Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis

Jaechul Sung[1], Sangjin Lee[1], Jongin Lim[1], Seokhie Hong[1], and Sangjoon Park[2]

[1] Center for Information and Security Technologies(CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, KOREA
{sjames, sangjin, jilim, hsh}@cist.korea.ac.kr
[2] National Security Research Institute(NSRI), Taejon, KOREA
sjpark@etri.re.kr

Abstract. In this paper we introduce a structure iterated by the rule A of Skipjack and show that this structure is provably resistant against differential or linear attacks. It is the main result of this paper that the upper bound of r-round ($r \geq 15$) differential(or linear hull) probabilities are bounded by p^4 if the maximum differential (or linear hull) probability of a round function is p, and an impossible differential of this structure does not exist if $r \geq 16$. Application of this structure which can be seen as a generalized Feistel structure in a way to block cipher designs brings out the provable security against differential and linear attacks with some upper bounds of probabilities. We also propose an interesting conjecture.

1 Introduction

The most powerful known attacks on block ciphers are Differential Cryptanalysis(DC) [2,3] and Linear Cryptanalysis(LC) [10,11]. Since such cryptanalyses have been proposed, designers of block ciphers have tried to give the provable security against DC and LC. Kanda et al [7] classified four measures to evaluate the security of a cipher against DC and LC as follows;

1. Precise measure : The maximum average of differential and linear hull probabilities.
2. Theoretical measure : The upper bounds of the maximum average of differential and linear hull probabilities.
3. Heuristic measure : The maximum average of differential characteristic and linear approximation probabilities.
4. Practical measure : The upper bounds of the maximum average of differential characteristic and linear approximation probabilities.

Among the above four measures, the first two are the measures of the theoretical point of view and the last two are the measures of the practical point of

T. Okamoto (Ed.): ASIACRYPT 2000, LNCS 1976, pp. 274–288, 2000.

view. If the number of rounds increases, it is computationally infeasible to compute exactly with the point of the precise and heuristic measures. Therefore the theoretical and practical measures are important measures to show the security of a cipher against DC and LC. However the practical measure does not give a sufficient condition for the security of a cipher against DC and LC. It is only a necessary condition, so the theoretical measure is the only left one to give the provable security against DC and LC.

K.Nyberg and R.Knudsen showed that the r-round differential(or linear hull) probabilities in the Feistel structure are bounded by $2p^2$ if the maximal differential(or linear hull) probability of round function is p and $r \geq 4$ [16]. Furthermore, the probability can be reduced to p^2 if the round function is bijective and $r \geq 3$ [1]. So the construction of a round function with a small maximal probability of differentials(linear hull) is a very important factor to give the provable structure against DC(LC). M.Matsui gave an example of such a construction using the iterative nested Feistel structures [12,13].

In this paper we will prove the security of an iterated cipher which follows the rule A of Skipjack structure against DC and LC. The r-round($r \geq 15$) differential probabilities are bounded by p^4 if the maximal differential probability of the round function is p. Since the proof of linear hull probabilities in LC is almost same as that of differential probabilities [12,16,17], we will just prove the upper bound of differential probabilities of the structure. Furthermore we will show that there does not exists an impossible differential if $r \geq 16$ in the generalized Feistel structure and Skipjack-like structure. Also we give some conjectures in the generalized Feistel and Skipjack-like structures.

2 Preliminaries

Differential cryptanalysis uses the non-uniformity of the output differences given input differences and linear cryptanalysis relies on the correlations of input/ouput bits and key bits. Block ciphers are usually constructed iteratively with the same round function. So in order to avoid DC and LC it needs to use the round functions which have the good properties against such attacks with sufficient rounds.

In this section we consider a round function F: $GF(2)^n \rightarrow GF(2)^n$. We assume that round keys are independent and uniformly random. Furthermore, input data are also independent and uniformly random.

Definition 1. *[12] For any given $\Delta X, \Delta Y, \Gamma X, \Gamma Y \in GF(2)^n$, the differential and linear hull probabilities of a round function F are defined as;*

$$DP^F(\Delta X \rightarrow \Delta Y) = \frac{\#\{x \in GF(2)^n \mid F(X) \oplus F(X \oplus \Delta X) = \Delta Y\}}{2^n}$$

$$LP^F(\Gamma X \rightarrow \Gamma Y) = \left(\frac{\#\{x \in GF(2)^n \mid \Gamma X \bullet X = \Gamma Y \bullet F(Y)\}}{2^{n-1}} - 1 \right)^2$$

where $\Gamma x \bullet \Gamma y$ denotes the parity of bitwise exclusive-or of Γx and Γy.

In the above definitions the probabilities mean the average probabilities for all the possible keys. To give the provable security against DC and LC with the theoretical measure we need the following definitions.

Definition 2. *The maximal differential and linear hull probability of F are defined by*

$$DP^F_{max} = \max_{\Delta x \neq 0, \Delta y} DP^F(\Delta x \to \Delta y)$$

and

$$LP^F_{max} = \max_{\Gamma x, \Gamma y \neq 0} LP^F(\Gamma x \to \Gamma y)$$

respectively.

On the point of view of the provable security DP^F_{max}, LP^F_{max} are the very important factors. With above two definitions, we can easily get the following two theorems.

Theorem 1. *[12] (i) For any function F,*

$$\sum_{\Delta Y} DP^F(\Delta X \to \Delta Y) = 1, \ \sum_{\Gamma X} LP^F(\Gamma X \to \Gamma Y) = 1.$$

(ii) For any bijective function F,

$$\sum_{\Delta X} DP^F(\Delta X \to \Delta Y) = 1, \ \sum_{\Gamma Y} LP^F(\Gamma X \to \Gamma Y) = 1.$$

If F_1 and F_2 which are functions from $GF(2)^n$ to $GF(2)^n$ are used as consecutive round functions and relatively independent, we can calculate differential and linear hull probabilities with the following theorem.

Theorem 2. *[12] For any $\Delta X, \Delta Z, \Gamma X, \Gamma Z \in GF(2)^n$,*

$$DP^{F_1,F_2}(\Delta X \to \Delta Z) = \sum_{\Delta Y} DP^{F_1}(\Delta X \to \Delta Y) \cdot DP^{F_2}(\Delta Y \to \Delta Z)$$

and

$$LP^{F_1,F_2}(\Gamma X \to \Gamma Z) = \sum_{\Gamma Y} LP^{F_1}(\Gamma X \to \Gamma Y) \cdot LP^{F_2}(\Gamma Y \to \Gamma Z).$$

Since the method of calculating linear hull probabilities can be calculated with the reverse order of the method of calculating differential probabilities [12,16,17], we will only consider the differential probabilities in this paper.

3 Provable Security for Block Cipher Structures against DC and LC

Structures of block ciphers can be roughly classified by the Feistel structure and the SPN structure. Since there has been much progress in the structures of

bijective functions with good properties, the interest in the SPN structure has been increased. There are Square [5], Riindael [6], and Crypton [8] which are constructed by considering the branch number [18] in the SPN structure from the practical point of view. However the Feistel structure has been used more widely since it has no limit of round function. In this section we consider the security of the Feistel structure and its modifying structure against DC and LC. We assume that the round keys of round function F are mutually independent and uniformly distributed and the maximal differential probability of the round function F, DP^F_{max}, is p.

K.Nyberg and R.Knudsen showed that the r-round differential(or linear hull) probabilities in the Feistel structure are bounded by $2p^2$ if the maximal differential(or linear hull) probability of round function is p and $r \geq 4$ in Feistel structure. Furthermore, the probability can be reduced to p^2 if the round function is bijective and $r \geq 3$. So the smaller probability p is, the better security level against DC and LC we can give. For example, consider the Feistel structure block cipher which has bijective round function $F : GF(2)^{32} \rightarrow GF(2)^{32}$ with more than or equal to 3 round. If the maximal differential probability is close to 2^{-32}, then the upper bound of differential of the cipher is close to 2^{-64}. So we can give the almost perfect security against DC. M.Matsui gave the example of such a construction using the iterated nested Feistel structures [12,13].

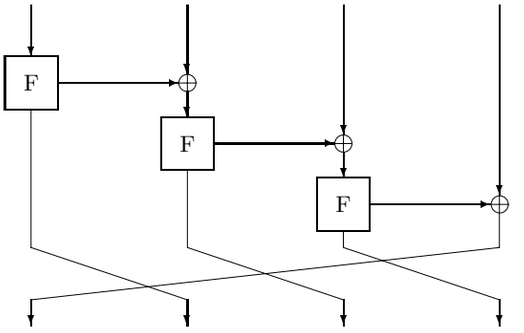

Fig. 1. Skipjack-like structure

Since AES(Advanced Encryption Standard) have been proposed, the 128-bit block ciphers are usually adopted. If we construct 128-bit block ciphers with the Feistel structure, we need to design 64-bit round function. However, to construct 64-bit round function are usually more difficult than to design 32-bit round function and it is also a hard problem to give the provable security against DC and LC. So the generalized Feistel structure which divides input blocks by 4 was proposed and used in MARS, RC6, TWOFISH, and etc. We also have Skipjack [19] which is the 64-bit block cipher with the generalized Feistel

structure dividing input blocks by 4 and it has 32 rounds where half of them are ruled by A type and the others by B type. Fig. 1 describe the structure of iterated ciphers using the rule A of Skipjack. Since the output block of a round function F has effects on the next block and its own block, Skipjack-like structure is different to the generalized Feistel structure and data randomization is faster than the generalized Feistel structure. However the Skipjack-like structure needs a bijective round function. In the next section we will prove the upper bound of differential probabilities of the Skipjack-like structure as in the Feistel structure case.

4 The Main Result - Provable Security against DC and LC in the Skipjack-like Structure

In this section we prove the upper bound of differential probabilities in the iterated Skipjack-like structure from the theoretical point of view. We assume that a round function F is bijective and the maximal differential of F is p.

Now we consider the 15-round Skipjack-like iterated block cipher. In Fig. 2 the α_i's mean the input block differences, β_i's mean the output block differences and δ_i's are variables which mean i-th round output differences. Set an input difference to $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and an output difference $\beta = (\beta_1, \beta_2, \beta_3, \beta_4)$. By the assumption that a round function is bijective we just consider $\alpha \neq 0$ and $\beta \neq 0$. Therefore for the given nonzero input difference α the probability that an output difference is β is calculated as following. We denote the 15-round differential probability as $DP(\alpha \rightarrow \beta)$ and $DP^F(\Delta X \rightarrow \Delta Y)$ as $DP(\Delta X \rightarrow \Delta Y)$.

$$\begin{aligned} DP(\alpha \rightarrow \beta) \;=\; & \sum_{\delta_i, 1 \le i \le 11} DP(\alpha_1 \rightarrow \delta_1) \cdot DP(\alpha_2 \oplus \delta_1 \rightarrow \delta_2) \cdot DP(\alpha_3 \oplus \delta_2 \rightarrow \delta_3) \\ & \cdot DP(\alpha_4 \oplus \delta_3 \rightarrow \delta_4) \cdot DP(\delta_1 \oplus \delta_4 \rightarrow \delta_5) \cdot DP(\delta_2 \oplus \delta_5 \rightarrow \delta_6) \\ & \cdot DP(\delta_3 \oplus \delta_6 \rightarrow \delta_7) \cdot DP(\delta_4 \oplus \delta_7 \rightarrow \delta_8) \cdot DP(\delta_5 \oplus \delta_8 \rightarrow \delta_9) \\ & \cdot DP(\delta_6 \oplus \delta_9 \rightarrow \delta_{10}) \cdot DP(\delta_7 \oplus \delta_{10} \rightarrow \delta_{11}) \cdot DP(\delta_8 \oplus \delta_{11} \rightarrow \beta_3 \oplus \beta_4) \\ & \cdot DP(\delta_9 \oplus \beta_3 \oplus \beta_4 \rightarrow \beta_1) \cdot DP(\delta_{10} \oplus \beta_1 \rightarrow \beta_2) \cdot DP(\delta_{11} \oplus \beta_2 \rightarrow \beta_3) \end{aligned} \tag{1}$$

Using the equation(1) we prove the following main theorem.

Theorem 3. *If a round function of the Skipjack-like structure is bijective and $r \geq 15$, then r-round differential probabilities are bounded by p^4 where p is the maximal average differential probability of a round function.*

Proof. We prove the case r=15. If r is greater than 15, we can easily prove by the case r=15 and the Theorem 1,2. We will prove the theorem case by case and the cases are classified by 8, i.e. , the β_i's $(1 \leq i \leq 3)$ are zero or not.

Case 1($\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$)
Since we do not consider the case $\beta \neq 0$, β_4 is nonzero. By the case assumption, we have $\delta_7 = \delta_{10} = \delta_{11} = 0$ and $\delta_3 = \delta_6 = \delta_9 = \beta_4 \neq 0$. Therefore $\delta_3, \delta_6, \delta_7, \delta_9, \delta_{10}, \delta_{11}$ is fixed and variable $t = \{\delta_1, \delta_2, \delta_4, \delta_5, \delta_8\}$ will be only summed over in equation (1). So we have the following;

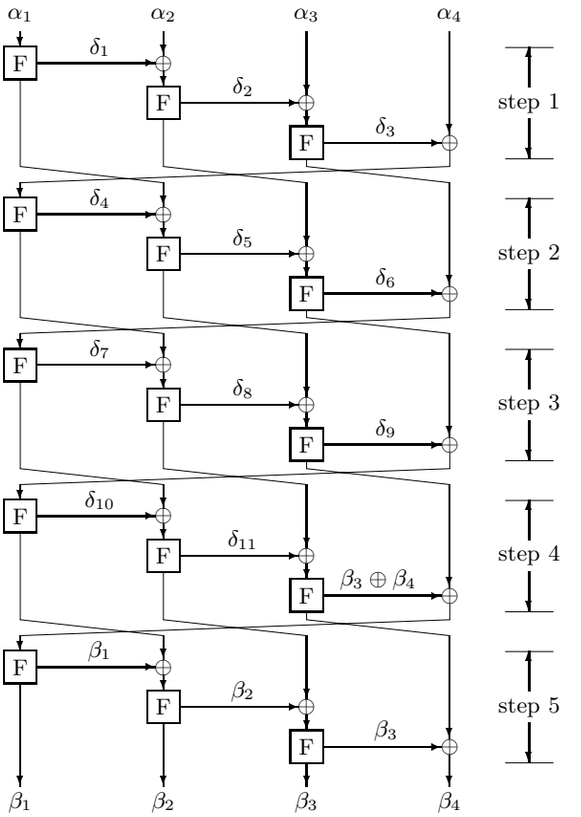

Fig. 2. Notations of 15-round differential

Table 1. Notations of Proof

Relations			
Variable t			
step 1	$DP(\alpha_1 \rightarrow \delta_1)$	$DP(\alpha_2 \oplus \delta_1 \rightarrow \delta_2)$	$DP(\alpha_3 \oplus \delta_2 \rightarrow \delta_3)$
step 2	$DP(\alpha_4 \oplus \delta_3 \rightarrow \delta_4)$	$DP(\delta_1 \oplus \delta_4 \rightarrow \delta_5)$	$DP(\delta_2 \oplus \delta_5 \rightarrow \delta_6)$
step 3	$DP(\delta_3 \oplus \delta_6 \rightarrow \delta_7)$	$DP(\delta_4 \oplus \delta_7 \rightarrow \delta_8)$	$DP(\delta_5 \oplus \delta_8 \rightarrow \delta_9)$
step 4	$DP(\delta_6 \oplus \delta_9 \rightarrow \delta_{10})$	$DP(\delta_7 \oplus \delta_{10} \rightarrow \delta_{11})$	$DP(\delta_8 \oplus \delta_{11} \rightarrow \beta_3 \oplus \beta_4)$
step 5	$DP(\delta_9 \oplus \beta_3 \oplus \beta_4 \rightarrow \beta_1)$	$DP(\delta_{10} \oplus \beta_1 \rightarrow \beta_2)$	$DP(\delta_{11} \oplus \beta_2 \rightarrow \beta_3)$

$$DP(\alpha \to \beta) = \sum_t DP(\alpha_1 \to \delta_1) \cdot DP(\alpha_2 \oplus \delta_1 \to \delta_2) \cdot DP(\alpha_3 \oplus \delta_2 \to \delta_3)$$
$$\cdot DP(\alpha_4 \oplus \beta_3 \to \delta_4) \cdot DP(\delta_1 \oplus \delta_4 \to \delta_5) \cdot DP(\delta_2 \oplus \delta_5 \to \beta_4)$$
$$\cdot DP(\delta_4 \to \beta_4) \cdot DP(\delta_5 \oplus \delta_8 \to \beta_4) \cdot DP(\delta_8 \to \beta_4)$$

Among the above equation $DP(\alpha_3 \oplus \delta_2 \to \delta_3), DP(\delta_2 \oplus \delta_5 \to \beta_4), DP(\delta_5 \oplus \delta_8 \to \beta_4)$ and $DP(\delta_8 \to \beta_4)$ are bounded by p since the output differences are nonzero and F is bijective. So we have

$$DP(\alpha \to \beta) \leq p^4 \cdot \sum_t DP(\alpha_1 \to \delta_1) \cdot DP(\alpha_2 \oplus \delta_1 \to \delta_2) \cdot DP(\alpha_4 \oplus \beta_3 \to \delta_4)$$
$$\cdot DP(\delta_1 \oplus \delta_4 \to \delta_5) \cdot DP(\delta_4 \to \beta_4) \leq p^4.$$

From now on we will use the table such as Table 1. In the Table 1 relations mean the relations of variable α_i's,β_i's and δ_i's. Therefore the variables of the relations in the table relations are fixed and variables$(= t)$ are only summed over in the equation (1). Using the notations of Table 1 we can represent the proof of Case 1 by the following table.

Table 2. Proof of Case 1 : $\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$

Relations	$\delta_7 = \delta_{10} = \delta_{11} = 0,\ \delta_3 = \delta_6 = \delta_9 = \beta_4 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_4, \delta_5, \delta_8$		
step 1	sum over δ_1	sum over δ_2	$\leq p$
step 2	sum over δ_4	sum over δ_5	$\leq p$
step 3	1	sum over δ_8	$\leq p$
step 4	1	1	$\leq p$
step 5	1	1	1

Case 2($\beta_1 = 0, \beta_2 = 0, \beta_3 \neq 0$)
We divide Case 2 by 2 cases whether $\beta_3 \oplus \beta_4$ is zero or not. In the Case 2-1 $DP(\alpha \to \beta)$ is bounded by p^5 and in the Case 2-2 $DP(\alpha \to \beta)$ is bounded by p^4.

Proofs of other cases can be proved in the similar way. More details are in the Appendix. All the cases $DP(\alpha \to \beta)$ is bounded by p^4.

Since the Skipjack-like structure can be regarded as one of the generalizations of the Feistel structure in a way, provable security against LC is also obtained as in [12,16,17].

Theorem 4. *If a round function of the Skipjack-like structure is bijective and $r \geq 15$, then r-round linear hull probabilities are bounded by q^4 where q is the maximal average linear hull probability of a round function.*

Table 3. Proof of Case 2-1 : $\beta_1 = 0, \beta_2 = 0, \beta_3 \neq 0, \beta_3 \oplus \beta_4 = 0$

Relations	$\delta_6 = \delta_9 = \delta_{10} = 0,\ \delta_2 = \delta_5 = \delta_7 = \delta_{11}$		
Variable t	$\delta_1, \delta_3 \neq 0, \delta_4, \delta_{11} \neq 0$		
step 1	sum over δ_1	$\leq p$	sum over δ_3
step 2	sum over δ_4	$\leq p$	1
step 3	$\leq p$	$\leq p$	1
step 4	1	$\leq p$	1
step 5	1	1	sum over δ_{11}

Table 4. Proof of Case 2-2 : $\beta_1 = 0, \beta_2 = 0, \beta_3 \neq 0, \beta_3 \oplus \beta_4 \neq 0$

Relations	$\delta_{10} = 0,\ \delta_6 = \delta_9 = \beta_3 \oplus \beta_4$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_7 \neq 0, \delta_8, \delta_{11} \neq 0$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	$\leq p$
step 3	$\leq p$	sum over δ_7	sum over δ_8
step 4	1	$\leq p$	$\leq p$
step 5	1	1	sum over δ_{11}

Now, let's consider one of the generalization of the Feistel structure as Fig. 3.

Assume that the round function is bijective. In the case $m = 2$ (the Feistel structure), if $r \geq 3 = 1 \cdot 3$, then r-round differential probabilities are bounded by p^2. In the case $m = 3$, S.Sung [21] proved that r-round differential probabilities are bounded by p^3 if $r \geq 8 = 2 \cdot 4$. Also in the case $m = 4$, r-round differential probabilities are bounded by p^4 if $r \geq 15 = 3 \cdot 5$. So we can conjecture the following.

Conjecture 1. In the generalized Feistel structure and Skipjack-like structure, r-round differential probabilities are bounded by p^m if $r \geq (m-1)(m+1)$.

5 Impossible Truncated Differential of the Generalized Feistel Structure and Skipjack-like Structure

In this section we consider an impossible truncated differential of (i) the generalized Skipjack-like structure whose one-round transformation is $F_k(x_1, x_2, \cdots, x_m) = (f_k(x_1) \oplus x_2, x_3, , \cdots, x_m, f_k(x_1))$, and (ii) the generalized(CAST256-like) Feistel structure whose one-round transformation is $F_k(x_1, x_2, \cdots, x_m) = (f_k(x_1) \oplus x_2, x_3, \cdots, x_m, x_1)$, where $f_k : \{0,1\}^n \to \{0,1\}^n$ is a keyed-round function.

Now we can consider the relation of an impossible truncated differential and a number of round in $(i), (ii)$. We assume that round functions are bijective, random, and pairwise independent. Let $\Delta X = (\Delta X_1, \cdots, \Delta X_m)$ and $\Delta Y =$

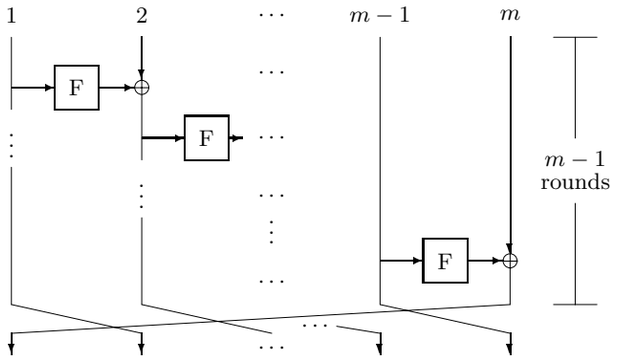

Fig. 3. Generalized Feistel Structure

$(\Delta Y_1, \cdots, \Delta Y_m)$ be an input and output difference respectively. Then we have the following results.

Proposition 1. *If $r = m^2 - 1$, there exist an impossible truncated differential whose form is $(0, 0, \cdots, 0, \Delta\alpha) \nrightarrow (\Delta\beta, 0, \cdots, 0)$ in (i) and (ii), where $\Delta\alpha$ and $\Delta\beta$ are nonzero.*

Note : In the case of $m = 3$, we can find the 8-round impossible truncated differential whose form is $(0, 0, \Delta\alpha) \nrightarrow (\Delta\beta, 0, 0)$ in (ii), where $\Delta\alpha$ and $\Delta\beta$ are nonzero (similarly it holds in (i)). Consider the following figure. Since we assumed that round functions are bijective and $\Delta\alpha$ is nonzero, Δt is nonzero. But the four round output differential is zero. This is the contradiction.

With Proposition 1 and the notion of pseudorandomness in Luby and Rackoff [9], we can conjecture that impossible differentials and the pseudorandomness are closely related. However, the number of queries in the impossible differential attack model are more than that in the distinguishing attack model [14]. Also we can conjecture the followings.

Conjecture 2. If $r \geq m^2$, there does not exist an impossible truncated differential in (i) and (ii).

Conjecture 2 can be proved by a computer programming if m is small enough, say less than 32. A similar method can be seen in [20]. However, since we could not find a general rule of proof, we just do conjecture it in the case that m is large. So we need further works.

We can find the impossible differential whose form is $(0, 0, 0, \Delta\alpha) \nrightarrow (\Delta\beta, 0, 0, 0)$ in the Skipjack-like structure($m = 4$) if $r = 15$. Skipjack is the 64-bit block cipher with 80-bit key and 32-round($A^8B^8A^8B^8$) using rules A and B iteratively. There has been the impossible differential attack [4] which use the weakness of this cipher to apply the rule B only after 8-round of rule A. These attacks only

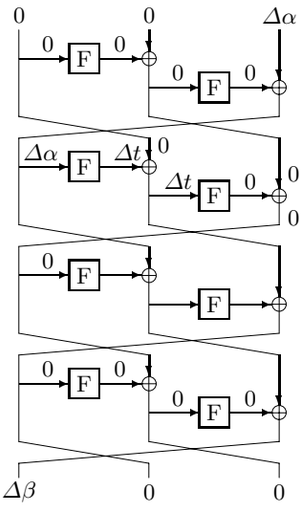

Fig. 4. 8-round impossible truncated differential in the case of $m = 3$

use the structural weakness. However, if Skipjack algorithm use $A^{16}B^{16}$ or A^{32} then the impossible differential attack can not be applied any more by Conjecture 2 in case $m = 4$.

6 Conclusion

In this paper we give the provable security for the Skipjack-like cipher against DC from the theoretical point of view. If the maximal differential of a round function of a Skipjack-like cipher is p and $r \geq 15$, then r-round differential probabilities are bounded by p^4. Also we suggest the conjecture that r-round differential probabilities are bounded by p^m if $r \geq (m-1)(m+1)$ and there does not exists an impossible differential if $r \geq m^2$ in the generalized Feistel structure and Skipjack-like structure.

It seems a hard problem to give the provable security against DC and LC in the block cipher. Until now, there have been no 128-bit block cipher with the provable security against DC and LC from the theoretical point of view. So we believe our result to be very helpful to design provably secure block ciphers against DC and LC.

References

1. K. Aoki and K. Ohta, *Stict evaluation for the maximum average of differential probability and the maximem average of linear probability*, IEICE Transcations fundamentals of Elections, Communications and Computer Sciences, No.1, pp 2-8, 1997.

2. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Advances in Cryptology - CRYPTO'90, LNCS 537, Springer-Verlag, 1991, pp. 2–21.
3. E. Biham and A. Shamir, *Differential cryptanalysis of the full 16-round DES*, Advances in Cryptology - CRYPTO'92, LNCS 740, Springer-Verlag, 1992, pp. 487–496.
4. E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials*, Advances in Cryptology - EUROCRYPT'99, LNCS 1592, Springer-Verlag, 1992, pp. 12–23.
5. J. Daemen, Lars R.Knudsen, and Vincent Rijmen. *The block cipher SQUARE*, Fast Software Encryption Workshop 97, 1997, pp 137–151.
6. J. Daemen and V. Rijndael, *The Rijndael block cipher*, AES proposal, 1998.
7. M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta, *A strategy for constructing fast functions with practical security against differential and linear cryptanalysis*, Selected Areas in Cryptography, LNCS 1556, 1999, pp 264–279.
8. C.H. Lim, *CRYPTON: A new 128-bit block cipher*, AES proposal, 1998.
9. M. Luby and C. Rackoff, *How to construct pseudorandom permutations from pseudorandom functions*, SIAM J.Comput., vol. 17, pp.373-386, 1988.
10. M. Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology - EUROCRYPT'93, LNCS 765, Springer-Verlag, 1994, pp. 386–397.
11. M. Matsui, *The first experimental cryptanalysis of the Data Encryption Standard*, Advances in Cryptology - CRYPTO'94, LNCS 839, Springer-Verlag, 1994, pp. 1–11.
12. M. Matsui, *New structure of block ciphers with provable security against differential and linear cryptanalysis*, Fast Software Encryption Workshop 96, 1996, pp. 205–218.
13. M. Matsui, *New Block Encryption Algorithm MISTY*, Fast Software Encryption Workshop 97, 1997.
14. Shiho Moriai and Serge Vaudenay, *Comparision of Randomness Provided by Several Schemes for Block Ciphers*, Presented at Third AES Workshop, April 2000.
15. M. Naor and O. Reingold, *On the construction of pseudorandom permutations : Luby-Rackoff Revisited*, J.Cryptology, pp.29-66, 1999.
16. K. Nyberg and Lars R. Knudsen, *Provable security against differential cryptanalysis*, Advances in Cryptology - CRYPTO'92, LNCS 740, Springer-Verlag, 1992, pp. 566–574.
17. K. Nyberg, *Linear approximation of block ciphers*, Presented at rump session, Eurocrypt'94, May 1994.
18. Vincent Rijmen, J. Daemen, Bart Preneel, Antoon Bosselaers, and Erik De Win, *The cipher SHARK*, Fast Software Encryption Workshop 96, 1996, pp. 99–112.
19. *Skipjack and KEA Algorithm Specifications, version 2.0*, Technical report, Available at the National Institute of Standard and Technology web page, http://crsc.nist.gov/encryption/skipjack-kea.htm, May 1998.
20. M. Sugita, K Kobara, K. Uehara, S. Kubota, and H. Imai, *Relations among Differential, Truncated Differential, Impossible Differential Cryptanalyses against Word-Oriented Block Ciphers like Rijndael, E2*, Presented at Third AES Workshop, April 2000.
21. Suhak Sung, Private Communications, 1999.

Appendix: Proof of Theorem 3

Table 5. Proof of Case 3-1 : $\beta_1 = 0, \beta_2 \neq 0, \beta_3 = 0, \beta_4 = 0$

Relations	$\delta_9 = 0,\ \delta_5 = \delta_8 = \delta_{11} = \beta_2 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_6, \delta_7, \delta_{10}$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	$\leq p$	sum over δ_6
step 3	sum over δ_7	$\leq p$	1
step 4	sum over δ_{10}	$\leq p$	1
step 5	1	$\leq p$	1

Table 6. Proof of Case 3-2 : $\beta_1 = 0, \beta_2 \neq 0, \beta_3 = 0, \beta_4 \neq 0$

Relations	$\delta_9 = \beta_4 \neq 0,\ \delta_{11} = \beta_2 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_{10}$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	sum over δ_6
step 3	sum over δ_7	sum over δ_8	$\leq p$
step 4	$\leq p$	sum over δ_{10}	$\leq p$
step 5	1	$\leq p$	1

Table 7. Proof of Case 4-1 : $\beta_1 \neq 0, \beta_2 = 0, \beta_3 = 0, \beta_4 = 0$

Relations	$\delta_8 = \delta_{11} = 0,\ \delta_4 = \delta_7 = \delta_{10} = \beta_1 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_5, \delta_6, \delta_9$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	$\leq p$	sum over δ_5	sum over δ_6
step 3	$\leq p$	1	sum over δ_9
step 4	$\leq p$	1	1
step 5	$\leq p$	1	1

Table 8. Proof of Case 4-2 : $\beta_1 \neq 0, \beta_2 = 0, \beta_3 = 0, \beta_4 \neq 0$

Relations	$\delta_{11} = 0,\ \delta_7 = \delta_{10} = \beta_1 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_8, \delta_9,$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	sum over δ_6
step 3	$\leq p$	sum over δ_8	sum over δ_9
step 4	$\leq p$	1	$\leq p$
step 5	$\leq p$	1	1

Table 9. Proof of Case 5-1 : $\beta_1 \neq 0, \beta_2 \neq 0, \beta_3 = 0, \beta_4 = 0$

Relations	$\delta_8 = \delta_{11} = \beta_2 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_9 \neq 0, \delta_{10}$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	sum over δ_6
step 3	sum over δ_7	$\leq p$	$\leq p$
step 4	sum over δ_{10}	$\leq p$	1
step 5	sum over δ_9	$\leq p$	1

Table 10. Proof of Case 5-2 : $\beta_1 \neq 0, \beta_2 \neq 0, \beta_3 = 0, \beta_4 \neq 0$

Relations	$\delta_{11} = \beta_2 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{10}$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	sum over δ_6
step 3	sum over δ_7	sum over δ_8	sum over δ_9
step 4	sum over δ_{10}	$\leq p$	$\leq p$
step 5	$\leq p$	$\leq p$	1

Table 11. Proof of Case 6 : $\beta_1 \neq 0, \beta_2 = 0, \beta_3 \neq 0$

Relations	$\delta_{10} = \beta_1 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{11}$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	sum over δ_6
step 3	sum over δ_7	sum over δ_8	sum over δ_9
step 4	$\leq p$	$\leq p$	sum over δ_{11}
step 5	$\leq p$	1	$\leq p$

Table 12. Proof of Case 7-1 : $\beta_1 = 0, \beta_2 \neq 0, \beta_3 \neq 0, \beta_3 \oplus \beta_4 = 0$

Relations	$\delta_9 = 0,\ \delta_5 = \delta_8 = \delta_{11}$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_6 \neq 0, \delta_7, \delta_{10}, \delta_{11} \neq 0$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	$\leq p$	$\leq p$
step 3	sum over δ_6	sum over δ_7	1
step 4	$\leq p$	sum over δ_{10}	1
step 5	1	$\leq p$	sum over δ_{11}

Table 13. Proof of Case 7-2 : $\beta_1 = 0, \beta_2 \neq 0, \beta_3 \neq 0, \beta_3 \oplus \beta_4 \neq 0$

Relations	$\delta_9 = \beta_3 \oplus \beta_4 \neq 0$		
Variable t	$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_{10}, \delta_{11}$		
step 1	sum over δ_1	sum over δ_2	sum over δ_3
step 2	sum over δ_4	sum over δ_5	sum over δ_6
step 3	sum over δ_7	sum over δ_8	$\leq p$
step 4	sum over δ_{10}	sum over δ_{11}	$\leq p$
step 5	1	$\leq p$	$\leq p$

Table 14. Proof of Case 8-1 : $\beta_1 \neq 0, \beta_2 \neq 0, \beta_3 \neq 0, \alpha_1 \neq 0$

Relations			
Variable t	$\delta_1 \neq 0, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{10}, \delta_{11}$		
step 1	$\leq p$	sum over δ_1	sum over δ_2
step 2	sum over δ_3	sum over δ_4	sum over δ_5
step 3	sum over δ_6	sum over δ_7	sum over δ_8
step 4	sum over δ_9	sum over δ_{10}	sum over δ_{11}
step 5	$\leq p$	$\leq p$	$\leq p$

Table 15. Proof of Case 8-2 : $\beta_1 \neq 0, \beta_2 \neq 0, \beta_3 \neq 0, \alpha_1 = 0, \alpha_2 \neq 0$

Relations	$\delta_1 = 0$		
Variable t	$\delta_2 \neq 0, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{10}, \delta_{11}$		
step 1	1	$\leq p$	sum over δ_2
step 2	sum over δ_3	sum over δ_4	sum over δ_5
step 3	sum over δ_6	sum over δ_7	sum over δ_8
step 4	sum over δ_9	sum over δ_{10}	sum over δ_{11}
step 5	$\leq p$	$\leq p$	$\leq p$

Table 16. Proof of Case 8-3 : $\beta_1 \neq 0, \beta_2 \neq 0, \beta_3 \neq 0, \alpha_1 = 0, \alpha_2 = 0, \alpha_3 \neq 0$

Relations	$\delta_1 = \delta_2 = 0$		
Variable t	$\delta_3 \neq 0, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{10}, \delta_{11}$		
step 1	1	1	$\leq p$
step 2	sum over δ_3	sum over δ_4	sum over δ_5
step 3	sum over δ_6	sum over δ_7	sum over δ_8
step 4	sum over δ_9	sum over δ_{10}	sum over δ_{11}
step 5	$\leq p$	$\leq p$	$\leq p$

Table 17. Proof of Case 8-4 : $\beta_1 \neq 0, \beta_2 \neq 0, \beta_3 \neq 0, \alpha_1 = 0, \alpha_2 = 0, \alpha_3 = 0, \alpha_4 \neq 0$

Relations	$\delta_1 = \delta_2 = \delta_3 = 0$		
Variable t	$\delta_4 \neq 0, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{10}, \delta_{11}$		
step 1	1	1	1
step 2	$\leq p$	sum over δ_4	sum over δ_5
step 3	sum over δ_6	sum over δ_7	sum over δ_8
step 4	sum over δ_9	sum over δ_{10}	sum over δ_{11}
step 5	$\leq p$	$\leq p$	$\leq p$