New Integral Distinguisher for Rijndael-256

Yuechuan Wei[1], Bing Sun[2] and Chao Li[1,2,3]

[1] School of Computer Science, National University of Defense Technology, Changsha, China, 410073
[2] System Science, Science College of National University of Defence Technology, Changsha, China, 410073
[3] State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing, China, 100049
wych004@163.com

Abstract. The known 3-round distinguisher of Rijndael-256 is byte-oriented and 2^8 plaintexts are needed to distinguish 3-round Rijndael from a random permutation. In this paper, we consider the influence of the order of the plaintexts and present a new 3-round distinguisher which only needs 32 plaintexts.
Key words: block cipher, integral attack, Rijndael-256

1 Introduction

The known integral distinguishers of Rijndael-256 are based the square property which is byte-oriented[1–5, 7]. For example, the known 3-round integral distinguisher shows that, if only one byte of the input is active and the others are constant, each byte of the output of the third round is balanced. To construct such a distinguisher, 256 plaintexts are needed.

In traditional integral methods, the order of the plaintextes are not considered since it doesn't influence the sum. However, Z'aba shows that though the order has no relations with the sum, they can facilities the process of computing when finding distinguishers in bit-pattern based integral attack[6]. In $\mathbb{F}_{2^n}$, if $\int_V f(x) = a$, then $\int_V f^{(i)}(x) = a^{(i)}$, where $f^{(i)}(x)$ and $a^{(i)}$ denote the ith coordinate of the $f(x)$ and a respectively. To ascertain the value of $a^{(i)}$, one can count how many times that each different elements appear in the sequence of $(f^{(i)}(x))$. The number is denote by N, if N is even, $a^{(i)} = 0$, which means that the corresponding sequence is balanced. Otherwise it can't be certain generally. For counting the times that different elements appear, the order of the plaintexts can be useful.

In this paper, we consider the influence of the order of the plaintexts and present a new 3-round distinguisher which only needs 32 plaintexts.

The remainder of the paper is organized as follows: Section 2 provides a brief outline of Rijndael-256. Section 3 recalls some notations of bit-patterns proposed in ref.[6]. Section 4 introduce the new 3-round distinguisher of Rijndael-256. Section 5 concludes the paper.

2 Outline of Rijndael-256

Rijndael-256 is a symmetric block cipher that uses a parallel and byte-oriented structure. The key length and the block length are both 256 bits. The block of the input is represented by a 4×8 matrix of bytes:

$$P = \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} & x_{16} & x_{20} & x_{24} & x_{28} \\ x_1 & x_5 & x_9 & x_{13} & x_{17} & x_{21} & x_{25} & x_{29} \\ x_2 & x_6 & x_{10} & x_{14} & x_{18} & x_{22} & x_{26} & x_{30} \\ x_3 & x_7 & x_{11} & x_{15} & x_{19} & x_{23} & x_{27} & x_{31} \end{pmatrix} \in \mathbb{F}_{2^8}^{4\times 8},$$

The key schedule derives $Nr + 1$ 256-bits round keys K_0 to K_{Nr} from the master key K.

The round function, repeated $Nr - 1$ times, involves four elementary mappings, all linear except the first one:

-SubBytes: a bytewise transformation that applies on each byte of the current block an 8×8 non linear S-box composed of the inversion in the Galois Field $\mathbb{F}_{2^8}$ and of an affine transformation.

-ShiftRows: a linear mapping that rotates on the left all the rows of the matrix(0 for the first row, 1 for the second, 3 for the third and 4 for the fourth[3]).

-MixColumns: a linear mapping represented by a 4×4 matrix chosen for its good properties of diffusion. Each column of the input matrix is multiplied by the MixColumns matrix M.

-AddRoundKey: XOR operation between the current block and the subkey.

There is an initial key addition with the subkey K_0 before the first round and the MixColumns operation is omitted in the final round.

3 Some Definitions and Notations

In Z'aba's bit-pattern integral attack, the order of the plaintexts plays an important role in finding distinguishers. However, the order has no relations with integral distinguishers, it is used only to count the times that different elements appear. If each element appears even times, the correspondence sequence is a balanced one. In this section, we briefly introduce some notations and results presented in ref.[6].

In text, every bit position has a pattern, which is defined by the sequence in this position how the "0"and "1"are repeated. All positions with correspondig patterns compose a structure.

-**Constant** The pattern **c** in a position means all bits in this position within the structure consists of only bit "0"or "1". E.g. 00000000 or 11111111.

-**Active** The pattern a_i means that the first block of 2^i consecutive bits in this position are constant, the next 2^i consecutive bits all have the opposite value. E.g. a_1: 11001100.

-The pattern b_i means blocks of 2^i consecutive bits in this position are constant, but the values of the blocks are not necessarily repeated in an alternating

way. E.g. b_1:11000011, b_0:10000000.

A pattern is *balanced* means that the XOR sum of all the bits in this position is 0. A structure is balanced means that the XOR sum of all the texts in this structure only has 0-bits. All patterns described above are balanced, except b_0 pattern is not necessarily. The authors of ref.[6] distinguish them by writing b_0^* when the pattern is balanced and b_0 otherwise.

Patterns $a_0 a_1 \dots a_n$ can reach the 2^n possible values of n-bit text. Further, some easy but important properties are presented again.

-$c \oplus p = p$ for any pattern p.
-$a_i \oplus a_i = c$.
-$p_j \oplus q_i = b_i$ for $j > i$ and p, $q \in a, b$. If $i = 0$, the right-hand side will be b_0^*.

when the input bit-patterns pass through an S-box, every output-bit will have a b_j pattern, where j is the smallest index found in the input patterns.

For more details of bit-pattern integral cryptanalysis, we refer to ref.[6].

4 New 3-Round Integral Distinguisher of Rijndael-256

The known integral distinguisher of Rijndael-256 are byte-oriented. For example, the known 3-round integral distinguisher in Fig.1 shows that, if only one byte of the input take over all the possible values and the others are constant, each byte of the output of the third round is balanced. It means that, in order to distinguish 3-round Rijndael-256 from a random permutation, 2^8 cipertexts and encryptions are needed.

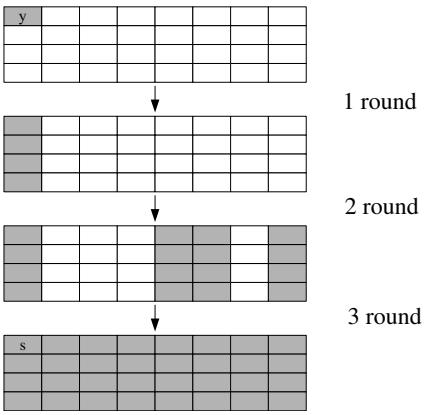

Fig. 1. 3-round distinguisher of Rijndael-256

For extending the bit-pattern integral cryptanalysis to byte(word)-oriented cipher,we first give the definition of patterns of words.

Definition 1. *$v_k(L)$ is defined by a sequence of values $\{v_i\}$ with $i = 0, \ldots, N-1$, in which L length subsequence$\{v_{k_1}, \ldots, v_{k_2}\}$ is repeated, and there are k different values in the subsequence. $v_k(N)$ denotes that there is no such repeated subsequence in $\{v_i\}$.*

Definition 2. *$V_2(L)$ is defined by a sequence of values has the property of $v_2(L)$ and in every L-block, the first $L/2$ consecutive values are "a"s, and the next $L/2$ consecutive values are "b"s, where a and b are the two different values and L is even.*

For example, the sequence $\{ababa bab\}$ can be described by both $V_2(2)$ and $v_2(2)$, and the sequence $\{abbaabba\}$ can be described only by $v_2(4)$.

Let the input to an S-box be $X = (X_0 X_1 \ldots X_{n-1})$. If X_t is a_i pattern, and other positions are constant patterns, then from the definition we know that the input to this S-box can be described by $V_2(2^{i+1})$. Since S-box operation is bijective, the output will also have the form of $V_2(2^{i+1})$.

The above notation is a kind of period description, one can verify that the following proposition holds.

Proposition 1. *For k $N(N \geq 4)$ bit sequences with the form of*

$$V_2(2^{t_1}), V_2(2^{t_2}), \ldots, V_2(2^{t_r})$$

where $t_i \neq t_j$, the sum of the sequences holds the form of $v_{2^r}(2^{t_{max}})$, where t_{max} is the maximum of $\{t_1, \ldots, t_r\}$. Further more, every value of the sum sequence is repeated even times.

According to the definition and proposition mentioned above, we can find new integral distinguishers of Rijndael-256.

Theorem 1. *Assume the input to Rijndael-256 be*

$$P = \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} & x_{16} & x_{20} & x_{24} & x_{28} \\ x_1 & x_5 & x_9 & x_{13} & x_{17} & x_{21} & x_{25} & x_{29} \\ x_2 & x_6 & x_{10} & x_{14} & x_{18} & x_{22} & x_{26} & x_{30} \\ x_3 & x_7 & x_{11} & x_{15} & x_{19} & x_{23} & x_{27} & x_{31} \end{pmatrix} \in \mathbb{F}_{2^8}^{4\times 8},$$

and let $x_{0,0} \| x_{1,0} \| x_{2,0} \| x_{3,0} \| x_{4,0}$ takes all value of $\mathbb{F}_{2^5}$ where $x_{m,0}$ represents the least significant bit of x_m. Then each byte of the output of the third round of Rijndael-256 is balanced.

Proof. Set the $x_{i,0}$ by a_i pattern, where$0 \leqslant i \leqslant 4$. The input has the pattern of

$$\begin{pmatrix} V_2(2) & V_2(32) & c & c & c & c & c & c \\ V_2(4) & c & c & c & c & c & c & c \\ V_2(8) & c & c & c & c & c & c & c \\ V_2(16) & c & c & c & c & c & c & c \end{pmatrix}.$$

Since AddRoundKey operation and S-box do not change the way of a sequence repeats, we omit the influence of the key and S-box. The pattern after the first round ShiftRow operation is:

$$\begin{pmatrix} V_2(2) & V_2(32) & c & c & c & c & c & c \\ c & c & c & c & c & c & c & V_2(4) \\ c & c & c & c & c & V_2(8) & c & c \\ c & c & c & c & V_2(16) & c & c & c \end{pmatrix}.$$

The output of the first round MixColumn operation has the following pattern:

$$\begin{pmatrix} V_2(2) & V_2(32) & c & c & V_2(16) & V_2(8) & c & V_2(4) \\ V_2(2) & V_2(32) & c & c & V_2(16) & V_2(8) & c & V_2(4) \\ V_2(2) & V_2(32) & c & c & V_2(16) & V_2(8) & c & V_2(4) \\ V_2(2) & V_2(32) & c & c & V_2(16) & V_2(8) & c & V_2(4) \end{pmatrix}.$$

Then the output of the ShiftRow in the second round is:

$$\begin{pmatrix} V_2(2) & V_2(32) & c & c & V_2(16) & V_2(8) & c & V_2(4) \\ V_2(32) & c & c & V_2(16) & V_2(8) & c & V_2(4) & V_2(2) \\ c & V_2(16) & V_2(8) & c & V_2(4) & V_2(2) & V_2(32) & c \\ V_2(16) & V_2(8) & c & V_2(4) & V_2(2) & V_2(32) & c & c \end{pmatrix}.$$

We can determine the pattern till the end of the third round, the input to the third MixColumn is:

$$\begin{pmatrix} v_8(32) & v_8(32) & v_2(8) & v_4(16) & v_{16}(16) & v_8(32) & v_4(32) & v_4(4) \\ v_8(32) & v_2(8) & v_4(16) & v_{16}(16) & v_8(32) & v_4(32) & v_4(4) & v_8(32) \\ v_4(16) & v_{16}(16) & v_8(32) & v_4(32) & v_4(4) & v_8(32) & v_8(32) & v_2(8) \\ v_{16}(16) & v_8(32) & v_4(32) & v_4(4) & v_8(32) & v_8(32) & v_2(8) & v_4(16) \end{pmatrix},$$

and the output is:

$$\begin{pmatrix} v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) \\ v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) \\ v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) \\ v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) & v_*(32) \end{pmatrix}.$$

We replace the number of different values by " * "since we can't decide it again. The input to the third MixColumn operation is balanced, because there are 2,4,8 and 16 different values in byte positions and every value is repeated even times. The output is also balanced as the MixColumn operation is linear.

The period of $v_*(32)$ is can't be decided, and the balance expect to be destroyed by the next S-box.

□

Note 1. we should point that in the above proof, k in $v_k(L)$ may not be the exact number of different values of the sequence. This is because that we take two values which are calculated in different ways as different. For example, $2P + 3Q$ may equal to $4P + 2Q$, however, we consider them different values since they are calculated in two different ways.

Note 2. The distinguisher in Theorem 1 indicates a series of distinguishers. For example, let $x_{0,n_0} \| x_{1,n_1} \| x_{2,n_2} \| x_{3,n_3} \| x_{4,n_4}$ takes all value of $\mathbb{F}_{2^5}$ where x_{m,n_i} represents the arbitrary bit of x_m. Then each byte of the output of the third round of Rijndael-256 is balanced.

Although the output in the new distinguisher is the same as the traditional 3-round integral distinguisher, the inputs of the two are extremely different. Only 32 plaintexts are needed in the new distinguisher.

5 Discussions on Revelent Attack

Compared with the byte-oriented ones, the integral distinguisher presented in Theorem 1 only needs 2^5 chosen plaintexts to distinguish the cipher from random permutations. As a result, when attacking reduced round Rijndael-256 by adding one or more rounds at the end of 3-round distinguisher, the new one is more efficient. For example, the complexity of 4 rounds and 5 rounds attack are negligible. However, if we want to extend the above distinguisher to higher order one, instead of one active entry used in the square attack, attack based the new distinguisher uses 5 active entries. Therefore, the byte-oriented one is better than the bit-oriented one since the number of active S-boxes is 1 vs 5. One can use the new distinguisher to develop new attacks on Rijndael-256.

On the other hand, it is interesting to observe the effect of the order of plaintexts. The distinguisher illustrates that the square properties are not restricted to the cases for which only one cell takes all the possible values.

6 Conclusion

In this paper, we show a new distinguisher of Rijndael-256 which only needs 32 chosen plaintexts. It indicates that the bit-pattern integral cryptanalysis is not only suitable for bit-oriented ciphers, but also suitable for byte(word)-oriented ciphers. The efficiency of bit-pattern integral attacks on byte(word)-oriented ciphers is under study.

References

1. S. Galice, M. Minier. Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds. Africacrypt 2008, LNCS 5023, pp.1–15. Springer–Verlag, 2008
2. J. Daemen, L. R. Knudsen, and V. Rijmen. The Block Cipher Square. FSE 1997, LNCS 1267, pp. 149–165, Springer–Verlag, 1997.
3. J. Daemen, and V. Rijmen. The Design of Rijndael: AES—The Advanced Encryption Standard (Information Security and Cryptography). Springer–Verlag, 2002.
4. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved Cryptanalysis of Rijndael. FSE 2000, LNCS 1978, pp. 213–230, Springer–Verlag, 2001.

5. J. Nakahara Jr, D. Freitas, and R. Phan. New Multiset Attacks on Rijndael with Large Blocks. Advances in Cryptology — Mycrypt 2005, LNCS 3715, pp. 277–295, Springer–Verlag, 2005.
6. M. R. Z'aba, H. Raddum, M. Henricksen, and E. Dawson. Bit-Pattern Based Integral Attack. FSE 2008, LNCS 5086, pp. 363–381. Springer–Verlag, 2008.
7. H. Demirci, A. A. Selçuk. A Meet-in-the-Middle Attack on 8-Round AES. FSE 2008, LNCS 5086, pp. 116–126. Springer–Verlag, 2008.