社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

ブロック暗号 Twofish の解析 (その 2)

盛合 志帆 * 尹 依群 †

*NTT 情報流通プラットフォーム研究所
〒 239-0847 神奈川県 横須賀市 光の丘 1-1
shiho@isl.ntt.co.jp

†NTT Multimedia Communications Laboratories
250 Cambridge Ave., Palo Alto, CA 94306, USA
yiqun@nttmcl.com

あらまし 米国次期標準暗号 AES の最終候補の一つであるブロック暗号 Twofish の差分解析を行なった。計算機実験により truncated differential を探索した結果、確率約 $2^{-57.3}$ で成立する 16 段 truncated differential が見つかった。2^{51} 個の選択平文に対し、この truncated differential に従う "good pair" は 1 組存在し、このような good pair は合計 2^{77} 組存在すると試算できる。また、Knudsen により open problem とされていた、5 段の Twofish を random permutation と識別できる可能性のある truncated differential が見つかった。

和文キーワード 暗号解析, 差分解析, truncated differential, Twofish, AES

Cryptanalysis of Twofish (II)

Shiho Moriai * Yiqun Lisa Yin †

* NTT Information Sharing Platform Laboratories
1-1 Hikarinooka, Yokosuka, 239-0847, Japan
shiho@isl.ntt.co.jp

† NTT Multimedia Communications Laboratories
250 Cambridge Ave., Palo Alto, CA 94306, USA
yiqun@nttmcl.com

Abstract We present truncated differential cryptanalysis of the block cipher Twofish, which is one of the five finalists for the Advanced Encryption Standard (AES). From our experimental results, we found a 16-round truncated differential with probability of about $2^{-57.3}$. One can expect to get one good pair following the truncated differential from 2^{51} chosen plaintexts, and there are a total of 2^{77} such good pairs. We also found 5-round truncated differentials which can be useful in distinguishing Twofish reduced to 5 rounds from a random permutation. This was considered to be an open problem by Knudsen.

key words cryptanalysis, differential cryptanalysis, truncated differential, Twofish, AES

1 Introduction

Twofish is a 128-bit block cipher proposed by Schneier et al. [SKW+98]. It is one of the five finalists of AES, and it is used in many products such as GnuPG, SSH Secure Shell, and so on [C99]. The best known attack on variants of Twofish claimed by the designers is an impossible differential attack on 6-round Twofish [F99]. Recently Knudsen [K00] showed that there are differentials for Twofish for up to 16 rounds, predicting at least 32 bits of nontrivial information in every round. The probability of the truncated differentials are too small to distinguish Twofish with more than a few rounds from a random permutation, but he claimed that it is possible, at least in theory, to find one good pair of plaintexts following the differential through all 16 rounds. Murphy and Robshaw [MR00] made some observations on key-dependent S-boxes and differential cryptanalysis of Twofish. Their approach was to choose the S-box to fit the differential characteristic, instead of choosing the differential characteristic to fit the S-box. They found a 6-round differential characteristic which holds for a fraction of at least 2^{-20} of the S-boxes and claimed possible attacks of 8-round Twofish. Table 1 summarizes the known results on cryptanalysis of Twofish.

In this paper we study truncated differential cryptanalysis of Twofish. The type of truncated differentials to be used are "byte characteristics," that is, the values of the difference in a byte are distinguished between non-zero and zero, and the measure of difference is exclusive-or. Note that Knudsen's truncated differentials were based on the integer subtraction difference between two 32-bit words. By using byte wise characteristics instead, we can make a thorough investigation of the non-uniformity in the distribution of the differences, which was left as an open question by Knudsen [K00].

Twofish consists of both byte-oriented and non-byte-oriented operations as shown in Figure 1. The non-byte-oriented operations include the 1-bit rotates, addition with subkeys, and PHT (pseudo-Hadamard transform), which comprises of two additions modular 2^{32}. To search for byte characteristics of Twofish, we begin by computing the truncated differential probability of addition modular 2^n. Based on the efficient computation of differential probability of addition modular 2^n shown in [M00], we give an efficient computation of truncated differential probability of addition modular 2^n in Section 2. In Section 3, we consider truncated differential probability of the MDS. Finally in Section 4 we present the truncated differentials that we found by computer experiments.

2 Efficient Computation of Truncated Differential Probabilities of Addition Modular 2^n

In [M00], an efficient algorithm was presented for computing differential probabilities of addition mod 2^n. The algorithm can be extended to compute truncated differential probabilities of addition of 2^n, but a straightforward extension to the case of truncated differentials can still be computationally very expensive. In this section, we study how to further speed up the

round	whitening	key size	cryptanalysis	complexity	conditions	reference
4	w/	any	distinguishing attack			[K00]
6	w/o	128	impossible differential	2^{128}		[F99]
6	w/o	192	impossible differential	2^{160}		[F99]
6	w/o	256	impossible differential	2^{192}		[F99]
6	w/	256	impossible differential	2^{256}		[F99]
8*	w/	any	differential attack	—	$> 2^{-20}$ fraction of the S-boxes	[MR00]

Table 1: Twofish cryptanalysis

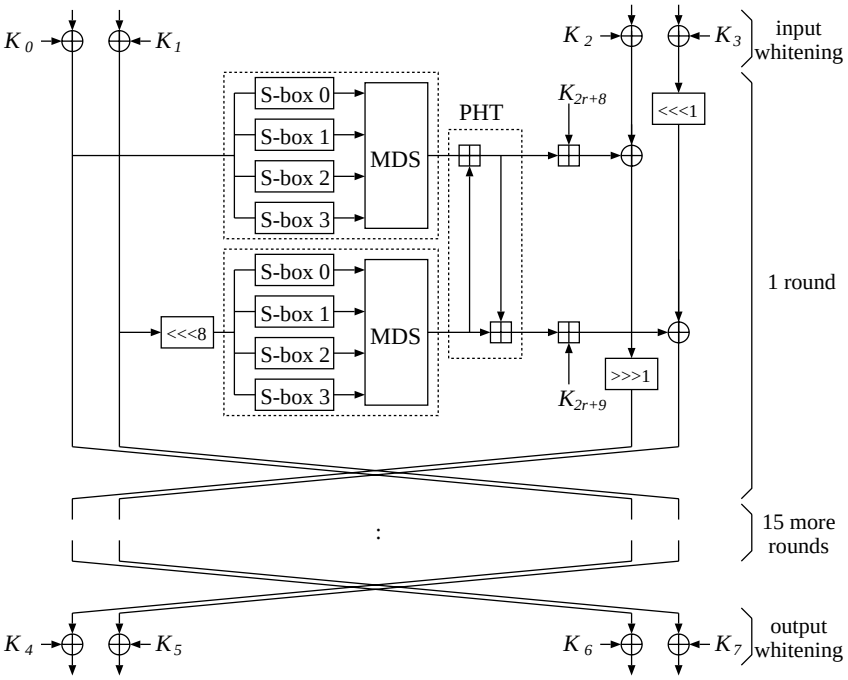

Figure 1: Twofish

computation of truncated differential probabilities.

We will follow the definitions and notation in [M00], and here we will only restate some of them if they are directly related to our discussion below.

For $x, y, z \in \mathrm{GF}(2)^n$, the function addition mod 2^n is defined as follows:

$$f(x, y) = x + y = z \pmod{2^n}.$$

We divide $\Delta x \in \mathrm{GF}(2)^n$ into t-bit sub-blocks and denote them by $\Delta x_0^{[t]}, \Delta x_1^{[t]}, \ldots$ from the least significant sub-block. So

$$\Delta x = (\Delta x_{m-1}^{[t]}, \ldots, \Delta x_1^{[t]}, \Delta x_0^{[t]}),$$

where $m = n/t$ is the number of sub-blocks.

A very efficient algorithm for computing differential probabilities of f (denoted by $\mathrm{DP}_f(\Delta x, \Delta y, \Delta z)$) is given in [M00]. For each triplet $(\Delta x, \Delta y, \Delta z)$, the running time of the algorithm is $O(n)$[1], while a naive approach would require a running time of $O(2^{2n})$.

The truncated differential probabilities for f are defined as follows.

$$\mathrm{TDP}_f(\delta x, \delta y, \delta z) = \frac{1}{c} \sum_{\chi(\Delta x, \Delta y, \Delta z) = (\delta x, \delta y, \delta z)} \mathrm{DP}_f(\Delta x, \Delta y, \Delta z), \tag{1}$$

where c is the number of pairs $(\Delta x, \Delta y)$ satisfying the condition $\chi(\Delta x, \Delta y) = (\delta x, \delta y)$. Let $w_{\mathrm{H}}(x)$ denote the Hamming weight of x. Then it is easy to see that

$$c = (2^t - 1)^{w_{\mathrm{H}}(\delta x) + w_{\mathrm{H}}(\delta y)}.$$

In a typical setting (e.g., byte characteristics), we have $n = 32$ and $t = 8$. So the number of possible truncated differentials is $(2^{n/t})^3 = 2^{12}$. Some of these truncated differentials may have a very large c value. For example, when $w_{\mathrm{H}}(\delta x) + w_{\mathrm{H}}(\delta y) \geq 6$, we have $c \geq 2^{48}$. Therefore, computation of *all* truncated differential probabilities using Equation (1) can still be very expensive, even when the differential probabilities themselves can be calculated efficiently.

[1] Later the complexity was further improved to $\Theta(\log n)$ in the worst-case and $\Theta(1)$ in the average-case.

2.1 Basic idea

The main idea for speeding up the computation of truncated differential probabilities is to treat each sub-block somewhat independently. More specifically, we will first compute some properly defined "partial sums of differential probabilities" for each sub-block ignoring the carry from one sub-block to the next, and then we will join these probabilities together to obtain the total truncated differential probability for f.

For each sub-block, we need to consider both the difference in the carryin (denoted by Δcin) from the previous sub-block and difference in the carryout (denoted by $\Delta cout$) to the next sub-block.

- There are two possible values for Δcin: 0, 1.
- Let $P_{\Delta cout}$ denote the probability that there is carry from one sub-block to the next. That is,

  $$P_{\Delta cout} = \Pr[\Delta cout = 1].$$

  Based on the results in [M00], there are only three possible values for $P_{\Delta cout}$: 0, 0.5, 1.

For a give sub-block (the ith sub-block), let $(\delta x_i, \delta y_i, \delta z_i)$ be the values of $(\delta x, \delta y, \delta z)$ restricted to the sub-block. Below, we define 6 partial sums for the differential probabilities, one corresponding to a possible combination of $(\Delta cin, P_{\Delta cout}) = (d, p)$ for $d = 0, 1$ and $p = 0, 0.5, 1$.

$$\begin{aligned} & \mathrm{PS}(\delta x_i, \delta y_i, \delta z_i, d, p) \\ = & \sum_{\text{Condition PS}} \mathrm{DP}(\Delta x_i^{[t]}, \Delta y_i^{[t]}, \Delta z_i^{[t]}), \end{aligned} \tag{2}$$

where Condition PS is

$$\begin{aligned} \chi(\Delta x_i^{[t]}, \Delta y_i^{[t]}, \Delta z_i^{[t]}) &= (\delta x_i, \delta y_i, \delta z_i), \\ \Delta cin &= d, \\ P_{\Delta cout} &= p. \end{aligned}$$

2.2 Detailed algorithm

Our algorithm for computing truncated differential probabilities contains two major components: precomputing partial sums and joining partial sums of sub-blocks.

Precomputing partial sums We observe that the partial sums defined by Equation (2) only depend on the δ values restricted to a particular sub-block. Therefore, these partial sums can be precomputed and stored in a table. Typically, each $\delta x_i, \delta y_i, \delta z_i$ is just a single bit. So the total number of partial sums to be stored is $2^3 \times 6 = 48$.

Joining sub-blocks Given the partial sums for any two consecutive sub-blocks H and L (each of length t bits), we can compute the partial sums for the sub-block $H||L$ of length $2t$ bits.

Let

$$\begin{aligned} & \mathrm{PS}_L(\delta x_i, \delta y_i, \delta z_i, d, p), \\ & \mathrm{PS}_H(\delta x_{i+1}, \delta y_{i+1}, \delta z_{i+1}, d, p), \text{ and} \\ & \mathrm{PS}_{H||L}(\delta x_{i+1}||\delta x_i, \delta y_{i+1}||\delta y_i, \delta z_{i+1}||\delta z_i, d, p) \end{aligned}$$

denote the partial sums of differential probabilities for the corresponding sub-blocks. Then $\mathrm{PS}_{H||L}$ is computed as

$$\begin{aligned}\mathrm{PS}_{H||L}(\cdot,\cdot,\cdot,d,p) = [\quad & \mathrm{PS}_H(\cdot,\cdot,\cdot,0,p) \times \mathrm{PS}_L(\cdot,\cdot,\cdot,d,0) \\ + \quad & \mathrm{PS}_H(\cdot,\cdot,\cdot,1,p) \times \mathrm{PS}_L(\cdot,\cdot,\cdot,d,1) \\ + \quad & \mathrm{PS}_H(\cdot,\cdot,\cdot,0,p) \times \mathrm{PS}_L(\cdot,\cdot,\cdot,d,0.5) \times 0.5 \\ + \quad & \mathrm{PS}_H(\cdot,\cdot,\cdot,1,p) \times \mathrm{PS}_L(\cdot,\cdot,\cdot,d,0.5) \times 0.5 \\ ].\end{aligned}$$

In general, the two sub-blocks H and L can have any number of bits, say t_1 and t_2, respectively. Using the above formula, we can compute the new partial sums for the sub-block $H||L$ of length $(t_1 + t_2)$ bits.

Computing the total TDP By repetitively joining successive sub-blocks, we can obtain the 6 partial sums $\mathrm{PS}(\delta x, \delta y, \delta z, d, p)$ for the entire block of length n. Since $\Delta cin = 0$ for the least significant sub-block, 3 of these partial sums (for which $d = 1$) actually have value zero. Therefore, the total truncated differential probability is

$$\begin{aligned}\mathrm{TDP}_f(\delta x, \delta y, \delta z) = \frac{1}{c} \times [\quad & \mathrm{PS}(\delta x, \delta y, \delta z, 0, 0) \\ + \quad & \mathrm{PS}(\delta x, \delta y, \delta z, 0, 1) \\ + \quad & \mathrm{PS}(\delta x, \delta y, \delta z, 0, 0.5) \\ ].\end{aligned}$$

Efficiency analysis The algorithm given in this section is independent of the Hamming weight of δx and δy. For $n = 32$ and $t = 8$, each of the 2^{12} truncated differential probabilities can be computed using a constant number of table lookups, additions, and multiplications. Experiments show that all the 2^{12} probabilities can be computed in less than one second on a PC.

3 Truncated Differential Probabilities of MDS

The truncated differential probabilities for the MDS are defined as follows.

$$\mathrm{TDP}_{\mathrm{MDS}}(\delta x, \delta y) = \frac{1}{c} \sum_{\chi(\Delta x, \Delta y) = (\delta x, \delta y)} \Pr[\mathrm{MDS}(x) \oplus \mathrm{MDS}(x \oplus \Delta x) = \Delta y], \tag{3}$$

where c is the number of Δx satisfying the condition $\chi(\Delta x) = \delta x$.

The distribution of $\mathrm{TDP}_{\mathrm{MDS}}(\delta x, \delta y)$ is related to the weight distribution of the MDS (Maximum Distance Separable) code. $\mathrm{TDP}_{\mathrm{MDS}}(\delta x, \delta y)$ is determined by the Hamming weights of δx and δy, as Table 2 shows.

4 Search for Truncated Differentials of Twofish

In this section, we present our search results for truncated differentials of Twofish. Our search uses the differential probabilities of PHT and MDS computed in Sections 2 and 3.

For speeding up the search, we first set the probability to be one for 1-bit rotations. Once we found the truncated differentials, we then adjust the probability as follows. If the input difference (32-bit) of the 1-bit rotation is `f`[2], the output difference is still `f`. Otherwise, we need some adjustment. For example, if the input difference of the 1-bit right rotation is `8`, the output

[2] In this section we use `typewriter` font for the hexadecimal representation of truncated differentials.

	$w_{\mathrm{H}}(\delta y)$				
$w_{\mathrm{H}}(\delta x)$	0	1	2	3	4
0	1	0	0	0	0
1	0	0	0	0	1
2	0	0	0	$2^{-7.994}$	$2^{-0.023}$
3	0	0	$2^{-15.989}$	$2^{-8.017}$	$2^{-0.023}$
4	0	$2^{-23.983}$	$2^{-16.012}$	$2^{-8.017}$	$2^{-0.023}$

Table 2: Truncated differential probabilities of MDS

difference is `8` with probability 2^{-1}, `c` with probability $2^{-1} - 2^{-8}$ and `4` with probability 2^{-8} (here we have multiple paths, but in most cases the multiple paths join at the next MDS).

For additions with subkeys (i.e., $f(x,k) = x + k = z \pmod{2^n}$, where k is some subkey), the value corresponding to $\delta k = 0$ in our precomputed table gives the truncated differential probability when we average over all possible keys. For any fixed subkey k, the probability depends on k, and it can be larger or smaller than the average probability: the maximum probability can be 1 for a fraction of the subkeys. For easy treatment of probability after the search, we set the probability to be one for additions with subkeys.

4.1 Truncated differentials with high probability

First, we searched for truncated differentials that hold with relatively high probability, although they may not be exploited in general (well-known) cryptanalytic attacks. As Knudsen [K00] wrote, such differentials can provide some bits of nontrivial information in every round.

Our computer experiments found a 12-round truncated differential with probability of about $2^{-40.9}$. In Table 3, the output difference of each round are shown in hexadecimal representation. One can expect to get one good pair following the truncated differential from about 2^{34} chosen plaintexts by using a structure in the last byte of the plaintext. There are a total of 2^{94} such good pairs.

More interestingly, we found a truncated differential for the full 16 rounds of Twofish with probability of about $2^{-57.3}$ (see Table 4). One can expect to get one good pair following the truncated differential from about 2^{100} chosen plaintexts, and there are 2^{28} such good pairs. In [K00] Knudsen showed a 16-round truncated differential with probability 2^{-256}. The probability of our 16-round truncated differential is much higher than what was found by Knudsen, and the total number of good pairs for our differential is also much larger.

4.2 Truncated differentials useful for distinguishing attacks

We also searched for truncated differentials that may be useful in distinguishing attacks. As a result, we found one 4-round truncated differential, and four 5-round truncated differentials (see Tables 6 and 5). The 4-round truncated differential is a path included in the 4-round truncated differential that Knudsen used for the χ^2-tests in [K00, Section 5.2]. Note that Knudsen's 4-round truncated differential contains multiple paths and the probability is much higher.

Knudsen concluded that for more than 4 rounds, it is an open question how nonuniform the distribution of differences can be. Now that we found 5-round truncated differentials with probability slightly higher than a random permutation, in theory we can perform statistical tests such as χ^2 tests. Note that the probabilities in Table 5 can be a little smaller due to 1-bit rotations or a little larger due to the effect of multiple paths.

round		probability
1	0 0 0 1	$2^{0.000000}$
2	0 1 f f	$2^{-0.028330}$
3	f f f e	$2^{-8.118785}$
4	f e f f	$2^{-8.209239}$
5	f f 7 f	$2^{-16.299694}$
6	7 f f f	$2^{-16.390147}$
7	f f b f	$2^{-24.480603}$
8	b f f f	$2^{-24.571056}$
9	f f 7 f	$2^{-32.661511}$
10	7 f f f	$2^{-32.751965}$
11	f f b f	$2^{-40.842420}$
12	b f f f	$2^{-40.932874}$

Table 3: 12-round truncated differential

round		probability
1	0 0 0 1	$2^{0.000000}$
2	0 1 f f	$2^{-0.028330}$
3	f f f e	$2^{-8.118785}$
4	f e f f	$2^{-8.209239}$
5	f f 7 f	$2^{-16.299694}$
6	7 f f f	$2^{-16.390147}$
7	f f b f	$2^{-24.480603}$
8	b f f f	$2^{-24.571056}$
9	f f 7 f	$2^{-32.661511}$
10	7 f f f	$2^{-32.751965}$
11	f f b f	$2^{-40.842420}$
12	b f f f	$2^{-40.932874}$
13	f f 7 f	$2^{-49.023329}$
14	7 f f f	$2^{-49.113783}$
15	f f b f	$2^{-57.204238}$
16	b f f f	$2^{-57.294692}$

Table 4: 16-round truncated differential

5 Conclusion

We presented truncated differential cryptanalysis of the block cipher Twofish. We performed the search by computer experiments, and found a 16-round truncated differential with probability of about $2^{-57.3}$, which is much larger than previously known results. We also found 5-round truncated differentials which can be useful in distinguishing Twofish reduced to 5 rounds from a random permutation. We will implement some tests to confirm our conjecture.

References

[C99] http://www.counterpane.com/twofish-products.html

[F99] N. Ferguson, "Impossible differentials in Twofish," Twofish Technical Report #5, October 5, 1999. http://www.counterpane.com/twofish-impossible.html

[K00] L. R. Knudsen, "Trawling Twofish (revisited)," Presentation at rump session of AES3. http://csrc.nist.gov/encryption/aes/round2/conf3/aes3agenda.html, Public comment on AES Candidate Algorithms – Round 2. http://csrc.nist.gov/encryption/aes/round2/comments/20000515-lknudsen-2.pdf

[K95] L. R. Knudsen, "Truncated and Higher Order Differentials," Fast Software Encryption — Second International Workshop, Lecture Notes in Computer Science 1008, pp.196–211, Springer-Verlag, 1995.

[KN96] L. R. Knudsen and T. A. Berson, "Truncated differentials of SAFER," Fast Software Encryption, — 3rd International Workshop, Lecture Notes in Computer Science 1039, pp.15–26, Springer-Verlag, 1996.

[KRW99] L. R. Knudsen, M. J. B. Robshaw, and D. Wagner, "Truncated Differentials and Skipjack," Advances in Cryptology — CRYPTO'99, Lecture Notes in Computer Science 1666, pp.165–180, Springer-Verlag, 1999.

[M00] S. Moriai,"Cryptanalysis of Twofish (I)", In Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 26-28, 2000.

round		probability
1	0 0 8 0	$2^{0.000000}$
2	8 0 f f	$2^{-0.011377}$
3	f f 8 0	$2^{-55.977519}$
4	8 0 0 0	$2^{-119.988896}$
5	0 0 8 0	$2^{-119.988896}$
1	0 0 c 0	$2^{0.000000}$
2	c 0 e e	$2^{-8.001936}$
3	e e c 0	$2^{-55.981278}$
4	c 0 0 0	$2^{-111.983214}$
5	0 0 c 0	$2^{-111.983214}$
1	0 0 e 0	$2^{0.000000}$
2	e 0 c c	$2^{-15.992496}$
3	c c e 0	$2^{-55.985038}$
4	e 0 0 0	$2^{-103.977534}$
5	0 0 e 0	$2^{-103.977534}$
1	0 0 f 0	$2^{0.000000}$
2	f 0 8 8	$2^{-23.983060}$
3	8 8 f 0	$2^{-55.988804}$
4	f 0 0 0	$2^{-95.971864}$
5	0 0 f 0	$2^{-95.971864}$

Table 5: 5-round truncated differentials

round		probability
1	0 0 8 0	$2^{0.000000}$
2	8 0 f f	$2^{-0.011377}$
3	f f 8 0	$2^{-55.977519}$
4	8 0 f f	$2^{-55.988896}$

Table 6: 4-round truncated differential

[MR00] S. Murphy and M.J.B Robshaw, "Differential Cryptanalysis, Key-dependent S-boxes, and Twofish", Public comment on AES Candidate Algorithms - Round 2. http://csrc.nist.gov/encryption/aes/round2/comments/20000515-smurphy.pdf

[MSAK99] S. Moriai, M. Sugita, K. Aoki, and M. Kanda, "Security of E2 against Truncated Differential Cryptanalysis," SAC'99, 6th Annual International Workshop on Selected Areas in Cryptography, Workshop Record, pp.133–143, 1999, (to appear in Lecture Notes in Computer Science, Springer-Verlag, 2000).

[MT99] M. Matsui and T. Tokita, "Cryptanalysis of a Reduced Version of the Block Cipher E2," Fast Software Encryption, 6th International Workshop, Lecture Notes in Computer Science 1636, pp.71–80, Springer-Verlag, 1999.

[SKW+98] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher". http://www.counterpane.com/twofish.html