Cryptanalysis of the Rijndeal

2001093
Jung-Yeun Lee

Information Security Group, School of Engineering in ICU

1 Introduction

The cipher Rijndael [6] was submitted to the AES(Advanced Encryption Standard) candidates and was later selected as the AES [1]. It is based on the Square cipher [5] and so has SPN(Substitution-Permutation Network) structure. The original design of Square cipher concentrates on the resistance against differential and linear cryptanalysis. Thus, it's known that it has the resistance against those attacks. Although this cipher has the above merits, it has a weakness which results from the characteristics of the optimal linear layer. The known attacks against each cipher, using the weakness, are the impossible differential attack [3] and the Square attack [3, 4], which were described by the designers of the Square cipher. These attacks are chosen plaintext attacks and are independent of the specific choice of sbox, the multiplication polynomial of Mixcolumn and the key schedule. They are only related to the characteristics of the linear layer. That is the branch number, which is introduced by the designers to explain the diffusion power. Up to now, the attack papers of Rijndael use 4-round characteristics. Thus, this term project goal is to improve this characteristics to 5-round characteristics. In order to do this work, it is needed to implement the Mixcolumn layer and then find the probabilistic characteristics for the 5-round Rijndael. If this work result in success, I can combine these two cryptanalyses and increase the number of the attacked rounds.

This report is organized as follows: The description of Rijndael is given in section 2 and then survey the Square attack and the impossible differential attack in section 3 and 4, respectively. Finally, in section 5 the future work is given.

2 Description of Rijndeal

The AES requirements state that the length of the key can be specified to be 128, 192, or 256 bits while the length of the block is 128 bits. The designers of Rijndael cipher also allow the length of the block to be 128, 192,or 256 bits, independently of the length of the key.In this report we deal with the variant in which the lengths of both are 128 bits. in this case the cipher consists of 10 rounds (the number of rounds reaches 14 when the length of the block is 256 bits). The intermediate state is arranged in 4×4 matrix as in Fig. 1. Every round except for the last consists of the following:

– *ByteSubstitution*
  This transformation is applied to each byte separately and is a nonlinear byte-wise substitution to use the sbox. This transformation is the only non-linear transformation in the cipher.
– *ShiftRow*
  The first low remains constant, the second row is shifted one byte to the right, the third row is shifted two bytes to the right, and the last row is shifted three bytes to the right.

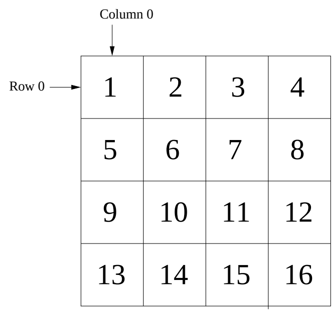

Fig. 1. Byte Coordinate of 128-bit

- *MixColumn*
  We consider each column of the matrix as a polynomial of degree less than 4 over $GF(2^8)$ and multiply this polynomial by the polynomial $03_x x^3 + 01_x x^2 + 01_x x + 02_x$ where a_x denotes hexadecimal value) modulo (x^4+1). This transformation is linear. This layer has a special characteristics by which the above two attacks are passible. This characteristics is described in the following subsection.
- *AddRoundKey*
  A 128-bit round key, which is derived of the key by the KeyExpansion algorithm, is bytewise XORed to the state.

Before the first round AddRoundKey is performed using the key as the round key. In the last round the MixColumn is omitted

2.1 Key Expansion

The round key of each round is derived of the key using the Key Expansion algorithm. Each round key is of length 128 bit and by the design knowing a round key of any round is enough to recover the key. The round key is derived as follows: Let us denote the bytes of the expanded key by $K_0, K_1, K_2, ...$ where the key is $K_0, K_1, idots, K_15$. Then the expanded key is derived from the formulae:

$$\text{If 16 is not a divisor of n, } K_n = K_{n-1} \oplus K_{n-16}.$$
$$\text{Otherwise, } K_n = K_{n-16} \oplus ByteSubstitution(ShiftedK_{n-1}) \oplus Rcon.$$

We can see that the Key Expansion is not linear but there is strong connection between bytes of the k'th round key and those of the $(k+1)th$: $K_n \oplus K_{n-1} = K_{n-16}$. It gives us more information when guessing some bytes of a round key.

2.2 Branch number

This property is related to the Linear layer of the Square cipher and is introduced by the designers to explain the diffusion power. In the design strategy of Rijndeal, this property of the linear transformation of MixColumn is essential.

Definition 1 (branch number).
Let $W()$ be the byte weight function. The branch number of a linear transformation F is $min_{a \neq 0}(W(a) + W(F(a)))$

The Rijndael has the following property for the branch number.

– Rijndael : Rijndael has a branch number 5, that is, if a state is applied with a single nonzero byte, the output has 4 nonzero bytes.

Using the above property of branch number, we can deduce the characteristics for the relation of input and output of each cipher reduced to 4 rounds: if two plain text differ by one byte, then before the third Mixcolumn the data differ by all 16 bytes. It leads to the following interesting properties:

1. Consider a set 256 plaintexts which are equal in all bytes except for one and in this one assume all the possible values. Because of the property the inputs of the third Mixcolumn assume all 256 possible values in each byte. Since the Mixcolumn is a linear transformation, this property holds after the Mixcolumn too. This is the property on which Square attack is based.
2. Consider two plaintexts which differ by only one byte. Then, the corresponding ciphertexts of the 4-round variant should differ in the special combinations of bytes. We call those combinations impossible differential. The impossible differential described in [3]. See Fig. 2.

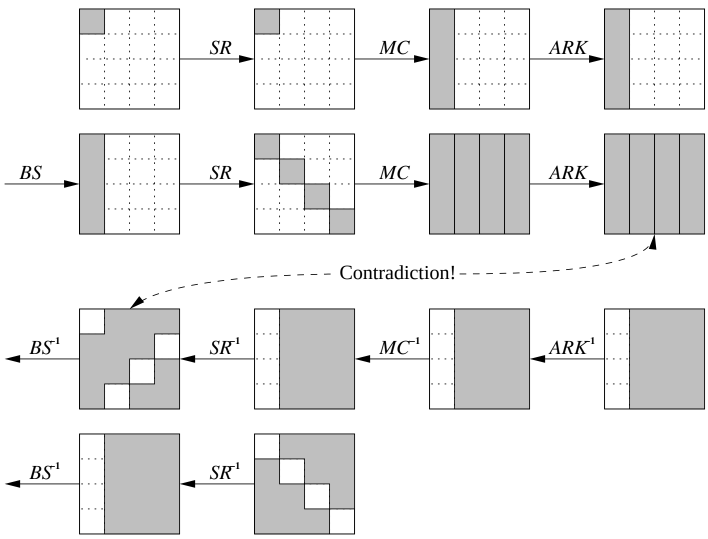

Fig. 2. Four Rounds Impossible Differential of Rijndael

Property 1 (Impossible Differential of Rijndael).
Given plaintext pair which are equal at all bytes but one, the ciphertexts after 4-round cannot be equal in any of the following *prohibited* combinations of bytes: (1,6,11,16), (2,7,12,,13), (3,8,9,14), nor (4,5,10,15).

This is the property on which impossible differentiable attack is based.

3 Square attack

Let us consider now 256 chosen plaintexts which assume all of the values in the first byte and all equal 0 in the other bytes. In the attack we guess one byte in the round key of the forth round and decrypt the forth round in the corresponding byte in all of the 256 ciphertexts. We get the 256 inputs of the ByteSubstitution of the fourth round. If the key is right, then XOR of them is equal to 0. If not, then the guess is wrong. The probability of this event (that the XOR equals 0) is 1/256 so on average only one wrong guess os left. We can check it by the forth RoundKey and from that RoundKey we derive the key.

This attack was extended to Rijndael reduced to 5 and 6 rounds by adding one round in the beginning or in the end or both of them. At recent, this attack succeed to the 7 round Rijndael assuming the whole seventh round key. The complexities of those attacks are summerized in Table 1.

4 Impossible differential attack

This attack use Impossible Differential, described in the previous section, and was extended to Rijndael reduced to 5 and 6 rounds by adding one round in the beginning or in the end or both of impossible differential.

The 5-round impossible differentiable attack is briefly introduced as the followings: Let's add one round at the end of the 4-round impossible differential and decrypt one round with assuming the fifth round key. Then, if there appears the impossible differential among them, that is a wrong key. Continuing this process we can find the fifth round key.

In the following subsection, 6-round impossible differential attack is described.

Lemma 1. *The output of MC (or MC^{-1} transformation) has zero difference in three bytes with probability about 2^{-22} over all possible input pairs.*

This lemma holds even if some values of input differences for fixed bytes are restricted. This lemma will be used when analyzing the complexity of the proposed impossible differential attack.

4.1 Rijndael Reduced to Six Rounds

In this subsection, we describe an impossible differential cryptanalysis of Rijndael reduced to six rounds. The attack is based on the four round impossible differential with additional one round at each of the beginning and the end as in Fig. 4. Note that the last round of Rijndael does not have MixColumn transformation before KeyAddition.

The procedure is as follow:

1. A structure is defined as a set of plaintexts which have certain fixed values in all but the four bytes (1, 8, 11, 14). One structure consists of 2^{32} plaintexts and proposes $2^{32} \times 2^{32} \times \frac{1}{2} = 2^{63}$ pairs of plaintexts.
2. Take $2^{59.5}$ structures($2^{91.5}$ plaintexts, $2^{122.5}$ plaintext pairs). Choose pairs whose ciphertext pairs have zero difference at the row 2 and 3. The expected number of such pairs is $2^{122.5} \times 2^{-64} = 2^{58.5}$.
3. Assume a 64-bit value at the row 0 and 1 of the last round key K_6.

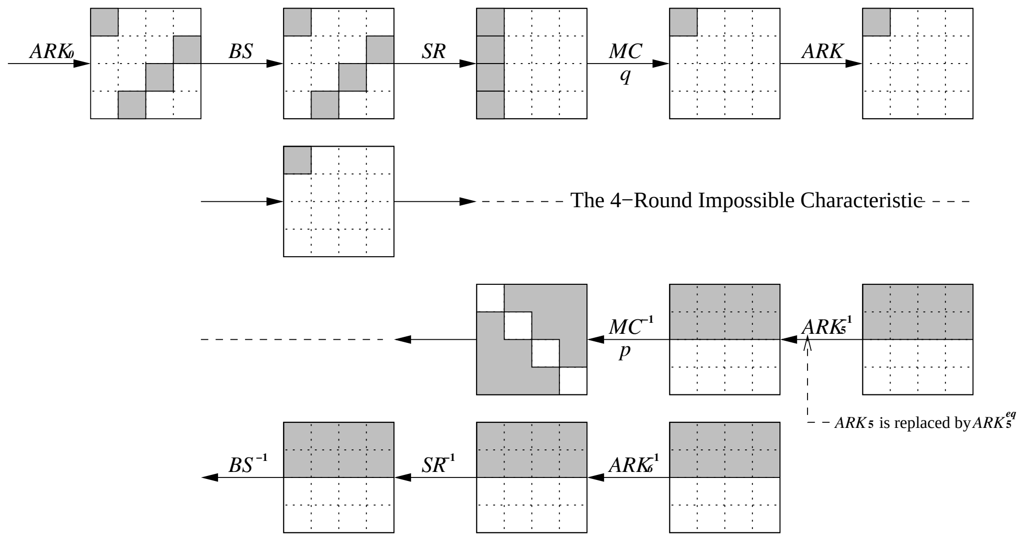

Fig. 3. Impossible Attack against Rijndael Reduced to Six Rounds

4. For each ciphertext pair (C, C^*), compute $C_5 = BS^{-1} \circ SR^{-1}(C + K_6)$ and $C_5^* = BS^{-1} \circ SR^{-1}(C^* + K_6)$ and choose pairs whose difference $MC^{-1}(C_5 + C_5^*)$ is zero at the prohibited four bytes (1,6,11,16), (2,7,12,13), (3,8,9,14) or (4,5,10,15) after the inverse of MC transformation. Since the probability is about $p = 2^{-32} \times 4 = 2^{-30}$, the expected number of the remaining pairs is $2^{58.5} \times 2^{-30} = 2^{28.5}$.
5. For a pair (P, P^*) with such ciphertext pairs and 32-bit value at the four bytes (1,8,11,14) of the initial key K_0, calculate

$$MC \circ SR(BS(P + K_0) + BS(P^* + K_0))$$

and choose pairs whose difference is zero except only one byte after MC transformation. The probability is about $q = 2^{-24} \times 4 = 2^{-22}$ since MC is linear for each byte of input values.
6. Since such a difference is impossible, every key that proposes such a difference is a wrong key. After analyzing $2^{28.5}$ ciphertext pairs, there remain only about $2^{32}(1 - 2^{-22})^{2^{28.5}} \approx 2^{32}e^{-2^{6.5}} \approx 2^{-98.5}$ wrong values of the four bytes of K_0.
7. Unless the initial assumption on the final round key K_6 is correct, it is expected that we can get rid of the whole 32-bit value of K_0 for each 64-bit value of K_6 since the wrong value (K_0, K_6) remains with the probability $2^{-34.5}$. Hence if there remains a value of K_0, we can assume the key K_6 is a right key. So if we repeat Step 2 through Step 5 after changing the row 2 and 3 into the row 0 and 1, we can get the whole value of K_6.
8. Step 4 requires about $2^{123.5}(= 2 \times 2^{64} \times 2^{58.5})$ one round operations. Step 5 requires about 2^{119} one round operations since

$$2^{64} \times 2 \times 2^{32}\{1 + (1 - 2^{-22}) + (1 - 2^{-22})^2 + \cdots + (1 - 2^{-22})^{2^{28.5}}\} \approx 2^{119}.$$

Consequently, since we repeat this procedure two times, this attack requires about $2^{91.5}$ chosen plaintexts and 2^{122} encryptions of Rijndael reduced to 6 round.

cipher	attack	round	chosen ciphertexts	complexity
Rijndael	Square attack	6 round	2^{32}	2^{72}
	impossible differentiable attack	5 round	$2^{29.5}$	2^{31}
		6 round	$2^{91.5}$	2^{122}
Crypton	Square attack	6 round	$2^{32}(2^{32} Mem.)$	2^{56}
	impossible differentiable attack	6 round	2^{91}	2^{124}

Table 1. complexity of 6-round impossible differentiable attack

5 future work

In the above attacks, it is used the 4-round property of MixColumn, but anyone does not think about improving the property itself. They only want to improve the attack skill based on the 4-round property. I will try to find the probabilistic characteristics for the 5-round Rijndael. In order to do this, I must implement the Mixcoumn layer. Then, through the theoretic approach, if I find the new property for the 5-round Rijndael, I can combine the Square attack and impossible differential attack.

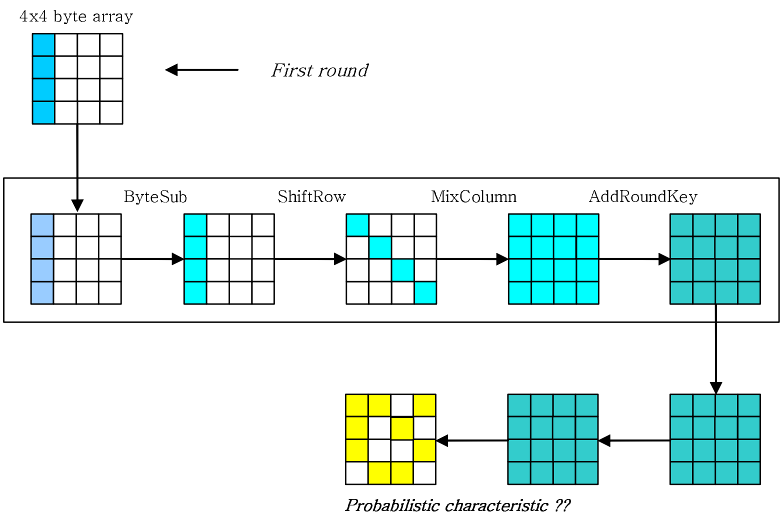

Fig. 4. Description of future work

References

1. The Advanced Encryption Standard, *http://www.nist.gov/aes*
2. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," J. of Cryptology, Vol. 3, pp.27-41, 1990.
3. E. Biham and N. Keller, "Cryptanalysis of Reduced Variants of Rijndael," *http://csrc.nist.gov/encryption /aes/round2/conf3/aes3papers.html*
4. C. D'Halluin, G. Bijnens, V. Rijmen, and B. Preneel, "Attack on Six Rounds of Crypton," Proc. of Fast Software Encryption'99, Lecture Notes in Computer Science Vol. 1636, pp. 46 – 59, Springer-Verlag, 1999.
5. J. Daemen, L. Knudsen, and V. Rijmen, "The Block Cipher Square," Proc. of Fast Software Encryption'97, Lecture Notes in Computer Science Vol. 1267, pp. 149–165, 1997.
6. J. Daemen and V. Rijmen, "AES Proposal: Rijndael," *http://csrc.nist.gov/encryption/aes/rijndael/*
7. M. Matsui, "Linear Cryptanalysis Method for DES cipher," Proc. of Eurocrypt'93, Lecture Notes in Computer Science Vol. 765, pp.386 – 397, Springer-Verlag, 1993.
8. Stefan Lucks, "Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys," Proc. of Third AES Candidate Conference, AES3, 2000.
9. Jung Hee Cheon, MunJu Kim, Kwangjo Kim and JungYeun Lee "Improved Impossible Differential Cryptanalysis of Rijndael and Crypton", Wisc, 2001.