VERSITA

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/v10127-012-0046-4
Tatra Mt. Math. Publ. **53** (2012), 189–199

TOWARDS PROVABLE SECURITY OF RIJNDAEL-LIKE SPN CIPHERS AGAINST DIFFERENTIAL ATTACKS

Victor Ruzhentsev — Victor Dolgov

ABSTRACT. The strength of Rijndael-like ciphers to the truncated differential attack is considered. Theorems about the absence of effective truncated (byte) differential characteristics and effective truncated (byte) differentials for ciphers with sufficient number of rounds are proved.

1. Introduction

Nowadays Rijndael [1] is one of the most popular ciphers and its strength to the cryptanalytic attacks is interesting and relevant direction of research. Differential cryptanalysis is one of the most powerful types of attack on block cipher. Truncated differentials are the variant of this type of attacks. The strength of Rijndael to truncated differential attack was researched in [2], [3]. But the complexity of the known methods increase rapidly when the number of rounds and the size of block grow. Thus, for some variants of ciphers the complexity can be too high to use these methods. The purpose of this work is to get theoretical proof of the effective truncated (byte) differentials absence for Rijndael-like SPN ciphers with sufficient number of rounds. This can make possible to prove the security of Rijndael-like cipher with large block to truncated differential attack.

The attack of truncated differentials was proposed by L. Knudsen [4]. Knudsen proposed to consider propagation of a difference part through the cipher transformations. In [4] he has shown that this technique is effective when cipher transformations provide not enough good diffusing.

The variation of truncated differential attack was proposed in [5], [6] and named the byte differentials attack. This type of attack is used for byte-oriented ciphers. Instead of transition the usual difference the adversary consider the

2010 Mathematics Subject Classification: 94A60, 68P25.
Keywords: Rijndael, Rijndael-like cipher, truncated differential, truncated differential characteristic, probability of truncated differential.

transition of *activity patterns* in this type of attack. Each bit of activity pattern reflects the activity of one byte in usual difference. The bit is 1 if byte is active, and bit is 0 if byte has zero difference. The number of bits in activity pattern is equal to the number of bytes in ciphers block.

It is quite clear that the number of possible 16-bit active patterns is much less than the number of possible 128-bit difference values at input, output or between the rounds of cipher. So, the analysis of all variants of byte differentials has much less complexity than the same task in case of conventional differentials. Methods from [2], [3] can be used to estimate the probabilities of byte differentials for cipher with size of block not much higher than 128 bits. But today there are many 256-bit block ciphers and some hash-algorithms use the 512- and 1024-bit block ciphers. The known method from [2], [3] cannot be used for ciphers with such large blocks. Thus, the purpose of this work is to propose the method of security research for Rijndael-like SPN ciphers with arbitrary size of blocks against truncated differential attack.

The paper has the following structure: some definitions and notations concerning truncated differentials and security of ciphers against this attack are presented in Section 2, the truncated differential properties of MixColumns are considered in Section 3, the useful properties of byte differential characteristics and their probabilities are presented in Section 4; in Section 5 we consider the properties of byte differentials for Rijndael-like ciphers and in Section 6 we compare obtained and already known results.

2. Definitions and notations

The one-round byte differential characteristic is the set of input activity pattern, output activity pattern and probability of such transition of activity pattern through one round. The multi-round byte differential characteristic has fixed activity patterns after each round and its probability equal to product of all one-round characteristics from which it consists.

All r-round byte differential characteristics with the same input and output activity patterns belong to one r-round byte differentials. The probability of byte differential is the sum of probabilities of all such characteristics.

The byte differential characteristic or byte differential is effective when its probability (P_{BDC} or P_{BD}) is noticeably exceeding the probability of getting the same output activity pattern with random input activity pattern. So, the criterion of effectiveness is

$$P_{BDC} \gg p_{rand} \quad \text{or} \quad P_{BD} \gg p_{rand}, \tag{1}$$

where $p_{rand} \approx (2^{-8})^u$, and u is the number of passive bytes in the output difference.

According to the papers [5], [6], the effective r-round byte differential allows to organize an attack on the r- or $(r+1)$-round cipher.

We refer readers to [2], [3], [6], [8] for more background information concerning truncated differential attacks.

Particularly, in this paper we consider only variants of Rijndael [1], but research method can be applied to many other Rijndael-like ciphers. By Rijndael--like ciphers with k columns and w rows in the block (state) we mean a cipher which consists of four main transformations of Rijndael in each round. These transformations are BS, SR, MC and AddKey. The first transformation BS (analogue of ByteSub in Rijndael) performs substitution for each byte of the state of cipher. The second transformation SR (analogue of ShiftRow in Rijndael) performs the byte permutation in the state. The third transformation MC (analogue of MixColumn in Rijndael) performs the multiplication of each of k, w-byte columns on a fixed MDS-matrix with size $w \times w$ bytes. The fourth transformation AddKey makes XOR-ing of round keys to the state. For simplicity, let the size of key be equal to size of block in all considered variants of ciphers.

The BS and AddKey do not change the activity patterns. The SR changes only the positions of active and passive bits in the activity patterns. The MC makes the maximum influence on activity patterns.

Further, we use the notion *active column*. By active column we understand the column of state with at least one active byte (the difference is not zero in at least one byte of column). We will consider the probabilities of active column transitions through MC-transformation in the next section. The column without active bytes passes to the non-active column at output of MC with the probability 1. The probability of 1-round byte differential characteristic is the multiplication of probabilities which each column of state has when it passes through the MC.

3. Truncated differential properties of MixColumns

It is known that for active w-byte column the minimal overall number of active bytes at input and output of MC-transformation is $w + 1$. Moreover, for the fixed positions of active bytes at input and output of MC the number of possible input differences when overall number of active bytes is minimal (i.e., $w + 1$) is always equal to 255. Computational experiments confirm that the number of input differences is always equal and for each other variants of overall number of active bytes at input and output of this transformation.

These numbers of input differences could be computed by consecutive considering of situations with 1, 2, 3 and 4 active bytes at input and 4 active bytes at output of MC.

So, there is $q_1 = 255$ variants of input differences with fixed position of 1 active bytes which make 4 active bytes at output. The number of input differences q_2 for transition $2 \to 4$ with fixed positions of input active bytes is $q_2 = 255^2 - C_4^3 \cdot q_1$, that is overall number of input differences with fixed positions of 2 active bytes (255^2) without all variants with 3 active bytes at output. C_j^i is the number of i elements combinations on the set of j elements (binomial coefficient).

Using the same arguments for transition $3 \to 4$ we will get the number of input differences $q_3 = 255^3 - C_4^2 \cdot q_1 - C_4^3 \cdot q_2$.

The common expression for q_i $(i = 1, \ldots, w)$ is

$$q_i = 255^i - \sum_{j=1}^{i-1} \left(C_w^{w-i+j} \cdot q_j \right).$$

Using the array of q_i there can be computed the probability of transition of the input activity pattern with a active bits to output activity pattern with b active bits

$$P_{MC}(a \to b) = \frac{q_{a+b-w}}{255^a}.$$

In Table 1 There are the probabilities for one column activity pattern transformations through MC of Rijndael.

TABLE 1. The probabilities of the activity patterns transformations through MC of Rijndael, $\log_2$ (*Probability*).

Output / Input	0	1	2	3	4
0	0	-	-	-	-
1	-	-	-	-	0
2	-	-	-	-7.99	-0.023
3	-	-	-15.99	-8.017	-0.0226
4	-	-23.983	-16.0115	-8.0171	-0.0226

In Table 1 the number of active bytes at input of MC is changed by rows and the number of active bytes at output is changed by columns.

According to Table 1, each passive byte at output of MC decreases the probability of byte characteristics by about 2^8 times. If the output difference has 4 active bytes (see the last column of Table 1), then the probability is a little bit smaller than 1 in case of more than 1 active bytes at input.

4. Probabilities of byte differential characteristics

We consider the byte differential characteristics and its probabilities in this section.

Using the results from Table 1 there can be proved the following lemma about the effective byte differential characteristics.

Lemma 1. *The effective byte differential characteristics of Rijndael-like cipher may not have any round with all active columns at the input of MC-transformation.*

P r o o f. According to Table 1 at the output of each active column we get all active bytes with probability about 1 or for each passive byte pays with loss of probability of characteristic by 2^8 times. Thus, all active columns at the input of MC-transformation guarantee all active bytes at output of characteristic with probability about 1 or each active byte at output reduced the characteristic's probability by 2^8 times. So, at the best we will get a characteristic with probability about $p_{rand} \approx (2^{-8})^u$ (where u is the number of passive bytes in the output difference) and such characteristic is not effective. □

This lemma makes it possible the proving of effective byte differential characteristics absence for ciphers with 1 or 2 columns in block. According to this lemma ciphers with 1 column in block have no effective byte differential characteristics after 1 round. Ciphers with 2 columns in block have no effective byte differential characteristics after 3 rounds because three consecutive rounds always have at least one round with 2 active columns at input of MC-transformation. But this lemma is useless for ciphers with more columns in block. For example, the byte differential characteristics of 128-bits block Rijndael with 4 columns in block can have only 3 active columns in many consecutive rounds. This variant of cipher will be considered in the following theorem. But in general, there can be used methods from [7], [8] to get the boundary number of rounds for effective byte differential characteristics existence for ciphers with more than 2 columns in block.

The lemma about the number of active columns in two consecutive rounds was proved for Rijndael in [1]. According to this lemma, the total number of active columns at input and output of two consecutive rounds is at least 5. Using this lemma, it can be shown that for Rijndael with 128-bit block the following theorem is true.

Theorem 1. *For Rijndael with 128 bit block size there are no effective differential byte characteristics for 3 or more rounds.*

P r o o f. Let a, b and c ($a > 0$, $b > 0$, $c > 0$) be the number of active columns at input of MC-transformations in 1, 2 and 3 rounds, correspondingly. There must

be not more than b active bytes in each active column at output of the first round MC-transformation (in other case, we will get more than b active columns after the second round SR at input of the second round MC-transformation). According to the Table 1, each passive byte at output of MC-transformation decreases the probability of characteristic by about 2^8 times. Thus, the probability of a byte differential characteristic after first round will be at most $2^{-(4-b)8a}$.

Using the same arguments, the probability after two rounds will be not greater than $2^{-(4-b)8a} \cdot 2^{-(4-c)8b}$.

Assume that every active column at output of MC-transformation in the third round has 4 active bytes. In this case the number of active bytes in output difference will be $4c$ and $p_{rand} = 2^{-(4-c)\cdot 32}$.

To prove the theorem we must prove that the following inequality is true

$$2^{-(4-b)8a} \cdot 2^{-(4-c)8b} \leq 2^{-(4-c)\cdot 32}. \tag{2}$$

Every additional passive byte at output of the third round MC-transformation puts the additional multiplier 2^{-8} to the both sides of inequality (2).

The inequality (2) gives

$$-(4-b)8a - (4-c)8b \leq -(4-c)\cdot 32. \tag{3}$$

According to the lemma about the number of active columns from [1], $a+c \geq 5$. Thus, the minimal value of a is $5-c$, the maximal value is 4. Let us show that inequality (3) is true in both cases. In case $a = 5-c$ the inequality (3) is equivalent to $8b \leq 32$; in case $a = 4$ the inequality (3) is equal to $8bc \leq 32c$. These two inequalities are true because $b \leq 4$. □

Computional experiments using methods from [7], [8] are constant with the theorem. The results are given in Table 2.

TABLE 2. The effective byte differential characteristics which cover maximal number of rounds.

Size of block, bits	Number of columns	Max. number of rounds	Max. probability of characteristics, P_{BDC}	P_{BDC}/p_{rand}
128	4	2	$\approx 2^{-8}$	1,68e+7
192	6	3	$\approx 2^{-16}$	62991
256	8	5	$\approx 2^{-80}$	60101

In accordance to the results presented in Table 2, probably, almost the same theorems as Theorem 1 can be proved for Rijndael with 192-bit block and 4 rounds and for Rijndael with 256-bit block and 6 rounds.

5. Probabilities of byte differentials

In this section we will consider byte differentials for Rijndael, the types and probabilities of byte differential characteristics which belong to differentials.

The following statement is true if the number of rounds is higher than any effective byte differential characteristic can cover.

Statement 1. *There is always one and only one byte characteristic with probability about $p_{rand} \cdot 2^{-0,0904 \cdot R}$ in each non impossible R-round ($R \geq 3$) byte differential for 128-bit Rijndael.*

P r o o f. There are several known impossible 3-round differentials which are used in impossible differential attacks. For each other differentials there is such byte differential characteristic which use transitions of activity patterns with probability about 1 for each active columns in all rounds except the last and the last but one. The results of these transitions for each column is the activity pattern with 4 active bytes (see Table 1). The transitions of activity patterns through the MC transformation in the last and the last but one rounds are chosen according to the output activity pattern. For each passive byte in output difference we pay by decreasing of characteristic's probability by about 2^8 times. Thus, the characteristic's probability will be at most p_{rand}.

The using of the mentioned above transitions of activity patterns with probability 1 through the MC transformations guarantee that after at most one round all columns will be active and that after at most two rounds all bytes will be active. According to Table 1, probability of getting output activity pattern with 4 active bytes from input activity pattern with 4 active bytes is $2^{-0,0226}$. If all 4 columns are active, then probability is $2^{-0,0904}$. And it is the number by which we have multiply for every additional round. So, the probability of such byte differential characteristic is about $p_{rand} \cdot 2^{-0,0904 \cdot R}$. □

We will call such byte differential characteristic as *primary* byte characteristic and all others characteristics which belong to the same byte differential as *additional* byte characteristics.

If we consider the primary characteristics more precisely, it can be seen that its probability depends on input activity pattern. For example, if the input activity pattern has only one active bit, then after the next two rounds we will get 16 active bits without lost of probability (with probability 1). So, the probability of r-round primary byte characteristic with such input pattern will be $p_{rand} \cdot 2^{-0,0904 \cdot (R-2)}$. For some variants of activity patterns with small number of active bits in the input the probability will be $p_{rand} \cdot 2^{-0,0904 \cdot (R-1)}$. But in these cases, as we will see later, there will be less number of additional characteristics and overall probability will be the same.

The next statement is about additional byte differential characteristics.

Statement 2. *In the byte differential with 3 or more rounds each additional (non-primary) byte differential characteristic with m additional passive bytes has the probability at least by about 2^{8m} times less than primary characteristic.*

P r o o f. Each additional characteristic must be differ from primary one. Thus, there must be different transition of activity pattern in some rounds. The transition of activity pattern in the last and last but one rounds cannot be different as output activity pattern must be the same as in primary characteristic. So, different transition must be in other rounds where in primary characteristic are used transitions with probability about 1. According to Table 1, each additional passive byte at the output of MC makes the probability of characteristic by about 2^8 times less than probability of primary characteristic. □

Now we can prove the theorem about the existence of effective byte differentials for Rijndael-like ciphers.

Theorem 2. *There are no effective byte differentials for Rijndael with 3 or more rounds and size of block 128 bits.*

P r o o f. At first, let us count how many additional characteristics with one additional passive byte we may get for R rounds. The number of such additional characteristics is at most $C_R^1 C_{16}^1 = 16R$, where C_j^i is number of i elements combinations on the set of j elements (binomial coefficients). The first multiplier is the number of variants for choosing the round with this passive byte, and the second multiplier is the number of available positions for this passive byte in the cipher block. So, additional probability from additional characteristics with one additional passive byte according to Statements 1 and 2 is $16R \cdot 2^{-8} \cdot 2^{-0,0904 \cdot R}$.

There are three variants of disposition for two additional passive bytes:

- one column – number of variants is $C_R^1 \cdot C_4^1 \cdot C_4^2 = 24R$;
- one round but different columns – number of variants is $C_R^1 \cdot C_4^2 \cdot \left(C_4^1\right)^2 = 96R$;
- two different rounds – number of variants is $C_R^2 \cdot \left(C_{16}^1\right)^2 = \frac{R!}{(R-2)!\cdot 2!} \cdot 256 = 128R^2 - 128R$.

Thus, overall additional probability from characteristics with two additional passive bytes is $(128R^2 - 8R) \cdot 2^{-16} \cdot 2^{-0,0904 \cdot R}$.

By the same way, we have considered situation with three additional passive bytes. In this case there are more variants of passive bytes disposition and overall additional number of variants is $683R^3 - 128R^2 + 5R$. As in case with two passive bytes, it can be chosen the most important item in the last equation, it is $683R^3$ (for two passive bytes it is $128R^2$). We can neglect other items and estimate overall additional probability from characteristics with three additional passive

bytes as $\approx 683R^3 \cdot 2^{-24} \cdot 2^{-0,0904 \cdot R}$ and with two additional passive byte as $\approx 128R^2 \cdot 2^{-16} \cdot 2^{-0,0904 \cdot R}$.

The most important items correspond to situations when additional passive bytes are distributed by one in different rounds.

The general formula for additional probability in case of i additional passive bytes and using only the most important item is

$$\frac{R^i \cdot 16^i \cdot 2^{-8i}}{i!} \cdot 2^{-0,0904 \cdot R} = \frac{\left(\frac{R}{16}\right)^i}{i!} \cdot 2^{-0,0904 \cdot R},$$

for $i = 0, \ldots, R$ ($i = 0$ corresponds to the primary byte characteristic and if $i > R$, then there are not the most important item in formula of additional probability). We have to estimate the sum of such series. From theory of series it is known that

$$\sum_{i=0}^{\infty} \frac{x^i}{i!} = e^x.$$

So, in our case,

$$\sum_{i=0}^{R} \frac{\left(\frac{R}{16}\right)^i}{i!} < \sum_{i=0}^{\infty} \frac{\left(\frac{R}{16}\right)^i}{i!} \approx e^{\frac{R}{16}}$$

Now we can estimate the overall probabilities of byte differentials with number of rounds greater than any effective byte characteristics can cover.

$$\begin{aligned} P_{BD} &= e^{\frac{R}{16}} \cdot 2^{-0,0904 \cdot R} \cdot p_{rand} \\ &= \left(e^{\frac{1}{16}} \cdot 2^{-0,0904}\right)^R \cdot p_{rand} \approx 1^R \cdot p_{rand} \\ &= p_{rand}. \end{aligned}$$

So, the probability of each byte differential is about p_{rand} and such differentials are not effective. □

Now we can return to the particular situation with one active bit in the input pattern. As it was mentioned above, in this case, there are some higher probabilities of characteristics, but there is less number of additional characteristics, so, the last equation will be

$$\begin{aligned} P_{BD} &= e^{\frac{R-2}{16}} \cdot 2^{-0,0904 \cdot (R-2)} \cdot p_{rand} \\ &= \left(e^{\frac{1}{16}} \cdot 2^{-0,0904}\right)^{(R-2)} \cdot p_{rand} \approx 1^{R-2} \cdot p_{rand} \\ &= p_{rand}. \end{aligned}$$

We get the same result.

We consider only 128-bit Rijndael now. In the same manner it can be proved that other variants of Rijndael-like ciphers with number of rounds higher than any effective byte characteristic can cover have no effective byte differentials.

6. Compearing with known results

There are known results about byte differentials of Rijndael from [2], [3], [9]. Rijndael with 128-bit block and reduced last round (without MC in last round) was considered in these papers. As the only one transformation which has ambiguity for value of output activity pattern is MC, then, from point of view of byte differential probability, r-round cipher with reduced last round is equal to $(r-1)$-round cipher with full rounds. In other words, the conclusion of Theorem 2 is that there are no effective byte differentials for 4 or more rounds of Rijndael with 128 bit block and reduced last round.

The same result was presented in [3]. In [3] there is a conclusion about security of SPN-cipher with 4 or more rounds to differential attack.

There is information about 4-round conventional differential with probability $1,0065 \cdot 2^{-128}$ and about 5-round conventional differential with probability $1,00007 \cdot 2^{-128}$ in [2], but the input and output difference of these differentials and the corresponding byte (truncated) differentials was not presented in [2]. In any case, on our opinion, differentials with such negligible increasing of probability from 2^{-128} cannot lead to effective differential attack and probability of corresponding byte (truncated) differentials do not agree with (1), so corresponding byte (truncated) differentials are not effective.

Presented in [9] effective byte differential were found with using the method from [2] and they cover 3 rounds of Rijndael with reduced last round. Thus, there are no contradictions between obtained and known results from [2], [3], [9].

7. Conclusions

The main conclusion is that we confirm the non-existence of effective byte differentials for 128-bits block Rijndael with 3 or more full rounds. Thus, this cipher with one additional round is secure against byte (truncated) differential attacks.

Also, the new approach to prove the absence of effective byte differentials for Rijndael-like ciphers was presented. This approach has no restrictions on the block size, so it can be used to block ciphers with much larger size of blocks than the known methods which could be applied.

REFERENCES

[1] DAEMEN, J.—RIJMEN, V.: *AES proposal Rijndael*, AES Round 1 Technical Evaluation CD1: Documentation, National Institute of Standards and Technology, 1998, http://www.nist.gov/aes.

[2] SUGITA, M.—KOBARA, K.—UEHARA, K.—KUBOTA, S.—IMAI, H.: *Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block cipher like Rijndael, E2*, in: Proc. of the 3rd AES Candidate Conference, New York, USA, 2000, National Institute of Standards and Technology, 2000, pp. 242–254, http://www.nist.gov/aes.

[3] SUGITA, M.—KOBARA, K.—IMAI, H.: *Pseudorandomness and maximum average of differential probability of block ciphers with SPN-structures like E2*, in: Proc. of the 2nd AES Candidate Conference, AES Workshop, Rome, Italy, 1999, pp. 200–214.

[4] KNUDSEN, L. R.: *Truncated and higher order differentials*, in: Fast Software Encryption—FSE '95, 2nd Internat. Workshop (B. Preneel, ed.), Leuven, 1995, Lecture Notes in Comput. Sci., Vol. 1008, Springer-Verlag, Berlin, 1995, pp. 196–211.

[5] KNUDSEN, L. R.—BERSON, T. A.: *Truncated differentials of SAFER*, in: Fast Software Encryption—FSE '96, 3rd Internat. Workshop (D. Gollmann, ed.), Cambridge, UK, Lecture Notes in Comput. Sci., Vol. 1039, Springer-Verlag, Berlin, 1996, pp. 15–25.

[6] MATSUI, M.—TOKITA, T.: *Cryptanalysis of reduced version of the block cipher E2*, Fast Software Encryption—FSE '99, 6th Internat. Workshop (L. Knudsen, ed.), Lecture Notes in Comput. Sci., Vol. 1636, Springer-Verlag, Berlin, 1999, pp. 71–80.

[7] RUZHENTSEV, V. I.: *About methods of an estimation of resistance to truncated differentials attack*, Radioelektronika i informatika **4** (2003), 130–133. (In Russian)

[8] MORIAI, S.—SUGITA, M.—AOKI, K.: *Security of E2 against truncated differential cryptanalysis*, in: Selected Areas in Cryptography—SAC '99, 6th Annual Internat. Workshop (H. Heys, C. Adams, eds.), Lecture Notes in Comput. Sci., Vol. 1758, Springer-Verlag, Berlin, 2000, pp. 106–117.

[9] DOLGOV, V. I.—RUZHENTSEV, V. I.: *About the method of evaluation the resistance of cipher Rijndael to differential attacks*, Radioelektronika i informatika **1** (2002), 136–138. (In Russian)

Received August 28, 2012

Victor Ruzhentsev
Department of Secure Information Technologies
Faculty of Computer Engineering and Control
Kharkov National University of Radioelectronics
Lenins av. 14
61166 Kharkov
UKRAINE

E-mail: vityazik@rambler.ru

Victor Dolgov
JSC Institute of Information Technologies
Bakulina str. 12
61166 Kharkov
UKRAINE

E-mail: dolgovvi@mail.ru