A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent

Joo Yeon Cho, Miia Hermelin, and Kaisa Nyberg

Helsinki University of Technology,
Department of Information and Computer Science,
P.O. Box 5400, FI-02015 TKK, Finland
{joo.cho,miia.hermelin,kaisa.nyberg}@tkk.fi

Abstract. In this paper, we present a new technique for Matsui's algorithm 2 using multidimensional linear approximation. We show that the data complexity of the attack can be reduced significantly by our method even when the linear hull effect is present. We apply our method to the key recovery attack on 5-round Serpent and demonstrate that our attack is superior to previous attacks. We present evidence that it is theoretically possible to reduce the data complexity of the linear attack against 10 round Serpent by factor of 2^{20} when multiple approximations are used.

Keywords: Block Ciphers, Linear Cryptanalysis, Serpent, Multidimensional Linear Approximation.

1 Introduction

Linear cryptanalysis is one of the most important methods of attack against block ciphers. Since Matsui introduced the linear cryptanalysis on DES in 1993, several attempts to generalize linear attack have been published. One approach is to use multiple linear approximations for the linear attack. In 1994, Kaliski and Robshaw [9] showed that the efficiency of the attack could be improved by using multiple linear approximation depending on the same key parity bit. In 2004, Biryukov, et al., [4] proposed a statistical framework for Matsui's algorithm 1 and 2 using multiple linear approximations and assuming similarly to [9] that the approximations are statistically independent. More rigorous statistical framework was proposed independently by Baignères, et al., in [2]. In 2008, Hermelin, et al., proposed a multidimensional statistical framework for Matsui's algorithm 1, for which the assumption on statistical independence is not needed [8].

In 2008, Collard, et al., [6] presented experimental results on the linear attack of Biryukov, et al., against reduced round Serpent. They showed that a linear attack on Serpent using Matsui's algorithm 1 could be improved significantly by exploiting multiple linear approximations, whereas a similar reduction of data complexity was not achieved using Matsui's algorithm 2. Authors claimed that

P.J. Lee and J.H. Cheon (Eds.): ICISC 2008, LNCS 5461, pp. 383–398, 2009.

this inconsistency was caused by the lack of good theoretical estimations of the correlations of the approximations due to the linear hull effect [10].

In this paper, we propose new techniques for Matsui's algorithm 2 using multiple linear approximations. In a similar way as in [8], we focus on the distribution of the multiple approximations rather than individual correlations. We present an efficient algorithm to apply the relative entropy between distributions for finding the right key in Matsui's algorithm 2. We also show that the maximum entropy of the distributions can be used to improve the efficiency of the key recovery attack when the distributions satisfy a certain general condition. We apply our techniques to reduced round Serpent and demonstrate that our method can reduce the data complexity of the attack significantly compared to the results of [6]. Hence, it seems to us that the linear hull effect is not the only reason to account for the experimental results of Matsui's algorithm 2 presented in [6].

This paper is organized as follows. In Section 2, the technical background of our attack method is presented. In Section 3, multiple linear approximations for reduced round Serpent are set up and the dependency of the theoretical advantage of the attack is illustrated for different cases according to the number of linearly independent linear approximations. In Section 4, previously proposed generalizations of linear attacks are described and the experimental results are shown. In Section 5, the new techniques are applied to reduced round Serpent and the experimental results are presented. Section 6 concludes this paper.

2 Technical Background

The first step in a traditional linear attack using Matsui's algorithm 2 is to find a linear approximation for the cipher that has the largest bias. Then, an attacker collects a large amount of plaintext-ciphertext pairs and counts the number of pairs that satisfy the linear approximation for each possible key values. The maximum bias over the counted samples indicates the right key value.

In a multidimensional linear attack, the attacker finds a class of linearly independent approximations whose biases are non-negligible. We call such linear independent approximations *base approximations.* If m linearly independent approximations are established, then additional $2^m - 1 - m$ approximations can be constructed as linear combinations of the m base approximations.

Provided that we have $2^m - 1$ approximations and their probabilities are $p_1, \ldots, p_{2^m-1}$, the *capacity* of the approximations, which is denoted by C, is defined as [4]

$$C = \sum_{i=1}^{2^m-1} (2p_i - 1)^2 = \sum_{i=1}^{2^m-1} c_i^2,$$

where $c_i = 2p_i - 1$ is called the *correlation* of the ith approximation.

In [2], a generalized statistical framework of the multidimensional linear attack was proposed. Let us consider a process that generates independent random variables $Z_{1,K}, Z_{2,K}, \ldots, Z_{2^m,K}$ depending on the key $K \in GF(2^l)$. Let K_0 denote the right key and $K_1, \ldots, K_{2^l-1}$ be the wrong key values. We assume that for $K = K_0$, all variables $Z_{i,K}$'s follow the distribution D_0, whereas for $K \neq K_0$, all $Z_{i,K}$'s follow the distribution D_1.

Suppose that we target to recover l-bit last round key. Once m base approximations have been established over all rounds of the cipher except for the last round, the linear attack using multiple approximations proceeds in four phases.

- **Counting Phase.** Collect the samples of the plaintext-ciphertext pairs on the targeted cipher and counts the number of samples which satisfy m-dimensional linear approximation.
- **Analysis Phase.** For each of the 2^l candidate keys, measure the distance of the empirical distribution from the theoretical distribution.
- **Sorting Phase.** Sort 2^l candidate keys according to their distances.
- **Searching Phase.** Exhaustively try all the candidate keys in the sorted order until the correct key is found.

In the analysis phase, the relative entropy between two distributions is measured as follows:

Definition 1. *The relative entropy or Kullback-Leibler distance between two distribution D_0 and D_1 is defined as*

$$D(D_0||D_1) = \sum_{z \in Z} Pr_{D_0}[z] \log \frac{Pr_{D_0}[z]}{Pr_{D_1}[z]}$$

with the assumptions that $p \log \frac{p}{0} = 0$ and $0 \log \frac{0}{p} = 0$.

Let $\Delta(D)$ denote the Squared Euclidean Imbalance [2] of the distribution D of a random variable taking values in the set $Z \subset GF(2^m)$. It is defined as

$$\Delta(D) = |Z| \sum_{z \in Z} (Pr_D[z] - \frac{1}{|Z|})^2.$$

Note that $C = \Delta(D)$ if D is the probability distribution of m base approximations as shown in [8].

Let N denote the number of samples and $\Phi(t)$ denote the cumulative normal distribution function that is defined as

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{1}{2}u^2} du.$$

We apply the key ranking procedure, originally developed in [2] for the LLR-statistic, to the Kullback-Leibler distance, and assume that $D(D_0||D_1)|_{K=K_0} - D(D_0||D_1)|_{K \neq K_0}$ is approximately normally distributed with mean $\mu = N\Delta(D)$ and standard deviation $\sigma = \sqrt{2N\Delta(D)}$ [2]. Thus, the probability that a wrong key $K \neq K_0$ has a better rank than K_0 is approximately $\Phi(-\mu/\sigma) = \Phi(-\sqrt{N\Delta(D)/2})$ when the number of samples is large. Since the rank of K_0 is

$$1 + \sum_{K} 1_{D(D_0||D_1)|_{K=K_0} < D(D_0||D_1)|_{K \neq K_0}}$$

so the expected rank of K_0 is $1 + (2^l - 1)\Phi(-\sqrt{N\Delta(D)/2})$ [12,2].

In [11], Selçuk provided a statistical analysis of the success probability of linear cryptanalysis. If the correct value of the l-bit key is ranked at the r-th position out of 2^l possible candidates, the attack obtains an $(l - \log r)$-bit *advantage* over exhaustive search [11].[1] Therefore, the advantage a of the attack is expressed as

$$a = l - \log r = l - \log(1 + (2^l - 1)\Phi(-\sqrt{N\Delta(D)/2})) \qquad (1)$$

3 Multiple Linear Approximations of 4 Round Serpent

Suppose that we have m base approximations which are described as follows:

$$u_i \cdot P \oplus v_i \cdot C = \kappa_i \cdot K, \quad i = 1, \ldots, m$$

where u_i, v_i and κ_i stand for the input mask, output mask and the key mask, respectively. Also, P, C and K represent the plaintext, ciphertext and the key, respectively. The "$\cdot$" operation means a standard inner product. Given $\gamma = (\gamma_1, \ldots, \gamma_m)$ where $\gamma_i \in \{0, 1\}$ and $\gamma \neq (0, \ldots, 0)$, a combined approximation is constructed by

$$\bigoplus_{i=1}^{m} \gamma_i (u_i \cdot P \oplus v_i \cdot C) = \bigoplus_{i=1}^{m} \gamma_i (\kappa_i \cdot K).$$

Hence, we obtain $2^m - 1$ approximations in total.

We target to attack the 5-round Serpent using Matsui's algorithm 2. For this, we need to establish a chain of linear approximations over 4 rounds that has a significant bias. The best linear approximations for the 4-round Serpent were presented in [3] and [7]. Due to the structure of the round function of Serpent, one can obtain several linear approximations that hold with equal or slightly smaller bias based on the same round approxiamtions. The input and output masks on the base approximations used for our attack are listed in Table 3 in Appendix B. The linear approximations start from round 4 (using S-box 4) and end up in round 7 (using S-box 7). The output mask is chosen in such a way the number of active S-box in round 8 is minimal. Hence, the multiple approximations use only a single output mask and it is denoted as v_1 in Table 3.

Table 1 shows the correlations and the capacity of approximations for different numbers m of base approximations by which $2^m - 1$ approximations are obtained in total. Note that the base approximations are taken from the top of the list from Table 3 in order. Using Equation (1) and Table 1, we derive, for different values of m, the relation between the advantage of the attack and data complexity, which is illustrated in Figure 1.

So far, two types of linear attacks using multiple linear approximations have been investigated in the literature: linear attack using correlation (or type-I attack) and linear attack using distribution (or type-II attack). The attacks presented in [4] and [6] can be classified as type-I attack, whereas the multidimensional attack in [8] is a type-II attack. In the next section, we apply type-I attack to reduced round Serpent and show the experimental results.

[1] A slightly different measure of success was proposed for use in [4] where it was called as *gain*.

Table 1. The correlations and capacities according to 1, 4, 7, 10 and 12 base approximations

# base appr.		1	4	7	10	12
# combined appr.		0	11	120	1013	4083
correlation	2^{-13}	1	8	8	8	8
	2^{-14}	0	0	32	64	80
	2^{-15}	0	0	0	128	256
	2^{-16}	0	0	0	0	256
	0	0	7	87	823	3495
capacity		2^{-26}	2^{-23}	2^{-22}	2^{-21}	$2^{-20.42}$

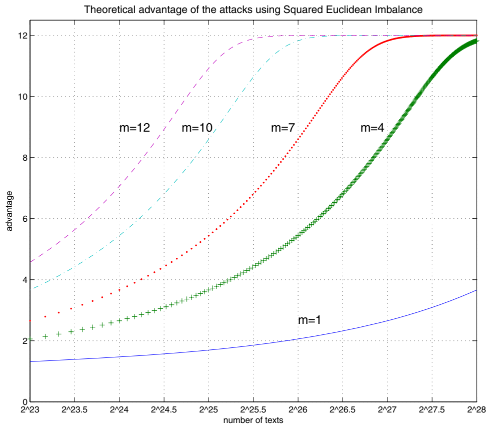


Fig. 1. Evaluation of the theoretical advantage of attacks using 1,4,7,10 and 12 base approximations

4 Linear Attacks Using Correlations of Multiple Approximations

Suppose that we have M linear approximations with correlations $c_1, \ldots, c_M$. The empirical correlations of M approximations by the key K are denoted by $\hat{c}_{1,K}, \ldots, \hat{c}_{M,K}$. Then, we consider the sum of the square of the correlations

$$||\hat{c}_K||^2 = \sum_{i=1}^{M} \hat{c}_{i,K}^2, \text{ where } K = 0, \ldots, 2^l - 1. \tag{2}$$

According to the wrong key hypothesis, it is assumed that $\hat{c}_{i,K \neq K_0}$ does not have any correlation (just like a random variable). Thus, the distance $||\hat{c}_K||^2$ by the correct key $K = K_0$ is expected to be significantly higher than the one induced by incorrectly guessed key $K \neq K_0$. Hence, the correct key can be recovered by taking K whose $||\hat{c}_K||^2$ is maximal.

In this method, it is not important whether the empirical correlations by the right key are matched to the theoretically calculated values or not. On the other hand, a method which Biryukov, et al., suggested in [4] is to extend Matsui's algorithm 1 for Matsui's algorithm 2 using multiple approximations. Hence, the accuracy of theoretically calculated correlations affects the performance of the attack.

Let us denote the parity key bits of the M approximations by $G = (g_1, \ldots, g_M)$, that is, $u_i \cdot P + v_i \cdot C = g_i$ where $1 \leq i \leq M$. For each value of a pair (K, G), a vector of theoretical correlations is constructed as follows:

$$c_{K,G} = (0, \ldots, 0, (-1)^{g_1} c_1, \ldots, (-1)^{g_M} c_M, 0, \ldots, 0),$$

where the location of the subvector $((-1)^{g_1} c_1, \ldots, (-1)^{g_M} c_M)$ depends on the value of K. Hence, the vector $c_{K,G}$ has $M \times 2^l$ entries and the number of possible pairs is $2^m \times 2^l$. Then, the distance between empirical correlation and theoretical correlation is measured using the following equation:

$$||\hat{c}_K - c_{K,G}||^2 = \sum_{j=1}^{M} (\hat{c}_{j,K} - (-1)^{g_j} c_j)^2 + \sum_{\kappa \neq K} \sum_{j=1}^{M} \hat{c}_{j,\kappa}^2. \tag{3}$$

The correct key is recovered by taking the key value whose $||\hat{c}_K - c_{K_i,G}||^2$ is minimal. If the linear hull effect [10] is not present, Equation (3) is slightly better than Equation (2) since two terms in Equation (3) are distinguishable for each value of K and G.

We applied two type-I attacks to the 5-round Serpent with various multiple linear approximations taken from Table 1. The experimental results are displayed in Figure 2. We can see in this figure that the advantage of the attack is far worse than the theoretical expectation shown in Figure 1. Furthermore, when more than 4 base approximations are used, the advantage of the attack becomes worse even though the capacity increases. This exemplifies that the data complexity required for the type-I attacks depends not only on the capacity but also on the distribution of approximations. The (exact) relation between the capacity, the number of approximations and data complexity required for the type-I attack remains an open problem.

5 Linear Attacks Using Distribution of Multiple Approximations

In this section, we propose new techniques on the linear attack using the distribution of multiple approximations. Our attack can be seen as an extension of the multidimensional linear attack [8] that was applied to Matsui's algorithm 1.

Suppose we have m base approximations and the boolean values of m approximations are $G = (g_1, \ldots, g_m)$. Using m base approximations, we build $2^m - 1$ approximations whose correlations are $c_1, \ldots, c_{2^m-1}$. Then, the theoretical prob-

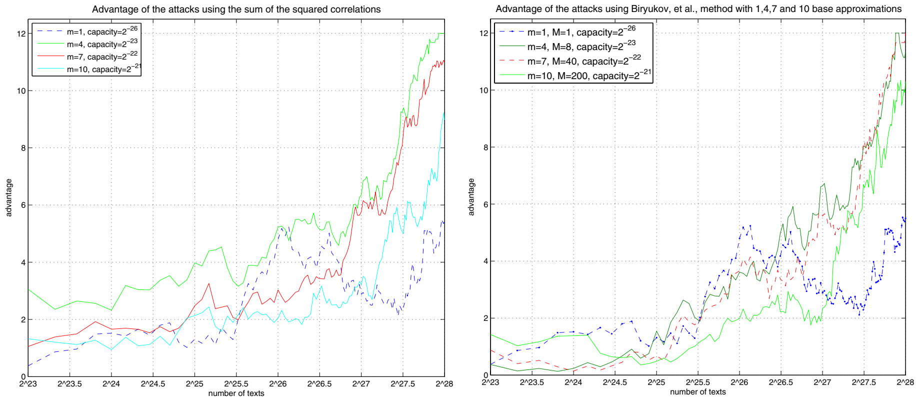


Fig. 2. Type-I linear attacks with 1, 4, 7 and 10 base approximations using Equation (2) (left) and (3) (right)

ability distribution of approximations is constructed in the following way [8]:

$$p_{i,G} = 2^{-m} + 2^{-m} \sum_{j=1}^{2^m-1} (-1)^{j \cdot i \oplus j \cdot G} c_j, \text{ where } i, G \in \{0,1\}^m. \tag{4}$$

Note that the size of theoretical distribution is $2^m \times 2^m$.

Let $P_G = (p_{0,G}, \dots, p_{2^m-1,G})$ denote the theoretical distributions by the G. Then, it is clear from Equation (4) that the distribution G has the following property:

Property 1. A distribution $P_{G'}$ is a permutation of P_G for all $G' \neq G$. In particular, $p_{i,G} = p_{\bar{i},\bar{G}}$ where $\bar{X}$ is a bitwise negation of X.

Let us remind that only one output mask is used for the base approximations. This is a common situation for Matsui's algorithm 2 using multiple approximations for minimizing the active S-boxes. Since the output mask v_i for all base approximations is the same, only odd number of combinations of the base approximations have nonzero correlations among $2^m - 1$ possible approximations. Thus, Equation (4) is equivalently expressed as

$$p_{i,G} = 2^{-m} + 2^{-m} \sum_{j \in V_m} (-1)^{j \cdot i \oplus j \cdot G} c_j. \tag{5}$$

where $V_m = \{\nu | 0 < \nu < 2^m, \text{Hamming weight of } \nu \text{ is odd}\}$. From Equation (5), we can derive the following property:

Property 2. Since $\nu \cdot G \oplus \nu \cdot \bar{G} = 1$ for $\nu \in V_m$, we have

$$p_{i,G} = 2^{-m} + 2^{-m} \sum_{j \in V_m} (-1)^{j \cdot i \oplus j \cdot G} c_j = 2^{-m} + 2^{-m} \sum_{j \in V_m} (-1)^{j \cdot i \oplus j \cdot \bar{G} \oplus 1} c_j = 2^{-m+1} - p_{i,\bar{G}}.$$

By similar reason, we get $p_{\bar{i},G} = 2^{-m+1} - p_{i,G}$.

Since we target to recover l-bit of the last round key, we obtain 2^l empirical distributions for each of candidate key in the counting phase. Let $\hat{Q}_K = (\hat{q}_{0,K}, \dots, \hat{q}_{2^m-1,K})$ denote the empirical distribution by the key K. It is known that a relative entropy between two distributions is measured optimally by Kullback-Leibler distance [2,8]. According to Definition 1, the Kullback-Leibler distance between the empirical distribution $\hat{Q}_K = (\hat{q}_{0,K}, \dots, \hat{q}_{2^m-1,K})$ by K and the theoretical distributions $P_G = (p_{0,G}, \dots, p_{2^m-1,G})$ by G is calculated as follows:

$$D(\hat{Q}_K||P_G) = \sum_{i=0}^{2^m-1} \hat{q}_{i,K} \log \frac{\hat{q}_{i,K}}{p_{i,G}}. \tag{6}$$

Once the empirical distribution for each candidate key is obtained, the analysis phase of our attack proceeds in two steps:

- **Step 1:** For each K, measure the distances $D(\hat{Q}_K||P_G)$ for all candidates of $G \in \{0,1\}^m$ and sort the candidates of G according to their distances.
- **Step 2:** For sorted values of G, measure $D(\hat{Q}_K||P_G)$ for all candidates of $K \in \{0,1\}^l$.

The step 1 applies Matsui's algorithm 1 to determine the right value of G, whereas in the step 2, Matsui's algorithm 2 is applied to recover the right value of K.

5.1 Using the Maximum Distance

In the original Matsui's algorithm 1, the correct parity key bit has the minimum Euclidean distance, whereas the maximum Euclidean distance indicates the opposite sign of the correct parity key. When multiple approximations are applied to Matsui's algorithm 1, it is natural to think that the correct values of multiple parity key bits hold the minimum squared Euclidean distance by Equation (2), whereas the opposite signed key parity bits have the maximum squared Euclidean distance. In this way, the maximum distance has the same amount of information as the minimum distance. However, it has been often ignored and not used for the linear attacks on the block ciphers.

When the distribution of the approximations is taken into account under the condition that all multiple approximations have the same output masks, a similar intuition can be applied. Due to Property 1, if $p_{i,G} = 2^{-m} + \epsilon_i$, then, $p_{i,\bar{G}} = 2^{-m} - \epsilon_i$. Hence, if the right value of G has the minimum value of $D(\hat{Q}_K||P_G)$, then, equivalently, the right value of $\bar{G}$ is expected to have the maximum value of $D(\hat{Q}_K||P_{\bar{G}})$. This intuition is proved in the following lemma:

Lemma 1. *Suppose that only a single output mask is used for m base approximations. Let G_{min} (resp. G_{max}) denote the G such that $D(\hat{Q}_K||P_G)$ is minimal (resp. maximal). If K is the correct key, then G_{min} and G_{max} are expected to have equivalent information and $G_{max} = \bar{G}_{min}$ where $\bar{X}$ is a bitwise negation of X.*

Proof. (*sketch*) For fixed G_0, we can write

$$D(\hat{Q}_K||P_{G_0}) - D(\hat{Q}_K||P_G) = \sum_{i=0}^{2^m-1} \hat{q}_{i,K} \log \frac{p_{i,G}}{p_{i,G_0}} = \sum_{i=0}^{2^m-1} \hat{q}_{i,K} \log \frac{p_{\bar{i},\bar{G}}}{p_{\bar{i},\bar{G}_0}}. \tag{7}$$

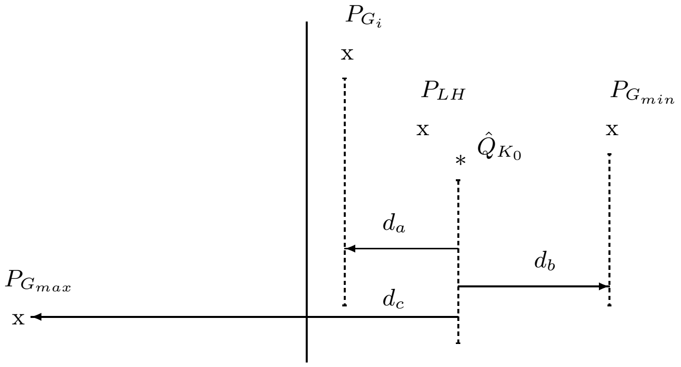


Fig. 3. An example of the usage of G_{max} when linear hull effect is present

It is expected that $\hat{Q}_K \approx P_G$ for some G if K is the right key. Thus, by Property 2, we can put $\hat{q}_{i,K} \approx 2^{-m+1} - \hat{q}_{\bar{i},K}$. Then, Equation (7) is approximated by

$$\sum_{i=0}^{2^m-1} (2^{-m+1} - \hat{q}_{\bar{i},K}) \log \frac{p_{\bar{i},\bar{G}}}{p_{\bar{i},\bar{G}_0}} = -\sum_{i=0}^{2^m-1} \hat{q}_{\bar{i},K} \log \frac{p_{\bar{i},\bar{G}}}{p_{\bar{i},\bar{G}_0}} = -\sum_{i=0}^{2^m-1} \hat{q}_{i,K} \log \frac{p_{i,\bar{G}}}{p_{i,\bar{G}_0}}$$
$$= D(\hat{Q}_K||P_{\bar{G}}) - D(\hat{Q}_K||P_{\bar{G}_0}).$$

since $\sum_{i=0}^{2^m-1} \log \frac{p_{\bar{i},\bar{G}}}{p_{\bar{i},\bar{G}_0}} = 0$ from Property 1. Hence, for any $G \neq G_0$, if $D(\hat{Q}_K||P_{G_0}) > D(\hat{Q}_K||P_G)$, then $D(\hat{Q}_K||P_{\bar{G}}) > D(\hat{Q}_K||P_{\bar{G}_0})$. □

However, our experiments showed that G_{max} was not always equal to $\bar{G}_{min}$. The reason is that, in practice, the theoretical distributions (which are constructed by the theoretical correlations) are not accurate due to the linear hull effect. In particular, our experiments show that the maximum distance is more reliable than the minimum distance.

Figure 3 provides an example of this situation. Let us assume that K_0 is the right key and P_{LH} is a true distribution. (LH denotes the linear hull.) Then, it is expected that an empirical distribution Q_{K_0} is close to P_{LH}. If a distribution $P_{G_{min}}$ is different from P_{LH}, there exist possibilities that $D(\hat{Q}_{K_0}||P_{G_{min}}) > D(\hat{Q}_{K_0}||P_{G_i})$ for some $G_i \neq G_{min}$. However, in the same situation, the relation $D(\hat{Q}_{K_0}||P_{G_{max}}) > D(\hat{Q}_{K_0}||P_{G_i})$ persists as illustrated in Figure 3. If the minimum distance is measured, G_i is (wrongly) guessed as a correct G since $d_b > d_a$. On the other hand, if the maximum distance is measured, G_{max} is guessed as a negation of correct G, since $d_c > d_a$. Our experimental results also show that a key recovery attack using G_{max} is superior to that using G_{min}. Hence, the right key is more reliably recovered by taking the key value from

$$\max_K \max_G D(\hat{Q}_K||P_G).$$

This observation is experimentally verified in Figure 4. More discussions on the experiments will be given in Subsection 5.4.

5.2 Summary of Our Method for Matsui's Algorithm 2

Given N plaintext-ciphertext pairs, our attack is described as follows.

- Initialize 2^l counters where l denotes the targeted key bits of the last round key.
- Compute the theoretical distribution of m approximations for each value of m parity bits and store them in a $2^m \times 2^m$-table.

- For each of the l-bit value of the last round key,
    - Decrypt the ciphertext partially using the guessed l-bit value of the last round key.
    - Compute the XOR of the input parity and output parity for each approximation.
    - Build an m-bit vector whose coordinates correspond the XORed parity bits of approximations.
    - Increment the counter indexed by both the vector and the l-bit guessed key.

- For each of the l-bit value of the last round key
    - For each of the m-bit value of the parity key, measure the Kullback-Leibler distance between the empirical distributions indexed by the l-bit value and the theoretical distribution indexed by the m-bit value.
    - Choose the maximum value of $D(\hat{Q}_K||P_G)$ for each K and store it as $D(\hat{Q}_K||P_{G_{max}})$.

- Sort all the candidate last round key using their values of $D(\hat{Q}_K||P_{G_{max}})$.
- Exhaustively try all keys from the sorted list of all candidate until the correct key is found.

5.3 Comparison of Time and Memory Complexity

Suppose that the number of base approximations for multidimensional linear attack is m and the targeted key size is l bits. For type-I attacks, we assume that M linear dependent approximations are used where m parity key bits are involved. Thus $m \leq M < 2^m$.

In the counting phase, for each key candidate and for each plaintext-ciphertext pair, type-I attacks need to update M counters by evaluating M approximations, while multidimensional attacks need to update one of 2^m counters by evaluating m base approximations. In the analysis phase, type-I attacks evaluate M correlations for each candidate of the last round key. In the multidimensional attacks, one distribution consisting of 2^m empirical frequencies is compared with 2^m different theoretical distributions by computing KL distances, where each KL distance has 2^m terms. The time complexity of multidimensional attack and type-I attacks using N plaintext-ciphertext pairs are summarized in Table 2.

Table 2. The time complexity of type-I attacks and multidimensional attack

	Squared Correlations Sum (Eq. (2))	Biryukov, et al., (Eq. (3))	Multidimensional
Counting phase	$N \cdot M \cdot 2^l$	$N \cdot M \cdot 2^l$	$N \cdot m \cdot 2^l$
Analysis phase	$M \cdot 2^l$	$M \cdot 2^{2l+m}$	2^{l+2m}
Recovered Key	l bits	$(l+m)$ bits	$(l+m)$ bits

For memory complexity, type-I attacks require 2^m storage for counters and multidimensional attack requires 2^{2m+1} storage for both the counters and the theoretical distribution.

Note that the multidimensional attack and the method of Biryukov, et al., can retrieve the information on the last round key K and the key parity G together. On the other hand, type-I attack using the sum of squares of correlations, see Equation (2), can recover the last round key K only.

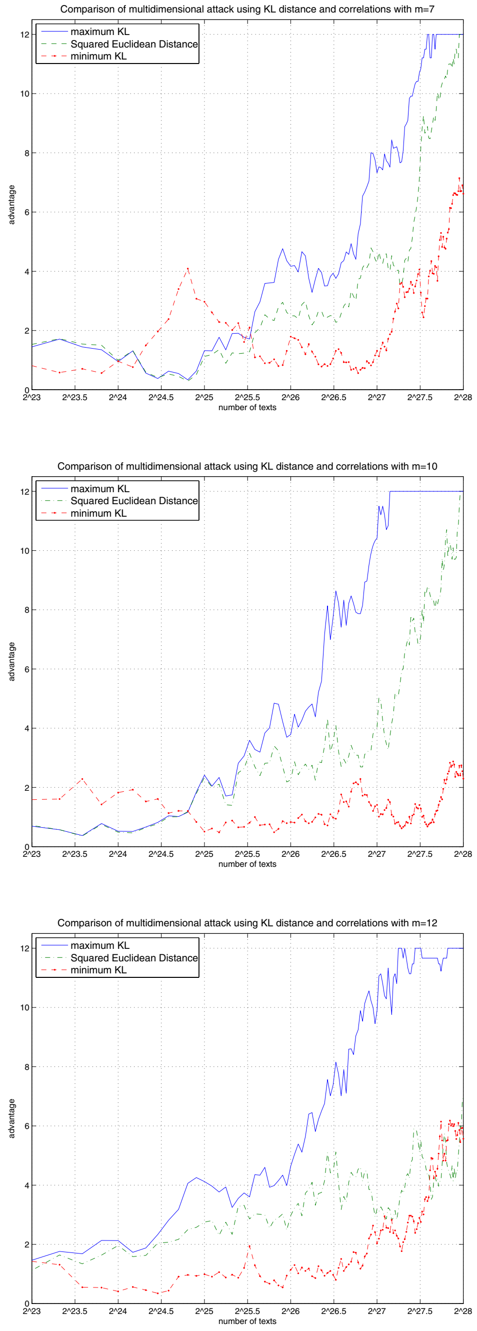
5.4 Experimental Results

We applied our attack algorithm to the 5-round Serpent. We picked up 7, 10 and 12 base approximations from Table 1 and targeted to recovering of 12 bits of the last round key. The experimental results are displayed in Figure 4 and the results of type-I attacks are compared to them. In the experiments, the 128-bit secret keys and plaintexts were randomly generated and ciphertexts were collected by encrypting the plaintexts using 5-round Serpent.

Figure 4 shows that the advantage of the multidimensional linear attack using the maximum Kullback-Leibler Distance is significantly higher than for the other attacks. We also show that multidimensional attack using the minimum Kullback-Leibler Distance is worse than the other attacks. This suggests that the linear attack using the minimum distance may be more vulnerable to the linear hull effect. Finally, we note that our experimental results are still worse than the theoretical curves in Figure 1 that were drawn by Equation (1). Further research is required for the statistical modeling of multidimensional linear approximation and to find the optimal multidimensional extension of Matsui's algorithm 2 and to accurately predict its performance.

5.5 Extension for Further Rounds of Serpent

Our attack can be further applied for a larger number of round of Serpent since we can obtain multiple approximations simply by applying various input masks in the first round. For instance, the linear attacks on 10-round Serpent in [3] use a 9-round linear approximation with probability of $\frac{1}{2}(1-2^{-57})$. Thus, the capacity of the best single approximation is $2^{-2\times 57} = 2^{-114}$. On the other hand, we can construct multiple linear approximations from the same linear trail of 9-round Serpent. The first round of the linear trail includes 10 active S-boxes and each S-box has 10 non-negligible approximations (2 for 2^{-1} and 8 for 2^{-2} correlations for each S-box) for a fixed output. Thus, we can construct in total $10^{10} \approx 2^{33}$ approximations that have non-negligible correlations. The best correlation of the


Comparison of multidimensional attack using KL distance and correlations with m=7

Comparison of multidimensional attack using KL distance and correlations with m=10

Comparison of multidimensional attack using KL distance and correlations with m=12

Fig. 4. Comparison of multidimensional attacks and other attacks with various base approximations

first round approximation is 2^{-10} and the number of approximations with the best correlations is 2^{10}. In the same way, the second best correlation of the first round approximation is 2^{-11} and 10×2^{12} approximations hold such correlation, and so on. Hence, the capacity of 2^{33} approximations can be computed as

$$C = 2^{10}\binom{10}{0}2^{-57\times 2} + 2^{12}\binom{10}{1}2^{-58\times 2} + \cdots + 2^{30}\binom{10}{10}2^{-67\times 2} = 2^{-94}. \quad (8)$$

Therefore, the data complexity of linear attack on 10 round Serpent can be reduced theoretically by a factor of 2^{20} at the cost of increased time complexity.

In [5], Collard et al. also presented the multiple linear attacks against 10-round Serpent. According to [5], the best attack on 10-round Serpent needs 2^{99} known plaintexts with 2^{99} time complexity and 2^{55} memory for recovering 44 bits of the last round key. This attack uses $M = 2^{11}$ linear approximations and each approximation has the equal bias of 2^{-55}. Hence, the capacity is $(2 \cdot 2^{-55})^2 \cdot 2^{11} = 2^{-97}$.

On the other hand, the multidimensional linear attack method allows us to use all the linear approximation involved in 9-round linear trails within the span of the base approximations. Since the number of active S-boxes of the first round is 11 and each S-box has 10 linear approximations, the number of possible approximations is actually 10^{11}. Hence, the capacity is computed as $2^{11}\binom{11}{0}2^{-54\times 2} + \cdots + 2^{33}\binom{11}{11}2^{-65\times 2} = 2^{-86}$. Therefore, it is theoretically possible to reduce the data complexity of the attack further by a factor of 2^{11}. Instead, the time complexity increases by around $2^{l+2m} = 2^{132}$ with the memory complexity of around $2^{2m+1} = 2^{89}$.

6 Conclusion

In this paper, we proposed a new technique for the multidimensional linear attacks. We showed that the multidimensional linear attack could be very powerful with Matsui's algorithm 2 when multiple linear approximations are available in the block ciphers. The improvements we achieved using the new techniques stem from two reasons. Firstly, we take the distribution of the approximations in a multidimensional way and we measure the distances between two distributions using Kullback-Leibler distance instead of the sum of the squared correlations. Secondly, by taking the maximal value of the distances, our method eliminated errors in the situation where correlations of individual linear approximations could not be calculated accurately due to the linear hull effect. However, it is an open problem whether our heuristic technique is optimal and what is its expected performance.

References

1. Anderson, R., Biham, E., Knudsen, L.: Serpent: A proposal for the advanced encryption standard. In: First Advanced Encryption Standard (AES) conference (1998)
2. Baignères, T., Junod, P., Vaudenay, S.: How Far Can We Go Beyond Linear Cryptanalysis? In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 432–450. Springer, Heidelberg (2004)

3. Biham, E., Dunkelman, O., Keller, N.: Linear cryptanalysis of reduced round Serpent. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 219–238. Springer, Heidelberg (2002)
4. Biryukov, A., De Cannière, C., Quisquater, M.: On multiple linear approximations. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 1–22. Springer, Heidelberg (2004)
5. Collard, B., Standaert, F., Quisquater, J.: Improved and multiple linear cryptanalysis of reduced round Serpent. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 47–61. Springer, Heidelberg (2008)
6. Collard, B., Standaert, F., Quisquater, J.: Experiments on the multiple linear cryptanalysis of reduced round serpent. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 382–397. Springer, Heidelberg (2008)
7. Collard, B., Standaert, F., Quisquater, J. (Accessed on 31.07.2008), `http://www.dice.ucl.ac.be/fstandae/PUBLIS/50b.zip`
8. Hermelin, M., Cho, J., Nyberg, K.: Multidimensional linear cryptanalysis of reduced round Serpent. In: Mu, Y., Susilo, W., Seberry, J. (eds.) ACISP 2008. LNCS, vol. 5107, pp. 203–215. Springer, Heidelberg (2008)
9. Kaliski, B., Robshaw, M.: Linear cryptanalysis using multiple approximations. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 26–39. Springer, Heidelberg (1994)
10. Nyberg, K.: Linear approximation of block ciphers. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 439–444. Springer, Heidelberg (1995)
11. Seluk, A.: On probability of success in linear and differential cryptanalysis. Journal of Cryptology 21(1), 131–147 (2008)
12. Vaudenay, S.: An experiment on DES statistical cryptanalysis. In: CCS 1996: Proceedings of the 3rd ACM conference on Computer and communications security, pp. 139–147. ACM, New York (1996)

A Brief Description of Serpent Algorithm

We use the notation of [1]. Each intermediate value of round i is denoted by $\hat{B}_i$ (a 128-bit value). Each $\hat{B}_i$ is treated as four 32-bit words X_0, X_1, X_2, X_3 where bit j of X_i is bit $4 * i + j$ of the $\hat{B}_i$. Serpent has a set of eight 4-bit to 4-bit S Boxes $S_0, \ldots, S_7$ and a 128-bit to 128-bit linear transformation LT. Each round function R_i uses a single S-box 32 times in parallel.

Serpent ciphering algorithm is formally described as follows.

$$\begin{aligned} \hat{B}_0 &= P \\ \hat{B_{i+1}} &= R_i(\hat{B}_i) \\ C &= B_{32} \end{aligned}$$

where

$$\begin{aligned} R_i(X) = LT(\hat{S}_i(X \oplus \hat{K}_i)), &\quad i = 0, \ldots, 30 \\ R_i(X) \quad = \hat{S}_i(X \oplus \hat{K}_i) \oplus \hat{K}_{32}, &\quad i = 31 \end{aligned}$$

The linear transformation LT is described as follows.

$$X_0, X_1, X_2, X_3 = S_i(B_i \oplus K_i)$$

$$\begin{aligned}
X_0 &= X_0 \lll 12\\
X_2 &= X_2 \lll 3\\
X_1 &= X_1 \oplus X_0 \oplus X_2\\
X_3 &= X_3 \oplus X_2 \oplus (X_0 \lll 3)\\
X_1 &= X_1 \lll 1\\
X_3 &= X_3 \lll 7\\
X_0 &= X_0 \oplus X_1 \oplus X_3\\
X_2 &= X_2 \oplus X_3 \oplus (X_1 \lll 7)\\
X_0 &= X_0 \lll 5\\
X_2 &= X_2 \lll 22\\
B_{i+1} &= X_0, X_1, X_2, X_3
\end{aligned}$$

The detailed description of Serpent can be found in [1].

B Linearly Independent Approximations on 4 Round Serpent

In our experiments, we used 12 base approximations from the linear trail of 4 round Serpent. The linear approximations start from round 4 (using S-box 4) and end up in round 7 (using S-box 7). Table 3 shows the input and output masks of the base approximations that are expressed as

$$u_i \cdot P \oplus v_i \cdot C = \kappa_i \cdot K, \quad i = 1, \ldots, m$$

where the u_i and v_i denote the input and out masks, respectively. Hence, u_i is an input mask of round 4 and v_i is an output mask of round 7. We omit the key mask κ_i since the exact knowledge of κ_i is not required for our attack.

Table 3. Input and output masks for the multidimensional linear attack using Matsui's algorithm 2

type	index	mask = (MSB, ..., LSB)
input mask	u_1	(0x70000000, 0x00000000, 0x00000000, 0x07000900)
	u_2	(0x70000000, 0x00000000, 0x00000000, 0x07000B00)
	u_3	(0x70000000, 0x00000000, 0x00000000, 0x0B000900)
	u_4	(0xB0000000, 0x00000000, 0x00000000, 0x07000900)
	u_5	(0x70000000, 0x00000000, 0x00000000, 0x07000500)
	u_6	(0x70000000, 0x00000000, 0x00000000, 0x07000600)
	u_7	(0x70000000, 0x00000000, 0x00000000, 0x07000C00)
	u_8	(0x70000000, 0x00000000, 0x00000000, 0x01000900)
	u_9	(0x70000000, 0x00000000, 0x00000000, 0x0A000900)
	u_{10}	(0xB0000000, 0x00000000, 0x00000000, 0x03000B00)
	u_{11}	(0x10000000, 0x00000000, 0x00000000, 0x07000900)
	u_{12}	(0x40000000, 0x00000000, 0x00000000, 0x0B000B00)
output mask	v_1	(0x00001000, 0x01000000, 0x00000000, 0x00000000)

The notation of masks are following [3]. For instance, in the input mask

$$u_1 = (0x70000000, 0x00000000, 0x00000000, 0x07000900)$$

the first 4 bits (which is '7') is an input of the leftmost S-Box of the first round. Hence, there are three active S-boxes in the first round. In the same way, there are two active S-boxes in the second last round by the output mask v_1.