Cryptanalysis of Five Rounds of CRYPTON Using Impossible Differentials

Haruki Seki[1] and Toshinobu Kaneko[2]

[1] TAO (Telecommunications Advancement Organization of Japan)
1-1-32 Shin'urashima-cho, Kanagawa-ku, Yokohama, 221-0031 Japan
hseki@yokohama.tao.go.jp
[2] Science University of Tokyo
2641 Yamazaki, Noda-shi, Chiba, 278-8510 Japan
kaneko@ee.noda.sut.ac.jp

Abstract. An block cipher CRYPTON based on the structure of SQUARE is a candidate algorithm for the AES. Recently Lim changes the S-box construction and key scheduling, and suggested modified version(version 1.0) in FSE'99. In this paper we present an attack on CRYPTON reduced to 5 rounds. This attack is based on impossible differentials[7]. 4 rounds of CRYPTON has impossible differential, we use this to show that CRYPTON version 1.0 reduced to 5 rounds can be attacked using $2^{83.4}$ chosen plaintext and ciphertext pairs. This attack can be also applied to CRYPTON version 0.5 using less chosen plaintext and ciphertext pairs.

1 Introduction

C.H.Lim proposed an block cipher CRYPTON[1] based on the structure of SQUARE[5]. It is a candidate algorithm for the AES. Several analyses were proposed to this cipher. Weak keys are discovered in CRYPTON version 0.5[3]. In[4], G.Bijnens applied higher order differential attack to 6 rounds of CRYPTON. To overcome some weakness, recently Lim suggested modified version(version 1.0)[2]. This new version changes the S-box construction and key scheduling.

In this paper we applied a variant of differential cryptanalysis, which is called impossible differential cryptanalysis, to CRYPTON reduced to 5 rounds. The idea of cryptanalysis with impossible differentials was applied to DES S-boxes by E.Biham[6]. Recently Skipjack reduced to 31 rounds was attacked by cryptanalysis with impossible differentials[7]. It seems that this attack is powerful for some ciphers with impossible differentials. Both version of CRYPTON has impossible differential, which ensure that for all keys there are no pairs of inputs with particular differences with the property that after 4 rounds of encryption the outputs have some other particular differences. This impossible differential is applied to attack on CRYPTON reduced to 5 rounds. Using $2^{83.4}$ chosen plaintext and ciphertext pairs, fifth roundkey of 128 bits of CRYPTON version 1.0 can be obtained. CRYPTON version 0.5 can be also attacked using $2^{75.6}$ chosen plaintext and ciphertext pairs.

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 43–51, 1999.

This paper is organized as follows. Section 2 gives a preliminary. Section 3 briefly reviews algorithms of CRYPTON. In section 4 we describe a 4-round impossible differential of CRYPTON. In section 5 we discuss the attack on CRYPTON version 1.0 reduced to 5 rounds. In section 6 we discuss the attack on CRYPTON version 0.5 reduced to 5 rounds. We conclude in section 7.

2 Preliminary

In this paper we use next definitions.

Definition 1. $A^i_\gamma, A^i_\pi, A^i_\tau, A^i_\sigma$: Input of $\gamma, \pi, \tau, \sigma$ transformation in round i
Definition 2. $B^i_\gamma, B^i_\pi, B^i_\tau, B^i_\sigma$: Output of $\gamma, \pi, \tau, \sigma$ transformation in round i
Definition 3. A': Differential value of a pair of A
Definition 4. P, C: Plaintext, ciphertext
Definition 5. K^i_e: A 128-bit roundkey in round i
Definition 6. $A[i][j]$: A 8-bit word of i-th row and j-th column of 4×4 matrix

3 Description of CRYPTON

A[0][3]	A[0][2]	A[0][1]	A[0][0]
A[1][3]	A[1][2]	A[1][1]	A[1][0]
A[2][3]	A[2][2]	A[2][1]	A[2][0]
A[3][3]	A[3][2]	A[3][1]	A[3][0]

Fig. 1. Byte coordinate of CRYPTON

The block cipher CRYPTON is designed based on SQUARE. The data is arranged to a 4×4 byte array as shown in Fig.1. CRYPTON uses next transformation in each round.

- Nonlinear byte substitution γ : Two different transformations γ_o,γ_e are used alternatively in successive rounds. γ_o is used in odd rounds,γ_e is used in even rounds. This transformation consists of byte-wise substitutions.
- Linear columnwise bit permutation π: Two different transformation π_e,π_o are used. π_e is used in even rounds, π_o is used in odd rounds. These transformations calculates two bits at once by exoring the value of two bits in corresponding positions in three different bytes of the column. They can be implemented using four mask bytes, denoted $m_0 = fc_x, m_1 = f3_x, m_2 = cf_x, m_3 = 3f_x$.

$$B_{\pi_o}[i][j] = \bigoplus_{k=0}^{3} \left((A[k][j]) \wedge m_{(i+j+k) mod\ 4}\right) \qquad for\ odd\ rounds\ .$$

$$B_{\pi_e}[i][j] = \bigoplus_{k=0}^{3} \left((A[k][j]) \wedge m_{(i+j+k+2) mod\ 4}\right) \qquad for\ even\ rounds\ .$$

  For even rounds of CRYPTON version 0.5 $m_{(i+j+k+2) mod\ 4}$ is replaced by $m_{(i+j+k+1) mod\ 4}$.
- Linear column-to-row transposition τ: This operation simply rearranges 4×4 byte array by moving the byte at the (i, j)-th position to the (j, i)-th position.
- Key addition $\sigma_{K_e^i}$: This operation is xoring data with i-th roundkey K_e^i of 128 bits.

The encryption round functions are defined for odd and even rounds as follows.

- $\rho_{oK_e^i}(A) = (\sigma_{K_e^i} \circ \tau \circ \pi_o \circ \gamma_o)(A)$ for odd rounds
- $\rho_{eK_e^i}(A) = (\sigma_{K_e^i} \circ \tau \circ \pi_e \circ \gamma_e)(A)$ for even rounds

And linear output transformation ϕ_e is used at last round.

- $\phi_e = \tau \circ \pi_e \circ \tau$

Then encryption of full 12-round CRYPTON is described as

- $Enc = \phi_e \circ \rho_{eK_e^{12}} \circ \rho_{oK_e^{11}} \circ \cdots \circ \rho_{eK_e^2} \circ \rho_{oK_e^1} \circ \sigma_{K_e^0}$

We don't consider the use of ϕ_e in our attack, because this function uses only known quantities.

4 A 4-Round Impossible Differential

In this section we show CRYPTON has a 4-round impossible differential. Fig. 2 describes one pattern of an impossible differential.

An Impossible Differential **:** Given an input of the form (a), then there cannot be pairs $B_\gamma^{4\prime}$ of the form (b) after byte substitution γ in round 4.

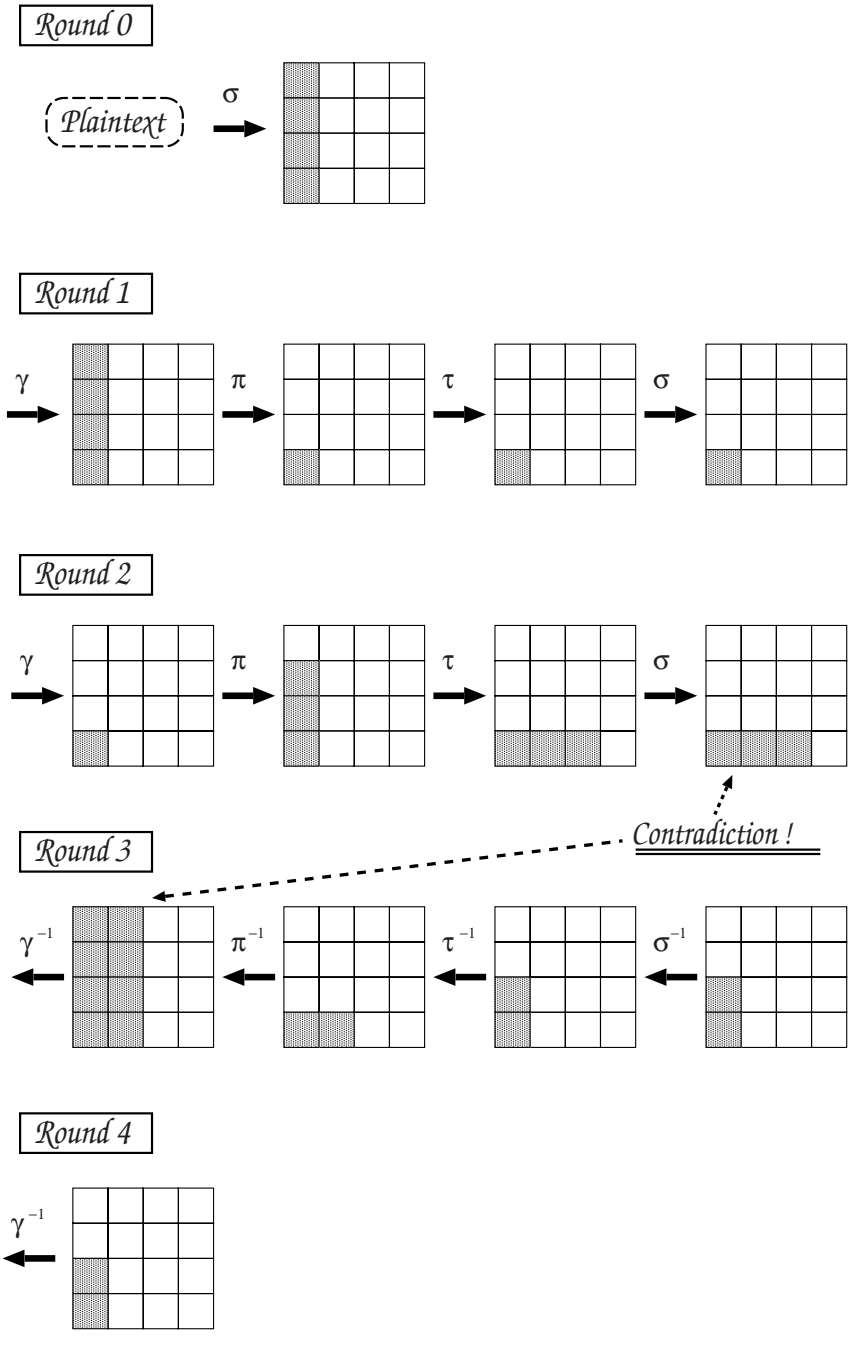

Fig. 2. The 4-round impossible differential. White squares represents zero differences, gray squares represents nonzero differences.

(a) The differences of 4 words in only one column of the plaintext pair are nonzero, and the differences of all 12 words in other 3 columns are zero. For example,

$$P' = \begin{bmatrix} a\,0\,0\,0 \\ b\,0\,0\,0 \\ c\,0\,0\,0 \\ d\,0\,0\,0 \end{bmatrix}$$

(b) The differences of one or two words in any one column of $B_\gamma^{4\prime}$ are nonzero, and those of all other 15 or 14 words are zero. For example,

$$B_\gamma^{4\prime} = \begin{bmatrix} 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ e\,0\,0\,0 \\ f\,0\,0\,0 \end{bmatrix}$$

To prove this, we make the following observations:(see Fig.2).

1. If $B_\gamma^{4\prime}$ has the form stated in (b), then all 8 words of 2 columns of $B_\gamma^{3\prime}$, which is the difference after γ transformation in round 3, are zero(for example, column 0 and 1 in Fig. 2). So all 8 words of 2 columns of $B_\sigma^{2\prime}$, which is the difference after σ transformation in round 2, are zero.
2. If the difference of plaintext pair has the form stated in (a), then some words of only one row of $B_\tau^{1\prime}$, which is the difference after τ transformation in round 1, are nonzero. 3 or 4 words of any column of $B_\pi^{2\prime}$, which is the difference after π transformation in round 2, are nonzero. [1] So the difference of 3 or 4 words of at least one row of $B_\sigma^{2\prime}$, i.e., 3 or 4 columns, are nonzero.
3. From *1* just 2 columns of $B_\sigma^{2\prime}$ are zero. From *2* at least 3 columns of $B_\sigma^{2\prime}$ are nonzero. This is a contradiction.

5 An Attack on CRYPTON Version 1.0 Reduced to 5 Rounds

In this section we describe cryptanalysis of CRYPTON version 1.0 reduced to 5 rounds. The attack is based on the 4-round impossible differential with additional one round at the end. An attack is as follows.

1. Choose structure of 2^{32} plaintexts which differ at four words of only column 3, i.e.,$P[0][3], P[1][3], P[2][3], P[3][3]$, having all the possible values in it. Such structure proposes about 2^{63} pairs of plaintexts(see Fig.2).

[1] π transformation always transform one nonzero differential word into 3 or 4 nonzero differential words.

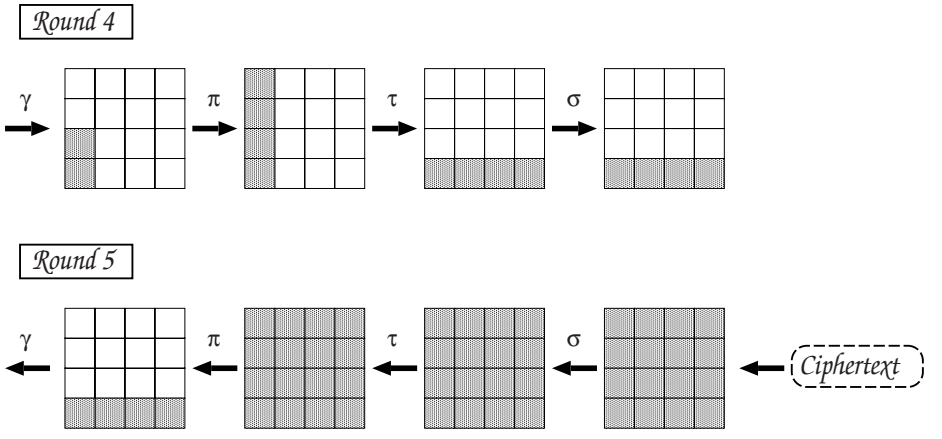

Fig. 3. Ciphertext pattern used in an attack. The impossible differentials in round 4 always satisfy $B_\gamma^{5\prime}$ pattern used.

2. Given $2^{51.4}$ structures ($2^{83.4}$ plaintexts), we calculate B_γ^5 using linear transformation of ciphertexs C as follows.

$$B_\gamma^5 = \pi_o\left(\tau(C)\right) \ . \tag{1}$$

3. We collect all those pairs which differ only at four words of the i-th row of B_γ^5, which are pairs after γ transformation in round 5(see Fig.3).
Only pairs, which has nonzero difference in 1 or 2 words of i-th column of $B_\gamma^{4\prime}$ and zero differences in all other 14 or 15 words, satisfy this $B_\gamma^{5\prime}$. By this operation on average one structure proposes $2^{-33}(= 2^{-96} \times 2^{63})$ such pairs, and thus only about $2^{18.4}(= 2^{-33} \times 2^{51.4})$ pairs remain.

4. We decrypt remaining pairs with all possible 32-bit value of i-th row of K_{eq}^5. The decryption is expressed as follows.

$$\begin{aligned}(A_\gamma^5[i][0] \ &, A_\gamma^5[i][1], A_\gamma^5[i][2], A_\gamma^5[i][3]) \\ &= \big(\gamma_o(B_\gamma^5[i][0] \oplus K_{eq}^5[i][0]), \gamma_o(B_\gamma^5[i][1] \oplus K_{eq}^5[i][1]) \\ &\quad , \gamma_o(B_\gamma^5[i][2] \oplus K_{eq}^5[i][2]), \gamma_o(B_\gamma^5[i][3] \oplus K_{eq}^5[i][3])\big) \ .\end{aligned} \tag{2}$$

Where we express equivalent key K_{eq}^5 of round key K_e^5 as follows.

$$K_{eq}^5 = \pi_o\left(\tau(K_e^5)\right) \ . \tag{3}$$

5. Next we calculate the difference of the i-th column of $B_\gamma^{4\prime}$ as follows.

$$\begin{aligned}(B_\gamma^{4\prime}[0][i] \ &, B_\gamma^{4\prime}[1][i], B_\gamma^{4\prime}[2][i], B_\gamma^{4\prime}[3][i])^t \\ &= \Big(\pi_e\big(\tau(A_\gamma^{5\prime}[i][0], A_\gamma^{5\prime}[i][1], A_\gamma^{5\prime}[i][2], A_\gamma^{5\prime}[i][3])\big)\Big)^t \ .\end{aligned} \tag{4}$$

As we know that such a difference as those of the form (b) is impossible, every key that proposes such a difference is a wrong key. For each pair we try all the 2^{32} possible values of the i-th row of equivalent key K^5_{eq}, and verify whether the decrypted values have the form (b). It is expected that about 6×2^{16} values proposed this difference, and thus we are guaranteed that these 6×2^{16} values are not the correct equivalent key of round 5. After analyzing the $2^{18.4}$ pairs, there remain only about $2^{32} \times (1 - 6 \times 2^{-16})^{2^{18.4}} = 2^{-14}$ wrong values of the equivalent key of round 5. It is thus expected that only one value remains, and this value must be the correct 32-bit equivalent key of i-th row of K^5_{eq}.

6. If we do above procedure for $i = 0, 1, 2, 3$, then 32-bit equivalent key of i-th row of K^5_{eq} can be obtained independently. Finally 128-bit round key of round 5 is obtained by linear transformation as follows.

$$K^5_e = \tau \circ \pi_o \circ K^5_{eq} \ . \tag{5}$$

The time complexity of recovering 128-bit roundkey of round 5 is equivalent to about $2^{83.4}$ $\pi \circ \tau$ transformation and 2^{43} encryptions. [2]

6 An Attack on CRYPTON Version 0.5 Reduced to 5 Rounds

The procedure of an attack on CRYPTON version 0.5 is the same as that on version 1.0. The number of plaintext and ciphertext pairs needed for an attack is less than that needed on version 1.0.

We can collect pairs which have nonzero differences only in 4 words of i-th row of $B^{5\prime}_{\gamma}$ with higher probability than the case of version 1.0. This is caused by the difference in the S-box construction. We explain this as follows (see appendix for details).

1. When 4 words of only the third column of P' are nonzero, we can collect pairs which have nonzero difference in 4 words of only the first row of $B^{5\prime}_{\gamma}$ with probability $2^{-87.2}$. From the same plaintexts we can also collect pairs which have nonzero difference in 4 words of only the third row of $B^{5\prime}_{\gamma}$ with probability $2^{-87.2}$.

2. Similarly when 4 words of only the 0-th column of P' are nonzero, we can collect pairs which have nonzero difference in 4 words of only the 0-th row (and only the second row) of $B^{5\prime}_{\gamma}$ with probability $2^{-87.2}$.

So we can obtain the first row and the third row of K^5_{eq} using $2^{42.6}$ structures ($2^{74.6}$ plaintexts) as shown in *1*, and 0-th row and the second row of K^5_{eq} using $2^{42.6}$ structures ($2^{74.6}$ plaintexts) as shown in *2*.[3] Totally $2^{75.6}$ plaintext and ciphertext pairs are needed for an attack.

[2] $2^{32} + 2^{32} \times (1 - 6 \times 2^{-16}) + 2^{32}(1 - 6 \times 2^{-16})^2 \cdots + 2^{32} \times (1 - 6 \times 2^{-16})^{2^{18.4}} = 1.3 \times 2^{45}$ $\pi \circ \tau \circ \gamma \circ \sigma_{K_e}$ computations are needed. Since 5 round encryption consists of 5 applications of $\pi \circ \tau \circ \gamma \circ \sigma_{K_e}$, this time complexity is equal to about 2^{43} encryptions.

[3] $2^{42.6} \times 2^{63} \times 2^{-87.2} = 2^{18.4}$ pairs remain for each case as shown in *1* or *2*.

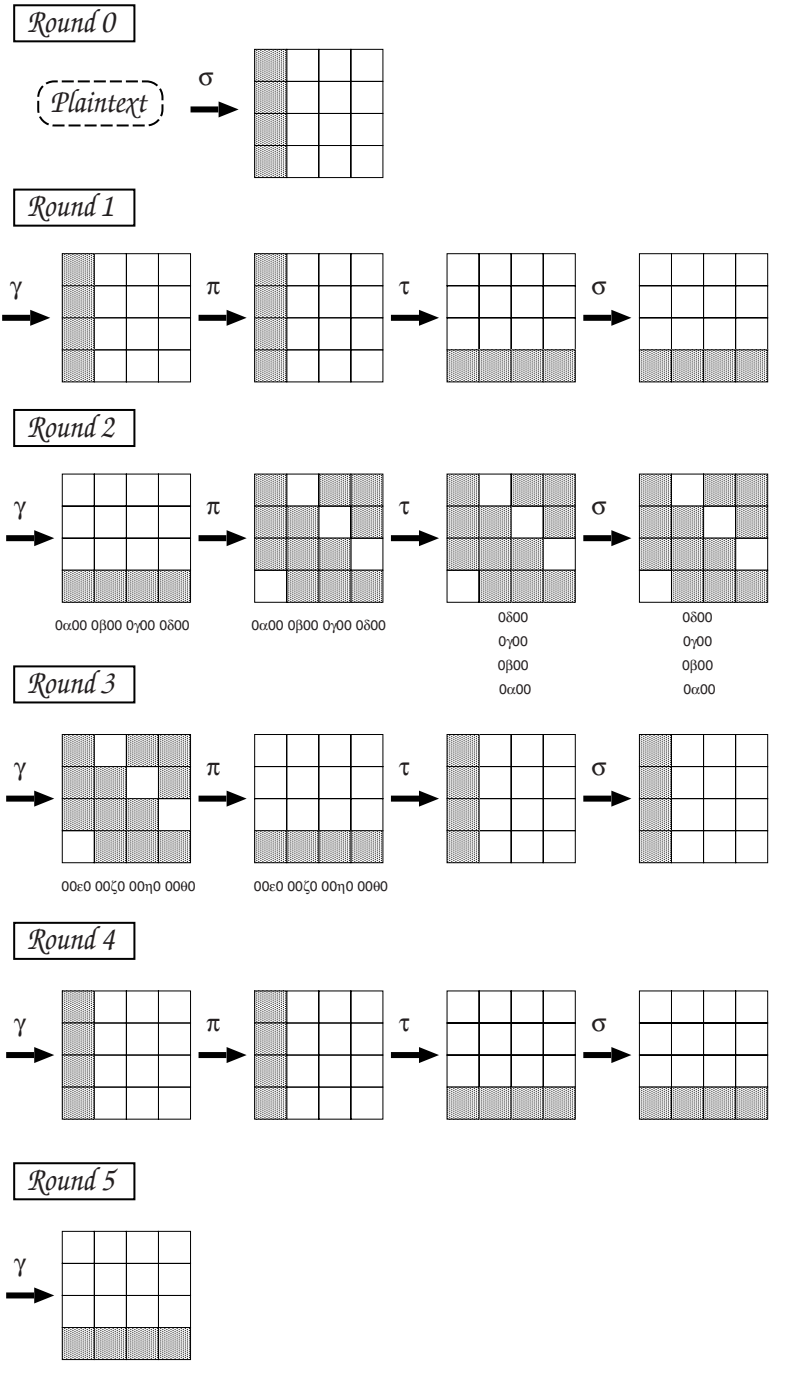

Fig. 4. One of differential patterns of CRYPTON version 0.5 used for an attack

7 Conclusion

In this paper we described an attack on CRYPTON reduced to 5 rounds using impossible differential on 4-round CRYPTON. To obtain 128-bit roundkey of round 5 of CRYPTON version 1.0, we need $2^{83.4}$ chosen plaintext and ciphertext pairs. This attack can be also applied to CRYPTON version 0.5 using $2^{75.6}$ chosen plaintext and ciphertext pairs.

References

1. C.H.Lim., *"http://www.nist.gov/aes"* 43
2. C.H.Lim., *"A Revised Version of CRYPTON: CRYPTON Version 1.0,"* Fast Software Encryption, 1999, pp. 31-46. 43
3. S.Vaudenay., *"Weak keys in CRYPTON,"* announcement on NIST's electronic AES forum, http://www.nist.gov/aes. 43
4. C.D'Halluin,G.Bijnens,V.Rijimen,and B.Preneel., *"Attack on Six Rounds of CRYPTON,"* Fast Software Encryption, 1999, pp.47 -60. 43
5. J.Daemen, L.Knudsen and V.Rijmen, *"The block cipher Square,"* Fast Software Encryption,1997, Spring-Verlag, LNCS 1267, pp.149-165. 43
6. E.Biham, A.Shamir., *"Differential Cryptanalysis of DES-like Cryptosystems,"* CRYPTO'90 Proceedings,Spring-Verlag, 1990, pp.2-21. 43
7. E.Biham, A.Biryukov, and A.Shamir., *"Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials,"* EUROCRYPT'99 Proceedings,Spring-Verlag,LNCS 1952, 1999, pp.12-23. 43

Appendix

We explain the case of *1* in section 6. When only the third column of P' is nonzero, we can collect pairs which have nonzero difference of 4 words of only the third row of $B_\gamma^{5\prime}$ with probability $2^{-87.2}$. Fig.4 shows this differential pattern. 4 words of $B_\gamma^{2\prime}$ with nonzero difference have next form.

$$\left(B_\gamma^{2\prime}[3][0], B_\gamma^{2\prime}[3][1], B_\gamma^{2\prime}[3][2], B_\gamma^{2\prime}[3][3]\right) = (0\delta 00, 0\gamma 00, 0\beta 00, 0\alpha 00) \ . \qquad (6)$$

$0\alpha 00$ is 8-bit word which has nonzero difference on 4-5 bits. After π, τ and σ transformation in round 2, $A_\gamma^{3\prime}$ has the form shown in Fig.4. When every 3 words of each column of $B_\gamma^{3\prime}$ has the same value as $00\varepsilon 0$, after π transformation in round 3 $B_\pi^{3\prime}$ has nonzero differences of 4 words of only the third row. The probability of γ transformation in round 2 is $2^{-24}\left(=(2^{-6})^4\right)$. The probability of γ transformation in round 3 is $2^{-63.2}\left(=(\frac{5}{3}\times 2^{-6})^{12}\right)$. So the probability of $B_\gamma^{5\prime}$ having nonzero difference of 4 words of only third row is $2^{-87.2}$. From the same plaintexts we can also collect $B_\gamma^{5\prime}$ having nonzero difference of 4 words of only first row with probability $2^{-87.2}$. The case of *2* in section 6 can be also explained by the similar procedure as above.