bit quantities.

The filtering processes are carried out at the last half round, the first round and the fifth round. The filtering process at the last half round is very similar to that in Knudsen and Bersonís attack except that the value of x may be odd and even. After this filtering process, 2^{41} pairs are left. Each pair suggests 16 values for the bytes 1,4,5 and 8 of the last round key ($K_{11,1}$ $K_{11,4}$ $K_{11,5}$ $K_{11,8}$). It is the same as to say that 16 values are suggested for $k_{2,}$ $k_{5,}$ k_6 and k_9 according to the key schedule of SAFER SK-64. Next we carry out the filtering process at the first round. For each of these 16 values, the check in the first round of differentials will give us about 2^{-6} values of the key bytes k_5, k_6, k_7 and k_8. Thus, each remaining pair suggests $16\times2^{-6} = 2^{-2}$ values for the key bytes $k_{2,}$ $k_{5,}$ $k_{6,}$ $k_{7,}$ k_8 and k_9. The remaining 2^{41} pairs suggest 2^{39} values for these 6 key bytes. We denote each remaining pair with one of its suggested 48-bit key as a unit. We are left with 2^{39} units after the filtering processes at the last half round and at the first round. An exhaustive key search at this point can be done in time about $\Omega \times 2^{39} \times 2^{16} = 2^{54}$. However, an additional filtering process at the fifth round will reduce the complexity of the key search by a factor of 2^8. This additional filtering process is the major improvement of our filtering processes compared with that of Knudsen and Berson. Before introducing this filtering process at the fifth round, we first present the following theorem.

Theorem 1. Consider the following two equations (X denotes the exponential permuation)

$$X[V \oplus K] - X[V' \oplus K] = 128$$
$$\Delta V = V - V'$$

Then each pair (ΔV, K) suggests one value of V on average.

Proof: The result is obtained by direct calculation.

In applying Theorem 1, all the solutions $(\Delta V, K, V)$ are precomputed, so that table lookup can be used to find out the value of V quickly once the values of ΔV and K are given.

For the fifth round, the value at the seventh byte of the input to the *PHT*-transformation is expressed as

$$\begin{aligned} V = (c_1 \oplus K_{11,1}) - 2(c_2 - K_{11,2}) - (c_3 - K_{11,3}) + 2(c_4 \oplus K_{11,4}) \\ - 2(c_5 \oplus K_{11,5}) + 4(c_6 - K_{11,6}) + 2(c_7 - K_{11,7}) - 4(c_8 \oplus K_{11,8}) \end{aligned} \quad (16)$$

This expression is obtained by using the expression of M^{-1}, see (1). If the value of V is known, (16) reveals 8-bit information of the key. Since the key bytes $k_{2,}$ $k_{5,}$ $k_{6,}$ $k_{7,}$ k_8 and k_9 are suggested already, the values of ($K_{11,1}$ $K_{11,4}$ $K_{11,5}$ $K_{11,6}$ $K_{11,7}$ $K_{11,8}$) are suggested. So (16) can be written as

$$2K_{11,2} + K_{11,3} = T \quad (17)$$

where T is calculated from

$$T = V - ((c_1 \oplus K_{11,1}) - 2c_2 - c_3 + 2(c_4 \oplus K_{11,4}) - 2(c_5 \oplus K_{11,5}) \\ + 4(c_6 - K_{11,6}) + 2(c_7 - K_{11,7}) - 4(c_8 \oplus K_{11,8})) \tag{18}$$

Next we carry out the filtering process at the fifth round. We are left with 2^{39} units after the filtering processes at the last half round and at the first round. For each unit, we know the values of x (the output difference at the third byte) and $K_{10,7}$ (which is derived from k_7 according to the key schedule of SAFER SK-64), they are the ΔV and K in Theorem 1, respectively (the *S* box *L* in the encryption becomes *S* box *X* in the decryption). So each unit suggests one value of V on average according to Theorem 1. The value of V is used to calculate the value of T in (18). From (17), we can predict 8-bit value for the key $K_{11,2}$ $K_{11,3}$. Thus, each unit suggests 2^8 values for the 64-bit key and 2^{39} units suggest $2^{39} \times 2^8 = 2^{47}$ values for the 64 bit key. The rest of the key can be found out by exhaustive key search in time about $\Omega \times 2^{47} = 2^{46}$ encryptions of 5-round SAFER.

Compared with Knudsen and Bersonís attack on 5 round SAFER K-64, the truncated differential used in our attack is better. Consider one of the truncated differentials in Knudsen and Beronís attack

$$1458 \to 1357 \to 1357 \to 13 \to 4$$

The probabilities of the truncated differential for the first round and second round are each of 2^{-16}. So the probability of the truncated differential for the first two rounds is 2^{-32}. The filtering process at the first round has the filtering power of about 2^{16} (which means that it is able to discard all but one out of 2^{16} suggested keys). Letís consider one of the truncated differentials used in our attack

$$5678 \to 12 \to 1256 \to 15 \to 7.$$

The probabilities for the first round and second round are 2^{-24} and 2^{-8} respectively. So the probability of the truncated differential for the first two rounds is 2^{-32}. This probability is the same as that of Knudsen and Berosn. But the filtering process at the first round has the filtering power of about 2^{24}, about 2^8 times larger than that in Knudsen and Bersonís attack. So we see that the differential in our attack increases the filtering power at the first round by a factor of about 2^8 while keeping the probabilities almost the same as that in Knudsen and Bersonís attack (when we consider only one of the differentials).

An additional filtering process at the fifth round is also used in our attack. A similar filtering process can be applied in Knudsen and Bersonís attack and can increase the filtering power by a factor of about 2^7.

4.2 5 Round SAFER K-64, SAFER K-128 and SAFER SK-128

Our attack on 5 round SAFER K-64 is very similar to that on 5 round SAFER SK-64. The same differential is used and the same result is obtained. Our attack is much better than the attack on 5 round SAFER K-64 in [5] as mentioned at the beginning of this section.

For 5 round SAFER K-128, the attack in [5] is better than of ours. Applying our attack to 5 round SAFER K-128 directly, 2^{38} chosen plaintexts suggest 2^{63} values for 80 bits of the key. The filtering process is much tedious and it is infeasible to repeat the attack since the memory requirement is too large.

For 5 round SAFER SK-128, our attack seems better than the attack in [5] since here our truncated differential and the filtering process can predict 17 bits information of the 128-bit key while Knudsen and Bersonís attack can determine only two bits of the key. However, both our attack and the attack in [5] cannot be carried out in reasonable time.

5 Attack on 6 Round SAFER

Knudsen and Bersonís attack is not successful to 6 round SAFER [5]. We improve their attack by using similar methods as we used in attacking 5 round SAFER. Our differential attack on 6 round SAFER (SAFER K-64 and SAFER SK-64) needs about 2^{53} chosen plaintexts and runs in time similar to 2^{61} encryptions of 6-round SAFER.

5.1 Attack on 6 Round SAFER-K64

Consider the following 5-round truncated differential with input difference

$$[0, 0, a, b, 0, 0, c, d]$$

and output difference [0, 0, 0, 128, 0, 0, 0, 0]. There are 16 differentials in this truncated differential. The probabilities are $2^{-87.68}$ for half of the differentials, and are $2^{-88.19}$ for another half of the differentials. These probabilities are determined in a very similar way as in Section 3.2. These differentials are

$$3478 \rightarrow 15 \rightarrow 1357 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{19}$$
$$3478 \rightarrow 15 \rightarrow 1357 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{20}$$
$$3478 \rightarrow 15 \rightarrow 2468 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{21}$$
$$3478 \rightarrow 15 \rightarrow 2468 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{22}$$
$$3478 \rightarrow 48 \rightarrow 1357 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{23}$$
$$3478 \rightarrow 48 \rightarrow 1357 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{24}$$
$$3478 \rightarrow 48 \rightarrow 2468 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{25}$$
$$3478 \rightarrow 48 \rightarrow 2468 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{26}$$
$$3478 \rightarrow 26 \rightarrow 1357 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{27}$$
$$3478 \rightarrow 26 \rightarrow 1357 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{28}$$
$$3478 \rightarrow 26 \rightarrow 2468 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{29}$$
$$3478 \rightarrow 26 \rightarrow 2468 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{30}$$
$$3478 \rightarrow 37 \rightarrow 1357 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \tag{31}$$
$$3478 \rightarrow 37 \rightarrow 1357 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \tag{32}$$

$$3478 \rightarrow 37 \rightarrow 2468 \rightarrow 1357 \rightarrow 13 \rightarrow 4 \quad (33)$$

$$3478 \rightarrow 37 \rightarrow 2468 \rightarrow 2468 \rightarrow 13 \rightarrow 4 \quad (34)$$

The 6 round differential is

$$[0, 0, 0, 128, 0, 0, 0, 0], [0, 0, 0, x, 0, 0, 0, 0], [2x, x, 2x, x, 2x, x, 2x, x],$$

where the value of x is odd. This differential has probability 1 since an input difference 128 to the exponentiation permutation always yields an odd output difference. Therefore we obtain a 6 round truncated differential with input difference [0, 0, a, b, 0, 0, c, d] and output difference [2x, x, 2x, x, 2x, x, 2x, x] for odd x and with a probability $16 \times 2^{-87.9} = 2^{-83.9}$.

We need about 2^{84} pairs to get one right pair. We can use structures of each 2^{32} plaintexts yielding 2^{63} pairs with the desired difference in the inputs. Therefore about 2^{21} structures are needed, a total of 2^{53} plaintexts. We can perform our analysis on each structure and thus the memory requirements are 2^{32} 64-bit quantities.

After the final transformation in SAFER, the output difference is

$$[z_1, x, 2x, z_2, z_3, x, 2x, z_4] \quad (35)$$

where x is odd and z_1 and z_3 are even numbers while z_2 and z_4 are odd numbers.

The filtering processes are carried out at the last half round, the first round and the sixth round. Firstly, we carry out the filtering process at the last half round. This is the same as that in Knudsen and Bersonís attack on 5 round SAFER K-64. 2^{55} pairs are left and each pair suggests 16 values for the bytes 1, 4, 5 and 8 of the last round key. Next we carry out the filtering process at the first round. For each of these 16 values, the check in the first round of differentials will give us about 2^{-6} values of the key bytes k_3, k_4, k_7 and k_8. Thus, each remaining pair suggests $16\times2^{-6} = 2^{-2}$ values for the key bytes $k_{1,}$ $k_{3,}$ $k_{4,}$ $k_{5,}$ k_7 and k_8. Hence, 2^{55} pairs suggest 2^{53} values for these 6 key bytes. We denote each pair with one of its suggested 48 bit key as a unit. We are left with 2^{53} units. Then we carry out the filtering process at the sixth round. It will increase the filtering power by a factor of 2^7. Before the discussion of this filtering process, we introduce the following theorem.

Theorem 2. Consider the following two equations where L denotes the logarithmic permutation:

$$L[V] - L[V'] = 128$$
$$\Delta V = V - V'$$

Then each odd value of ΔV suggests two values of V.

Proof: The result can be obtained by direct calculation.

To use this theorem efficiently, all the solutions (ΔV, V) are listed in a table so that table lookup can be used to find V quickly when ΔV is given.

For the fifth round, the fourth byte of the output of the *S* box is expressed as

$$V=((c_1 \oplus K_{13,1})-(c_2-K_{13,2})-2(c_3-K_{13,3})+2(c_4 \oplus K_{13,4})-$$
$$2(c_5 \oplus K_{13,5})+2(c_6-K_{13,6})+4(c_7-K_{13,7})-4(c_8 \oplus K_{13,8}))-K_{12,4} \quad (36)$$

If the value of V is known, (36) indicates 8 bits information of the key. Since the key bytes $k_{1,}$ $k_{3,}$ $k_{4,}$ $k_{5,}$ k_7 and k_8 are suggested already, the values of ($K_{13,1}$ $K_{13,3}$ $K_{13,4}$ $K_{13,5}$ $K_{13,7}$ $K_{13,8}$) are suggested. So (36) can be written as

$$K_{13,2}-2K_{13,6}=T \quad (37)$$

where T is calculated as

$$T=V+K_{12,4}-((c_1 \oplus K_{13,1})-2c_2-2(c_3-K_{13,3})+2(c_4 \oplus K_{13,4})$$
$$-2(c_5 \oplus K_{13,5})+2c_6+4(c_7-K_{13,7})-4(c_8 \oplus K_{13,8})) \quad (38)$$

Now, we carry out the filtering process at the sixth round. We are left with 2^{53} units after the filtering process at the last half round and the filtering process at the first round. For each unit, we know the values of x (the output difference at the third byte), it is ΔV in Theorem 2 (we note that the S box X in encryption is the S box L in decryption). So each unit suggests two values of V. The value of V is used to calculate the value of T in (38). Each value of W suggests 2^8 values for the key $K_{13,2}$ and $K_{13,6}$. Thus, each unit suggests 2^9 values for the 64-bit key and 2^{53} units suggests $2^{53} \times 2^9 = 2^{62}$ values for the 64 bit key. The rest of the key can be found by exhaustive search in time about $\Omega \times 2^{62} = 2^{61}$ encryptions of 6-round SAFER.

5.2 Attack on 6 round SAFER SK-64

To attack 6 round SAFER SK-64, we use the same truncated differential and similar filtering process as that in the attack of 6 round SAFER K-64. This attack needs about 2^{53} chosen plaintexts and runs in time similar to 2^{61} encryptions of 6-round SAFER. The result is the same as that obtained in the attack on 6 round SAFER K-64.

The filtering processes carried out at the last half round is the same as that in the attack of 6 round SAFER K-64. After this filtering process, about 2^{55} pairs are left, each pair suggests 16 values for the bytes 1, 4, 5 and 8 of the last round key. It is the same as to say that 16 values of k_2 k_4, k_7 and k_8 are suggested by each remaining pair. The filtering processes at the first round and the sixth round are different from those in Section 5.1 due to the difference in key schedules. Next, we carry out the filtering process at the first round. For each of these 16 values, the check in the first round of differentials will give us about 2^{-14} values of the key bytes k_3, k_4, k_7 and k_8. Thus, each remaining pair suggests $16 \times 2^{-14} = 2^{-10}$ values for the key bytes $k_{2,}$ $k_{3,}$ $k_{4,}$ $k_{7,}$ k_8. The remaining 2^{55} pairs suggest 2^{45} values for these 5 key bytes. We denote each pair with one of its suggested 40-bit key as a unit. We are left with 2^{45} units. Then we carry out the filtering process at the sixth round.

Since the key bytes k_2, k_3, k_4, k_7 and k_8 are suggested already, the values of ($K_{13,1}$ $K_{13,4}$ $K_{13,5}$ $K_{13,8}$) are suggested. So (36) can be written as

$$K_{13,2} + 2K_{13,3} - 2K_{13,6} - 4K_{13,7} - K_{12,4} = T \tag{39}$$

where T is calculated as

$$T = V - ((c_1 \oplus K_{13,1}) - c_2 - 2c_3 + 2(c_4 \oplus K_{13,4}) \\ - 2(c_5 \oplus K_{13,5}) + 2c_6 + 4c_7 - 4(c_8 \oplus K_{13,8})) \tag{40}$$

Also, we note that

$$k_9 = k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus .... \oplus k_8 \tag{41}$$

Now, we continue with the filtering process. We are left with 2^{45} units. For each unit, we know the value of x (the output difference at the second byte), it is the ΔV in Theorem 2. So each unit suggests two values of V . The value of V is used to calculate the value of T in (40). For each value of T , we can solve for 2^{16} values of k_1, k_5 and k_6 (It can be done simply through table lookup as explained later). Thus, each unit suggests 2^{17} values for the 64-bit key and 2^{45} units suggests $2^{45} \times 2^{17} = 2^{62}$ values for the 64-bit key. The rest of the key can be found out by exhaustive search in time about $\Omega \times 2^{62} = 2^{61}$ encryptions of 6-round SAFER. This result is the same as that obtained in the attack on 6 round SAFER K-64.

In the filtering process at the sixth round, we need to find the value of k_1, k_5 and k_6 when the value of T is given. It can be done in short time through table lookup. From (39), (41) and the information that ($K_{12,4}$ $K_{13,2}$ $K_{13,3}$ $K_{13,6}$ $K_{13,7}$) are derived from (k_6 k_5 k_6 k_9 k_1) respectively, we can precompute the values of k_1, k_5 and k_6 for all the values of T and list the results in a table. In the filtering process, once the value of T is known, we can obtain the related 2^{16} values through table lookup. Thus, this filtering process can be implemented in relatively short time.

6 7 Round SAFER

For 7 round SAFER, we apply the similar truncated differential as that in the attack on 6 round SAFER. It has input difference [0, 0, a, b, 0, 0, c, d] and output difference [2x, x, 2x, x, 2x, x, 2x, x] with a probability of about 2^{-99}. To get a right pair, 2^{68} chosen plaintexts are required. Thus, it is impossible to carry out our attack.

7 Conclusion

In this paper, we improved the truncated differential attack on 5 round SAFER SK-64. We also carried out attacks on 6 round SAFER K-64 and SAFER SK-64. Our attack on 5 round SAFER SK-64 can find out the secret key in time much faster than by exhaustive search. Also, our attack uses less chosen plaintexts compared with Knudsen and Bersonís attack. Our attack on 6 round SAFER runs in time faster than by exhaustive search. However, our attack is not efficient when applied to 7 round SAFER. We strongly believe that 8 round SAFER is invulnerable to our attacks.

References

1 E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

2 C. Harpes, G.G. Kramer, and J.L. Massey. A generalization of linear cryptanalysis and the applicability of Matsuiís piling-up lemma. In L. Guillou and J.J. Quisquater, editors, *Advancess in Cryptology – Eurocrypt'95, LNCS 921*, pages 24-38. Springer Verlag, 1995.

3 L.R. Knudsen. A key-schedule weakness in SAFER K-64. In C. Copersmith, editor, *Advances in cryptology – CRYPTO'95, LNCS 963*, pages 274-286. Springer Verlag, 1995.

4 L.R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, *Fast Software Encryption, LNCS 1008*, pages 196-211, Springer Verlag, 1995.

5 L.R. Knudsen, T.A. Berson. Truncated Differentials of SAFER. In D. Gollmann, editor, *Fast Software Encryption – Third International Workshop, LNCS 1039*, pages 15-25, Springer Verlag, 1996.

6 J.L. Massey. Safer K-64: A byte-oriented block-ciphering algorithm. In R. Anderson, editor, *Fast Software Encryption – Proc. Cambridge Security Workshop, Cambridge, U.K., LNCS 809*, pages 1-17. Springer Verlag, 1994.

7 J.L. Massey. SAFER K-64: One year later. In B. Preneel, editor, *Fast Software Encryption – Proc. Second International Workshop, LNCS 1008,* pages 212-241, Springer Verlag, 1995.

8 J.L. Massey. Strengthened Key Schedule for the Cipher SAFER, posted to the USNET newsgroup sci.crypt, September, 1995.

9 M. Matsui, Linear Cryptanalysis Method for DES Cipher. In T. Helleseth, editor, *Advances in Cryptology – Proc. of Eurocrypt '93, LNCS 765*, pages 386-397, Springer-Verlag, 1994.

Appendix

For the attack of 5 round SAFER SK-64, we illustrate one of the differentials to show the detail of the truncated differential. This example differential is

$$5678 \rightarrow 12 \rightarrow 1256 \rightarrow 15 \rightarrow 7$$

1st round: [0, 0, 0, 0, a, b, c, d], [0, 0, 0, 0, e, -e, -e, e], [e, e, 0, 0, 0, 0, 0, 0], $p = 2^{-24}$
2nd round: [e, e, 0, 0, 0, 0, 0, 0], [f, -f, 0, 0, 0, 0, 0, 0], [4f, 2f, 0, 0, 2f, f, 0, 0], $p = 2^{-8}$
3rd round: [4f, 2f, 0, 0, 2f, f, 0, 0], [g, -g, 0, 0, -g, g, 0, 0], [2g, 0, 0, 0, g, 0, 0, 0], $p = 2^{-24}$
4th round: [2g, 0, 0, 0, g, 0, 0, 0], [128, 0, 0, 0, 128, 0, 0, 0], [0, 0, 0, 0, 0, 0, 128, 0],

The probability for this round varies with the key and is larger than $2^{-15.7}$ in average.