情報保護學會論文誌
第12券 第5號, 2002. 10

Rijndael 유사 구조의 차분 공격과 선형 공격에 대한 안전성에 관한 연구

박 상 우*, 성 수 학**, 지 성 택*, 윤 이 중*, 임 종 인***

On the Security of Rijndael-like Structures against Differential and Linear Cryptanalysis

Sangwoo Park*, Soo Hak Sung**, Seongtaek Chee*, E-Joong Yoon*, Jong-In Lim***

요 약

Rijndael 유사 구조는 SPN 구조의 특수한 형태이다. Rijndael 유사 구조의 확산 단계는 두 가지 종류의 확산 단계의 결합으로 구성되는데, 그중 하나는 바이트 치환 π이고, 다른 하나는 확산 단계 $\theta=(\theta_1, \theta_2, \theta_3, \theta_4)$로서, 각 θ_i는 라운드 입력의 4개의 행 각각에 적용된다. 블록 암호 Rijndael은 Rijndael 유사 구조의 하나의 예가 된다. 본 논문에서는 Rijndael 유사 구조의 최대 차분 확률과 최대 선형 hull 확률의 상한을 구하는 알고리즘을 제안한다.

ABSTRACT

Rijndael-like structure is the special case of SPN structure. The linear transformation of Rijndael-like structure consisits of linear transformations of two types, the one is byte permutation π and the other is linear tranformation $\theta=(\theta_1, \theta_2, \theta_3, \theta_4)$, where each of θ_i separately operates on each of the four rows of a state. The block cipher, Rijndael is an example of Rijndael-like structures. In this paper, we present a new method for upper bounding the maximum differential probability and the maximum linear hull probability for Rijndael-like structures.

Keyword : *Block Ciphers, Rijndael, Differential cryptanalysis, Linear cryptanalysis*

Ⅰ. 서 론

SPN(Substitution-Permutation Network) 구조는 비교적 간단한 라운드 함수를 반복하여 만든 반복 구조로, 한 라운드가 키 덧셈 단계(key addition layer), 대치 단계(substitution layer) 단계, 그리고 확산 단계(diffusion layer)로 구성된다. 블록 암호 Square[3]는 SPN 구조이며, 확산 단계 부분이 바이트들을 교환하는 치환 π와 비트들을 교환하는 치환 θ의 두 가지 형태의 확산 단계로 구성된다. 미국 표준 블록 암호 AES(Advanced Encryption Standard)로 선정된 블록 암호 Rijndael[4]과 AES 1차 후보 알고리즘 중의 하나인 블록 암호 Crypton[9,10]도 확산 단계가 Square의 확산 단계와 동일한 형태인 SPN 구조의 블록 암호이다. 본 논문에서는 Square의 확산 단계 형태의 확산 단계를 가지는 SPN 구조를 Rijndael 유사 구조(Rijndael-like structure)라 부르기로 한다.

* 국가보안기술연구소({psw, chee, yej}@etri.re.kr)
** 배재대학교 전산정보수학과(sungsh@paichai.ac.kr)
*** 고려대학교 정보보호대학원(jilim@tiger.korea.ac.kr)

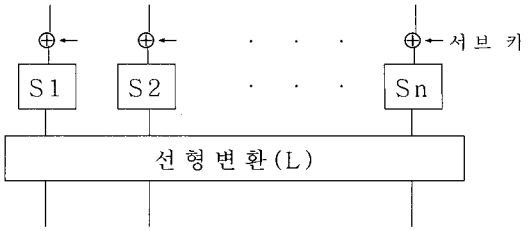
블록 암호의 차분 공격(DC, differential cryptanalysis)[1]과 선형 공격(LC, linear cryptanalysis)[11]에 대한 안전성은 각각 최대 차분 확률(maximum differential probability)과 최대 선형 hull 확률(maximum linear hull probability)에 의존한다.

최근에 Keliher, Meijer, Tavares는 SPN 구조 블록 암호에 대한 최대 선형 hull 확률의 상한을 찾는 알고리즘을 제안하였으며, 이를 Rijndael 블록 암호에 적용하여 라운드의 수가 7 이상일 때 상한이 2^{-75} 임을 보였다[7]. 그리고, 이 상한을 얻는데 Sun Ultra 5로 44,000 시간이 소요되었다고 한다. 또 그들은 Rijndael 암호의 s-box의 선형 hull 확률 값의 분포를 사용하여 9 라운드 Rijndael의 최대 선형 hull 확률의 상한을 2^{-92}으로 개선할 수 있다고 주장하였다[8]. 그들은 상한을 구하기 위하여 필요한 계산량의 43% 정도를 수행한 후 이런 주장을 하였으며 전체 계산을 마치는데는 Sun Ultra 5로 200,000 시간이 소요될 것으로 예측하였다. 따라서 Keliher, Meijer, Tavares가 개발한 알고리즘은 수행 시간이 너무 커서 다른 Rijndael 유사 구조에 적용하는데 많은 어려움이 있다.

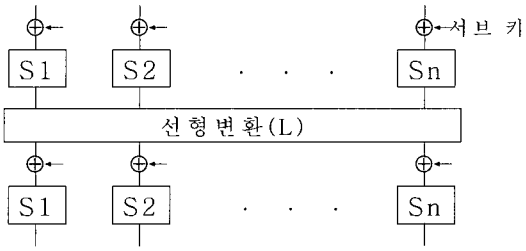
본 논문에서는 s-box의 최대 차분 확률이 $p \le 2^{-3}$ 일 때 4 라운드 Rijndael 유사 구조에 대한 최대 차분 확률의 상한은 $4p^{19}+6p^{18}+4p^{17}+p^{16}$, s-box의 최대 선형 hull 확률이 $q \le 2^{-3}$일 때 4 라운드 Rijndael 유사 구조에 대한 최대 선형 hull 확률의 상한은 $4q^{19}+6q^{18}+4q^{17}+q^{16}$ 임을 증명한다. 본 논문의 결과를 블록 암호 Rijndael에 적용하면 최대 차분 확률의 상한과 최대 선형 hull 확률의 상한은 1.06×2^{-96}으로 Keliher, Meijer, Tavares[7,8]의 상한 보다 훨씬 좋다.

II. SPN 구조의 차분 확률 및 선형 hull 확률

SPN 구조 블록 암호의 한 라운드는 키 덧셈, 대치 그리고 확산의 3 부분으로 구성된다. 키 덧셈 부분은 라운드의 입력과 서브키 간의 비트별 배타적 논리합(EXOR)이며, 대치 부분은 입력을 n개의 작은 블록으로 나눈 다음 각각의 소 블록을 s-box라고 부르는 비선형 변환을 적용하여 출력을 얻은 과정으로 혼동(confusion) 효과를 주기 위한 것이다. 선형변환은 대치 부분의 결과를 확산(diffusion)시키는 역할을 한다. SPN의 한 라운드 구조는 [그림 1]



[그림 1] SPN 구조의 한 라운드



[그림 2] 2라운드 SPN 구조

과 같이 나타낼 수 있으며 이 구조를 r번 반복하여 만든 것을 r 라운드 SPN 구조라고 부른다. 이 때 마지막 라운드의 선형변환은 암호적으로 의미가 없기 때문에 생략된다. 따라서 2 라운드 SPN 구조는 [그림 2]와 같이 나타낼 수 있다.

SPN 블록 암호가 복호화 되기 위해서 s-box는 역변환을 가져야 한다. 그래서 본 논문에서 s-box는 정의역과 공변역이 Z_2^m인 전단사 함수라고 가정한다. 또 라운드 키(서브 키)는 서로 독립이며 일양분포를 가진다고 가정한다. 이 가정 하에서 라운드 키는 차분 공격과 선형 공격에 아무런 영향을 주지 않으므로 라운드 키가 없는 SPN 구조를 고려하기로 한다.

(정의 1)

S를 Z_2^m 상에서 정의된 전단사(bijective) 함수라고 하자. 임의의 $a, b, \Gamma_a, \Gamma_b \in \{0,1\}^m$에 대해 S의 차분 확률과 선형 hull 확률을 각각

$$DP^S(a,b) = \frac{\#\{x \in Z_2^m \mid S(x) \oplus S(x \oplus a) = b\}}{2^m},$$

$$LP^S(\Gamma_a, \Gamma_b) = \left(\frac{\#\{x \in Z_2^m \mid \Gamma_a \cdot x = \Gamma_b \cdot S(x)\}}{2^{m-1}} - 1 \right)^2$$

로 정의한다. 여기서 $x \cdot y$는 x와 y의 비트별 곱의 패리티(0 또는 1)를 의미한다. 또 a와 b를 각각 S의

입력 차분(input difference)과 출력 차분(output difference)이라고 부르며 Γ_a와 Γ_b를 각각 S의 입력 mask와 출력 mask라고 부른다.

차분 확률과 선형 hull 확률은 s-box에서 정의될 뿐만 아니라 블록 암호에 대해서도 정의 가능하다. s-box의 입·출력 크기는 비교적 작기 때문에(보통 8비트), 차분 확률과 선형 hull 확률을 쉽게 계산할 수 있으나 블록 암호의 입·출력 크기는 크기 때문에(현재는 주로 128 비트), 차분 확률과 선형 hull 확률을 계산하는 것이 쉽지 않다.

차분 공격에 대한 s-box S의 강도는 최대 차분 확률인 $\max_{a\neq 0,b} DP^S(a,b)$에 의해서 결정된다. 최대 차분 확률이 작을수록 S는 차분 공격에 보다 안전하다. 같은 방법으로 선형 공격에 대한 S의 강도는 최대 선형 hull 확률인 $\max_{\Gamma_a,\Gamma_b\neq 0} LP^S(\Gamma_a,\Gamma_b)$에 의해서 결정된다.

어떤 s-box에 0이 아닌 어떤 입력 차분이 주어졌을 때 그 s-box를 차분 공격 관점에서의 active s-box(differentially active s-box)라 한다. 그리고 어떤 s-box에 0이 아닌 출력 mask 값이 주어졌을 때 그 s-box를 선형 공격 관점에서의 active s-box(linearly active s-box)라 한다. SPN 구조에서 사용되는 s-box는 모두 전단사이므로 차분 공격 관점에서의 active s-box이면 0이 아닌 출력 차분을 가지며 선형 공격 관점에서의 active s-box이면 0이 아닌 입력 mask 값을 가진다.

한편 SPN 구조 블록 암호에서 차분 확률은 차분 공격 관점에서의 active s-box의 개수와 밀접한 관계가 있다. 차분 공격 관점에서의 active s-box의 개수가 많으면 차분 확률은 작을 가능성이 크며 반대로 차분 공격 관점에서의 active s-box의 개수가 작으면 차분 확률이 클 가능성이 크다. 이런 이유로 2 라운드 SPN 구조에서 branch 수(branch number)라는 개념을 정의한다[3]. 2 라운드 SPN 구조에서 차분 공격 관점에서의 active s-box의 최소 개수를 차분 공격 관점에서의 branch 수로 정의하며 선형 공격 관점에서의 active s-box의 최소 개수를 선형 공격 관점에서의 branch 수로 정의한다.

다음으로 선형변환 $L: (Z_2^m)^n \rightarrow (Z_2^m)^n$의 차분 공격 및 선형 공격 특성을 살펴보자. 선형변환 L은 $n\times n$ 행렬 $M=(m_{ij})$에 의해서 $L(x)=Mx$로 나타낼 수 있다. 여기서 x는 $(Z_2^m)^n$의 원소이며 덧셈은 비트별 xor이다. 그러나 곱셈은 행렬 M의 원소에 따라 달리 정의된다. 블록 암호 E2[12]에서 사용된 확산 단계와 같이 M의 원소가 Z_2의 원소일 때 곱셈의 정의는 자명하다. 블록 암호 Crypton[9,10]에서는 M의 원소가 Z_2^m의 원소이며 곱셈은 비트별 논리곱으로 정의된다. 블록 암호 Rijndael[4]에서와 같이 M의 원소가 갈로아 체 $GF(2^m)$의 원소이면 곱셈은 그 체 상에서 정의된 곱셈 연산이다.

확산 단계 L에 대해 $L(x)\oplus L(x^*)=L(x\oplus x^*)$이 성립함을 쉽게 알 수 있다[2]. 즉 $DP^L(a,L(a))=1$이다. 따라서 branch 수를 다음과 같이 정의할 수 있다.

(정의 2)

L을 $(Z_2^m)^n$ 상에서 정의된 확산 단계라고 하자. L의 차분 공격 관점에서의 branch 수 β_d를 $\beta_d=\min_{x\neq 0}\{wt(x)+wt(L(x))\}$로 정의한다. 여기서 $wt(x)$는 x의 0이 아닌 component의 개수, 즉 $wt(x)=wt(x_1,\cdots,x_n)=\#\{1\leq i\leq n | x_i\neq 0\}$이다.

위의 정의에서 사용된 "$wt(x)$"는 우리가 잘 알고 있는 Hamming weight 정의를 일반화시킨 것이다. 만일 $x\in Z_2^n$이면 $wt(x)$는 x의 Hamming weight이다. 일반적으로 $x=(x_1,\cdots,x_n)\in A^n$일 때 $wt(x)$는 x의 0이 아닌 component의 개수, 즉 $wt(x)=\#\{1\leq i\leq n | x_i\neq 0\}$이다.

정의 2와 같이 확산 단계 L의 선형 공격 관점에서의 branch 수를 정의할 수 있으나 다소 복잡하다. 확산 단계에 대응되는 행렬 $M=(m_{ij})$의 원소가 Z_2의 원소일 경우에는 $LP^L(M^t\Gamma_b,\Gamma_b)=1$이 성립한다. 다시 말하면, $LP^L(\Gamma_a,(M^{-1})^t\Gamma_a)=1$이 성립한다. 만일 M의 원소가 갈로아 체 $GF(2^m)$의 원소일 때는 $GF(2^m)$ 상의 적당한 $n\times n$ 행렬 C에 대해 $LP^L(\Gamma_a,C\Gamma_a)=1$이 성립된다는 것이 최근에 증명되었다[6]. 따라서 L의 선형 공격 관점에서의 branch 수 β_l을 다음과 같이 정의할 수 있다.

- $m_{ij}\in Z_2 (1\leq i,j\leq n)$인 경우:
  $\min_{\Gamma_a\neq 0}\{wt(\Gamma_a)+wt((M^{-1})^t\Gamma_a)\}$
- $m_{ij}\in GF(2^m)$, $1\leq i,j\leq n$인 경우:
  $\min_{\Gamma_a\neq 0}\{wt(\Gamma_a)+wt(C\Gamma_a)\}$

(정의 3)

s-box들의 최대 차분 확률과 최대 선형 hull 확률을 각각 p,q로 쓰기로 한다. 즉

$p=\max_{1\le i\le n}\max_{a\neq 0,b} DP^{S_i}(a,b)$

$q=\max_{1\le i\le n}\max_{\Gamma_a,\Gamma_b\neq 0} LP^{S_i}(\Gamma_a,\Gamma_b)$

(정의 4)

$x=(x_1,\cdots,x_n)\in A^n$일 때 x의 패턴 γ_x를 $\gamma_x=(\gamma_1,\cdots,\gamma_n)\in Z_2^n$으로 정의한다. 여기서 x_i가 0이면 $\gamma_i=0$이고 그렇지 않을 경우 $\gamma_i=1$이다.

이젠 r 라운드 SPN 구조에 대한 차분 확률과 선형 hull 확률을 살펴보자. SPN 구조의 입력 차분을 $a=(a_1,\cdots,a_n)$ 그리고 출력 차분을 $b=(b_1,\cdots,b_n)$이라고 할 때 r 라운드 차분 확률을 $DP_r^L(a,b)$로 쓰기로 한다. 혼란이 없을 경우 확산 단계 L을 생략하여 간단히 $DP_r(a,b)$로 표기한다. 또 s-box인 S_i의 차분 확률 DP^{S_i}도 혼란이 없을 경우 S_i를 생략하여 간단히 DP로 표기한다.

1 라운드 SPN 구조의 차분 확률은 $DP_1(a,b)=DP(a_1,b_1)\cdots DP(a_n,b_n)$이며, 선형 hull 확률은 $LP_1(a,b)=LP(a_1,b_1)\cdots LP(a_n,b_n)$이다.

확산 단계의 branch 수가 $n+1$(최대) 또는 n일 때 2 라운드 SPN 구조에 대한 차분 확률 및 선형 hull 확률의 상한은 이미 알려져 있다[5,6].

(보조정리 1)([5],[6]).

$L:(Z_2^m)^n\to(Z_2^m)^n$을 선형변환이라고 하고 β_d와 β_l을 각각 L의 차분 공격과 선형 공격 관점에서의 branch 수라고 하자.

(i) 만일 $\beta_d=n+1$ 또는 n이면 $DP_2(a,b)\le p^{\beta_d-1}$이다.

(ii) 만일 $\beta_l=n+1$ 또는 n이면 $LP_2(a,b)\le q^{\beta_l-1}$이다.

라운드의 수가 3 이상인 SPN 구조에 대한 차분 확률 및 선형 hull 확률의 좋은 상한을 이론적으로 유도하는 것은 쉽지 않다. 그러나 Rijndael 유사 구조에 대해서는 좋은 상한을 유도할 수 있다. 다음 보조정리는 $r(r\ge 3)$ 라운드 Rijndael 유사 구조에 대한 차분 확률의 상한을 구하는데 사용된다.

(보조정리 2)

$L:(Z_2^m)^n\to(Z_2^m)^n$을 확산 단계라고 하고 β_d를 L의 차분 공격 관점에서의 branch 수라고 하자. $wt(\gamma)+wt(b)\ge\beta_d$를 만족하는 $\gamma\in Z_2^n$와 $b=(b_1,\cdots,b_n)\in(Z_2^m)^n$에 대해 집합 A를 다음과 같이 정의한다.

$A=\{y=(y_1,\cdots,y_n)\in(Z_2^m)^n \mid \gamma_x=\gamma$인 어떤 x에 대하여, $\gamma_y=\gamma_b, y=L(x)\}$

그러면 다음 식이 성립한다.

$$\sum_{y\in A}DP_1(y,b)=\sum_{y\in A}DP(y_1,b_1)\cdots DP(y_n,b_n)\le p^{\max\{0,\beta_d-wt(\gamma)-1\}}$$

(증명)

$\sum_{y\in A}DP_1(y,b)\le\sum_{y\in(Z_2^m)^n}DP_1(y,b)=1$이므로 $\beta_d-wt(\gamma)-1>0$일 때만 고려하면 된다. 표현을 간단히 하기 위해서 $b_1\neq 0,\cdots,b_k\neq 0, b_{k+1}=\cdots=b_n=0$이라고 가정한다. 그러면

$$\sum_{y\in A}DP_1(y,b)=\sum_{y\in A}DP(y_1,b_1)\cdots DP(y_k,b_k) \quad (1)$$

이다. $wt(\gamma)+wt(b)=\beta_d$와 $wt(\gamma)+wt(b)>\beta_d$의 두 가지 경우로 나누어 증명 하고자 한다.

경우 1. $wt(\gamma)+wt(b)=\beta_d$ 일 때

이 경우 식 (1)에 있는 k개의 변수 $y_1,\cdots,y_k$에서 각 y_i는 다른 값을 갖는다. 따라서

$\sum_{y\in A}DP_1(y,b)\le p^{k-1}$

$\sum_{y\in A}DP(y_1,b_1)\le p^{k-1}=p^{\beta_d-wt(\gamma)-1}$이 성립한다.

경우 2. $wt(\gamma)+wt(b)>\beta_d$ 일 때

이 경우 식 (1)에 있는 k개의 변수 $y_1,\cdots,y_k$에서 각 y_i는 다른 값을 반드시 갖지는 않는다. 그러나 $t=k+wt(\gamma)-\beta_d$개의 변수($y_1,\cdots,y_t$라고 하자)를 고정하면 나머지 변수 각각은 다른 값을 갖는다. 따라서 $\sum_{y\in A}DP_1(y,b)$는 아래와 같이 유계시킬 수 있다.

$$\sum_{y\in A}DP_1(y,b)\le\sum_{j_1=1}^{2^m-1}DP(j_1,b_1)\cdots\sum_{j_t=1}^{2^m-1}DP(j_t,b_t)\cdot$$

$$\sum_{y\in A, y_i=j_i, 1\le i\le t} DP(y_{t+1}, b_{t+1})\cdots DP(y_k, b_k)$$
$$\le p^{k-t-1}\sum_{j_1=1}^{2^m-1} DP(j_1, b_1)\cdots \sum_{j_t=1}^{2^m-1} DP(j_t, b_t)$$
$$\sum_{y\in A, y_i=j_i, 1\le i\le t} DP(y_{t+1}, b_{t+1})$$
$$\le p^{k-t-1}\sum_{j_1=1}^{2^m-1} DP(j_1, b_1)\cdots \sum_{j_t=1}^{2^m-1} DP(j_t, b_t)$$
$$\le p^{k-t-1} = p^{\beta_d - wt(\gamma)-1}$$

그러므로 경우 1과 2에 의해서 증명이 완성된다.

Ⅲ. Rijndael 유사 구조의 차분 확률 및 선형 hull 확률의 상한

Rijndael 유사 구조는 SPN 구조의 특수한 형태로 확산 단계가 바이트 기반 치환과 비트 기반 치환 두 가지 형태의 확산 단계의 결합으로 구성된다. 바이트 기반 치환을 $\pi:(Z_2^m)^{16}\rightarrow(Z_2^m)^{16}$, 그리고 비트 기반 치환을 $\theta=(\theta_1,\theta_2,\theta_3,\theta_4)$라고 할 때 π와 θ는 다음과 같은 조건을 만족한다고 가정한다.

π의 조건 :

입력을 $x_{11}, x_{12}, x_{13}, x_{14}, \ldots, x_{41}, x_{42}, x_{43}, x_{44}$이라고 하고 각 소 블록을 집합 A_i $(1\le i\le 4)$라고 두자. 즉

$A_1=\{x_{11}, x_{12}, x_{13}, x_{14}\}$, $A_2=\{x_{21}, x_{22}, x_{23}, x_{24}\}$,
$A_3=\{x_{31}, x_{32}, x_{33}, x_{34}\}$, $A_4=\{x_{41}, x_{42}, x_{43}, x_{44}\}$.

임의의 $i(1\le i\le 4)$에 대해 출력 $z_{i1}, z_{i2}, z_{i3}, z_{i4}$는 각각 서로 다른 집합의 원소이다.

$\theta=(\theta_1,\theta_2,\theta_3,\theta_4)$의 조건 :

$\theta_i(1\le i\le 4)$는 $(Z_2^m)^4$ 상에서 정의된 확산 단계로 차분 공격 관점에서의 branch 수 및 선형 공격 관점에서의 branch 수를 5라고 가정한다.

$$\beta_d^{\theta_1}=\beta_d^{\theta_2}=\beta_d^{\theta_3}=\beta_d^{\theta_4}=5,\ \beta_l^{\theta_1}=\beta_l^{\theta_2}=\beta_l^{\theta_3}=\beta_l^{\theta_4}=5$$

혼란이 없을 경우 θ_i를 생략하여 간단히 $\beta_d(\beta_l)$로 쓰기로 한다.

따라서 우리가 고려하는 Rijndael 유사 구조는 확산 단계가 $(\theta_1,\theta_2,\theta_3,\theta_4)\circ\pi$이며, 각 라운드에 16개의 s-box가 작용하는 SPN 구조이다. 블록 암호 Rijndael도 우리가 가정한 조건(π,θ)을 만족한다.

$r(r\ge 2)$ 라운드 Rijndael 유사 구조의 차분 확률을 계산하기 위해 필요한 기호를 다음과 같이 정의한다.

- 입력 차분 :
  $a=(a_1,\cdots,a_4)$
  $=(a_{11}, a_{12}, a_{13}, a_{14}, \cdots, a_{41}, a_{42}, a_{43}, a_{44})$
- 출력 차분 :
  $b=(b_1,\cdots,b_4)$
  $=(b_{11}, b_{12}, b_{13}, b_{14}, \cdots, b_{41}, b_{42}, b_{43}, b_{44})$
- 입력 차분이 a이고 출력 차분이 b인 r 라운드 차분 확률 : $DP_r(a,b)$:
- i 번째 라운드에서 π의 입력 :
  $x^{(i)}=(x_1^{(i)},\cdots,x_4^{(i)})$
  $=(x_{11}^{(i)}, x_{12}^{(i)}, x_{13}^{(i)}, x_{14}^{(i)}, \cdots, x_{41}^{(i)}, x_{42}^{(i)}, x_{43}^{(i)}, x_{44}^{(i)})$
- i 번째 라운드에서 π의 출력, 즉 i 번째 라운드에서 θ의 입력
  $z^{(i)}=(z_1^{(i)},\cdots,z_4^{(i)})$
  $=(z_{11}^{(i)}, z_{12}^{(i)}, z_{13}^{(i)}, z_{14}^{(i)}, \cdots, z_{41}^{(i)}, z_{42}^{(i)}, z_{43}^{(i)}, z_{44}^{(i)})$
- i 번째 라운드에서 θ의 출력
  $y^{(i)}=(y_1^{(i)},\cdots,y_4^{(i)})$
  $=(y_{11}^{(i)}, y_{12}^{(i)}, y_{13}^{(i)}, y_{14}^{(i)}, \cdots, y_{41}^{(i)}, y_{42}^{(i)}, y_{43}^{(i)}, y_{44}^{(i)})$

또 차분 확률의 상한을 간단히 표현하기 위해 다음 정의가 필요하다.

(정의 5)

π의 입력을 $x=(x_1, x_2, x_3, x_4)=(x_{11}, x_{12}, x_{13}, x_{14}, \cdots, x_{41}, x_{42}, x_{43}, x_{44})$ 그리고 출력을 $z=(z_1, \cdots, z_4)=(z_{11}, z_{12}, z_{13}, z_{14}, \ldots, z_{41}, z_{42}, z_{43}, z_{44})$라고 하자. 임의의 $\gamma\in Z_2^4$, $u=(u_1,u_2,u_3,u_4)\in Z^4$에 대해 $N[\gamma,u]$를 다음과 같이 정의한다.

$$N[\gamma,u]=\#\{(\gamma_{z_1},\gamma_{z_2},\gamma_{z_3},\gamma_{z_4})\in(Z_2^4)^4 \mid \gamma_x=\gamma,\ wt(z_i)=u_i, 1\le i\le 4\}$$

위의 정의에서 $N[\gamma,u]$는 잘 정의된다. 즉 π의 조건을 만족하는 어떤 치환에 대해서도 $N[\gamma,u]$의 값은 똑같다. 다음은 $N[\gamma,u]$의 주요 성질로 간단히 증

명할 수 있다.

(i) 적당한 i에 대해 $u_i > wt(\gamma)$이면 $N[\gamma, u]=0$이다 ($\because wt(z_i) \le wt(\gamma_x)$)

(ii) 만일 $u_1+u_2+u_3+u_4 < wt(\gamma)$이면 $N[\gamma, u]=0$이다($\because \sum_{i=1}^{4} wt(z_i) = \sum_{i=1}^{4} wt(x_i) \ge wt(\gamma_x)$)

(iii) 만일 $\max\{u_1, \cdots, u_4\} = wt(\gamma)$이면 다음이 성립한다.

$$N[\gamma, u] = \binom{wt(\gamma)}{u_1} \cdots \binom{wt(\gamma)}{u_4}$$

(iv) $\{1,2,3,4\}$상의 임의의 치환 ϕ와 ρ에 대해 다음 식이 성립한다.

$$N[(\gamma_1, \gamma_2, \gamma_3, \gamma_4), (u_1, u_2, u_3, u_4)] = N[(\gamma_{\phi(1)}, \gamma_{\phi(2)}, \gamma_{\phi(3)}, \gamma_{\phi(4)}), (u_{\rho(1)}, u_{\rho(2)}, u_{\rho(3)}, u_{\rho(4)})]$$

구체적인 γ와 u에 대해 $N[\gamma, u]$의 값을 계산하는 것은 쉽다. 다음 예제의 처음 3개는 각각 위의 성질 (i)~(iii)으로부터 바로 나온다.

예제 1.

$N[(1,1,1,0),(4,1,0,0)]=0.$
$N[(1,1,1,0),(1,1,0,0)]=0.$
$N[(1,1,1,0),(3,2,2,0)]=9.$
$N[(1,1,1,0),(2,1,0,0)]=3.$

2 라운드 Rijndael 유사 구조에 대한 차분 확률의 상한은 보조정리 1에 의해서 쉽게 구할 수 있다.

(정리 1)

2 라운드 Rijndael 유사 구조의 차분 확률 $DP_2(a, b)$의 상한은 다음과 같다.

$$DP_2(a,b) \le \begin{cases} p^{wt(\gamma_{\pi(a)})(\beta_d-1)}, & \gamma_{\pi(a)} = \gamma_b \text{일 때} \\ 0, & \text{그 이외} \end{cases}$$

(증명)

$\pi(a) = (a_1^*, a_2^*, a_3^*, a_4^*)$라고 두자. 그러면 $DP_2(a,b) = \prod_{i=1}^{4} DP_2^{\theta_i}(a_i^*, b_i)$이다. 여기서 $DP_2^{\theta_i}$는 선형변환이 θ_i인 2 라운드 SPN 구조의 차분 확률을 나타낸다. 보조정리 1에 의해서 $DP_2^{\theta_i}(a_i^*, b_i)$의 상한은 다음과 같다.

$$DP_2^{\theta_i}(a_i^*, b_i) \le \begin{cases} p^{\beta_d-1}, & a_i^* \neq 0, b_i \neq 0 \text{일 때} \\ 1, & a_i^* = 0, b_i = 0 \text{일 때} \\ 0, & \text{그 이외} \end{cases}$$

따라서 정리가 증명된다.

위의 정리로부터 2 라운드 Rijndael 유사 구조에 대한 최대 차분 확률의 상한은 p^{β_d-1}이다. 블록 암호 Rijndael에서 $\beta_d=5$, $p=2^{-6}$이므로 2 라운드 Rijndael의 최대 차분 확률의 상한은 2^{-24} 이다.

이젠 2 라운드 구조의 차분 확률의 상한을 이용하여 3 라운드 Rijndael 유사 구조의 차분 확률의 상한을 구해 보자.

(정리 2)

$wt(\gamma_{\pi(a)}) = l$, $wt(b) = k$라고 하자. 또 $b=(b_1, b_2, b_3, b_4)$의 0이 아닌 k개의 component를 $b_{t_1}, \cdots, b_{t_k}$라고 두자. 그러면 3 라운드 Rijndael 유사 구조에 대한 차분 확률 $DP_3(a,b)$의 상한은 다음과 같다.

$$DP_3(a,b) \le p^{l(\beta_d-1)} \sum_{j_1=\beta_d-wt(b_{t_1})}^{l} \cdots \sum_{j_k=\beta_d-wt(b_{t_k})}^{l} M[\gamma_{\pi(a)}, (u_1, u_2, u_3, u_4)] \cdot p^{\sum_{i=1}^{k} \max\{0, \beta_d-j_i-1\}}$$

여기서 $u_i (1 \le i \le 4)$는 아래와 같이 정의된다.

$$u_i = \begin{cases} j_s, & \text{적당한 } t_s \text{에 대해 } i=t_s \text{일 때} \\ 0, & \text{그 이외} \end{cases}$$

(증명)

일반성을 잃지 않고 $t_1=1, \cdots, t_k=k$라고 가정하자. 그러면 정리 1에 의해서 차분 확률 $DP_3(a,b)$는 다음과 같이 유계된다.

$$\begin{aligned} DP_3(a,b) &= \sum_{x^{(2)}} DP_2(a, x^{(2)}) DP_1(y^{(2)}, b) \\ &= \sum_{\gamma_{x^{(2)}} = \gamma_{\pi(a)}} DP_2(a, x^{(2)}) DP_1(y^{(2)}, b) \\ &\le \max_{\gamma_{x^{(2)}} = \gamma_{\pi(a)}} DP_2(a, x^{(2)}) \sum_{y^{(2)}} DP_1(y^{(2)}, b) \\ &\le p^{l(\beta_d-1)} \sum_{y^{(2)}} DP_1(y^{(2)}, b) \end{aligned} \quad (2)$$

여기서,

$y^{(2)} = L(x^{(2)}) = (\theta_1(z_1^{(2)}), \theta_2(z_2^{(2)}), \theta_3(z_3^{(2)}), \theta_4(z_4^{(2)}))$이다. 식 (2)의 합에 사용된 변수 $y^{(2)}$는

다음 조건을 만족한다.

$$\gamma_{y^{(2)}}=\gamma_{b_1},\cdots,\gamma_{y_k^{(2)}}=\gamma_{b_k},$$
$$\gamma_{y_{k+1}^{(2)}}=\cdots=\gamma_{y_4^{(2)}}=0,$$
$$z_1^{(2)}\neq 0,\cdots,z_k^{(2)}\neq 0,$$
$$z_{k+1}^{(2)}=\cdots=z_4^{(2)}=0,$$
$$\gamma_{x^{(2)}}=\gamma_{\pi(a)} \quad (3)$$

각 $i(1\le i\le k)$에 대해 $z_i^{(2)}$와 $y_i^{(2)}$는 각각 θ_i의 0이 아닌 입력과 출력이므로 $wt(z_i^{(2)})+wt(y_i^{(2)})\ge\beta_d$이다. 한편 $wt(b_i)=wt(y_i^{(2)})$이므로 $wt(z_i^{(2)})+wt(b_i)\ge\beta_d$이다. 또 $wt(z_i^{(2)})\le wt(\gamma_{x^{(2)}})$이므로 $wt(z_i^{(2)})$의 범위는 다음과 같다.

$$\beta_d-wt(b_i)\le wt(z_i^{(2)})\le wt(\gamma_{\pi(a)}),\ 1\le i\le k.$$

이젠 $\beta_d-wt(b_i)\le j_i\le wt(\gamma_{\pi(a)})\ (1\le i\le k)$을 만족하는 $j_i(1\le i\le k)$를 고려해 보자. $1\le i\le k$일 때 $wt(\gamma_i)=j_i$, $k+1\le i\le 4$일 때 $wt(\gamma_i)=0$을 만족하는 $(\gamma_1,\cdots,\gamma_4)$에 대해 집합 $A_{(\gamma_1,\cdots,\gamma_4)}$를 다음과 같이 정의한다.

$$A_{(\gamma_1,\cdots,\gamma_4)}=\{y^{(2)}=(y_1^{(2)},\cdots,y_4^{(2)})\mid \gamma_{z_i^{(2)}}=\gamma_i, 1\le i\le 4,\ y^{(2)}\ satisfies\ eq.\ (3)\}$$

위에서 정의한 $A_{(\gamma_1,\cdots,\gamma_4)}$는 공집합이 될 수 있으나 공집합이 아닌 것도 $N[\gamma_{\pi(a)},(j_1,\cdots,j_k,0,\cdots,0)]$개 존재한다. $A_{(\gamma_1,\cdots,\gamma_4)}$가 공집합이 아니면 보조정리 2에 의해서

$$\sum_{y^{(2)}\in A_{(\gamma_1,\cdots,\gamma_4)}} DP_1(y^{(2)},b)$$
$$=\sum_{y_1^{(2)}} DP_1(y_1^{(2)},b_1)\cdots\sum_{y_k^{(2)}} DP_1(y_k^{(2)},b_k)$$
$$\le\prod_{i=1}^{k} p^{\max\{0,\beta_d-j_i-1\}}$$

이다. 따라서

$$\sum_{y^{(2)}} DP_1(y^{(2)},b)$$
$$=\sum_{j_1=\beta_d-wt(b_1)}^{wt(\gamma_{\pi(a)})}\cdots\sum_{j_k=\beta_d-wt(b_k)}^{wt(\gamma_{\pi(a)})} N[\gamma_{\pi(a)},(j_1,\cdots,j_k,0,\cdots,0)]$$
$$\cdot p^{\sum_{i=1}^{k}\max\{0,\beta_d-j_i-1\}}$$

이므로 증명이 완성된다.

4 라운드 Rijndael 유사 구조의 차분 확률의 상한을 구하기 위해 먼저 다음 보조정리들을 증명한다.

(보조정리 3)

$wt(\gamma_{\pi(a)})=2, wt(b)=3$일 때
$DP_4(a,b)\le 4p^{19}+6p^{18}+4p^{17}+p^{16}$이다.

(증명)

일반성을 잃지 않고 $\gamma_b=(1,1,1,0)$이라고 가정하자. $DP_4(a,b)$는 다음과 같이 쓸 수 있다.

$$DP_4(a,b)=\sum_{x^{(3)}} DP_3(a,x^{(3)})DP_1(y^{(3)},b)$$
$$=\sum_{i=1}^{4}\sum_{wt(x^{(3)})=i} DP_3(a,x^{(3)})DP_1(y^{(3)},b)$$
$$:=I+II+III+IV.$$

한편 $wt(z_i^{(2)})\le wt(x^{(2)})=wt(\gamma_{\pi(a)})=2$ 이며 $wt(y_i^{(2)})=wt(x_i^{(3)})\le wt(b)=3$이다. 또 $\beta_d^{\theta_i}=5$이므로 $x^{(3)}$의 0이 아닌 component $x_i^{(3)}$의 weight 값은 3이다. 즉 $wt(x_i^{(3)})=3$이다.

이젠 I의 값을 계산해 보자. I는 다음과 같이 쓸 수 있다.

$$I=\sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a,x^{(3)})DP_1(y^{(3)},b)$$
$$+\sum_{\gamma_{x^{(3)}}=(0,1,0,0)} DP_3(a,x^{(3)})DP_1(y^{(3)},b)$$
$$+\sum_{\gamma_{x^{(3)}}=(0,0,1,0)} DP_3(a,x^{(3)})DP_1(y^{(3)},b)$$
$$+\sum_{\gamma_{x^{(3)}}=(0,0,0,1)} DP_3(a,x^{(3)})DP_1(y^{(3)},b)$$
$$:=I_1+I_2+I_3+I_4.$$

먼저 I_1의 값을 계산해 보자. $wt(x_1^{(3)})=3$이므로 정리 2에 의해서

$$\max_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a,x^{(3)})$$
$$\le p^8\sum_{j=2}^{2} N[\gamma_{\pi(a)},(j,0,0,0)]p^{4-j}=p^{10}$$

이다. 또 $wt(x_1^{(3)})=3$이고 $\gamma_b=(1,1,1,0)$이므로 $(z_1^{(3)},z_2^{(3)},z_3^{(3)},0)$은 $N[(1,1,1,0),(3,0,0,0)]=1$ 개의 패턴을 가진다. 패턴 $(\gamma_1,\gamma_2,\gamma_3,0)$에 대해 보조정리 2에 의해서

$$\sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_1(y^{(3)}, b)$$
$$= \sum_{\gamma_{x_1^{(3)}}=\gamma_1} DP_1(y_1^{(3)}, b_1) \sum_{\gamma_{x_2^{(3)}}=\gamma_2} DP_1(y_2^{(3)}, b_2)$$
$$\sum_{\gamma_{x_3}=\gamma_3} DP_1(y_3^{(3)}, b_3)$$
$$\le p^{12-(wt(\gamma_1)+wt(\gamma_2)+wt(\gamma_3))} = p^9$$

이다. 따라서,

$$I_1 \le \max_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a, x^{(3)}) \sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_1(y^{(3)}, b) \le p^{19}$$

이다. 같은 방법으로 I_2, I_3, I_4도 I_1과 같은 상한을 갖는다. 따라서 $I \le 4p^{19}$이다.

I을 계산한 방법과 같이 II와 III을 계산하면 $II \le 6p^{18}$이며 $III \le 4p^{17}$이다.

마지막으로 IV는 정리 1에 의해서 다음과 같이 계산된다.

$$IV \le \max_{wt(x^{(3)})=4} DP_3(a, x^{(3)})$$
$$= \max_{wt(x^{(3)})=4} \sum_{x^{(1)}} DP_1(a, x^{(1)}) DP_2(y^{(1)}, x^{(3)})$$
$$\le \max_{wt(x^{(3)})=4} \max_{y^{(1)}} DP_2(y^{(1)}, x^{(3)}) \le p^{16}$$

이다. 따라서,

$$DP_4(a, b) = I + II + III + IV \le 4p^{19} + 6p^{18} + 4p^{17} + p^{16}$$

이다.

(보조정리 4)

$wt(\gamma_{\pi(a)}) = 3, wt(b) = 2$일 때

$DP_4(a, b) \le 4p^{19} + 6p^{18} + 4p^{17} + p^{16}$이다.

(증명) 보조정리 3과 같이 증명할 수 있다.

(보조정리 5)

$wt(\gamma_{\pi(a)}) = 3, wt(b) = 3$일 때 $DP_4(a, b)$의 상한은 다음과 같다.

$$DP_4(a, b) \le 184p^{22} + 912p^{21} + 438p^{20} + 72p^{19} + 4p^{18} + p^{16}$$

(증명)

일반성을 잃지 않고 $\gamma_b = (1,1,1,0)$이라고 가정하자. $DP_4(a, b)$는 다음과 같이 쓸 수 있다.

$$DP_4(a, b) = \sum_{x^{(3)}} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$= \sum_{i=1}^{4} \sum_{wt(x^{(3)})=i} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$:= I + II + III + IV.$$

한편 $wt(z_i^{(2)}) \le wt(x^{(2)}) = wt(\gamma_{\pi(a)}) = 3$ 이며 $wt(y_i^{(2)}) = wt(x_i^{(3)}) \le wt(b) = 3$이다. 또 $\beta_d^{\theta_i} = 5$이므로 $x^{(3)}$의 0이 아닌 componen $x_i^{(3)}$의 weight 값은 2 또는 3이다. 즉 $wt(x_i^{(3)}) = 2$ 또는 3이다.

이젠 I의 값을 계산해 보자. I은 다음과 같이 쓸 수 있다.

$$I = \sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$+ \sum_{\gamma_{x^{(3)}}=(0,1,0,0)} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$+ \sum_{\gamma_{x^{(3)}}=(0,0,1,0)} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$+ \sum_{\gamma_{x^{(3)}}=(0,0,0,1)} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$= I_1 + I_2 + I_3 + I_4.$$

먼저 I_1의 값을 계산해 보자. $\sum_{i=1}^{4} wt(x_i^{(3)}) \ge wt(b) = 3$이므로 이 경우 $x^{(3)}$의 0이 아닌 component $x_1^{(3)}$의 weight 값은 3이다. 나머지 부분은 보조정리 3의 증명과 같으며 $I_1 \le p^{22}$. $I \le 4p^{22}$이다.

이젠 II의 계산을 해 보자. $\gamma_{x^{(3)}} = (1,1,0,0)$에 대한 합은 다음과 같이 쓸 수 있다.

$$\sum_{\gamma_{x^{(3)}}=(1,1,0,0)} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$
$$= \sum_{i=2}^{3} \sum_{j=2}^{3} \sum_{wt(x_1^{(3)})=i, wt(x_2^{(3)})=j} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$$

먼저 $\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)$의 상한을 계산해 보자. $wt(x_1^{(3)}) = 2, wt(x_2^{(3)}) = 2$이므로 정리 2에 의해서

$$\max_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)})$$
$$\le p^{12} \sum_{j_1=3}^{3} \sum_{j_2=3}^{3} M[\gamma_{\pi(a)}, (j_1, j_2, 0, 0)] p^{8-j_1-j_2}$$
$$= p^{12} M[(1,1,1,0), (3,3,0,0)] p^2$$
$$= p^{14}$$

이다. 또 $wt(x_1^{(3)})=2, wt(x_2^{(3)})=2$이고 $\gamma_b=(1,1,1,0)$이므로 $(z_1^{(3)}, z_2^{(3)}, z_3^{(3)}, 0)$은 $N[(1,1,1,0),(2,2,0,0)]=6$개의 패턴을 가진다. 각 패턴 $(\gamma_1, \gamma_2, \gamma_3, 0)$에 대해 보조정리 2에 의해서

$$\begin{aligned}&\sum_{\gamma_{z^{(3)}}=\gamma_i, 1\le i\le 3} DP_1(y^{(3)}, b)\\ &= \sum_{\gamma_{z_1^{(3)}}=\gamma_1} DP_1(y_1^{(3)}, b_1) \sum_{\gamma_{z_2^{(3)}}=\gamma_2} DP_1(y_2^{(3)}, b_2)\\ &\quad \sum_{\gamma_{z_3^{(3)}}=\gamma_3} DP_1(y_3^{(3)}, b_3)\\ &\le p^{12-(wt(\gamma_1)+wt(\gamma_2)+wt(\gamma_3))}=p^8\end{aligned}$$

이므로 $\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_1(y^{(3)}, b)\le 6p^8$이다. 따라서

$$\begin{aligned}&\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)\\ &\le \max_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)})\\ &\quad \sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_1(y^{(3)}, b)\\ &\le 6p^{22}\end{aligned}$$

이다. 같은 방법으로

$$\begin{aligned}&\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=3} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)\\ &\quad \le 3(3p^{15}+p^{14})p^7,\\ &\sum_{wt(x_1^{(3)})=3, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)\\ &\quad \le 3(3p^{15}+p^{14})p^7,\\ &\sum_{wt(x_1^{(3)})=3, wt(x_2^{(3)})=3} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)\\ &\quad \le (6p^{16}+6p^{15}+p^{14})p^6\end{aligned}$$

이다. 따라서

$$\begin{aligned}&\sum_{\gamma_{x^{(3)}}=(1,1,0,0)} DP_3(a, x^{(3)}) DP_1(y^{(3)}, b)\\ &\quad \le 6p^{22}+6(3p^{15}+p^{14})p^7+(6p^{16}+6p^{15}+p^{14})p^6\end{aligned}$$

이며, $wt(\gamma_{x^{(3)}})=2$인 다른 $\gamma_{x^{(3)}}$에 대한 합의 상한도 $\gamma_{x^{(3)}}=(1,1,0,0)$에 대한 합의 상한과 같은 값을 가지므로

$$II\le 6[6p^{22}+6(3p^{15}+p^{14})p^7+(6p^{16}+6p^{15}+p^{14})p^6]$$

이다.

*III*의 상한 계산도 *II*의 계산 과정과 같으며

$$\begin{aligned}III \le 4[&24p^{21}+27(3p^{16}+p^{15})p^5\\ &+9(9p^{17}+6p^{16}+p^{15})p^4\\ &+(24p^{18}+27p^{17}+9p^{16}+p^{15})p^3]\end{aligned}$$

이다.

마지막으로 *IV*는 정리 1에 의해서

$$\begin{aligned}IV &\le \max_{wt(x^{(3)})=4} DP_3(a, x^{(3)})\\ &\le \max_{wt(x^{(3)})=4, y^{(1)}} DP_2(y^{(1)}, x^{(3)})\\ &\le p^{16}\end{aligned}$$

이다.

따라서,

$$\begin{aligned}DP_4(a, b) &= I+II+III+IV\\ &\le 184p^{22}+912p^{21}+438p^{20}+72p^{19}+4p^{18}+p^{16}\end{aligned}$$

이다.

다음 정리는 본 논문의 가장 핵심이 되는 결과이다.

(정리 3)

4 라운드 Rijndael 유사 구조의 차분 확률 $DP_4(a, b)$의 상한은 다음과 같다.

$$\begin{aligned}DP_4(a, b)\le \max\{&4p^{19}+6p^{18}+4p^{17}+p^{16}, 184p^{22}\\ &+912p^{21}+438p^{20}+72p^{19}+4p^{18}+p^{16}\}\end{aligned}$$

(증명)

$wt(\gamma_{\pi(a)})$와 $wt(b)$의 값에 따라 $DP_4(a, b)$의 상한을 계산해 보자. $\beta_d=5$이므로 $wt(\gamma_{\pi(a)})+wt(b)\le 4$이면 $DP_4(a, b)=0$이다. 따라서 $wt(\gamma_{\pi(a)})+wt(b)\ge 5$일 때 $DP_4(a, b)$의 상한을 계산하면 된다. 여러 경우로 나누어 이 문제를 해결하고자 한다.

(i) $wt(\gamma_{\pi(a)})=4$일 때

정리 1에 의해서

$$\begin{aligned}DP_4(a, b) &= \sum_{x^{(2)}} DP_2(a, x^{(2)}) DP_2(y^{(2)}, b)\\ &\le \max_{x^{(2)}} DP_2(a, x^{(2)}) \le p^{16}\end{aligned}$$

(ii) $wt(b)=4$일 때

경우 (i)와 같이

$$\begin{aligned}DP_4(a, b) &= \sum_{x^{(2)}} DP_2(a, x^{(2)}) DP_2(y^{(2)}, b)\\ &\le \max_{y^{(2)}} DP_2(y^{(2)}, b) \le p^{16}\end{aligned}$$

(iii) $wt(\gamma_{\pi(a)})=2, wt(b)=3$일 때

보조정리 3에 의해서

$DP_4(a,b)\le 4p^{19}+6p^{18}+4p^{17}+p^{16}$

(iv) $wt(\gamma_{\pi(a)})=3, wt(b)=2$일 때

보조정리 4에 의해서

$DP_4(a,b)\le 4p^{19}+6p^{18}+4p^{17}+p^{16}$

(v) $wt(\gamma_{\pi(a)})=3, wt(b)=3$일 때

보조정리 5에 의해서

$DP_4(a,b)\le 184p^{22}+912p^{21}+438p^{20}+72p^{19}+4p^{18}+p^{16}$

따라서 경우 (i)~(iv)에 의해서 증명이 완성된다.

선형 hull 확률의 상 계산도 차분 확률의 상한 계산과 같은 방법으로 할 수 있다. 따라서 4 라운드 Rijndael-like 구조의 선형 hull 확률의 상한도 정리 3과 같이 쓸 수 있다. 단, p 대신 q로 바꾸면 된다.

(정리 4)

4 라운드 Rijndael 유사 구조의 선형 hull 확률 $LP_4(a,b)$의 상한은 다음과 같다.

$$LP_4(a,b) \le \max\{4q^{19}+6q^{18}+4q^{17}+q^{16}, 184q^{22}+912q^{21}+438q^{20}+72q^{19}+4q^{18}+q^{16}\}$$

한편 5 라운드의 차분 확률은 4 라운드의 최대 차분 확률보다 작거나 같다.

$$DP_5(a,b)=\sum_{x^{(4)}} DP_4(a,x^{(4)})DP_1(y^{(4)},b) \le \max_{x^{(4)}} DP_4(a,x^{(4)})$$

같은 방법으로 $r(r\ge 5)$ 라운드 차분 확률은 4 라운드의 최대 차분 확률보다 작거나 같다. 따라서 정리 3과 4에서 구한 상한은 $r(r\ge 5)$ 라운드에 대한 상한도 된다. 하지만 $r(r\ge 5)$ 라운드일 때 정리 3과 4에서 구한 상한보다 더 좋은 것을 구할 수는 없었다.

이젠 정리 3과 4를 Rijndael 블록 암호에 적용해 보자. Rijndael에서 $p=q=2^{-6}$, $\beta_d=\beta_l=5$이므로 $DP_4(a,b)$와 $LP_4(a,b)$의 상한은

$4\times 2^{-114}+6\times 2^{-108}+4\times 2^{-102}+2^{-96}\sim 1.06\times 2^{-96}$

이다. 최근에 Keliher, Meijer, Tavares[7,8]는 Rijndael 암호에 대한 최대 선형 hull 확률의 상한을 구할 수 있는 알고리즘을 개발하였으며, 라운드의 수가 4일 때 상한은 대략 2^{-80}이며 라운드의 수가 9 이상일 때 상한이 2^{-92}라고 주장하였다. 그들은 43%의 계산을 수행한 후 이런 주장을 하였으며 전체 계산을 마치는데는 Sun Ultra 5로 200,000 시간이 소요될 것으로 예측하였다. 따라서 우리의 결과는 그들의 결과보다 좋을 뿐만 아니라 상한을 계산하기도 아주 쉬우므로 Rijndael 유사 암호의 차분 공격 및 선형 공격에 대한 안전성을 증명하는데 사용할 수 있다.

4. 결 론

본 논문에서는 Rijndael 유사 구조에 대한 최대 차분 확률의 상한과 최대 선형 hull 확률의 상한을 이론적으로 증명하였다. 우리가 얻은 상한은 라운드 수에 의존할 뿐만 아니라 선형변환의 branch 수에도 의존한다. 본 결과는 Rijndael 유사 구조 블록 암호의 차분 공격 및 선형 공격에 대한 안전성을 증명하는데 사용할 수 있다.

참 고 문 헌

[1] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Advance in Cryptology-Crypto'90, LNCS Vol. 537, Springer-Verlag, pp. 2~21, 1991.

[2] J. Daemem, R. Govaerts, and J. Vandewlle, Correlation matrices, Fast Software Encryption-FSE'94, LNCS Vol. 1008, Springer-Verlag, pp. 275~285, 1995.

[3] J. Daemen, L. Knudsen, and V. Rijmen, The block cipher SQUARE, Fast Software Encryption-FSE'97, LNCS Vol. 1267, Springer-Verlag, pp. 149~165, 1997.

[4] J. Daemen and V. Rijmen, AES proposal: Rijndael, http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf.

[5] S. Hong, S Lee, J. Lim, J. Sung, and

D. Cheon, Provable security against differential and linear cryptanalysis for the SPN structure, FSE 2000, LNCS Vol. 1978, Springer-Verlag, pp. 273-283, 2000.

[6] J.-S. Kang, S. Hong, S. Lee, O. Yi, C. Park, and J. Lim, Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks, ETRI J. 23, pp. 158~167, 2001.

[7] L. Keliher, H. Meijer, and S. Tavares, New method for the upper bounding the maximum average linear hull probability for SPNs, Advances in Cryptology - Eurocrypt 2001, LNCS Vol. 2045, Springer-Verlag, pp. 420~436, 2001.

[8] L. Keliher, H. Meijer, and S. Tavares, Improving the upper bound on the maximum average linear hull probability for Rijndael, Selected Areas in Cryptography - SAC 2001, LNCS Vol. 2259, Springer-Verlag, pp. 112~128, 2001.

[9] C. H. Lim, CRYPTON: A new 128-bit block cipher, AES proposal, 1998.

[10] C. H. Lim, A revised version of CRYPTON-CRYPTON V1.0, FSE'99, LNCS Vol. 1636, Springer-Verlag, pp. 31~45, 1999.

[11] M. Matsui, Linear cryptanalysis method for DES cipher, Advance in Cryptology-Eurocrypt'93, LNCS Vol. 765, Springer-Verlag, pp. 386~397, 1994.

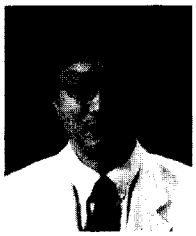
[12] NTT-Nippon Telegraph and Telephone Corporation, Specification of E2 - a 128 bit block cipher, AES proposal(available at http://info.isl.ntt.co.jp/e2/), 1998.

〈著者紹介〉

박 상 우 (Sangwoo Park) 정회원
1989년 2월 : 고려대학교 수학교육과 졸업
1991년 8월: 고려대학교 수학과 석사
1991년 8월~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 선임연구원

성 수 학 (Soo Hak Sung) 정회원
1982년 2월 : 경북대학교 수학과(학사)
1985년 2월 : KAIST 응용수학과(석사)
1988년 2월 : KAIST 응용수학과(박사)
1988년~1991년 : 한국전자통신연구원 선임연구원
1991년~현재 : 배재대학교 전산정보수학과 교수

지 성 택 (Seongtaek Chee) 정회원
1985년 2월 : 서강대학교 수학과 졸업
1987년 2월 : 서강대학교 수학과 석사
1999년 2월 : 고려대학교 수학과 박사
1989년~1999년 12월 : 한국전자통신연구원 선임연구원
2000년 1월~현재 : 국가보안기술연구소 책임연구원



윤 이 중 (E-Joong Yoon) 정회원
1990년 2월 : 인하대학교 전사과 석사
2002년 2월 : 충남대학교 컴퓨터과학과 박사
1990년 2월~2001년 2월 : 한국전자통신연구원 정보보호시스템연구부장
2001년 2월~현재 : 국가보안기술연구소 기반기술연구부장

임 종 인 (Jong-In Lim) 정회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사(대수학 전공)
1986년 2월 : 고려대학교 수학과 박사(대수학 전공)
1986년 2월~현재 : 고려대학교 수학과 정교수
2000년 10월~현재 : 고려대학교 정보보호 대학원 원장
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 암호프로토콜, 공개키 암호 알고리즘의 분석