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}.

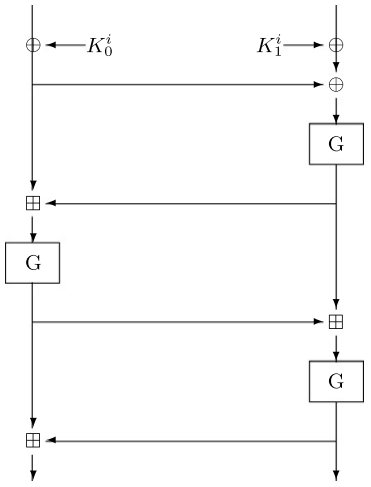

Fig. 1. Round function F of SEED.

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

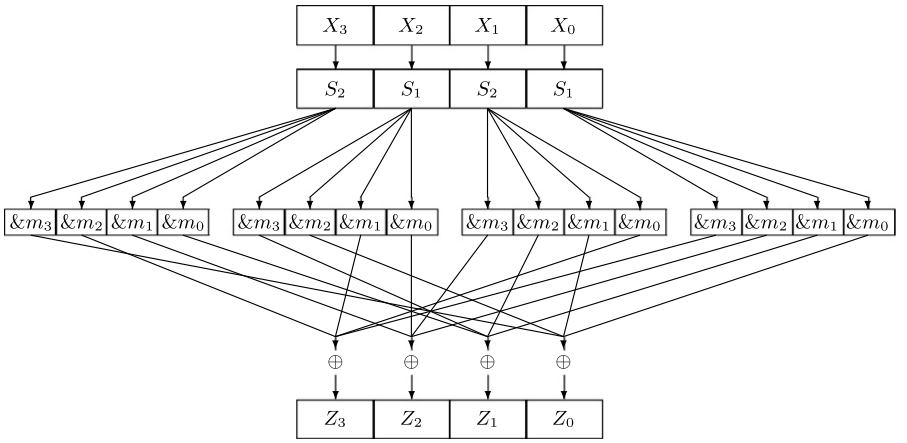

Fig. 2. Function G of SEED.

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.

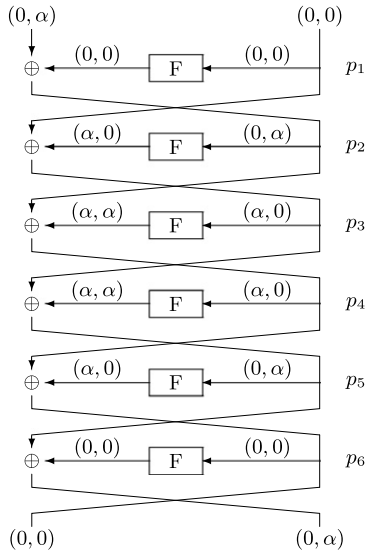

Fig. 3. Previous best 6-round differential characteristic.

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

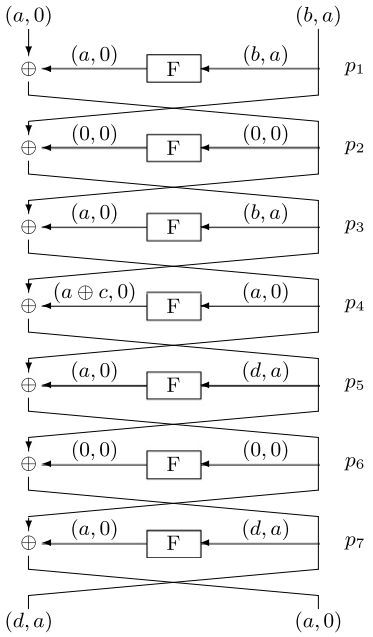

Fig. 4. New 7-round differential characteristic.

observe changes of the differentials in the round function F. The major impact factors on the probabilities in F are the active S-box numbers and addition operation in mod 2^{32}. In order to achieve a higher probability, we carefully find the values of a, b, c and d. Table 1 gives the possible values of our characteristic.

Let p_i denote the probability of the ith round differential characteristic. Then we easily have that $p_2 = p_6 = 1$, $p_3 = p_1$ and $p_7 = p_5$. So the probabilities of the characteristic up to 6 and 7 rounds are $p_1^2 p_4 p_5$ and $p_1^2 p_4 p_5^2$ respectively.

Let $DP[\Delta I \xrightarrow{f} \Delta O]$ denotes the differential probability whose input and output differences of f are ΔI and ΔO respectively. Also let $DP[(\Delta I_1, \Delta I_2) \xrightarrow{\boxplus} \Delta O]$ denotes the differential probability whose two input xor differences of addition operation are ΔI_1 and ΔI_2 and output difference is ΔO as in [7].

We now consider the probability p_1 of the round characteristic I of TYPE 1 more closely. An illustration of this is given in Fig. 5.

The probability p_1 is equal to $q_1 q_2 q_3 q_4 q_5 q_6$, where each q_i is defined as follows.

$$
\begin{aligned}
q_1 &= DP\big[07000000_x \xrightarrow{G} 80808000_x\big] \\
&= DP\big[07_x \xrightarrow{S_2} 80_x\big] = 2^{-6}, \\
q_2 &= DP\big[(8780800_x, 8080800_x) \xrightarrow{\boxplus} 07000000_x\big] = 2^{-5}, \\
q_3 &= DP\big[07000000_x \xrightarrow{G} 80808000_x\big] \\
&= DP\big[07_x \xrightarrow{S_2} 80_x\big] = 2^{-6}, \\
q_4 &= DP\big[(8080800_x, 8080800_x) \xrightarrow{\boxplus} 00000000_x\big] = 2^{-2}, \\
q_5 &= DP\big[00000000_x \xrightarrow{G} 00000000_x\big] = 1, \\
q_6 &= DP\big[(8080800_x, 0000000_x) \xrightarrow{\boxplus} 80808000_x\big] = 2^{-2}.
\end{aligned}
$$

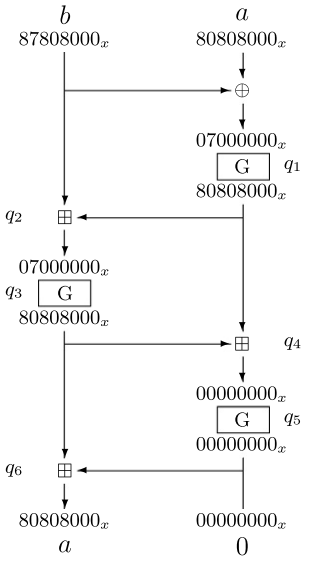

Fig. 5. Round characteristic I; $(b, a) \xrightarrow{F} (a, 0)$.

Table 1
Possible values of a, b, c and d.

	TYPE 1	TYPE 2
a	80808000_x	80808000_x
b	87808000_x	83808000_x
c	00808000_x	00808000_x
d	07808000_x	03808000_x

Table 2
Differential characteristic probabilities of TYPE 1 and 2.

Probabilities	TYPE 1	TYPE 2
p_1	2^{-21}	2^{-22}
p_4	2^{-45}	2^{-45}
p_5	2^{-23}	2^{-22}
6R: $p_1^2 p_4 p_5$	2^{-110}	2^{-111}
7R: $p_1^2 p_4 p_5^2$	2^{-133}	2^{-133}

Therefore the probability of the round characteristic I is 2^{-21}.

The probabilities of round characteristic II and III can be computed in a similar fashion. An illustration of this is given in Fig. 6.

In the above explanation, we have that $p_1 = 2^{-21}$, $p_4 = 2^{-45}$ and $p_5 = 2^{-23}$. So the probabilities of the characteristic up to 6 and 7 rounds are 2^{-110} and 2^{-133}.

For the TYPE 2 characteristic, we can easily calculate the probabilities in a similar fashion. Table 2 gives the probabilities of TYPE 1 and 2 characteristics. We can naturally consider the case that b and d are defined by 81808000_x and 01808000_x respectively. Of course, we fix the values a and c as in the case of TYPE 1 and 2. However, in this case, since $DP[81_x \xrightarrow{S_2} 80_x] = 0$, we cannot apply the characteristic in Fig. 4.

The probabilities of the characteristics up to 6 rounds are higher than that of the previous best-known 6-round characteristic. However we cannot use the seven-round characteristic directly since the probability is less than 2^{-128}. In order to attack more than seven rounds, we must improve the probabilities.

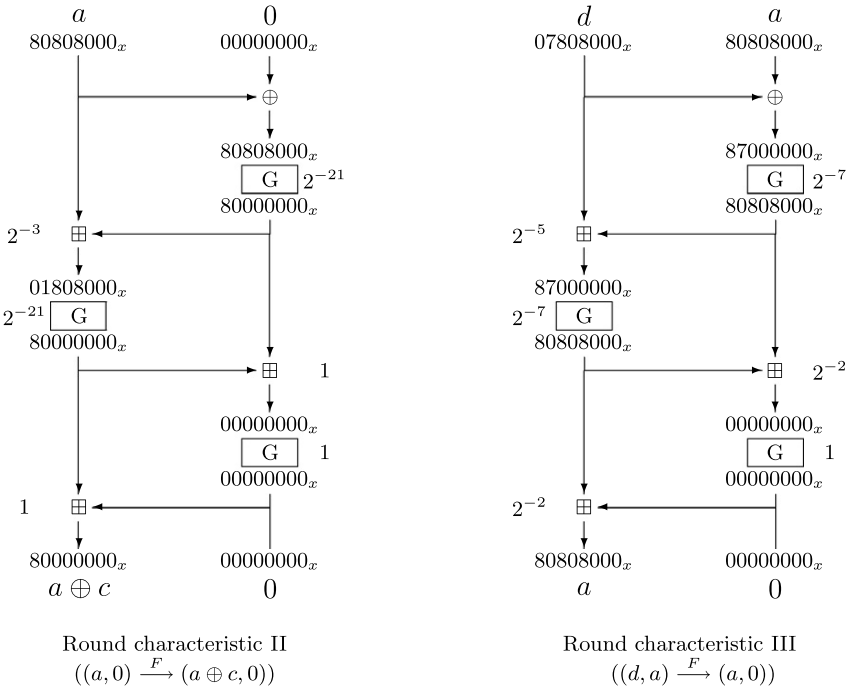

Fig. 6. Round characteristic II and III.

4.2. Improvement of the differential probabilities

In the differential cryptanalysis, we usually use one differential characteristic path which is relatively higher than any of the others. In the typical differential cryptanalysis, however, we only utilize the output difference for an input difference. So this differential characteristic probability is only a lower bound in differential cryptanalysis. If we can compute a multi-pass differential characteristic probability, we can improve the probability. However, in the general case of block ciphers, it is difficult or infeasible to compute this.

In our characteristic in Fig. 4, we use only a one-pass differential characteristic. If we can compute a multi-pass for possible differences between 2nd and 6th rounds, we can improve the probability. However, it is very difficult. Instead, we focus on the round characteristics. We hope to improve p_1, p_4 and p_5.

Let us first consider the round characteristic I of TYPE 1. Let an input and output difference of $f(= f_2 \circ f_1)$ be ΔI and ΔO respectively. Then the exact differential probability is defined as follows.

$$DP\big[\Delta I \xrightarrow{f} \Delta O\big] = \sum_{\Delta T} DP\big[\Delta I \xrightarrow{f_1} \Delta T\big] \cdot DP\big[\Delta T \xrightarrow{f_2} \Delta O\big].$$

With the above definition, we can define p_1 exactly as the following.

$$p_1 = \sum_{\Delta T_4} \sum_{\Delta T_3} \sum_{\Delta T_2} \sum_{\Delta T_1} q_1 q_2 q_3 q_4 q_5 q_6.$$

Now consider the possible values of the ΔT_i's. Since it is infeasible to compute all the possible ΔT_i's, we fix some of the values. Since the output difference of the third G function is 0, ΔT_4 should be fixed as 0. Also in order to get a higher probability $DP[(\Delta T_3, 0) \xrightarrow{\boxplus} 80808000_x]$ we should also fix $\Delta T_3 = 80808000_x$. Furthermore, in order to increase $DP[(\Delta T_1, \Delta T_3) \xrightarrow{\boxplus} 00000000_x]$, we fix $\Delta T_1 = 80808000_x$. Therefore we have the following.

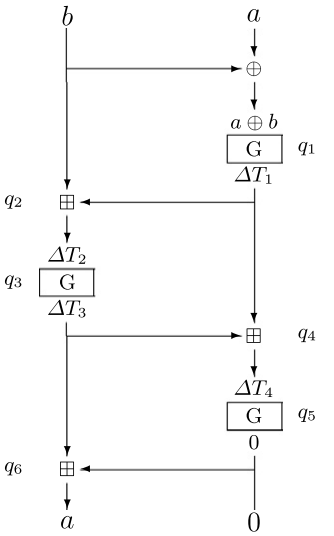

Fig. 7. Differential paths of round characteristic I.

$$\begin{aligned} p_1 &= \sum_{\Delta T_4} \sum_{\Delta T_3} \sum_{\Delta T_2} \sum_{\Delta T_1} q_1 q_2 q_3 q_4 q_5 q_6 \\ &= q_5 \sum_{\Delta T_3} \sum_{\Delta T_2} \sum_{\Delta T_1} q_1 q_2 q_3 q_4 q_6 \end{aligned}$$

Table 3
Possible ΔT_2 values in the round characteristic I of TYPE 1.

Index	$\Delta T_2 = A000000_x$	q_2	q_3	q_2q_3
1	01000000_x	2^{-5}	2^{-7}	2^{-12}
2	03000000_x	2^{-5}	2^{-7}	2^{-12}
3	04000000_x	2^{-5}	2^{-7}	2^{-12}
4	05000000_x	2^{-5}	2^{-7}	2^{-12}
5	07000000_x	2^{-5}	2^{-6}	2^{-11}
6	09000000_x	2^{-6}	2^{-7}	2^{-13}
7	$0b000000_x$	2^{-6}	2^{-7}	2^{-13}
8	$0d000000_x$	2^{-6}	2^{-7}	2^{-13}
9	$0f000000_x$	2^{-6}	2^{-7}	2^{-13}
10	18000000_x	2^{-7}	2^{-7}	2^{-14}
11	$1b000000_x$	2^{-7}	2^{-7}	2^{-14}
12	39000000_x	2^{-8}	2^{-7}	2^{-15}
13	$3e000000_x$	2^{-8}	2^{-7}	2^{-15}
14	79000000_x	2^{-9}	2^{-7}	2^{-16}
15	$7a000000_x$	2^{-9}	2^{-7}	2^{-16}
16	$7b000000_x$	2^{-9}	2^{-7}	2^{-16}
17	$7c000000_x$	2^{-9}	2^{-7}	2^{-16}
18	$7d000000_x$	2^{-9}	2^{-7}	2^{-16}
19	$7e000000_x$	2^{-9}	2^{-7}	2^{-16}
20	$f8000000_x$	2^{-9}	2^{-7}	2^{-16}
21	$fa000000_x$	2^{-9}	2^{-7}	2^{-16}
22	$fe000000_x$	2^{-9}	2^{-7}	2^{-16}
23	$ff000000_x$	2^{-9}	2^{-7}	2^{-16}
	$r = \sum_{\Delta_2} q_2q_3$			$0.002289 \simeq 2^{-9}$

$$\geqslant q_5q_6 \sum_{\Delta T_2} \sum_{\Delta T_1} q_1q_2q_3q_4$$

$$\geqslant q_1q_4q_5q_6 \sum_{\Delta T_2} q_2q_3 = 2^{-10} \cdot \sum_{\Delta T_2} q_2q_3.$$

In order to improve p_1, we have to increase $r = \sum_{\Delta T_2} q_2q_3$. The following is the more explicit expression of r.

$$r = \sum_{\Delta T_2} DP\big[(87808000_x, 80808000) \xrightarrow{\boxplus} \Delta T_2\big] \cdot DP\big[\Delta T_2 \xrightarrow{G} 80808000_x\big].$$

In order to satisfy $P[\Delta T_2 \xrightarrow{G} 80808000_x] > 0$, the last three bytes of ΔT_2 should be zero. This means that $\Delta T_2 = A000000_x$, where A is an arbitrary nonzero byte. In this circumstance we find all the possible values of ΔT_2, which satisfy $DP[A_x \xrightarrow{S_2} 80_x]$. Also ΔT_2 should be satisfied such that $DP\ [(87808000_x, 80808000) \xrightarrow{\boxplus} \Delta T_2]$ is nonzero. In our simulation we find 23 possible values of ΔT_2 and increase p_1 from 2^{-22} to 2^{-19}. This is summarized in Table 3.

In the similar fashion, we can compute p_4 and p_5 of TYPE 1. As a result, we have $p_4 = 2^{-44}$ and $p_5 = 2^{-20}$. We can apply this to TYPE 2 using the same method. We denote DCP as the differential characteristic probability, which considers only one-path. Also we denote *DP* as the differential probability, which considers multi-paths. Then our probabilities of TYPE 1 and 2 can be improved as shown in Table 4.

Table 4
Comparison between DCP and DP of TYPE 1 and 2.

	TYPE 1		TYPE 2	
	DCP	**DP**	DCP	**DP**
p_1	2^{-21}	$\mathbf{2^{-19}}$	2^{-22}	$\mathbf{2^{-20}}$
p_4	2^{-45}	$\mathbf{2^{-44}}$	2^{-45}	$\mathbf{2^{-44}}$
p_5	2^{-23}	$\mathbf{2^{-20}}$	2^{-22}	$\mathbf{2^{-20}}$
6R: $p_1^2p_4p_5$	2^{-110}	$\mathbf{2^{-102}}$	2^{-111}	$\mathbf{2^{-104}}$
7R: $p_1^2p_4p_5^2$	2^{-133}	$\mathbf{2^{-122}}$	2^{-133}	$\mathbf{2^{-124}}$

With the above result we can mount an eight-round attack on SEED by applying the typical differential attack, which is the same as the previous attack in [7]. The signal-to-noise S/N of our attack is about $2^6 (= 2^{-58} \cdot 2^{64})$, which is higher than 2^4 of the previous seven-round attack in [7]. Therefore we can deduce the right key with about $2^{125} \times (= 2 \cdot 4 \cdot 2^{122})$ chosen plaintexts. The attack requires less than $2^{122} (= 2 \cdot 2^{60} \cdot 2^{64} \cdot 1/8)$ eight-round encryptions.

5. Conclusion

We have proposed a new seven-round differential characteristic of SEED and firstly analyzed eight-round SEED. We have also calculated the probabilities more exactly. Our eight-round attack extended the previous differential attack, which only penetrated up to 7 rounds.

References

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, Camellia: A 128-bit block cipher suitable for multiple platforms – Design and analysis, in: Selected Areas in Cryptography, in: Lecture Notes in Computer Science, vol. 1281, Springer-Verlag, 2000, pp. 39–56.
[2] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystem, Journal of Cryptology 4 (1) (1991) 3–72.
[3] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, K. Ohta, A strategy for constructing fast functions with practical security against differential and linear cryptanalysis, in: Selected Areas in Cryptography, in: Lecture Notes in Computer Science, vol. 1556, Springer-Verlag, 1999, pp. 264–279.
[4] ISO/IEC 18033-3, Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers, International Organization for Standardization, 2005.
[5] Korea Information Security Agency, A design and analysis of 128-bit Block Cipher SEED, available at http://www.kisa.or.kr/kisa/seed/jsp/seed_1010.jsp, 1999.
[6] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS PUB 197, 2001.
[7] H. Yanami, T. Shimoyama, Differential cryptanalysis of a reduced-round SEED, in: SCN 2002, in: Lecture Notes in Computer Science, vol. 2576, Springer-Verlag, 2002, pp. 186–198.