情報保護學會論文誌
第17卷 第1號, 2007. 2

새로운 블록 암호 구조에 대한 차분/선형 공격의 안전성 증명*

김 종 성,[1†] 정 기 태,[1] 홍 석 희,[1‡] 이 상 진[1]
[1]고려대학교 정보보호기술연구센터

Provable Security for New Block Cipher Structures against Differential Cryptanalysis and Linear Cryptanalysis

Jongsung Kim,[1†] Kitae Jeong,[1] Seokhie Hong,[1‡] Sangjin Lee[1]
[1]Center for Information Security Technologies, Korea University

요 약

차분 공격 및 선형 공격은 강력한 블록 암호 분석 기법으로 블록 암호 알고리즘의 안전성을 평가하는 중요한 도구로 여겨지고 있다. 따라서 블록 암호 설계자들은 차분 공격과 선형 공격에 안전한 블록 암호를 설계하고자 노력해 왔다. 본 논문에서는 세 가지의 새로운 블록 암호 구조를 소개하며, 한 라운드 함수의 최대 차분 확률(최대 선형 확률)이 $p(q)$이고 라운드 함수가 전단사 함수일 때, 세 가지의 블록 암호 구조의 차분 확률(선형 확률)의 상한 값이 $p^2(q^2)$, $2p^2(2q^2)$으로 유계할 최소 라운드를 증명한다.

ABSTRACT

Differential cryptanalysis and linear cryptanalysis are the most powerful approaches known for attacking many block ciphers and used to evaluating the security of many block ciphers. So designers have designed secure block ciphers against these cryptanalyses. In this paper, we present new three block cipher structures. And for given r, we prove that differential (linear) probabilities for r-round blockcipher structures are upper bounded by $p^2(q^2)$, $2p^2(2q^2)$ if the maximum differential (linear) probability is $p(q)$ and the round function is a bijective function.

Keywords : *Block cipher, Differential Cryptanalysis, Linear Cryptanalysis, Feistel structure*

Ⅰ. 서 론

1.1 개 요

차분 공격(DC: Differential Cryptanalysis)과 선형 공격(LC: Linear Cryptanalysis)은 1990년 초에 소개된 블록 암호 분석 기법으로 현재까지 블록 암호의 안전성을 평가하는 대표적인 분석 도구로 여겨지고 있다[2,3]. 따라서 차분 공격 및 선형 공격에 대한 안전성을 부여하는 방법들이 다양하게 연구 되어 왔다. 차분 공격은 연속된 라운드의 최대 차분 특성 확률(DCP: Differential Characteristic Probability)을 고려하고 마지막 라운드의 키

접수일: 2007년 1월 16일; 채택일: 2007년 1월 26일
* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2006-(C1090-0603-0025))
† 주저자, joshep@cist.korea.ac.kr
‡ 교신저자, hsh@cist.korea.ac.kr

를 추측하여 키의 전수 조사량 보다 적은 계산량으로 키를 복구하는 분석 방법이다. 하지만 차분 공격법은 차분 특성 보다 큰 차분 확률 즉, 특정 입력 차분과 특정 출력 차분을 만족할 차분 특성 확률들의 합계를 따르는 공격법이므로 차분 특성 확률의 상한 값은 블록 암호의 안전성을 보장해 주지 못한다. 그러므로 차분 특성 확률이 아닌 차분 확률(Differential Probability)의 최적의 상한 값과 그 상한 값을 만족해 주는 최소 라운드 수를 구하여 차분 분석에 대한 안전성을 평가할 수 있다. 또한 선형 공격은 연속된 라운드의 최대 선형 특성 확률(LCP: Linear Characteristic Probability)을 고려하여 키의 정보를 복구하는 분석 방법이다. 차분 공격과 유사하게 선형 공격 또한 선형 특성 확률이 아닌 선형 확률(Linear hull Probability)의 최적의 상한 값과 그 상한 값을 만족해 주는 최소 라운드 수를 구하여 선형 공격에 대한 안전성을 평가할 수 있다. 차분 확률과 선형 확률에 대한 상한 값의 증명은 유사하므로 본 논문에서는 차분 공격 측면에서의 안전성만을 증명한다[4,6,7].

Nyberg와 Knudsen은 Feistel 구조에 사용된 라운드 함수의 최대 차분 확률이 p이면, 4라운드 후의 차분 확률의 상한 값이 $2p^2$임을 증명하였다[6]. 또한 Aoki와 Ohta는 Feistel 구조에 사용된 라운드 함수가 전단사 함수이고 최대 차분 확률이 p이면, 3라운드 Feistel 구조의 차분 확률 상한 값이 p^2임을 증명하였다[1]. 이러한 연구를 통해 차분 확률 상한 값을 작게 하는 전체 블록 암호 설계의 초점을 라운드 함수의 설계로 축소하여 차분 공격 및 선형 공격에 강한 블록 암호를 설계할 수 있다. 실질적인 예로 Matsui등은 차분 공격 및 선형 공격에 대해 안전성 증명 가능한 MISTY구조를 제안하였다[4,5].

본 논문에서는 차분 확률이 p인 전단사 라운드 함수를 사용하는 3가지의 블록 암호 구조에 대해 차분 확률 상한 값이 p^2 또는 $2p^2$임을 증명한다.

1.2 차분 공격과 선형 공격에 대한 기본적인 정의 및 정리

본 절에서는 n-비트 입·출력을 갖는 블록 암호 구조의 기본이 되는 라운드 함수 F를 $F: GF(2)^n \rightarrow GF(2)^n$와 같이 정의할 때, 차분 확률과 선형 확률에 대한 기본적인 정의와 정리를 요약한다.

정의1. 임의의 평문 쌍 $X, X' \in GF(2)^n$에 대한 입력, 출력 차분을 각각 $\Delta X = X \oplus X'$, $\Delta Y = F(X) \oplus F(X')$라 정의 하고, 임의의 평문 $X \in GF(2)^n$에 대한 입력 비트 마스크를 ΓX로, X의 출력 값 $F(X)$에 대한 출력 비트 마스크를 ΓY로 정의 한다.

정의2. 임의의 $\Delta X, \Delta Y, \Gamma X, \Gamma Y \in GF(2)^n$에 대해 라운드 함수 F의 차분 확률(Differential Probability)과 선형 확률(Linear hull Probability)을 다음과 같이 정의한다.

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

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

임의의 라운드 함수 F에 대해 입력 차분 ΔX와 출력 비트 마스크 ΓY가 0이 아닌 모든 경우에 대한 확률 값들이 작아야 차분 공격과 선형 공격에 대한 이론적인 측면에서의 좋은 안전성을 제시할 수 있다. 따라서 다음과 같이 최대 차분 확률과 최대 선형 확률을 정의한다.

정의3. 라운드 함수 F의 최대 차분 확률과 최대 선형 확률을 다음과 같이 정의 한다.

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

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

다음은 본 논문의 증명 과정에 사용되는 몇 가지 정리 내용을 살펴본다.

정리1.

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

(2) 만약 함수 F가 전단사 함수이면,
$\sum_{\Delta X} DP^F(\Delta X \rightarrow \Delta Y) = 1$, $\sum_{\Gamma Y} LP^F(\Gamma X \rightarrow \Gamma Y) = 1$
이 성립한다.

차분 확률 $DP^F(0 \rightarrow 0) = 1$이고, $\Delta X \neq 0$ 또는 $\Delta Y \neq 0$이면 $DP^F(\Delta X \rightarrow \Delta Y) \leq p$이다. 만약 라운드 함수 F가 전단사 함수이고, $\Delta X \neq 0$이면, $DP^F(\Delta X \rightarrow \Delta Y)$에서 $\Delta Y \neq 0$이 된다.

다음은 연속적으로 적용된 두 라운드 함수 F_1, F_2의 차분 확률과 선형 확률에 관한 정리이다.

정리2. 임의의 $\Delta X, \Delta Y, \Gamma X, \Gamma Y \in GF(2)^n$에 대하여 다음 식을 만족한다.

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

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

Ⅱ. 새로운 블록 암호 구조의 차분 공격에 대한 안전성

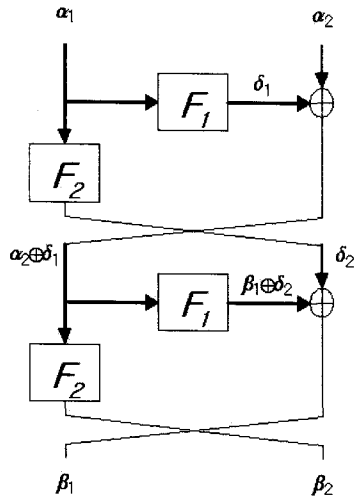
본 절에서는 3가지의 블록 암호 구조를 소개하며, 각 구조의 차분 확률 상한 값을 증명한다. 각 구조에 사용되는 라운드 함수 F_1, F_2, F_3는 전단사 함수이며, 최대 차분 확률을 p라고 가정한다. 또한 입력 차분을 $\alpha=(\alpha_1,\alpha_2)$로, 출력 차분을 $\beta=(\beta_1,\beta_2)$로 표시한다.

2.1 첫 번째 구조의 차분 공격에 대한 안전성

〔그림 1〕은 세 가지 중 첫 번째 형태인 2라운드 블록 암호 구조를 설명한다.

첫 번째 구조의 2 라운드 차분 확률 $DP^{(2)}=DP(\alpha\rightarrow\beta)$는 다음과 같이 나타낼 수 있다.

$$DP^{(2)} = \sum_{\delta_1,\delta_2} (\alpha_1\rightarrow\delta_1)\cdot(\alpha_1\rightarrow\delta_2)\cdot(\alpha_2\oplus\delta_1\rightarrow\beta_2) \cdot(\alpha_2\oplus\delta_1\rightarrow\beta_1\oplus\delta_2)$$



〔그림 1〕 첫 번째 Feistel 변형 구조

정리3.(결과) 첫 번째 블록 암호 구조의 차분 확률 상한 값이 p^2으로 유계할 최소 라운드는 2라운드 (4라운드 함수)이다.

[증명] 증명 방법은 다음과 같다. 입력 차분 α의 조건에 따른 모든 경우(단, $\alpha\neq 0$)에 대하여 순차적인 sum방식으로 각각의 경우에 대한 확률이 p^2으로 유계하다는 것을 보인다.

(경우 1) $\alpha_1\neq 0, \alpha_2\neq 0 (\delta_1\neq 0, \delta_2\neq 0)$

$$DP^{(2)} \le p^2 \sum_{\delta_1,\delta_2} (\alpha_2\oplus\delta_1\rightarrow\beta_2)\cdot(\alpha_2\oplus\delta_1\rightarrow\beta_1\oplus\delta_2)$$
$$= p^2\left(\sum_{\delta_1}(\alpha_2\oplus\delta_1\rightarrow\beta_2)\left(\sum_{\delta_2}(\alpha_2\oplus\delta_1\rightarrow\beta_1\oplus\delta_2)\right)\right)$$
$$= p^2$$

(경우 2) $\alpha_1=0, \alpha_2\neq 0 (\delta_1=0, \delta_2=0)$

$$DP^{(2)} = (\alpha_2\rightarrow\beta_2)\cdot(\alpha_2\rightarrow\beta_1) \le p^2$$

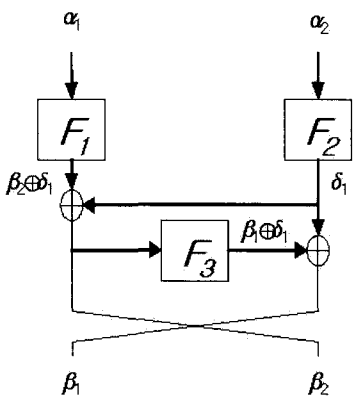
(경우 3) $\alpha_1\neq 0, \alpha_2=0 (\delta_1\neq 0, \delta_2\neq 0)$

$$DP^{(2)} \le p^2 \sum_{\delta_1,\delta_2} (\delta_1\rightarrow\beta_2)\cdot(\delta_1\rightarrow\beta_1\oplus\delta_2)$$
$$= p^2\left(\sum_{\delta_1}(\delta_1\rightarrow\beta_2)\left(\sum_{\delta_2}(\delta_1\rightarrow\beta_1\oplus\delta_2)\right)\right)$$
$$= p^2$$

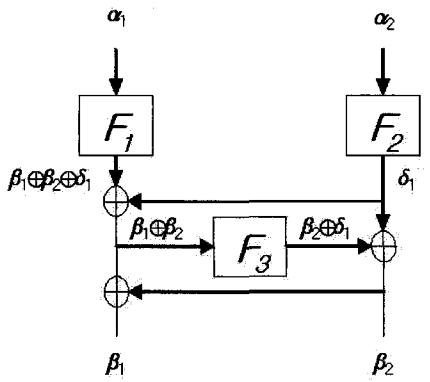
2.2 두 번째 구조의 차분 공격에 대한 안전성

〔그림 2〕는 세 가지 중 두 번째 형태인 1라운드 블록 암호 구조를 설명한다.

두 번째 구조의 1 라운드 차분 확률 $DP^{(1)}=DP(\alpha\rightarrow\beta)$는 다음과 같이 나타낼 수 있다.



〔그림 2〕 두 번째 Feistel 변형 구조



〔그림 3〕 세 번째 Feistel 변형 구조

$$DP^{(1)}=\sum_{\delta_1}(\alpha_1\rightarrow\beta_2\oplus\delta_1)\cdot(\alpha_2\rightarrow\delta_1)\cdot(\beta_2\rightarrow\beta_1\oplus\delta_1)$$

정리4.(결과) 두 번째 블록 암호 구조의 차분 확률 상한 값이 p^2으로 유계할 최소 라운드는 1라운드(3라운드 함수)이다.

[증명] 증명은 위의 방식을 따른다.

(경우 1) $\alpha_1\neq 0,\alpha_2\neq 0$

$DP^{(1)}\le p^2\sum_{\delta_1}(\beta_2\rightarrow\beta_1\oplus\delta_1)=p^2$

(경우 2) $\alpha_1=0,\alpha_2\neq 0(\delta_1=\beta_2)$

$DP^{(1)}=(\alpha_2\rightarrow\beta_2)\cdot(\beta_2\rightarrow\beta_1\oplus\beta_2)$

만약 $\beta_2=0$ 이면, $DP^{(1)}=0$

만약 $\beta_2\neq 0$ 라면, $DP^{(1)}\le p^2$

(경우 3) $\alpha_1\neq 0,\alpha_2=0(\delta_1=0)$

$DP^{(1)}=(\alpha_1\rightarrow\beta_2)\cdot(\beta_2\rightarrow\beta_1)\le p^2$

2.3 세 번째 구조의 차분 공격에 대한 안전성

〔그림 3〕은 세 가지 중 마지막 형태인 1라운드 블록 암호 구조를 설명한다.

세 번째 구조의 1 라운드 차분 확률 $DP^{(1)}=DP(\alpha\rightarrow\beta)$는 다음과 같이 나타낼 수 있다.

$$DP^{(1)}=\sum_{\delta_1}(\alpha_1\rightarrow\beta_1\oplus\beta_2\oplus\delta_1)\cdot(\alpha_2\rightarrow\delta_1)\cdot(\beta_1\oplus\beta_2\rightarrow\beta_2\oplus\delta_1)$$

정리5. (결과) 세 번째 블록 암호 구조의 차분 확률 상한 값이 p^2으로 유계할 최소 라운드는 1라운드(3라운드 함수)이다.

[증명] 증명은 위의 방식을 따른다.

(경우 1) $\alpha_1\neq 0,\alpha_2\neq 0(\delta_1\neq 0)$

$DP^{(1)}\le p^2\sum_{\delta_1}(\beta_1\oplus\beta_2\rightarrow\beta_2\oplus\delta_1)=p^2$

(경우 2) $\alpha_1=0,\alpha_2\neq 0(\delta_1=\beta_1\oplus\beta_2)$

$DP^{(1)}=(\alpha_2\rightarrow\beta_1\oplus\beta_2)\cdot(\beta_1\oplus\beta_2\rightarrow\beta_1)\le p^2$

(경우 3) $\alpha_1\neq 0,\alpha_2=0(\delta_1=0)$

$DP^{(1)}=(\alpha_1\rightarrow\beta_1\oplus\beta_2)\cdot(\beta_1\oplus\beta_2\rightarrow\beta_2)\le p^2$

Ⅲ. 결 론

본 논문에서는 3가지의 블록 암호 구조를 제시하고, 각각에 대해 차분 공격에 대한 안전성을 논의하였다. F_1,F_2,F_3함수가 최대 차분 확률 p를 갖는 전단사 라운드 함수를 사용한다면 3가지의 블록 암호 구조의 차분 확률 상한이 p^2 또는 $2p^2$임을 증명하였다. 본 논문을 통해 차분 공격 및 선형 공격에 대해 안전성 증명 가능한 새로운 블록 암호 설계 구조를 고려해 볼 수 있다.

참고문헌

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

〔2〕 E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Advances in Cryptology-CRYPTO'90*, LNCS 537, Springer-Verlag, pp. 2-21 ,1991.

〔3〕 M. Matsui, "Linear cryptanalysis method for DES cipher", *Advances in Cryptology-EUROCRYPT'93*, LNCS 765, Springer-Verlag, pp. 386-397, 1994.

〔4〕 M. Matsui, "New structure of block ciphers with provable security against differential and linear cryptanalysis", *Fast Software Encryption*

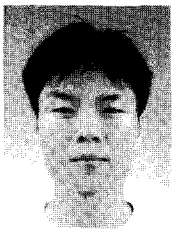
Workshop 96, pp. 205-218, 1996.

[5] M. Matsui, "New Block Encryption Algorithm MISTY", *Fast Software Encryption Workshop 97*, pp. 205-218, 1996.

[6] K. Nyberg, Lars R. Knudsen, "Provable security against differential cryptanalysis", *Journal of Cryptology*, Vol. 8, No. 1, pp. 27-37, 1995.

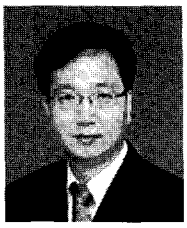
[7] K. Nyberg, "Linear approximation of block ciphers", Presented at rump session, *Eurocrypt '94*, May 1994.

〈著者紹介〉

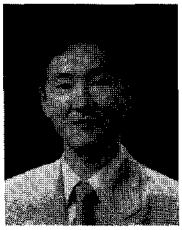


김 종 성 (Jongsung Kim) 학생회원
2000년 8월: 고려대학교 수학과 학사
2002년 8월: 고려대학교 수학과 석사
2006년 11월: K.U.Leuven 박사
2007년 2월: 고려대학교 정보보호대학원 박사
<관심분야> 대칭키 암호의 분석 및 설계

정 기 태 (Kitae Jeong) 학생회원
2004년 2월: 고려대학교 수학과 학사
2006년 2월: 고려대학교 정보보호대학원 석사
2006년 3월~현재: 고려대학교 정보보호대학원 박사과정
<관심분야> 블록 암호, 스트림 암호 및 해쉬 함수의 분석 및 설계



홍 석 희 (Seokhie Hong) 종신회원
1995년 2월: 고려대학교 수학과 학사
1997년 2월: 고려대학교 수학과 석사
2001년 2월: 고려대학교 수학과 박사
1999년 8월~2004년 2월: (주) 시큐리티 테크놀로지스 선임연구원
2003년 2월~2004년 2월: 고려대학교 시간강사
2004년 4월~2005년 2월: K.U.Leuven 박사후연구원
2005년 3월~현 재: 고려대학교 정보보호대학원 조교수
<관심분야> 암호 알고리즘 설계 및 분석, 컴퓨터 포렌식



이 상 진 (Sangjin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 2월: 고려대학교 수학과 박사
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현 재: 고려대학교 정보보호대학원 부교수
<관심분야> 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식