Improved Side-Channel Attack on DES with the First Four Rounds Masked

Jongsung Kim, Seokhie Hong, Dong-Guk Han, and Sangjin Lee

ABSTRACT—This letter describes an improved side-channel attack on DES with the first four rounds masked. Our improvement is based on truncated differentials and power traces which provide knowledge of Hamming weights for the intermediate data computed during the enciphering of plaintexts. Our results support the claim that masking several outer rounds rather than all rounds is not sufficient for the ciphers to be resistant to side-channel attacks.

Keywords—Side-channel attack, truncated differential, DES.

I. Introduction

A side-channel attack is an attack on implementations of cryptographic algorithms such as block ciphers, public-key ciphers, and digital signatures. Its general strategy is to observe the physical implementation properties of a system, such as power consumption, timing information, electromagnetic radiation, and sound waves, to obtain information that can be used to break a cryptographic algorithm. For example, DES [1] was broken by a differential power analysis with a data complexity of less than 1,000 plaintexts (that is, 1,000 power consumption measurements) [2].

The best known countermeasure to side-channel attacks is to randomize intermediate values over the cipher by masking each of its rounds. A disadvantage of this approach is that masking all the rounds of the cipher has a high implementation cost. To overcome the disadvantage of the full-round masking method, several researchers have suggested masking the first and last few rounds of the ciphers in the claim that such reduced-round masking is sufficient to provide resistance against side-channel attacks. However, for DES, the reduced-round masking method is known to be vulnerable to the side-channel approach through the Handschuh-Preneel attack [3].

In this letter, we use truncated differentials [4] to improve the data complexity of the Handschuh-Preneel attack on DES with the first four rounds masked. Our attack reduces the necessary data from 480,000 to 2,048 chosen plaintexts along with their associate power traces and Hamming weight measurements. Our time complexity is the same as that of the Handschuh-Preneel attack, which is 2^{16} encryptions. Note that the indicated data complexity of the Handschuh-Preneel attack is an approximate value required for a full-key recovery. It is based on the fact that their original attack recovers six bits of the key with a data complexity of 60,000 chosen plaintexts, and the indicated time complexity does not include the time required for data encrypted because what we need is their power traces. This improvement leads to the best known side-channel attack on DES with the first four rounds masked. See Table 1 for a summary of DES results from our study and [3].

Table 1. Summary DES results from [3] and our study.

Attack method	Masked rounds	Complexity		Work
		Data	Encryptions	
DC (HW)	4	480,000 CP	2^{16}	[3]
TDC (HW)	4	2,048 CP	2^{16}	Our study

DC: differential cryptanalysis, TDC: truncated DC
CP: chosen plaintexts with associate power traces
HW: attackers have the knowledge about Hamming weights of intermediate data computed during the enciphering of plaintexts
The attacks are all to recover the entire master key.

Manuscript received May 11, 2009; revised July 24, 2009; accepted Aug. 17, 2009.

Jongsung Kim (phone: +82 10 4711 8468, email: jongsung.k@gmail.com) is with the Division of e-Business, Kyungnam University, Masan, Rep. of Korea.

Seokhie Hong (phone: +82 17 201 6348, email: hsh@cist.korea.ac.kr) and Sangjin Lee (email: sangjin@korea.ac.kr) are with the Center for Information Security Technologies (CIST), Korea University, Seoul, Rep. of Korea.

Dong-Guk Han (email: christa@kookmin.ac.kr) is with the Department of Mathematics, Kookmin University, Seoul, Rep. of Korea.

doi:10.4218/etrij.09.0209.0144

II. Side-Channel Attack on DES with the First Four Rounds Masked Using Truncated Differentials

In [5], Akkar and others propose using two independent sets of S boxes for the first four and the last four rounds in order to protect DES against side-channel attacks:

$$S_1(x)=S(x)\oplus P^{-1}(\alpha),$$
$$S_2(x\oplus E(\alpha))=S(x)\oplus P^{-1}(\alpha) \text{ for } x\in\{0,1\}^{48},$$

where α is a 32-bit mask, and $S(\cdot)$ is the original DES S box. Hereafter, we denote the eight original S boxes mapping six bits to four bits by $s_1, s_2,\cdots, s_8$. (For a detailed description of DES, see [1].) The left side of Fig. 1 shows the first four rounds of DES using the $S_1(\cdot)$ and $S_2(\cdot)$ boxes. The first and fourth rounds apply $S_1(\cdot)$, and the rest of the rounds apply $S_2(\cdot)$. Figure 1(b) shows DES using the original S boxes.

In this section, we show how to use truncated differentials to reduce the data complexity of the Handschuh-Preneel attack, that is, 480,000, down to 2,048 chosen plaintexts in the same settings.

The basic idea behind our attack is to exploit the fact that, for a given plaintext, the value of the # position is the same as the value of the ## position (see Fig. 1). It follows that, for a given plaintext, the input values of the fourth-round S boxes obtained by the masked DES and by the unmasked DES are also equal. Working from this fact, we recover the key using truncated differentials. Our attack strategy is to recover the first round key six bits by six bits, and then to recover the entire master key by an exhaustive search for the remaining key bits.

In order to find the six-bit subkey of the first round that is entered into the third S box s_3, we exploit the four-round truncated differential with probability 3/16 shown in Fig. 1(b).

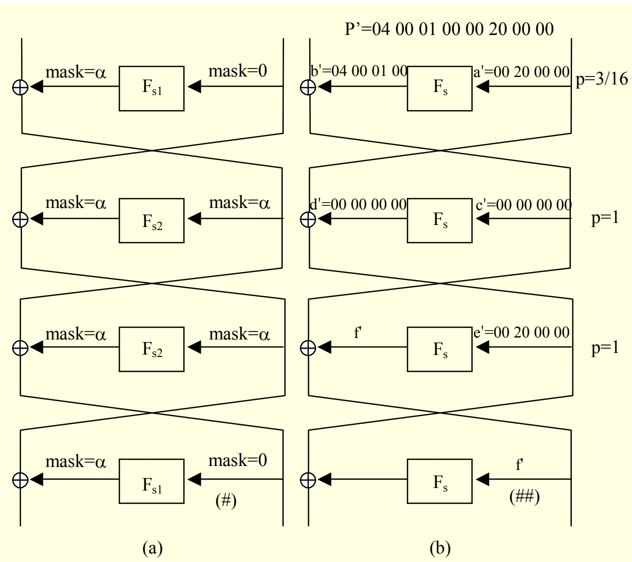

Fig. 1. (a) Akkar and others' four masked rounds and (b) our four-round truncated differential with its probability.

Our four-round truncated differential is constructed to maximize its differential probability. In the first-round function F_S, there are three possible input differences that affect only the s_3 box: 0x00200000, 0x00400000, and 0x00600000. These differences change into the input differences 0x04, 0x08, and 0x0C of the s_3 box due to the E expansion and the key addition. For the remaining S boxes in the first round, the input differences are all zero.

According to the difference distribution table for the s_3 box, there are three (input, output) difference pairs that have the maximal hit of 12: (0x04, 0x09), (0x0C, 0x05), and (0x0C, 0x06). In our attack, we select the (0x04, 0x09) difference pairs (leading to a selection of the input difference of the first-round function as 0x00200000); thus, the differential probability of the first round is 12/64=3/16. Note that because of the P permutation, the output difference of the first-round function is of the form 0x04000100.

If the left half of the plaintext difference is of the form 0x04000100, as shown in Fig. 1(b), then the input and output differences for the second-round function are all zero, and the input difference of the third-round function is the same as the input difference of the first-round function: 0x00200000. Next, we consider all possible output differences of the third-round function (f' in Fig. 1) when its input difference is 0x00200000. As previously noted, this input difference changes into the 0x04 input difference of the s_3 box in the third-round function. In the difference distribution table for the s_3 box, there are 11 possible output differences with respect to the input difference 0x04. Then, the resulting differences entered into the S boxes of the fourth round must have the following property due to those 11 possible output differences:

Property 1. If two plaintexts with the P' difference are encrypted by the DES with the first four and the last four masked rounds where P'=0x04000100 00200000, then their intermediate values x_i and y_i at the input position of the i-th S boxes s_i for the fourth round have the following property, with a probability of about 3/16:

$$hwt(x_i) = \begin{cases} hwt(y_i) & \text{for } i=1,3 \\ hwt(y_i) \text{ or } hwt(y_i)\pm 1 & \text{for } i=2,4,5,6,7,8, \end{cases}$$

where $hwt(x)$ is the bit Hamming weight of x.

The attack procedure based on property 1 is carried out as follows:

Step 1. Collect 128 plaintext pairs with difference P'.

Step 2. Encrypt the plaintext pairs using DES with the first four and the last four rounds masked. During the encryption process of each plaintext pair, measure the Hamming weights of the input values for the S boxes in the fourth round.

Step 3. Discard the plaintext pairs that do not satisfy property

1, and choose plaintext pairs that satisfy property 1 as correct pairs following our truncated differential.

Step 4. Analyze the s_3 box of the first round with the correct plaintext pairs in unmasked DES, using the difference distribution table of the s_3 box, which suggests key candidates for the 6-bit subkey entering into the s_3 box.

Step 5. Output the keys with a maximal hit in step 4.

Since our four-round truncated differential holds with probability 3/16, about 24 out of the 128 plaintext pairs are expected to be correct pairs, which implies that the correct subkey K should be suggested about 24 times in step 4. Due to the symmetric property, $K \oplus$ 0x04 has the same hits as the correct subkey K.

To compute the expected number of hits for an incorrect subkey, we need to know the filtering rate of step 3, which is computed as

$$\left[\sum_{i=0}^{6}\left(\frac{\binom{6}{i}}{2^6}\right)^2\right]^2 \times \left[\sum_{i=0}^{6}\left(\frac{\binom{6}{i}}{2^6}\right)^2 + \sum_{i=0}^{6}\left(6\times\frac{\binom{6}{i}}{2^{12}}\right)\right]^6 \approx 2^{-5.8},$$

where $\sum_{i=0}^{6}\left(\frac{\binom{6}{i}}{2^6}\right)^2$ and $\sum_{i=0}^{6}\left(6\times\frac{\binom{6}{i}}{2^{12}}\right)$ are the probabilities of $hwt(x_i) = hwt(y_i)$ and $hwt(x_i) = hwt(y_i) \pm 1$, respectively. Thus, about three of the 128 plaintext pairs are expected to be incorrect pairs that survive even after the filtering. This implies that a wrong subkey has $(24+3)\times 4/63 \approx 1.7$ hits on average. Hence, there is an overwhelming probability that the attack outputs the correct six-bit subkey together with its dual subkey. Note that its time complexity is negligible.

Similarly, we can recover six-bit subkey candidates entered into each of the remaining S boxes by using other truncated differentials that have a probability of approximately 1/4. Table 2 offers some information about our eight four-round truncated differentials to recover the whole first round key.

Each of our eight four-round truncated differentials holds with the probability shown in Table 2, which is derived from the first-round function. As in the previous s_3 box attack, we exploit 256 chosen plaintexts to recover each of the six-bit subkeys so that the total data complexity of our attack is 2,048 chosen plaintexts. Because each differential provides the right six-bit subkey with its dual subkey with a high probability, the entire master key can be extracted with 2^{16} trial encryptions; thus, the total time complexity of the attack is about 2^{16} encryptions.

To test our attack, we performed 1,000 simulations on DES with the first four rounds masked, where we used a randomly chosen key and plaintext pairs in each execution. About 970 out of 1,000 executions succeeded in recovering the master keys. We have also experimentally checked that our attack works with a high success rate, even when approximately 15% false alarms occur in measuring Hamming weights, which is the same error rate as the Handschuh-Preneel attack.

Table 2. Our eight 4-round truncated differentials.

S box[a]	Plaintext difference	Probability	S boxes[b]
s_1	0x00808202 60000000	7/32	s_1, s_5
s_2	0x40080000 04000000	1/4	s_2, s_6
s_3	0x04000100 00200000	3/16	s_1, s_3
s_4	0x00401000 00020000	3/16	s_2, s_4
s_5	0x00040080 00002000	5/32	s_5, s_8
s_6	0x00200008 00000400	1/4	s_4, s_6
s_7	0x00100001 00000060	7/32	s_5, s_7
s_8	0x00020820 00000002	3/16	s_3, s_8

[a] : the S box in the first round whose corresponding 6-bit subkey is recovered
[b] : the S boxes in the fourth round satisfying $hwt(x_i) = hwt(y_i)$

III. Conclusion

In this letter, we have improved the previous best known side-channel attack on DES with the first four rounds masked. Our attack requires a data complexity of 2,048 chosen plaintexts and a time complexity of 2^{16} encryptions, compared with the previous best known side-channel attack, which takes 480,000 chosen plaintexts and 2^{16} encryptions. This result supports the claim that in preventing side-channel attacks it is not sufficient to mask reduced rounds of block ciphers.

References

[1] National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standards Publication 46, Jan. 1977.

[2] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Proc. CRYPTO 1999, LNCS*, vol. 1666, 1999 pp. 388-397.

[3] H. Handschuh and B. Preneel, "Blind Differential Cryptanalysis for Enhanced Power Attacks," *Proc. SAC 2006, LNCS*, vol. 4356, 2007 pp. 163-173.

[4] L.R. Knudsen, "Truncated and Higher Order Differentials," *Proc. FSE 1994, LNCS*, vol. 1008, 1995, pp. 196-211.

[5] M.L. Akkar, R. Bevan, and L. Goubin, "Two Power Analysis Attacks against One-Mask Methods," *Proc. CHES 2004, LNCS*, vol. 3156, 2004, pp. 332-347.