通信情報保護學會論文誌
第 10 券 第 1 號, 2000. 3

Skipjack 구조에 대한 DC 및 LC의 안전성 증명*

성 재 철**, 이 상 진***, 김 종 수**, 임 종 인***

Provable Security for the Skipjack-like Structure

Jaechul Sung**, Sangjin Lee***, Jongsu Kim**, Jongin Lim***

요 약

본 논문에서는 Skipjack의 변환규칙 A와 같은 반복적인 구조에 대한 차분 특성 및 선형 근사식의 확률의 상한 값을 제시하고 이를 증명한다. 즉 라운드 함수에 대한 확률의 최대 값이 p이면 15라운드 후에 p^4이 됨을 보인다. 따라서 본 논문에서 고려한 구조는 현재까지 DC 및 LC에 대한 안전성을 증명할 수 있는 구조인 Feistel 구조 및 MISTY 구조와 더불어 블록 암호의 설계 방법에 대한 다양성을 제공한다.

ABSTRACT

In this paper we introduce a structure of block cipher which is an iterated cipher by the rule A of Skipjack and show 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) is p^4 if the maximum differential(or linear approximation) probability of a round function is p. We can consider this structure as a generalized Feistel structure. Therefore we can apply this structure to block ciphers and give the provable security against differential attack or linear attack with some upper bounds.

keyword : *differential cryptanalysis, linear cryptanalysis*

Ⅰ. 서 론

블록 암호 분석의 가장 대표적인 방법으로 DC (Differential Cryptanalysis)와 LC(Linear Cryptanalysis)가 있다.[2,5] 이 DC와 LC가 발표된 이후 이들 공격에 대한 안전성이 많이 연구되었다. DC와 LC의 안전성의 측도로, Kanda 등[4]은 DC의 characteristic과 differential, LC의 linear approximation과 linear hull 관점에서 다음의 4가지의 분석 측도를 제시하였다.

(1) Precise 측도 : differential과 linear hull 관점에서의 최대 확률 값
(2) Theoretical 측도 : differential과 linear hull 관점에서의 확률의 상한 값
(3) Heuristic 측도 : characteristic과 linear approximation 관점에서의 최대 확률 값
(4) Practical 측도 : characteristic과 linear approximation 관점에서의 확률의 상한 값

위의 4가지의 측도 중 (1)과 (2)는 이론적인 측면에서의 측도를 나타내는 값이고 (3)과 (4)는 실질적인 공격 측면에서의 측도를 나타내는 값이다. 실질적인 공격을 적용할 때에는 (1)과 (3)이 사용되지만

* 본 논문은 고려대학교 특별연구비를 지원받아 연구되었음.
** 고려대학교 정보보호기술연구소(sjames@gauss.korea.ac.kr),
*** 고려대학교 자연과학대학 교수(sangjin@tiger.korea.ac.kr)

라운드 수가 증가하면 조사해야 하는 비트 수가 기하급수적으로 증가하므로 대부분의 경우 정확한 계산이 용이하지 않으며, 계산 가능한 범위로 축소하여 최대 값을 찾는다. 따라서 (2)와 (4)가 DC와 LC에 대한 안전성을 평가할 때 중요한 측도가 된다. 그러나 (4)는 characteristic과 linear approximation의 확률의 상한 값을 나타내므로 엄밀한 의미에서는 이 값이 작다고 해서 DC나 LC에 강함을 나타내지는 못한다. 반면 (2)의 Theoretical 측도에서 differential과 linear hull에 대한 확률의 상한 값을 얻을 수 있다면 DC나 LC에 대한 안전성을 증명할 수 있다.

Nyberg와 Knudsen은 Theoretical 측도로 DC에 대한 안전성을 증명할 수 있는 구조인 4라운드 Feistel 구조를 제시하였다. 즉, Feistel 구조에서 라운드 함수에 대한 최대 차분 확률의 상한이 p이면 4라운드 후에는 $2p^2$이 되고 라운드 함수가 전단사 함수이면 3라운드 후에 $2p^2$이 됨을 증명하였다.[8] Aoki 등[1]은 이를 개선하여 라운드 함수가 전단사 함수이면 3라운드 후에 p^2이 됨을 증명하였다. 최대 차분 확률이 큰 라운드 함수를 설계하는 것은 어려운 문제인데, Matsui 등은 라운드 함수를 반복적인 Feistel 구조에 적용함으로써 이러한 난관을 효과적으로 극복하였고 안전성이 증명 가능한 새로운 형태인 MISTY 구조를 제안하였다.[6,7]

본 논문에서는 Skipjack 구조도 Theoretical 측면에서 안전성이 증명 가능한 구조로 라운드 함수의 차분 확률의 상한이 p이면 5라운드(1라운드는 3개의 라운드 함수가 작용) 후에 p^4이 됨을 보인다. 그런데 DC에서의 differential에 대한 상한 값의 증명과 linear hull에 대한 증명은 유사한 방법[6,8,9]으로 이루어지므로 본 논문에서 증명한 DC 측면에서의 안전성은 LC 측면에서의 안전성에도 동일하게 적용된다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 본 논문의 주 정리에 필요한 몇 가지의 기본 정의 및 정리에 대해 알아보고 3장에서는 일반적인 블록 암호의 구조와 Skipjack의 변환규칙 A를 이용한 구조에 대하여 알아본다.[10] 4장은 본 논문의 핵심으로 3장에서 제기된 구조에 대한 안전성을 증명한다. 그리고 이 구조를 일반화시켰을 때의 differential에 대한 확률의 상한 값에 대한 conjecture를 제시한다. 마지막으로 5장은 결론 부로 향후의 연구 과제에 대해 알아본다.

II. DC/LC에 대한 증명 가능한 안전성

DC는 두 개(한 쌍)의 입력 차분(difference)에 대한 출력 차분의 비균일성을 이용하는 분석 기법이고 LC는 특정 출력 비트들의 선형 결합과 특정한 입력 비트들 및 특정 키 비트들의 선형 결합의 연관성을 이용하는 분석 기법이다.

블록 암호는 보통의 경우 특정한 라운드 함수를 반복적으로 적용하여 설계된다. 따라서 DC나 LC에 강하기 위해서는 좋은 라운드 함수를 사용하여 라운드의 수를 필요한 만큼 반복시키는 과정이 필요하다.

본 장에서는 블록 암호에 기본이 되는 라운드 함수 $F: GF(2)^n \rightarrow GF(2)^n$에 대한 differential과 linear hull에 대한 기본적인 확률의 성질에 대해 알아본다.

정의 1.

임의의 평문 쌍 $X, X^* \in GF(2)^n$에 대해 입력 차분을 $\Delta X = X \oplus X^*$ 라하고 출력 차분을 $\Delta Y = F(X) \oplus F(X')$로 정의한다. 또한 임의의 평문 X에 대해 ΓX를 입력 마스크라고 하고 출력 $Y = F(X)$에 대해 ΓY를 출력 마스크라 한다.

정의 2.

임의의 $\Delta X, \Delta Y, \Gamma X, \Gamma Y \in GF(2)^n$에 대해 라운드 함수 F에 대한 difference 확률(DP)과 linear hull의 확률(LP)을 다음과 같이 정의한다.

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

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

위의 정의에서 각각의 확률은 가능한 모든 키에 대한 평균값을 의미한다. 입력 차분 ΔX나 출력 마스크 ΓY가 0이 아닌 모든 경우에 대한 확률 값들이 작아야 DC나 LC에 대한 Theoretical 측도에서의 좋은 안전성을 제시할 수 있다.

정의 3.

라운드 함수 F에 대한 최대 차분 확률과 최대 선형 확률을 다음과 같이 정의한다.

$$DP^F_{\max} = \max_{\Delta X \neq 0, \Delta Y} DP^F(\Delta X \rightarrow \Delta Y)$$

$$LP^F_{\max} = \max_{\Gamma X, \Gamma Y \neq 0} LP^F(\Gamma X \rightarrow \Gamma Y)$$

$DP^F_{\max}$, $LP^F_{\max}$는 안전성에 중요한 영향을 미치며 다음과 같은 결과를 쉽게 얻을 수 있다.

정리 1.

(i) 임의의 함수 F에 대해,

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

(ii) 만약 함수 F가 전단사 함수이면,

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

함수 F가 순차적으로 사용되는 경우의 differential과 linear hull의 확률을 구하는 방법에 대하여 알아보자. 두 함수 F_1, F_2가 순차적으로 라운드 함수로 적용되었다고 가정하면 differential과 linear hull의 확률은 다음의 정리를 만족한다.

정리 2.

임의의 $\Delta X, \Delta Z, \Gamma X, \Gamma Z \in GF(2)^n$에 대하여 다음을 만족한다.

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

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

정리 2는 라운드 함수를 이용하여 반복적으로 구성된 블록 암호에서 최대 차분 확률의 상한을 구하는데 중요한 역할을 한다. 그리고 differential에 대한 증명의 방법을 역순으로 적용하면, linear hull의 확률도 증명할 수 있다.[6,7] 따라서 본 논문에서는 differential의 확률에 대해서만 증명한다.

Ⅲ. 블록 암호의 구조와 DC및 LC에 대한 안전성

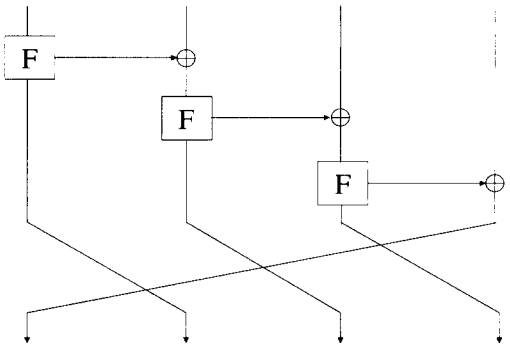
블록 암호의 구조는 크게 DES와 같은 Feistel 구조와 대치와 치환을 반복적으로 사용하는 SPN 구조로 나누어진다. Feistel 구조는 라운드 함수에 대한 특별한 제한이 없어 DES를 비롯한 많은 블록 암호에 광범위하게 사용되었다.

최근에는 안전성이 뛰어난 전단사 함수가 많이 개발되어 SPN 구조로 설계되는 블록 암호도 증가하고 있다. 예를 들면 Safer, Serpent 등이 있으며 Practical 측도 관점에서 branch number를 고려해 설계된 Square, Rijndeal, Crypton 등이 있다.

본 장에서는 Feistel 구조 및 이의 변형 구조의 DC 및 LC에 대한 안전성을 알아본다. 이들 구조에 사용되는 라운드 함수 F의 라운드 키는 독립이라 가정하고, 그 함수의 최대 차분 확률을 $DP^F_{\max} = p$라 정의한다.

Nyberg와 Knudsen[8]은 3라운드 이상의 Feistel 구조에서 차분 확률의 상한 값은 $2p^2$임을 증명하였고 Aoki 등[1]은 만약 F가 전단사 함수이면 그 상한이 p^2임을 증명하였다. 이는 라운드 함수의 차분 확률의 최대 값 p가 작으면 작을 수록 보다 나은 안전성을 제공함을 의미한다. 예를 들어 64비트 Feistel 구조의 블록 암호 알고리즘에서 키가 작용되는 라운드 함수 $F : GF(2)^{32} \rightarrow GF(2)^{32}$ 의 최대 차분 확률 p의 값이 2^{-32}의 값에 근접한다면 전체 알고리즘의 차분 확률의 상한은 2^{-64}에 근접하여 전수조사와 비슷한 복잡성을 가지므로 안전성을 보장할 수 있다. Matsui[6]는 이러한 Feistel 구조의 안전성에 대한 증명을 라운드 함수의 설계에 반복적으로 적용하면 구현이 용이한 블록 암호를 개발할 수 있음을 보였고, 전수조사가 가능한 m 비트 입출력인 S-box를 3번 반복한 2m 비트의 암호논리를 반복적으로 설계하는 형태로 MISTY라는 블록 암호 알고리즘을 개발하였다.[7]

최근에는 AES의 영향으로 128비트 블록 암호가 선호되고 있는데 기존의 Feistel 구조로 설계한다면 64비트 입출력의 라운드 함수가 필요하다. 그런데 64비트 입출력의 라운드 함수는 기존의 32비트 입출력의 라운드 함수에 비하여 구성이 어려우며, 차분 특성 확률의 상한을 계산하는 것도 어려운 일이다. 따라서 Feistel 구조와 같이 입력을 두 개로 나누는 방법을 일반화시켜 MARS, RC6, Twofish와 같이 블록을 4개로 나누어 한 라운드를 구성하는 방법이 제안되고 있다. 한편 최근에 공개된 Skipjack 역시 입력이 4개로 나뉘어 구성되었으며, 변환 규칙 A를 일반화된 Feistel 구조로 표시하면 그림 1의 형태로 표현할 수 있다.



〔그림 1〕 Skipjack의 변환규칙 A를 반복적으로 사용한 구조
〔Fig. 1〕 Skipjack-like structure using Rule A of Skipjack

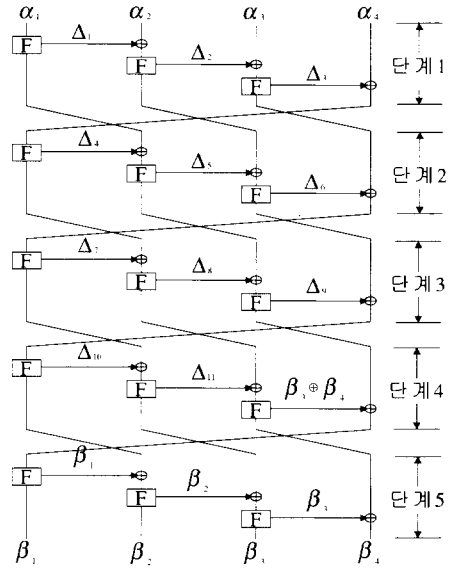
Skipjack의 구조는 기존의 Feistel 구조와 달리 F의 출력 결과가 다른 블록에 영향을 미치면서 동시에 입력 블록을 변화시키기 때문에 데이터의 복잡도를 빠르게 증가시키는 관점에서 좋은 구조라고 할 수 있다. 그러나 복호화 과정에서 F의 역함수가 필요하다는 단점이 있다. 다음장에서는 그림 1과 같은 Skipjack 구조가 Feistel 구조와 마찬가지로 DC에 대한 안전성이 증명될 수 있음을 보인다.

Ⅳ. Skipjack 구조의 대한 DC에 대한 안전성

본 장에서는 앞 장에서 제시한 그림 1의 구조를 반복적으로 사용하는 구조에 대한 Theoretical 측도인 차분 확률의 상한 값을 증명한다. 우선 라운드 함수 F의 최대 차분 확률을 p, F는 전단사 함수라고 가정한다.

그림 2와 같이 F함수를 15번 사용하는 15라운드의 Skipjack 구조를 생각하자. 차분 특성 확률의 상한을 구하기 위해서 그림 2의 각 변수는 두 평문에 대한 차분 혹은 라운드 함수 F에 대한 출력 차분을 의미한다.

위의 15개의 F함수를 사용한 구조에서 입력 차분을 $\alpha=(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$, 출력 차분을 $\beta=(\beta_1,\beta_2,\beta_3,\beta_4)$라 하자. 그리고 가정에 의해서 F가 전단사이므로 입력 차분과 출력 차분은 0이 아닌 경우에 대하여 확률의 상한 값을 알아본다. 따라서 0이 아닌 임의의 입력 차분 α에 대하여 출력 차분이 β일 확률은 다음과 같이 계산된다. 여기에서 $DP(\alpha\rightarrow\beta)$는 15라운드 후의 differential의 확률을 의미한다.



〔그림 2〕 15라운드 Skipjack구조에서의 차분의 기호
〔Fig. 2〕 Notations of 15-round differentials

$$DP(\alpha\rightarrow\beta) = \sum_{\Delta_i,\ 1\le i\le 11} DP(\alpha_1\rightarrow\Delta_1)$$
$$\cdot DP(\alpha_2\oplus\Delta_1\rightarrow\Delta_2)\cdot DP(\alpha_3\oplus\Delta_2\rightarrow\Delta_3)$$
$$\cdot DP(\alpha_4\oplus\Delta_3\rightarrow\Delta_4)\cdot DP(\Delta_1\oplus\Delta_4\rightarrow\Delta_5)$$
$$\cdot DP(\Delta_2\oplus\Delta_5\rightarrow\Delta_6)\cdot DP(\Delta_3\oplus\Delta_6\rightarrow\Delta_7)$$
$$\cdot DP(\Delta_4\oplus\Delta_7\rightarrow\Delta_8)\cdot DP(\Delta_5\oplus\Delta_8\rightarrow\Delta_9)$$
$$\cdot DP(\Delta_6\oplus\Delta_9\rightarrow\Delta_{10})\cdot DP(\Delta_7\oplus\Delta_{10}\rightarrow\Delta_{11})$$
$$\cdot DP(\Delta_8\oplus\Delta_{11}\rightarrow\beta_3\oplus\beta_4)\cdot DP(\Delta_9\oplus\beta_3\oplus\beta_4\rightarrow\beta_1)$$
$$\cdot DP(\Delta_{10}\oplus\beta_1\rightarrow\beta_2)\cdot DP(\Delta_{11}\oplus\beta_2\rightarrow\beta_3) \quad (4.1)$$

식 (4.1)을 이용하여 다음과 같은 정리를 증명한다. 아래에서 r은 F함수가 사용된 횟수를 의미한다.

〔표 1〕 증명의 기호
〔Table 1〕 Notations of proof

관계식			
자유변수 t			
단계 1	$DP(\alpha_1\rightarrow\Delta_1)$	$DP(\alpha_2\oplus\Delta_1\rightarrow\Delta_2)$	$DP(\alpha_3\oplus\Delta_2\rightarrow\Delta_3)$
단계 2	$DP(\alpha_1\oplus\Delta_3\rightarrow\Delta_4)$	$DP(\Delta_1\oplus\Delta_4\rightarrow\Delta_5)$	$DP(\Delta_2\oplus\Delta_5\rightarrow\Delta_6)$
단계 3	$DP(\Delta_3\oplus\Delta_6\rightarrow\Delta_7)$	$DP(\Delta_4\oplus\Delta_7\rightarrow\Delta_8)$	$DP(\Delta_5\oplus\Delta_8\rightarrow\Delta_9)$
단계 4	$DP(\Delta_6\oplus\Delta_9\rightarrow\Delta_{10})$	$DP(\Delta_7\oplus\Delta_{10}\rightarrow\Delta_{11})$	$DP(\Delta_8\oplus\Delta_{11}\rightarrow\beta_3\oplus\beta_4)$
단계 5	$DP(\Delta_9\oplus\beta_3\oplus\beta_4\rightarrow\beta_1)$	$DP(\Delta_{10}\oplus\beta_1\rightarrow\beta_2)$	$DP(\Delta_{11}\oplus\beta_2\rightarrow\beta_3)$

정리 3.

(그림 2)와 같은 구조에서 F가 전단사 함수이고 $r \geq 15$이면 differential의 확률은 p^4보다 작거나 같다 (linear hull에 대해서도 마찬가지로 성립한다).

증명) 이 정리의 증명은 r=15일 때에 대해서만 하면 그 이상에 대해서는 정리 1과 정리 2를 적용하면 자동적으로 성립한다. 증명의 방식은 입력 $\alpha \neq 0$이라는 가정 하에 출력의 차분 $\beta = (\beta_1, \beta_2, \beta_3, \beta_4)$에 대하여 크게 $\beta_1, \beta_2, \beta_3$ 각각이 0인 경우와 아닌 경우, 즉 모두 8가지의 경우에 대하여 증명한다. 각각의 경우도 필요하다면 세부적인 경우로 나누어서 증명한다.

경우 1. ($\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$)

차분이 0인 경우는 고려하지 않으므로 $\beta_4 \neq 0$이다. 이를 이용하여 뒤에서부터 순차적으로 적용하면 $\Delta_7 = 0, \Delta_{10} = 0, \Delta_{11} = 0$이고 $\Delta_3 = \Delta_6 = \Delta_9 = \beta_4 \neq 0$이 되어서 자유변수는 $t = \{\Delta_1, \Delta_2, \Delta_4, \Delta_5, \Delta_8\}$이 된다. 따라서 (4.1)의 확률은 다음과 같다.

$$DP(\alpha \rightarrow \beta) = \sum_t DP(\alpha_1 \rightarrow \Delta_1) \cdot DP(\alpha_2 \oplus \Delta_1 \rightarrow \Delta_2) \cdot DP(\alpha_3 \oplus \Delta_2 \rightarrow \beta_4) \cdot DP(\alpha_4 \oplus \beta_3 \rightarrow \Delta_4) \cdot DP(\Delta_1 \oplus \Delta_4 \rightarrow \Delta_5) \cdot DP(\Delta_2 \oplus \Delta_5 \rightarrow \beta_4) \cdot DP(\Delta_4 \rightarrow \Delta_8) \cdot DP(\Delta_5 \oplus \Delta_8 \rightarrow \beta_4) \cdot DP(\Delta_8 \rightarrow \beta_4)$$

이 중 $DP(\alpha_3 \oplus \Delta_2 \rightarrow \beta_4)$, $DP(\Delta_2 \oplus \Delta_5 \rightarrow \beta_4)$, $DP(\Delta_5 \oplus \Delta_8 \rightarrow \beta_4)$, $DP(\Delta_8 \rightarrow \beta_4)$의 확률은 출력 차분이 0이 아니고 F가 전단사이므로 입력 차분 또한 0이 아니므로 p보다 작거나 같다. 따라서 정리 1에 의해서 다음과 같은 결과를 얻을 수 있다.

$$DP(\alpha \rightarrow \beta) \leq p^4 \cdot \sum_{\Delta_1} DP(\alpha_1 \rightarrow \Delta_1) \cdot \sum_{\Delta_2} DP(\alpha_2 \oplus \Delta_1 \rightarrow \Delta_2) \cdot \sum_{\Delta_4} DP(\alpha_4 \oplus \beta_3 \rightarrow \Delta_4) \cdot \sum_{\Delta_5} DP(\Delta_1 \oplus \Delta_4 \rightarrow \Delta_5) \cdot \sum_{\Delta_8} DP(\Delta_4 \rightarrow \Delta_8) \leq p^4$$

이제 위의 경우 1의 증명을 표 1을 이용하여 증명하는 방법을 알아보자. 표 1에서 관계식은 변수들

(표 2) 경우 1의 증명
(Table 2) Proof of Case 1

관계식	$\Delta_7 = \Delta_{10} = \Delta_{11} = 0, \Delta_3 = \Delta_6 = \Delta_9 = \beta_4 \neq 0$		
자유변수 t	$\Delta_1, \Delta_2, \Delta_4, \Delta_5, \Delta_8$		
단계 1	sum over Δ_1	sum over Δ_2	$\leq p$
단계 2	sum over Δ_4	sum over Δ_5	$\leq p$
단계 3	1	sum over Δ_8	$\leq p$
단계 4	1	1	$\leq p$
단계 5	1	1	1

간의 관계식을 의미하고 자유변수는 t는 관계식에서 사라지는 변수들을 제외한 나머지 변수들, 즉 위의 식에서 합해지는 변수들을 의미한다. 변수에 대해 합해지는 연산 $\sum$를 sum over 라고 표현하여 이 sum over되는 변수의 확률은 1이 된다. 또한 입력 차분이 0인 경우의 확률은 1이 되고, 입력 차분이 0이 아닌 경우의 확률은 p보다 작거나 같다. 따라서 경우 1의 증명은 다음의 표 2와 같이 쓸 수 있다.

표 1을 이용한 경우 1의 증명은 differential의 확률 값이 p^4보다 작거나 같음을 의미한다. 앞으로의 증명에서는 위와 같이 표를 이용하여 증명을 할 것이다.

경우 2. ($\beta_1 = 0, \beta_2 = 0, \beta_3 \neq 0$)

경우 2-1 : $\beta_3 \oplus \beta_4 = 0$인 경우

경우 1의 방법과 같은 방법으로 변수들을 살펴보면 $\Delta_6 = \Delta_9 = \Delta_{10} = 0$이 되고 $\Delta_3 \neq 0, \Delta_2 = \Delta_5 = \Delta_7 = \Delta_{11} \neq 0$가 되어서 자유변수는 $t = \{\Delta_1, \Delta_3, \Delta_4, \Delta_7, \Delta_{11}\}$가 된다. 따라서 다음의 표와 같이 확률은 p^5보다 작거나 같다.

(표 3) 경우 2-1의 증명
(Table 3) Proof of Case 2-1

관계식	$\Delta_6 = \Delta_9 = \Delta_{10} = 0, \Delta_2 = \Delta_5 = \Delta_7 = \Delta_{11} \neq 0$		
자유변수 t	$\Delta_1, \Delta_3 \neq 0, \Delta_4, \Delta_{11} \neq 0$		
단계 1	sum over Δ_1	$\leq p$	sum over Δ_3
단계 2	sum over Δ_4	$\leq p$	1
단계 3	$\leq p$	$\leq p$	1
단계 4	1	$\leq p$	1
단계 5	1	1	sum over Δ_{11}

경우 2-2 : $\beta_3 \oplus \beta_4 \neq 0$인 경우

이 경우에 해당되는 변수들을 보면 $\Delta_{10}=0$, $\Delta_6=\Delta_9=\beta_3\oplus\beta_4$ $t=\{\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_5,\Delta_7,\Delta_8,\Delta_{11}\}$, $\Delta_{11}\neq 0$이고 자유변수는 가 되어서 전체 확률은 p^4 보다 작거나 같다.

〔표 4〕 경우 2-2의 증명
〔Table 4〕 Proof of Case 2-2

관계식	$\Delta_{10}=0, \Delta_6=\Delta_9=\beta_3\oplus\beta_4\neq 0$		
자유변수 t	$\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_5,\Delta_7\neq 0,\Delta_8,\Delta_{11}\neq 0$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	$\leq p$
단계 3	$\leq p$	sum over Δ_7	sum over Δ_8
단계 4	1	$\leq p$	$\leq p$
단계 5	1	1	sum over Δ_{11}

경우 3. ($\beta_1=0, \beta_2\neq 0, \beta_3=0$)

경우 3-1 : $\beta_4=0$인 경우

〔표 5〕 경우 3-1의 증명
〔Table 5〕 Proof of Case 3-1

관계식	$\Delta_9=0, \Delta_5=\Delta_8=\Delta_{11}=\beta_2\neq 0$		
자유변수 t	$\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_6,\Delta_7,\Delta_{10}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	$\leq p$	sum over Δ_6
단계 3	sum over Δ_7	$\leq p$	1
단계 4	sum over Δ_{10}	$\leq p$	1
단계 5	1	$\leq p$	1

경우 3-2 : $\beta_4\neq 0$인 경우

〔표 6〕 경우 3-2의 증명
〔Table 6〕 Proof of Case 3-2

관계식	$\Delta_9=\beta_4\neq 0, \Delta_{11}=\beta_2\neq 0$		
자유변수 t	$\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_5,\Delta_6,\Delta_7,\Delta_8,\Delta_{10}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	sum over Δ_6
단계 3	sum over Δ_7	sum over Δ_8	$\leq p$
단계 4	$\leq p$	sum over Δ_{10}	$\leq p$
단계 5	1	$\leq p$	1

경우 4. ($\beta_1\neq 0, \beta_2=0, \beta_3=0$)

경우 4-1 : $\beta_4=0$인 경우

〔표 7〕 경우 4-1의 증명
〔Table 7〕 Proof of Case 4-1

관계식	$\Delta_8=\Delta_{11}=0, \Delta_4=\Delta_7=\Delta_{10}=\beta_1\neq 0$		
자유변수 t	$\Delta_1,\Delta_2,\Delta_3,\Delta_5,\Delta_6,\Delta_9$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	$\leq p$	sum over Δ_5	sum over Δ_6
단계 3	$\leq p$	1	sum over Δ_9
단계 4	$\leq p$	1	1
단계 5	$\leq p$	1	1

경우 4-2 : $\beta_4\neq 0$인 경우

〔표 8〕 경우 4-2의 증명
〔Table 8〕 Proof of Case 4-2

관계식	$\Delta_{11}=0, \Delta_7=\Delta_{10}=\beta_1\neq 0$		
자유변수 t	$\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_5,\Delta_6,\Delta_8,\Delta_9$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	sum over Δ_6
단계 3	$\leq p$	sum over Δ_8	sum over Δ_9
단계 4	$\leq p$	1	$\leq p$
단계 5	$\leq p$	1	1

경우 5. ($\beta_1\neq 0, \beta_2\neq 0, \beta_3=0$)

경우 5-1 : $\beta_4=0$인 경우

〔표 9〕 경우 5-1의 증명
〔Table 9〕 Proof of Case 5-1

관계식	$\Delta_8=\Delta_{11}=\beta_2\neq 0$		
자유변수 t	$\Delta_1,\Delta_2,\Delta_3,\Delta_4,\Delta_5,\Delta_6,\Delta_7,\Delta_9\neq 0,\Delta_{10}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	sum over Δ_6
단계 3	sum over Δ_7	$\leq p$	$\leq p$
단계 4	sum over Δ_{10}	$\leq p$	1
단계 5	sum over Δ_9	$\leq p$	1

경우 5-2 : $\beta_4\neq 0$인 경우

〔표 10〕 경우 5-2의 증명
〔Table 10〕 Proof of Case 5-2

관계식	$\Delta_{11}=\beta_2\neq 0$		
자유변수 t	$\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_9, \Delta_{10}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	sum over Δ_6
단계 3	sum over Δ_7	sum over Δ_8	sum over Δ_9
단계 4	sum over Δ_{10}	$\leq p$	$\leq p$
단계 5	$\leq p$	$\leq p$	1

경우 6. ($\beta_1\neq 0, \beta_2=0, \beta_3\neq 0$)

〔표 11〕 경우 6의 증명
〔Table 11〕 Proof of Case 6

관계식	$\Delta_{10}=\beta_1\neq 0$		
자유변수 t	$\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_9, \Delta_{11}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	sum over Δ_6
단계 3	sum over Δ_7	sum over Δ_8	sum over Δ_9
단계 4	$\leq p$	$\leq p$	sum over Δ_{11}
단계 5	$\leq p$	1	$\leq p$

경우 7. ($\beta_1=0, \beta_2\neq 0, \beta_3\neq 0$)

경우 7-1 : $\beta_3\oplus\beta_4=0$ 인 경우

〔표 12〕 경우 7-1의 증명
〔Table 12〕 Proof of Case 7-1

관계식	$\Delta_9=0, \Delta_5=\Delta_8=\Delta_{11}\neq 0$		
자유변수 t	$\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_6\neq 0, \Delta_7, \Delta_{10}, \Delta_{11}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	$\leq p$	$\leq p$
단계 3	sum over Δ_6	sum over Δ_7	1
단계 4	$\leq p$	sum over Δ_{10}	1
단계 5	1	$\leq p$	sum over Δ_{11}

경우 7-2 : $\beta_3\oplus\beta_4\neq 0$ 인 경우

경우 8. ($\beta_1\neq 0, \beta_2\neq 0, \beta_3\neq 0$)

이 경우의 증명은 다른 경우의 증명과는 다른 방법을 사용한다. 우선 입력 및 출력 차분은 모두 0이 아니라는 성질을 이용하여 다음의 4가지의 경우로 나누어서 증명한다.

〔표 13〕 경우 7-2의 증명
〔Table 13〕 Proof of Case 7-2

관계식	$\Delta_9=\beta_3\oplus\beta_4\neq 0$		
자유변수 t	$\Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_{10}, \Delta_{11}$		
단계 1	sum over Δ_1	sum over Δ_2	sum over Δ_3
단계 2	sum over Δ_4	sum over Δ_5	sum over Δ_6
단계 3	sum over Δ_7	sum over Δ_8	$\leq p$
단계 4	sum over Δ_{10}	sum over Δ_{11}	$\leq p$
단계 5	1	$\leq p$	$\leq p$

경우 8-1 : 입력 차분이 $\alpha_1\neq 0$ 인 경우

〔표 14〕 경우 8-1의 증명
〔Table 14〕 Proof of Case 8-1

관계식			
자유변수 t	$\Delta_1\neq 0, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_9, \Delta_{10}, \Delta_{11}$		
단계 1	$\leq p$	sum over Δ_1	sum over Δ_2
단계 2	sum over Δ_3	sum over Δ_4	sum over Δ_5
단계 3	sum over Δ_6	sum over Δ_7	sum over Δ_8
단계 4	sum over Δ_9	sum over Δ_{10}	sum over Δ_{11}
단계 5	$\leq p$	$\leq p$	$\leq p$

경우 8-2 : 입력 차분이 $\alpha_1=0, \alpha_2\neq 0$ 인 경우

〔표 15〕 경우 8-2의 증명
〔Table 15〕 Proof of Case 8-2

관계식	$\Delta_1=0$		
자유변수 t	$\Delta_2\neq 0, \Delta_3, \Delta_4, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_9, \Delta_{10}, \Delta_{11}$		
단계 1	1	$\leq p$	sum over Δ_2
단계 2	sum over Δ_3	sum over Δ_4	sum over Δ_5
단계 3	sum over Δ_6	sum over Δ_7	sum over Δ_8
단계 4	sum over Δ_9	sum over Δ_{10}	sum over Δ_{11}
단계 5	$\leq p$	$\leq p$	$\leq p$

경우 8-3 : 입력 차분이 $\alpha_1=0, \alpha_2=0, \alpha_3\neq 0$ 인 경우

〔표 16〕 경우 8-3의 증명
〔Table 16〕 Proof of Case 8-3

관계식	$\Delta_1=\Delta_2=0$		
자유변수 t	$\Delta_3\neq0, \Delta_4, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_9, \Delta_{10}, \Delta_{11}$		
단계 1	1	1	$\leq p$
단계 2	sum over Δ_3	sum over Δ_4	sum over Δ_5
단계 3	sum over Δ_6	sum over Δ_7	sum over Δ_8
단계 4	sum over Δ_9	sum over Δ_{10}	sum over Δ_{11}
단계 5	$\leq p$	$\leq p$	$\leq p$

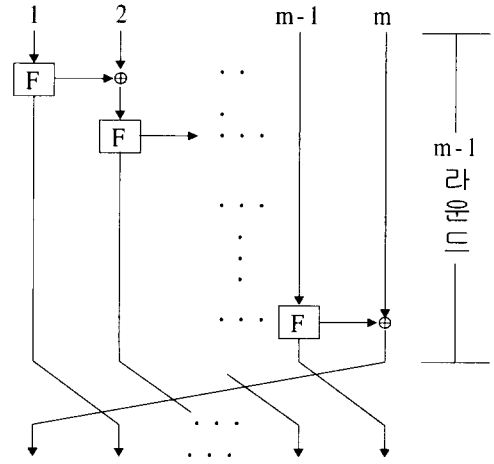
경우 8-4 : 입력 차분이 $\alpha_1=0, \alpha_2=0, \alpha_3=0, \alpha_4\neq0$ 인 경우

〔표 17〕 경우 8-4의 증명
〔Table 17〕 Proof of Case 8-4

관계식	$\Delta_1=\Delta_2=\Delta_3=0$		
자유변수 t	$\Delta_4\neq0, \Delta_5, \Delta_6, \Delta_7, \Delta_8, \Delta_9, \Delta_{10}, \Delta_{11}$		
단계 1	1	1	1
단계 2	$\leq p$	sum over Δ_4	sum over Δ_5
단계 3	sum over Δ_6	sum over Δ_7	sum over Δ_8
단계 4	sum over Δ_9	sum over Δ_{10}	sum over Δ_{11}
단계 5	$\leq p$	$\leq p$	$\leq p$

위의 정리 3의 결과는 입력 블록을 4개로 나누어서 Feistel 구조를 일반화시킨 알고리즘에 대한 Theoretical 측도에서의 안전성을 증명한 것이다.

Skipjack 알고리즘은 80비트의 키를 사용하는 64비트 블록 암호 알고리즘으로 변환규칙 A 와 변환규칙 B를 이용하여 $A^8B^8A^8B^8$을 순차적으로 적용하여 총 32번의 라운드 함수를 이용한다. 그러나 변환규칙 A를 8번 사용한 후 변환규칙 B로 넘어가는 과정에서 발생한 취약점으로 인해 Impossible differential이 발생하여 이를 이용한 Impossible DC가 제시되었다.[3] 그러나 위에서 보인 것처럼 변환규칙 A를 15번 이상 사용한다면 Impossible differential을 찾는 것이 현실적으로 불가능하므로 이러한 공격을 피할 수 있다. 즉 $A^{16}B^{16}$ 이나 A^{32}를 사용한다면 differential 대한 상한이 p^4이 되고 Impossible differential 역시 찾기 어려워 현재의 Skipjack 보다 안전성은 우수하며 동일한 구현 복잡도를 가질 것이다.



〔그림 3〕 일반화된 Skipjack-like 구조
〔Fig. 3〕 Generalized Skipjack-like Structure

한편 입력 블록을 m개로 나누어서 Skipjack 구조를 일반화시킨 구조에 대한 differential과 linear hull에 대한 확률의 상한 값에 대해 알아보자. 그림 3은 이러한 구조를 나타낸 것이다.

위의 증명을 일반화시키기 위해 라운드 함수 F는 전단사이고 각각의 라운드는 서로 독립이라고 가정하고 라운드 함수의 최대 차분의 확률을 p라고 한다. 입력 블록을 2개로 나눈 경우, 즉 m=2이면 Ohta 등이 증명하였듯이 라운드의 수 r 이 $3(=1\times3)$이상이면 differential의 확률은 p^2보다 작거나 같게된다. 이는 Skipjack-like 구조에서도 성립한다. 또한 m=3 이면 $r\geq8(=2\times4)$이면 differential의 확률은 p^3보다 작거나 같으며, m=4인 경우에서는 $r\geq15(3\times5)$이상이면 differential의 확률이 p^4이 되었다.

위의 결과들을 종합하면 우리는 다음과 같은 추측을 할 수 있다.

추측 1.

Skipjack-like 구조에서, 즉 입력 블록을 m개로 나눈 경우, $r\geq(m-1)(m+1)$ 이면 differential의 확률은 p^m보다 작거나 같다.

위의 추측 1은 m이 2,3,4인 경우에 대해서는 모두 성립함을 알 수 있다. 따라서 본 논문의 증명 방법을 이용하면 일반적인 m에 대해서도 증명이 가능하리라 생각된다. 본 논문의 증명 방식을 그대로 일반적인 m에 대해 적용한다는 것은 m이 커지면 너무 복잡하게

되므로 증명 방식에 대한 보다 많은 연구가 필요하다.

V. 결 론

본 논문에서는 Skipjack 구조를 반복적으로 사용한 구조에 대한 Theoretical 측도에서의 안전성을 증명하였다. 즉, 이 구조에서는 15라운드 이후에 최대 차분 확률의 상한이 p^4이 된다.

현재까지는 MISTY와 같이 라운드 함수를 Feistel structure로 사용하지 않는다면 DC 및 LC에 대한 안전성을 증명하면서도 효율적인 블록 암호를 만드는 방법이 불가능하였지만 본 논문의 결과를 이용한다면 Skipjack 구조를 15라운드 이상 사용하면 DC 및 LC에 대한 안전성을 증명할 수 있으며 효율적인 블록 암호를 설계할 수 있다.

한편 Skipjack은 변환 규칙 A와 B를 교번 사용함으로써 Impossible differential이라는 문제점이 발생하였지만 변환규칙 A만을 사용한다면 이러한 문제점은 발생하지 않을 것이며 보다 안전한 암호를 생성할 수 있을 것이다.

본 논문에서는 입력 블록을 4개로 나눈 경우에 대해 differential의 확률의 상한을 증명하였고, 이를 일반화시켜 m개로 나눈 구조에 대한 differential 확률의 상한이 라운드의 수가 (m-1)(m+1)이상이면 p^m이 될 것이라는 추측을 제시하였다.

참 고 문 헌

[1] K.Aoki and K.Ohta, "Strict Evaluation of the Maximum Average of Differential Probability and the Maximum Average of Linear probability", *IEICE Transactions Fundamental of Electronics, Communications and Computer Science*, Vol. E80-A, No. 1, pp. 2-8, 1997.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystem", *Journal of Cryptology*, Vol. 4, No. 1, 1991.

[3] E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of Skipjack Reduced 31 Rounds using Impossible Differentials", *Technical Report*, 1998.

[4] 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", to appear in *Proceedings of SAC'98*, 1998.

[5] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", *Advanced in Cryptology - EUROCRYPT'93*, LNCS 765, 1994.

[6] M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis", *Proceedings of the third international workshop of Fast Software Encryption*, 1996.

[7] M. Matsui, "New Block Encryption Algorithm MISTY", *Proceedings of the fourth international workshop of Fast Software Encryption*, 1997.

[8] K. Nyberg and L. R. Knudsen, "Provable Security against Differential Cryptanalysis", *Journal of Cryptology*, Vol. 8, No. 1, pp. 27-37, 1995.

[9] K. Nyberg, "Linear Approximation of Block Ciphers", *Advanced in Cryptotlogy - EUROCRYPT'94*, LNCS 950, 1995.

[10] Skipjack and KEA Algorithm Specifications, Version 2.0, 29 May 1998, Available at the National Institute of Standards and Technology's web page, http:// csrc.nist.gov/encryption/-skipjackkea.htm.

〈著者紹介〉

성 재 철 (Jaechul Sung)
1997년 8월 : 고려대학교 이과대학 수학과(학사)
1999년 8월 : 고려대학교 수학과(석사)
1999년 8월~현재 : 고려대학교, 수학과 박사과정, 고려대학교 정보보호 기술연구소 연구원
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계

이 상 진 (Sangjin Lee) 정회원
1987년 2월 : 고려대학교 이과대학 수학과(학사)
1989년 2월:고려대학교 수학과(석사)
1994년 8월 : 고려대학교 수학과(박사)
1989년 2월~1999년 2월:한국 전자통신 연구원, 선임 연구원
1999년 2월~현재:고려대학교 자연과학대학 부교수, 고려대학교 정보보호기술학과 교수, 고려대학교 정보보호기술연구소
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계

임 종 인 (Jongin Lim) 정회원
1980년 2월 : 고려대학교 이과대학 수학과(학사)
1982년 2월 : 고려대학교 수학과(석사)
1986년 2월 : 고려대학교 수학과(박사)
1986년 2월~현재:고려대학교 자연과학대학 정교수, 한국통신 정보보호학회 편집위원장, 고려대학교 정보보호기술연구소 소장
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘의 분석