Improved Impossible Differential Cryptanalysis of Rijndael and Crypton

Jung Hee Cheon[1], MunJu Kim[2], Kwangjo Kim[1], Jung-Yeun Lee[1], and SungWoo Kang[3]

[1] IRIS, Information and Communications University, Korea
{jhcheon,kkj,bushman}@icu.ac.kr
[2] Mathematics Department, Brown University, USA
mjkim@math.brown.edu
[3] Korea Information Security Agency, Korea
swkang@kisa.or.kr

Abstract. Impossible differential attacks against Rijndael and Crypton have been proposed up to 5-round. In this paper we expand the impossible differential attacks to 6-round. Although we use the same 4-round impossible differential as in five round attacks, we put this impossible differential in the middle of 6-round. That is, we will consider one round before the impossible differential and one more round after. The complexity of the proposed attack is bigger than that of the Square attack, but still less than that of the exhaustive search.

1 Introduction

The ciphers Rijndael [6] and Crypton [7] were submitted to the AES (Advanced Encryption Standard) candidates and Rijndael was later selected as the AES [1]. Both of them are based on the Square cipher [5] and so have SPN (Substitution-Permutation Network) structure. The original design of Square cipher concentrates on the resistance against differential and linear cryptanalysis. So it's known that two ciphers have the resistance against those attacks. Although these ciphers have those merits, they have a weakness which results from the characteristic of the optimal linear layer. The known attacks against each cipher, using this weakness, are impossible differential attack [3, 9] and 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 characteristic of the linear layer. That is the branch number which is introduced by the designers to explain the diffusion power.

Definition 1 (branch number).
Let $W(\cdot)$ be the byte weight function. The branch number of a linear transformation $F : {\mathbb{Z}_2}^8 \rightarrow {\mathbb{Z}_2}^8$ is

$$min_{a \neq 0, a \in {\mathbb{Z}_2}^8}(W(a) + W(F(a)))$$

.

This branch number makes the following property for each cipher.

- 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.
- Crypton: Crypton has a branch number 4 (designer refers this as diffusion order), namely, if a state is applied with a single nonzero byte, the output has 3 nonzero bytes

Next, each attack is described as the following:

1. Square attack
   Using the above property of branch number, we can deduce the characteristic for the relation of input and output of each cipher reduced to 4 rounds: if two plaintext differ by one byte then before the third MixColumn the data differ by all 16 bytes. It leads to the following interesting properties: 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. So the XOR of them in each byte is 0. Since the MixColumn is a linear transformation, this property holds after the MixColumn too. This is the property on which Square attack is based. Here we guess one byte in the round key of the fourth 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. Through this way we can derive the forth round 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.
2. Impossible differential attack
   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. This is the property on which impossible differential attack is based. The 5-round impossible differential 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 this paper, we propose impossible differential attacks against each cipher reduced to six rounds. Our attacks are based on the four round impossible differentials each of which was used in the impossible differential attack against each cipher reduced to five rounds [3, 9]. While the previous attacks have one additional round with the four round impossible differential, the proposed method has additional two rounds. In this method, we assume two round keys (the first round key and the last round key) and get rid of all wrong key pairs using the

impossible differentials. The complexity of the proposed attack is larger than that of the Square attack against each cipher reduced to six rounds, but still less than that of the exhaustive attack. We expect that this method may be applicable to other ciphers with SPN structure.
The rest of the paper is organized as follows: The description and 5-round impossible differential attack of Rijndael and Crypton is given in section 2 and 3, respectively. In section 4 we conclude by summarizing the efficiency of our attack together with those of previous works.

2 Rijndael

2.1 Description of Rijndael

Rijndael is a block cipher. The length of the block and the length of the key can be specified to be 128, 192 or 256 bits, independently of each other. In this paper we discuss the variant with 128-bit blocks and 128-bit keys. In this variant, the cipher consists of 10 rounds. We represent 128-bit data in 4×4 matrix as in Fig. 1.

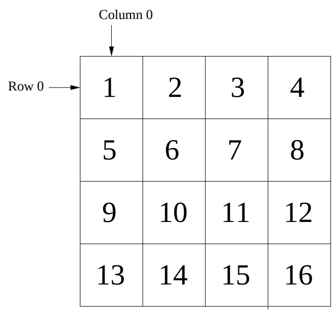

Fig. 1. Byte Coordinate of 128-bit

Every round except for the last consists of 4 transformation:

- *ByteSubstitution* is applied to each byte separately and is a nonlinear bytewise substitution to use the Sbox.
- *ShiftRow* is a cyclic shift of the bytes of each row by 0, 1, 2, or 3, respectively.
- *MixColumn* is a linear transformation applied to columns of the matrix. The branch number of this layer is 5.
- *AddRoundKey* is a key XOR.

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

Observe that MixColumn is a linear transformation over four bytes of input differences, since it is a linear transformation over four input bytes. If three bytes of output difference are zero, the choice of input differences is $2^8 - 1$ since MC is invertible. Hence the probability that output difference is zero at three bytes is $4 \times (2^8 - 1)/2^{32}$ since there are four choices on nonzero byte of output difference and the output difference is not zero for nonzero input difference.

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.

2.2 Impossible Differential

We use the same impossible differential described in [3]. See Fig. 2.

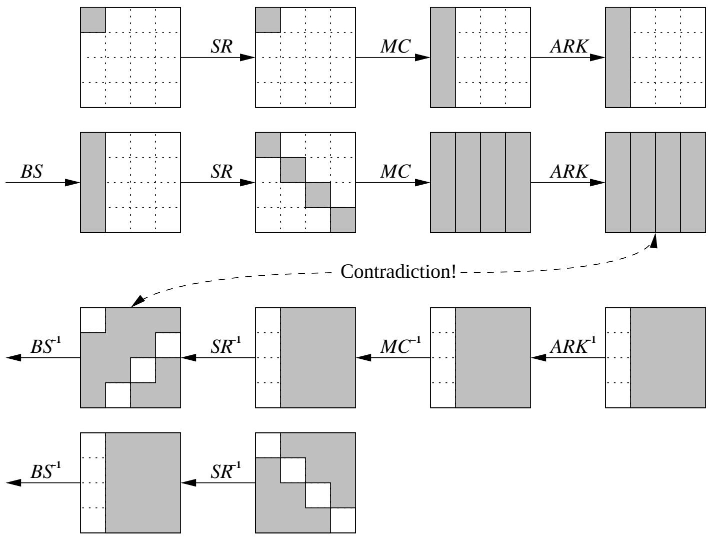

Fig. 2. Four Rounds Impossible Differential of Rijndael

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 property follows from the property of MixColumn transformation: if two inputs of this transformation differ by one byte then the corresponding outputs differ by all the four bytes.

2.3 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. 3. Note that the last round of Rijndael does not have MixColumn transformation before KeyAddition.

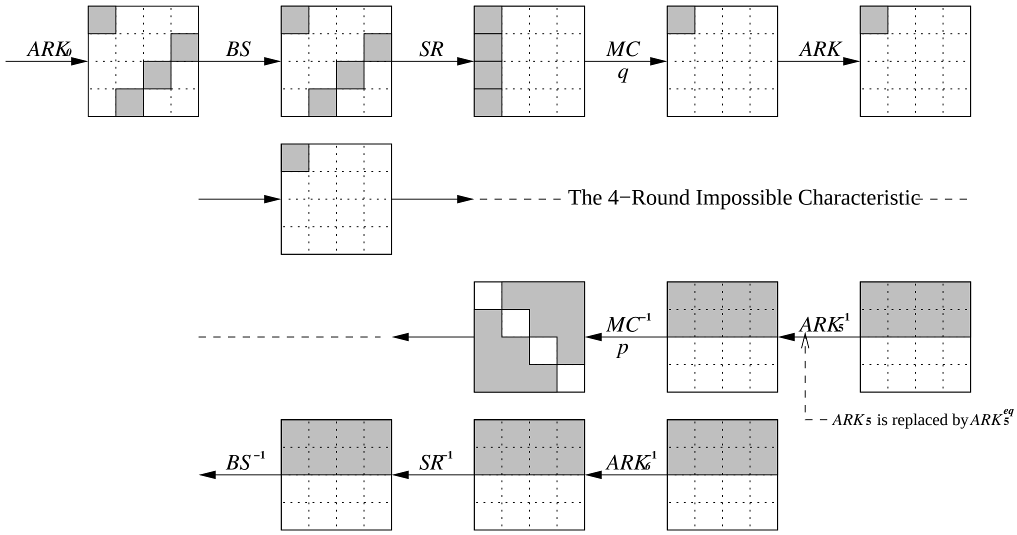

Fig. 3. Impossible Attack against Rijndael Reduced to Six Rounds

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.
4. For each ciphertext pair (C, C^*), compute $C_5 = BS^{-1} \circ SR^{-1}(C \oplus K_6)$ and $C_5^* = BS^{-1} \circ SR^{-1}(C^* \oplus K_6)$ and choose pairs whose difference $MC^{-1}(C_5 \oplus C_5^*)$ 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
$$MC \circ SR(BS(P \oplus K_0) \oplus BS(P^* \oplus K_0))$$
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.

3 Crypton

3.1 Description of Crypton

Crypton is a 128-bit block cipher. We represent 128-bit data in 4×4 matrix as in Fig. 4. The component functions, σ, τ, π, and γ, are as follows.

- γ is a nonlinear byte-wise substitution. There are two versions of γ: γ_o is for odd rounds and γ_e is for even rounds.
- π is a linear bit permutation. It bit-wisely mixes each column (4 bytes). In fact, there are two versions of π: π_o in odd rounds and π_e in even rounds. One important fact is both versions have the branch number 4 as maps from 4-byte input to 4-byte output [7].
- τ is a linear transposition. It simply moves the byte at A[i][j] to A[j][i].
- σ is a key XOR. We will use notation σ_K when the given key is K.

The $2n$-round encryption of Crypton can be described as
$$\phi_e \circ \rho_{e_{K_{2n}}} \circ \rho_{o_{K_{2n-1}}} \cdots \circ \rho_{e_{K_2}} \circ \rho_{e_{K_1}} \circ \sigma_{K_0},$$
where $\rho_{o_{K_i}} = \sigma_{K_i} \circ \tau \circ \pi_o \circ \gamma_o$ for odd rounds and $\rho_{e_{K_i}} = \sigma_{K_i} \circ \tau \circ \pi_e \circ \gamma_e$ for even rounds, and the linear output transformation $\phi_e = \tau \circ \pi_e \circ \tau$ is used at the last round.

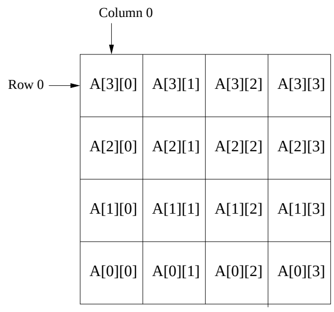

Fig. 4. Byte Coordinate of 128-bit

3.2 Impossible Differential of Crypton

We introduce a four round impossible differential of Crypton. Fig. 5 describes one pattern of impossible differentials. The impossible differentials comes from the following observation.

1. If an input pair has zero difference at a byte, then the output pair after σ, γ, σ^{-1}, or γ^{-1} also has zero difference at the byte.
2. If an input pair has zero difference at byte$[i][j]$, then the output pair after τ or τ^{-1} has zero difference at byte$[j][i]$.
3. π, the word transformation has the branch number 4 as a map from 4-byte input to 4-byte output. That is, if input pair has only one nonzero difference out of four bytes, then the output difference has at least three nonzero difference.

Property 2 (Impossible Differential). Given input pair to τ whose difference is zero at all bytes but one, the output difference after the four round starting with τ and ending with γ cannot be zero at all but two rows in the left two columns.

3.3 An Attack against Crypton Reduced to Six Rounds

In this subsection, we describe an impossible differential cryptanalysis on Crypton reduced to 6 rounds. The attack is based on the four round impossible differential. We compose the 6 rounds as in Fig. 6. One thing we need to notice is that we replace the 5th and 6th round key addition σ_{K_5} and σ_{K_6} by σ_{null} which is a key addition with zero key. We can compose the same encryption system by putting $\sigma_{K_5^{eq}}$ and $\sigma_{K_6^{eq}}$ between γ and π of their rounds. Here K^{eq} means the equivalent key *i.e.* $\pi^{-1} \circ \tau^{-1}(K)$

The procedure is as follow:

1. A structure is defined as a set of plaintexts which have certain fixed values in the column 1, 2, and 3. One structure consists of 2^{32} plaintexts and proposes $2^{32} \times 2^{32} \times \frac{1}{2} = 2^{63}$ pairs of plaintexts.

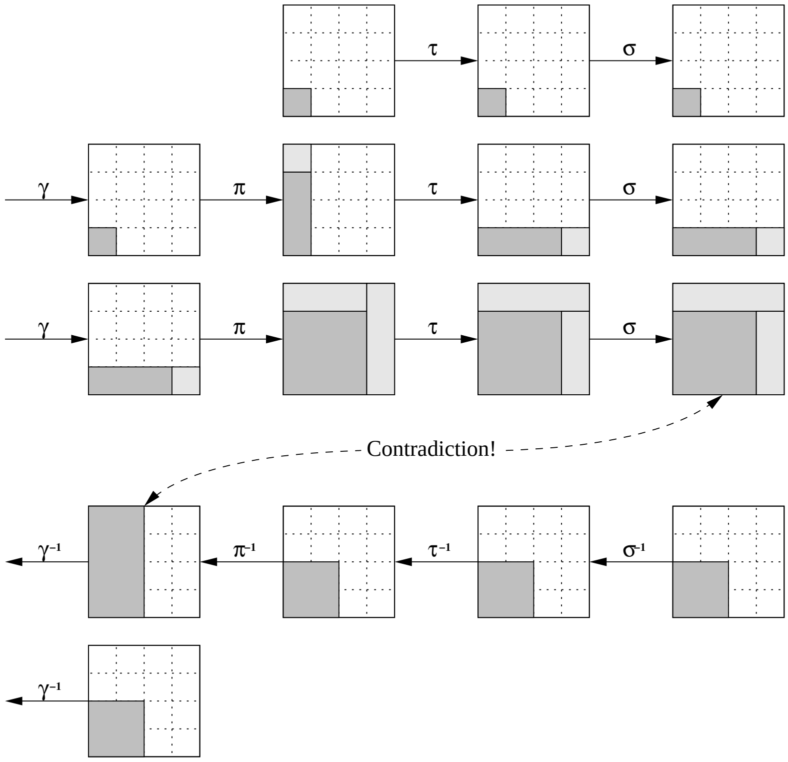

Fig. 5. Four Round Impossible Differential of Crypton

2. Take 2^{59} structures (2^{91} plaintexts, 2^{122} plaintext pairs). Choose plaintext pairs (P, P^*) such that the pairs (C_6, C_6^*) has zero difference at the row 0 and 1, where $C_6 = \pi_e^{-1} \circ \tau^{-1} \circ \sigma_{null} \circ \tau^{-1} \circ \pi_e^{-1} \circ \tau^{-1}(C)$ and C is a ciphertext of P. The expected number of such pairs is $2^{122} \times 2^{-64} = 2^{58}$.
3. Assume a 64-bit value of the row 2 and 3 of the last round key K_6^{eq}.
4. For each pair (C_6, C_6^*) satisfying Step 2, compute $C_5 = \gamma_e^{-1}(C_6 \oplus K_6^{eq})$ and $C_5^* = \gamma_e^{-1}(C_6^* \oplus K_6^{eq})$ and choose pairs whose difference $\pi_o^{-1} \circ \tau^{-1}(C_5 \oplus C_5^*)$ is zero at any two rows. Since the probability is about $p = 2^{-32} \times 6 \approx 2^{-29.5}$, the expected number of the remaining pairs is $2^{58} \times 2^{-29.5} = 2^{28.5}$.
5. For a pair (P, P^*) satisfying Step 4, consider 32-bit values of the first column of K_0 such that $\pi(\gamma_o(P \oplus K_0) \oplus \gamma_o(P^* \oplus K_0))$ is zero at all but one byte of the first column. The probability is $q = 2^{-24} \times 4 = 2^{-22}$
6. Since such a difference is impossible, every key that proposes such a difference is a impossible key with the chosen key K_6^{eq} in Step 3. After analyzing $2^{28.5}$ plaintext pairs, there remain only about $2^{32}(1 - 2^{-22})^{2^{28.5}} \approx 2^{32}e^{-2^{6.5}} \approx 2^{-98.5}$ possible values for the four bytes of the first column of K_0, which means no possibility.

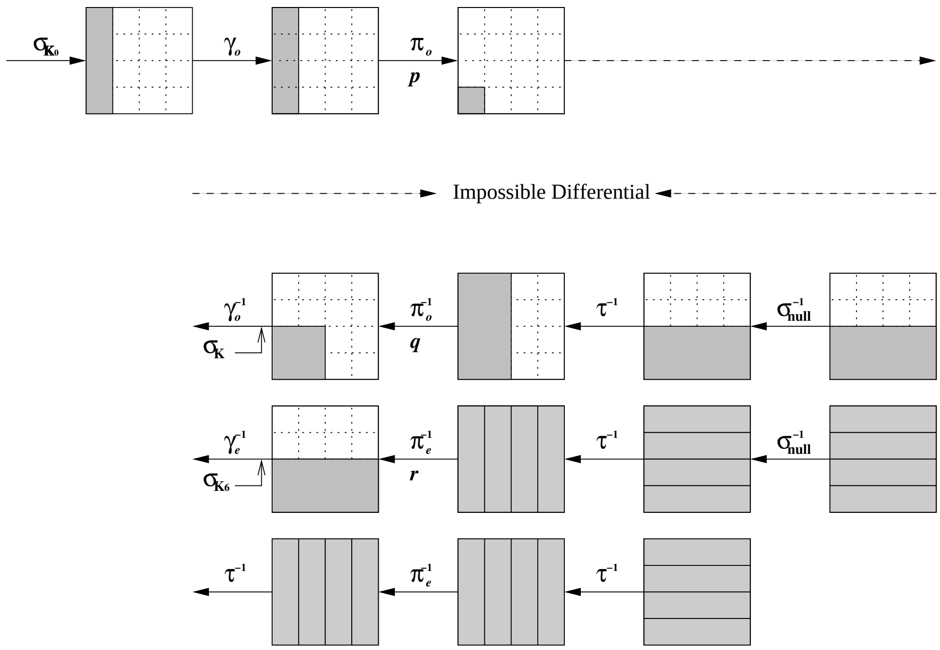

Fig. 6. Impossible Attack against Crypton Reduced to Six Rounds

7. Unless the initial assumption on the final round key K_6^{eq} is correct, it is expected that we can get rid of the whole 32-bit values of K_0 for each 64-bit value of K_6^{eq} since the wrong value (K_0, K_6^{eq}) remains with the probability $2^{64} \times 2^{-98.5} = 2^{-34.5}$. Hence if there remains a value of K_0, we can assume the key K_6^{eq} is a right key. So if we repeat Step 2 through Step 6 after changing the row 0 and 1 with the row 2 and 3, we can get the whole value of K_6^{eq}.
8. Step 2 requires about $2^{123}(= 2 \times 2^{122})$ of $\pi_e^{-1} \circ \pi_e^{-1} \circ \tau^{-1} \circ 6round$. Step 4 requires about $2^{125.5}(= 2^{64} \times 2 \times 2^{60.5})$ of $\pi_o^{-1} \circ \tau^{-1} \circ \sigma^{-1}$. Step 6 requires about 2^{119} of $\pi_o \circ \gamma_o$ 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 twice, this attack requires about 2^{91} chosen plaintexts and 2^{124} encryptions of Crypton reduced to 6 rounds.

3.4 A Variant of the Attack using Memory

In this subsection, we describe a variant of the impossible differential cryptanalysis of the former subsection using memory.

Precomputation Stage

Take all $2^{32} \times 2^8 \times 4 = 2^{42}$ pairs of four bytes in the first column which differ only in one byte(this is the data after one round encryption except the first round key addition). For these pairs, we undo the encryption of the first round, i.e., perform τ^{-1}, π^{-1} and γ^{-1}, and create a hash table containing one of the inputs of γ transformation and the XOR of two inputs $x \oplus y$, indexed by $x \oplus y$, where x, y are the inputs of the γ transformation.

Step 4'

At first, perform $\pi^{-1} \circ \gamma^{-1} \circ \pi^{-1} \circ \tau^{-1}$ operations for all $2^{93.5}$ ciphertexts, and store the pairs (C, U_C) where C is a ciphertext and U_C is a corresponding result after π^{-1} transformation. For each ciphertext pair (C, C^*), compare U_C and U_{C^*} and choose pairs whose difference $U_C \oplus U_{C^*}$ is zero at the row 0 and 1. Since the probability is $p = 2^{-32}$, the expected number of the remaining pairs is $2^{60.5} \times 2^{-32} = 2^{28.5}$.

Step 5'

For a pair (P, P^*) with ciphertext pairs passing Step 4, we compute $x \oplus y$ and use the hash table to fetch the about 2^{10} possibility of x which correspond to the computed $x \oplus y$. This process identities about 2^{10} wrong key by XORing the plaintexts and the x's.

If we replace Step 4 and Step 5 by Precomputation stage, Step 4' and Step 5', the complexity is as follows:

- Step 4 requires $2^{93.5}$ $\pi^{-1} \circ \gamma^{-1} \circ \pi^{-1} \circ \tau^{-1}$ operations and $2^{-124.5}$ operations of two times memory access and comparison which is about 2^{14} times faster than the 6-round Crypton . Hence Step 4 is equivalent to about $2^{110.5}$ encryptions. In addition, Step 4 requires $2^{93.5} \times 128 \times 128 = 2^{104.5}$ memory.
- In Step 5', for $2^{28.5}$ remaining plaintext pairs we get rid of 2^{10} impossible keys by XORing the plaintext and x's which requires about 2^{32} encryptions for each assumed key K_6^{eq}.
- To sum up, this attack requires $2^{93.5}$ plaintexts, $2^{110.5}$ encryptions and $2^{104.5}$ bytes of memory.

4 Conclusion

In this paper, we described an impossible differential attack against Rijndael and Crypton reduced to 6 rounds. The attack against Rijndael reduced to 6 rounds requires about $2^{91.5}$ chosen plaintexts and 2^{122} encryptions. The attack against Crypton reduced to 6 rounds requires about 2^{91} chosen plaintexts and 2^{124} encryptions, or $2^{93.5}$ plaintexts, $2^{110.5}$ encryptions and $2^{104.5}$ bytes of memory. We summarize the complexities of our attacks together with those of previous works in Table 1. We expect that this method can be applied to other block ciphers with SPN Structure.

Table 1. Complexity of 6-Round Impossible Differential Attack

Cipher	Attack	Round	Chosen Ciphertexts	Complexity
Rijndael	Square attack	6 round	2^{32}	2^{72}
	Impossible differential 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 differential attack	5 round	$2^{83.4}$	2^{43}
		6 round	2^{91}	2^{124}

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. C. Lim, "A Revised Version of Crypton - Crypton 1.0," Proc. of Fast Software Encryption'99, Lecture Notes in Computer Science Vol. 1636, pp. 31 – 45, Springer-Verlag, 1999.
8. 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.
9. H. Seki and T. Kaneko, "Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials," Proc. of Asiacrypt'99, Lecture Notes in Computer Science Vol. 1716, pp.43-51,1999.
10. Stefan Lucks, "Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys," Proc. of Third AES Candidate Conference, AES3, 2000.