Information Processing Letters 111 (2011) 474–478

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Differential cryptanalysis of eight-round SEED

Jaechul Sung

Department of Mathematics, University of Seoul, Seoul 130-743, Republic of Korea

ARTICLE INFO

Article history:
Received 18 August 2010
Received in revised form 11 February 2011
Accepted 11 February 2011
Available online 12 February 2011
Communicated by D. Pointcheval

Keywords:
Cryptography
Cryptanalysis
Block cipher
SEED

ABSTRACT

Block Cipher SEED is one of the standard 128-bit block ciphers of ISO/IEC together with AES and Camellia (Aoki et al., 2000, ISO/IEC 18033-3, 2005; Korea Information Security Agency, 1999; National Institute of Standards and Technology, 2001) [1,4–6]. Since SEED had been developed, there is no distinguishing cryptanalysis except a 7-round differential attack in 2002 [7]. For this, they used the six-round differential characteristics with probability 2^{-124} and analyzed seven-round SEED with 2^{126} chosen plaintexts. In this paper, we propose a new seven-round differential characteristic with probability 2^{-122} and analyze eight-round SEED with 2^{125} chosen plaintexts. The attack requires about 2^{122} eight-round encryptions. This is the best-known attack on a reduced version of SEED so far.

1. Introduction

SEED is a 128-bit block cipher with a 128-bit key. This is one of the standard algorithms together with AES and Camellia [1,6]. There are many analyses on AES and Camellia, however for SEED, the only known attack is the seven-round differential attack in 2002 [3].

In this paper, we extend the differential attack on SEED [2]. We propose a new seven-round differential characteristic with probability 2^{-122} which is the best known differential characteristic so far. With this we can attack eight-round SEED with 2^{125} chosen plaintexts by applying the traditional differential cryptanalysis technique.

2. Brief description of SEED

The overall design of SEED is based on the Feistel structure and its number of rounds is 16. A 128-bit input is divided into two 64-bit blocks and the right 64-bit block is an input to the round function F with a 64-bit subkey generated from the key scheduling. Fig. 1 shows the round function of SEED, which has the MISTY-type structure. It has four phases: a round key XOR phase and three phases of G function layer with addition mod 2^{32}.

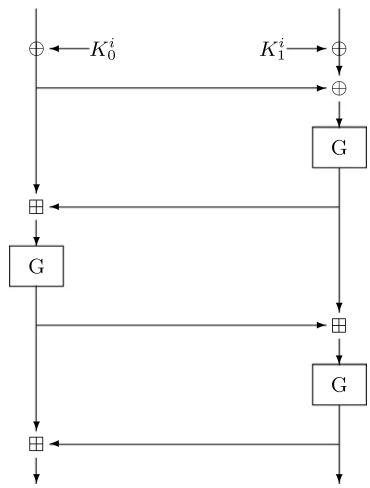

Fig. 1. Round function F of SEED.

The G function in F is a bijective function on $\{0,1\}^{32}$. It consists of the substitution layer with S_2 and S_1 and the permutation layer. The substitution layers S_2 and S_1 are S-boxes with 8-bit input/output length. In the permutation layer, four constants are defined by $m_0 = fc_x$, $m_1 = f3_x$, $m_3 = cf_x$ and $m_4 = 3f_x$. Here, a_x means that a is in hex-

E-mail address: jcsung@uos.ac.kr.

0020-0190/$ – see front matter
doi:10.1016/j.ipl.2011.02.004

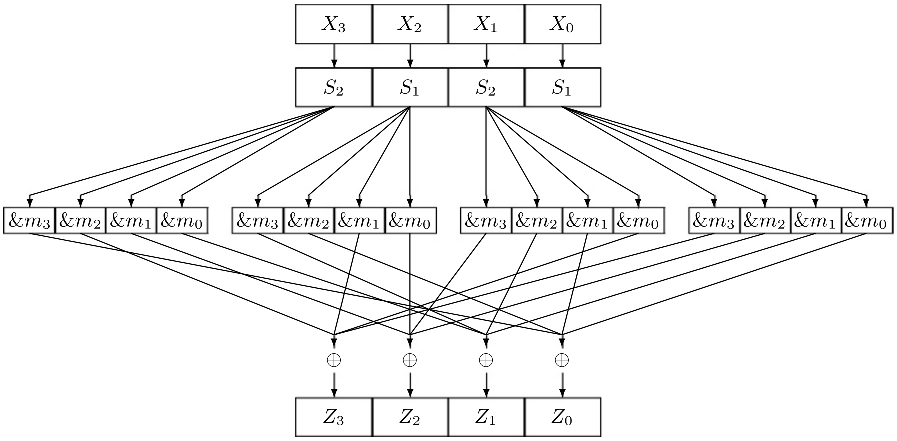

Fig. 2. Function G of SEED.

adecimal representation. An illustration of this is given in Fig. 2.

We omit the key scheduling of SEED since our attack does not use it. For details of SEED, see [4,5].

3. Previous results

In [7], a six-round differential characteristic of SEED with probability 2^{-124} was presented. The round function description in [7] was described in reverse direction; the right and left parts of F were swapped. However, this does not affect the overall attack procedure. By correcting this, we illustrate the 6-round differential characteristic in Fig. 3, where $\alpha = 80000080_x$.

In Fig. 3, $p_1 = p_6 = 1$ and $p_2 = p_3 = p_4 = p_5 = 2^{-31}$. Actually its probability of 2^{-124} is higher than 2^{-130}, the highest suggested by the proposers.

With this characteristic we can attack 7-round SEED by applying the typical differential cryptanalysis [2]. First we collect $2^{126}(= 4 \cdot 2^{124})$ plaintext pairs whose XOR difference is $((0,\alpha),(0,0))$. Then we exclude wrong pairs whose right 64-bit ciphertext difference is not equal to $(0,\alpha)$ in advance. For each last round subkey candidate, we compute the output difference in the last F function with the remaining pairs. If the difference is equal to the left 64-bit of the ciphertext pairs, we increment the counter by 1. After counting, we consider the highest one as the right subkey.

The signal-to-noise S/N is about $2^4(= 2^{-60} \cdot 2^{64})$. So we can deduce the right key with about $2^{126}(= 4 \cdot 2^{124})$ chosen plaintext pairs. After the filtering phase, the attack requires $2^{124.19}(= 2 \cdot 2^{62} \cdot 2^{64} \cdot 1/7)$ seven-round encryptions. Moreover, the 2^{127} plaintexts can be reduced to 2^{126} by applying a simple trick found in [2] using three characteristics with same probabilities. More details can be seen in [7].

4. Differential attack on eight rounds of SEED

In this section, we propose a new seven-round differential characteristic. The probabilities of this up to 6 and 7 rounds are 2^{-110} and 2^{-133}. The probabilities are higher than the previous one. However, we cannot mount an eight-round attack with the characteristic of up to 7 rounds. Therefore we improve the probabilities of our characteristic by utilizing a differential technique.

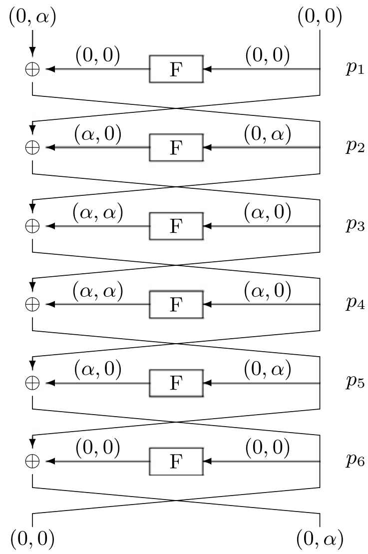

Fig. 3. Previous best 6-round differential characteristic.

4.1. New seven-round differential characteristic

Fig. 4 shows our new seven-round differential characteristic of SEED. We find the characteristic by modifying the second-best six-round differential characteristic of [7]. In Fig. 4, a, b, c and d denote 32-bit nonzero differences satisfying $a \oplus b \oplus c \oplus d = 0$.

Our new characteristic uses three nontrivial round characteristics I, II and III. Let the round characteristic I, II and III denotes $(b,a) \xrightarrow{F} (a,0)$, $(a,0) \xrightarrow{F} (a \oplus c, 0)$ and $(d,a) \xrightarrow{F} (a,0)$ respectively.

Since the exclusive-or operations of round keys in F do not affect the differences of input pairs, we omit these operations in what follows. In order to find a characteristic whose probability is relatively high, we should carefully