SPN 구조의 의사 난수성에 대한 향상된 결과

이 원 일*, 홍 석 희*, 성 재 철**, 이 상 진*

* 고려대학교 정보보호기술연구센터

** 한국정보보호진흥원

Improved Result on the Pseudorandomness of SPN-type transformation

Wonil Lee*, Seokhie Hong*, Jaechul Sung*, Sangjin Lee*

* CIST, Korea University

** KISA, Korea

요 약

Iwata 등은 SPN 구조에 기반한 블록 암호들 중 Serpent에 대한 의사 난수성을 분석하였다 [2]. 그들은 Serpent의 구조를 최대한 보존한 상태에서 의사 난수성을 분석하기 위하여 Serpent의 Diffusion layer의 특성을 그대로 보존하여 일반화 한 후 이론을 전개하였다. 본 논문에서는 Serpent가 취한 Diffusion layer 뿐만 아니라 SPN 구조에 기반한 블록 암호들이 취할 수 있는 임의의 Diffusion layer에 대하여 적용 가능한 일반적인 이론을 도출해낼 것이다.

I. 서론

블록 암호의 의사 난수성에 대한 연구는 DES나 Rijndael과 같은 구체적인 블록 암호에 대한 분석(예를 들면 차분 및 선형 공격)과는 기본적으로 다른 방향에서의 연구이다. 블록 암호의 의사 난수성에 대한 연구는 블록 암호가 취하는 기본 구조에 대한 증명 가능한 안전성을 복잡도 이론에 기반하여 제시하고자 하는 분야이다.

블록 암호의 의사 난수성에 대한 연구는 처음 Luby 와 Rackoff [1]에 의하여 시작되었다. 정확히 말하면 Luby 와 Rackoff는 블록 암호 구조의 의사 난수성을 보이고자 연구를 시작한 것이 아니라 그 당시 중요한 문제였던 '의사 난수 함수(pseudorandom function)가 존재할 때 의사 난수 순열(pseudorandom permutation)'을 어떻게 구성할 수 있을 것인가에 대한 한 가지 해답으로써 당시 유명했던 블록 암호인 DES의 구조(Fesitel 구조)를 이용하여 이를 보인 것이다.

그 이후 Luby 와 Rackoff가 제시한 의사 난수 함수를 이용한 의사 난수 순열 구성 방법을 더욱 효율적으로 만들기 위한 시도가 계속되었고 또한 DES 구조가 아닌 다른 구조들 (예를 들면 MISTY, KASUMI, RC6 등)에 기반하여 의사 난수 순열을 구성하기 위한 방법들이 제안되었고 분석되어져 왔다 [2,3,4,5,6].

그러나 블록 암호의 기본 구조 중 SPN 구조에 대한 연구는 Iwata 등이 처음이었다 [2]. 그들은 SPN 구조에 기반한 Serpent를 이론적으로 모델링하여 이에 대한 의사 난수성을 분석하였다. 여기서 주목할 점은 SPN 구조의 의사 난수성 연구에서 먼저 주어지는 것은 작은 크기의 의사 난수 순열이라는 것이다. 따라서 이때는 작은 크기의 의사 난수 순열을 이용하여 더욱 큰 크기의 의사 난수 순열을 만드는 것이 목적이 된다.

Iwata 등은 Diffusion layer를 Serpent 특성에 맞게 이론적으로 모델링하여 이론을 전개하였다. 여기서 주목할 점은 SPN 구조에 기반한 블록 암호들이 취할 수 있는 Diffusion layer는 여러 가지

가 있을 수 있다는 사실이다. Iwata는 이러한 여러 가지 Diffusion layer 중에서 Serpent가 이용한 것에 대한 이론만을 전개하였다. 본 논문은 이점에 착안하여 임의의 Diffusion layer에 대한 일반적인 이론을 도출해 내고자 노력한 과정에서 얻어낸 결과이다.

본 논문의 결과를 간략히 요약하면 다음과 같다. 본문에서 정의한 라운드 함수를 이용하여 설명할 때 처음 평문의 한 단어가 Diffusion layer에 의하여 각각의 단어(word)들에 모두 영향을 주게 되는 최소의 라운드에서는 의사 난수 순열을 만들 수 없고 그 라운드 수 보다 한 라운드 더 적용할 경우 의사 난수 순열이 된다는 것이다. 좀 더 정확한 설명은 본문에 자세하게 언급될 것이다. 우선 이를 위하여 약간의 준비 단계를 필요로 한다.

II. 준비 단계

I_n은 모든 n비트 이진 수열들의 집합을 나타낸다. 즉 $I_n=\{0,1\}^n$이다. F_n은 I_n에서 I_n으로 가는 모든 함수들의 집합을 나타낸다. P_n은 I_n에서 I_n으로 가는 모든 n비트 순열(전단사 함수)들의 집합을 나타낸다. 따라서 $P_n \subset F_n$이 성립한다. 본 논문에서 우리는 P_n에 대해서만 관심이 있다.

N을 자연수들의 집합, R을 실수들의 집합이라고 할 때에 어떤 함수 $h:N\rightarrow R$ 가 임의의 양의 상수 c에 대하여 어떤 자연수 M이 존재하여 모든 $n>M$에 대하여 $h(n)<\frac{1}{n^c}$ 가 만족한다면 이 때 h를 무시할 만한 함수(negligible function)라고 하자.

'순열 앙상블'(permutation ensemble)이란 어떤 분포들의 열(squence) $H=\{H_n\}_{n\in N}$ 을 나타낸다. 이 때 각각의 $n\in N$에 대하여 H_n은 P_n 위에서의 어떤 분포를 나타낸다. 어떤 순열 앙상블 $R=\{R_n\}_{n\in N}$이 임의의 $n\in N$에 대하여 R_n이 P_n 위에서의 균일 분포(uniform distribution)를 나타낸다면 이 때 우리는 $R=\{R_n\}_{n\in N}$ 를 '균일 순열 앙상블'(uniform permutation ensemble)이라고 부르기로 하자.

어떤 순열 앙상블 $H=\{H_n\}_{n\in N}$ 이 계산이 용이하다(efficiently computable)고 말하는 경우는 다음과 같다. 즉, 각 분포 H_n이 효율적으로 구현되고 또한 H_n 안에서 발생하는 함수 f 들이 효율적으로 계산될 수 있는 경우이다.

우리는 균일 순열 앙상블로부터 구별 불가능한 계산이 용이한 순열 앙상블에 관하여 관심이 있다. 본 논문에서 구별자(distinguisher)는 어떤 오라클에게 t개의 질문을 던질 수 있으며 최종적으로 한 비트를 출력으로 내는 오라클 머신이다.

여기서 우리는 입력 1^n에 대하여 구별자 A는 오직 n비트 크기의 질문들만을 던질 수 있다고 가정한다. 여기서 n은 안전성 파라미터의 역할을 한다.

A를 어떤 구별자라고 하자. 그리고 f를 P_n의 한 함수라고 하자. H_n은 P_n 위에서의 어떤 분포라고 하자. 이 때 $A^f(1^n)$은 A가 오라클에게 던지는 질문에 대한 답이 f로부터 얻어질 때의 A의 출력의 분포라고 하자. 또한 f가 H_n에 따라 분포되었을 때의 $A^f(1^n)$의 분포를 $A^{H_n}(1^n)$라고 표현하자. 이 때 구별자 A의 구별 이득(advantage) 함수 $Adv_A:N\rightarrow R$를 다음과 같이 정의한다.

$$Adv_A(n)=|\Pr[A^{H_n}(1^n)=1]-\Pr[A^{R_n}(1^n)=1]|$$

만일 H가 계산이 용이한 분포들의 열이고 임의의 효율적인 구별자 A에 대하여 Adv_A가 무시할 만한 함수라면 이 때 H를 의사 난수 순열 앙상블(pseudorandom permutation ensemble)이라고 부르기로 하자.

만일 함수 f가 의사 난수 순열 앙상블에 따라서 분포되었을 때 우리는 함수 f를 의사 난수 순열이라고 간단히 언급하기로 약속한다.

본 논문에서는 모든 질문을 오라클에서 동시에 보내는 비능동적(non-adaptive) 구별자에 대해서만 다루기로 한다.

III. SPN 구조의 의사 난수성

이번 절에서 우리는 블록 암호 구조 중 잘 알려진 SPN 구조의 의사 난수성에 대하여 알아본다. 잘 알려진 바와 같이 SPN 구조에서 중요한 부분은 Diffusion layer이다. Diffusion layer는 블록 암호가 지향해야 할 중요한 성질인 확산 효과를 발

생시키는 아주 중요한 요소이다. 본 논문에서 우리는 특정한 Diffusion layer에 국한된 의사 난수 이론이 아닌 임의의 Diffusion layer에도 적용될 수 있는 이론을 언급하고자 한다. 우선 SPN 구조에 대한 정확한 정의를 살펴보면 다음과 같다.

정의 1. 어떤 고정된 상수 m 이 정해져 있다고 하자. 임의의 n 비트 순열(permutation) $f_1, f_2, \ldots, f_m \in P_n$ 에 대하여 mn 비트 SPN 기본 순열 $G_{\hat{g}} \in P_{mn}$ ($\hat{g}=(f_1, \ldots, f_m)$) 는 다음과 같이 정의된다.

$G_{\hat{g}}(x_1, \ldots, x_m) = D(f_1(x_1), \ldots, f_m(x_m))$여 기서 $x_1, \ldots, x_m \in I_n$ 이고 D는 I_{mn}에서 I_{mn}으로 가는 임의의 Diffusion layer이다. □

이 기본 순열 $G_{\hat{g}}$를 라운드 함수라고 부르기도 한다. 이를 그림으로 표현하면 아래와 같다.

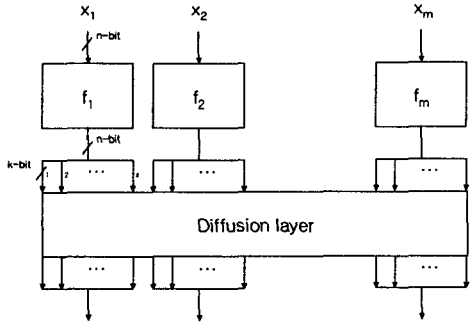

그림 1 mn 비트 SPN 구조 (s * k = n)

본 논문에서 우리는 I_n의 각 원소를 하나의 단어(word)라고 부르기로 하자. 위의 정의에서 D는 임의의 Diffusion layer가 될 수 있다. 예를 들면 D는 Serpent 블록 암호의 bit-wise diffusion layer에 기반하여 일반화 될 수 있다. 또한 Crypton의 2-bit-wise diffusion layer에 기반하여 일반화 될 수도 있고 Rijndael의 byte-wise diffusion layer에 기반하여 일반화 될 수도 있다. 여기서 주목할 점은 의사 난수성 이론에서 다루고 있는 블록 암호 구조의 안전성은 점진적 행동(asymptotic behavior)에 초점이 맞추어져 있다는 것이다. 그러므로 우리는 어떤 Diffusion layer의 입력으로 들어가는 각각의 n 비트 입력 단어를 점진적 행동에 초점을 맞추어 분석하기 위하여 어떤 고정된 상수 s개의 k 비트 데이터로 간주하고 이 때 k가 점진적으로 증가한다고 생각할 것이다. 즉, 다시 말하면 m과 s는 고정된 상수이며 k 만이 점진적으로 증가하는 변수이다. 구체적으로 예를 들면 Serpent의 경우 ($m=32, s=4$) 이고 Crypton의 경우 ($m=16, s=4$) 이고 Rijndael의 경우에는 ($m=16, s=1$) 로 볼 수 있다. 이러한 값들은 각각의 블록 암호 구조가 포함하고 있는 Diffusion layer에 의하여 결정된다.아래에서는 mn 비트 SPN 기본 순열을 이용하여 r 라운드 mn 비트 SPN 순열을 정의한다.

정의 2. $\hat{g_1}=(f_{11}, \ldots, f_{1m}), \ldots, \hat{g_r}=(f_{r1}, \ldots, f_{rm})$이 주어져 있다고 가정하자. 이 때 r 라운드 mn 비트 SPN 순열 $G^r \in P_{mn}$ 은 다음과 같이 정의된다.

$$G^r(x_1, \ldots, x_m) = G_{\hat{g_r}} \circ \cdots \circ G_{\hat{g_1}}(x_1, \ldots, x_m)$$

여기서 $x_1, \ldots, x_m \in I_n$ 이다. □

다음은 r 라운드 mn 비트 SPN 순열 안에서 발생하는 확산 효과를 표현하기 위한 정의이다. 이 정의를 이용하면 본 논문의 중요 결과를 효율적으로 설명할 수 있다.

정의 3. 어떤 r 라운드 mn 비트 SPN 순열 G^r이 주어져 있다. 이 때 $Avalanche_j(i)$를 j 번째 라운드 이후의 변화된 m 개의 단어들 중에서 처음 m 개의 단어들로 이루어진 평문 중 i 번째 단어에 의하여 영향을 받는 단어들의 총 개수라고 하자. 이 때 $1 \le i \le m, 1 \le j \le r$ 이다. 이 때 $MAX(j)$ 와 $MIN(j)$는 다음과 같이 정의된다.

$$MAX(j) = \max_{1 \le i \le m} \{Avalanche_j(i)\}$$

$$MIN(j) = \min_{1 \le i \le m} \{Avalanche_j(i)\}$$ □

정의 4. 어떤 r 라운드 mn 비트 SPN 순열 G^r이 주어져 있다. 만일 $MIN(r) = m$ 이라면 $RMIN(G^r)$ 은 다음과 같이 정의된다.

$$RMIN(G^r) = \min \{j \mid MIN(j) = m \text{ and } 1 \le j \le r\}$$

□

아래의 두 정리 1, 2는 본 논문의 주요 결과이다.

정리 1. 어떤 r 라운드 mn 비트 SPN 순열 G^r이 주어져 있다. 이 때 $f_{11},\ldots,f_{rm}$ 이 각각 독립적으로 어떤 의사 난수 순열 앙상블의 분포에 따라서 선택되었다고 가정하자. 이 때 만일 $RMIN(G^r)=r$ 이라면 G^r은 의사 난수 순열이 아니다.

증명) 우선 $\delta_j=(\delta_{j1},\ldots,\delta_{jm})$을 j 번째 라운드 후의 변화된 m개의 단어들을 나타내는 표현으로 놓자. 가정에 의하여 $RMIN(G^r)=r$ 이므로 $MIN(r-1)<m$ 이 성립한다. 따라서 어떤 $1\le v,w\le m$가 존재하여 $r-1$ 라운드 후에도 평문 중의 한 단어인 x_v에 의하여 영향을 받지 않는 단어 $\delta_{(j-1)w}$ 가 존재한다.

G^r이 의사 난수 순열이 아님을 보이기 위하여 우리는 효율적인 계산시간에 높은 구별 이득(advantage)을 가지고 공격에 성공하는 구별자 A를 다음과 같이 구성할 것이다.

1. A는 두 개의 평문 $x^{(1)}=(x_1^{(1)},\ldots,x_m^{(1)})$, $x^{(2)}=(x_1^{(2)},\ldots,x_m^{(2)})$를 선택한다. 이 때 $x_v^{(1)}\neq x_v^{(2)}$ 가 성립하고 모든 $i\neq v$ 에 대하여 $x_i^{(1)}\neq x_i^{(2)}$ 가 성립한다.

2. A 는 위의 두 개의 평문 $x^{(1)}$과 $x^{(2)}$를 오라클에게 보낸 후 이에 대한 답으로 r 라운드 후의 암호문 $y^{(1)}=(y_1^{(1)},\ldots,y_m^{(1)})$, $y^{(2)}=(y_1^{(2)},\ldots,y_m^{(2)})$ 를 얻는다.

3. A 는 다음을 계산 한다.

$\gamma^{(1)}\leftarrow D^{-1}(y^{(1)})$, $\gamma^{(2)}\leftarrow D^{-1}(y^{(2)})$

4. 만일 $\gamma_w^{(1)}=\gamma_w^{(2)}$가 성립하면 A 는 출력으로 1을 내보내고 그렇지 않으면 0을 내보낸다.

만일 오라클이 R의 분포를 따라서 답을 주었을 경우에 $\Pr[A^{R_r}(1^n)=1]=\frac{1}{2^n}$ 이 성립한다.

만일 오라클이 G^r의 구성 방법에 의하여 형성된 H에 따라 답을 주었을 경우 $\Pr[A^{H_r}(1^n)=1]=1$ 이 된다. 따라서 $Adv_A(n)=1-\frac{1}{2^n}$이 되므로 이는 무시할 만한 함수가 아니다. 그러므로 G^r은 의사 난수 순열이 아니다. □

정리 2. 어떤 $r+1$ 라운드 mn 비트 SPN 순열 G^{r+1}이 주어져 있다. 이 때 $f_{11},\ldots,f_{(r+1)m}$이 각각 독립적으로 어떤 의사 난수 순열 앙상블의 분포에 따라서 선택되었다고 가정하자. 이 때 만일 $RMIN(G^r)=r$ 이라면 G^{r+1}은 의사 난수 순열이다.

증명) 우선 $f_{11},\ldots,f_{(r+1)m}$ 각각이 독립적으로 R의 균일 분포들의 열에 따라 선택되었다고 가정하자. 그리고 G^{r+1}의 구성 방법에 의하여 형성된 분포들의 열을 H 라고 하자. 그리고 $\delta_j=(\delta_{j1},\ldots,\delta_{jm})$을 j 번째 라운드 후의 변화된 m개의 단어들을 나타내는 표현으로 놓자.

그리고 구별자 A는 총 t (n에 대한 다항식으로 표현됨) 개의 질문을 던질 수 있다고 가정하자. i 번째 질문에서 A는 $x^{(i)}=(x_1^{(i)},\ldots,x_m^{(i)})$를 오라클에게 보낸 뒤 답으로 $y^{(i)}=(y_1^{(i)},\ldots,y_m^{(i)})$를 받는다. 이 때 질문 $x^{(i)}$들은 서로 다르다고 가정하자. 이제 각각의 $u=1,\ldots,m$에 대하여 $\varepsilon[\delta_{ru}]$를 $\delta_{ru}^{(1)},\ldots,\delta_{ru}^{(t)}$가 모두 서로 다른 경우가 발생하는 사건을 나타내기로 하자. 그리고 $\varepsilon[\delta_r]$을 $\varepsilon[\delta_{r1}],\ldots,\varepsilon[\delta_{rm}]$이 모두 다같이 발생할 사건을 나타내기로 하자. 만일 $\varepsilon[\delta_r]$이 발생한다면 $y^{(1)},\ldots,y^{(t)}$은 완전히 랜덤하게 될 것이다. 왜냐면 $f_{(r+1)1},\ldots,f_{(r+1)m}$ 이 모두 완전한 랜덤 수열(truly random permutation)들이기 때문이다. 그러므로 임의의 구별자 A의 구별 이득 Adv_A은 다음과 같은 상한을 가진다.

$$Adv_A\le 1-\Pr[\varepsilon[\delta_r]]$$

또한 이는 아래와 같은 부등식을 이용하여 상한을 구할 수 있다.

$$Adv_A\le 1-\Pr[\varepsilon[\delta_r]]$$

$$\le \sum_{1\le i(\neq)\le t}\Pr[\delta_{r1}^{(i)}=\delta_{r1}^{(j)}]+\cdots\sum_{1\le i(\neq)\le t}\Pr[\delta_{rm}^{(i)}=\delta_{rm}^{(j)}]$$

위의 식에서 각각의 $\Pr[\delta_{nu}^{(i)}=\delta_{nu}^{(j)}]$ 에 대하여 확률의 상한을 계산한 후 전체 식의 상한을 계산하면 된다. 여기서 우리는 중간 계산 과정에서 앞의 어떤 단어에 의하여 영향을 받은 단어는 적어도 ck 비트 이상 영향을 받는다고 가정한다. 이 때 $1\le c\le s$, $n=s\times k$ 이다. 이 때 c는 각각의 Diffusion layer에 의존하여 결정되는 상수이다.

구체적인 확률 상한 값 계산은 지면이 늘어나는 이유로 생략하기로 한다. 그러나 이 계산은 Iwata 등의 증명 방법 [2]과 매우 유사하므로 이 논문을 참고 하면 누구나 쉽게 증명할 수 있을 것이다. 최종적으로 얻을 수 있는 구별 이득의 상한값은 아래와 같다.

$$Adv_A \le \frac{mt(t-1)}{2} \times \frac{MAX(r-1)[MAX(r-2)[\ldots[MAX(1)+1]\ldots]+1]+1}{2^{\frac{cn}{s}}}$$

여기서 t, m, r, c, s 는 모두 상수이다. 그러므로 이는 무시할 만한 함수이다. □

IV. 결론 및 고려 사항

본 논문에서는 Serpent가 취한 Diffusion layer 뿐만 아니라 SPN 구조에 기반한 블록 암호들이 취할 수 있는 임의의 Diffusion layer에 대하여 적용 가능한 일반적인 이론을 제시하였다. 그러나 여기서 앞으로 더욱 고려해야 할 사항은 다음과 같다. 만일 구체적인 블록 암호의 총 단어 수가 m개라고 하자. 그리고 이 블록 암호의 Diffusion layer가 각각의 단어에서 오직 한 비트 씩 만을 끌어내어 잘 섞는 함수라고 가정해보자. 이러한 Diffusion layer는 명백히 아주 좋지 않은 함수이다. 그러나 우리가 전개한 이론은 점진적인 행동에 관심이 있으므로 각 비트를 임의의 k비트로 확장하여 이론을 전개하였기에 이러한 Diffusion layer에 대해서도 전체적인 안전성 증명은 가능하였다. (물론 이러한 Diffusion layer를 가지는 구조에 대한 공격자의 이익 함수의 상한은 더욱 커지게 된다.) 따라서 앞으로는 Diffusion layer의 특성에 따라 좀 더 세분화하여 증명 가능한 안전성을 제시할 수 있는 방법에 대한 연구가 필요하다.

참고문헌

[1] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudoran -dom functions," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373-386, April. 1988.

[2] T. Iwata and K. Kurosawa, "On the pseudorandomness of the AES finalists-RC6 and Serpent," *FSE Workshop 2000, LNCS 1978, Springer-Verlag*, pp. 231-243, 2000.

[3] U. M. Maurer, "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators," *Advances in Cryptology-Eurocrypt'92, LNCS Vol. 658, Springer-Verlag*, 1992, pp. 239--255.

[4] Ju-sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho "Pseudorandomness of MISTY-type transformations and the block cipher KASUMI", *ACISP 2001, LNCS 2119, Springer-Verlag*, 2001, pp.205-318.

[5] K. Sakurai and Y. Zheng, "On non-pseudorandomness from block ciphers with provable immunity against linear cryptanalysis", *IEICE Trans. Fundamentals, Vol. E80A, No. 1*, 1997, pp. 19-24.

[6] M. Naor and O. Reingold, "On the construction of pseudorandom permutations: Luby-Rackoff revisited", *Journal of Cryptology, Vol.12*, 1999, pp. 29-66.