情報保護學會論文誌
第14券 第1號, 2004. 2

SPN 블록 암호 구조의 의사 난수성에 대한 향상된 결과

이 원 일†

고려대학교 정보보호기술연구센터

Improved Result on the Pseudorandomness of SPN-type transformations

Wonil Lee†

CIST, Korea University

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. 또한 이러한 일반적인 이론을 Serpent, Crypton, Rijndael 등과 같은 블록 암호들에 적용한 결과를 제시할 것이다.

ABSTRACT

Iwata et al. analyzed the pseudorandomness of the block cipher Serpent which is a SPN-type transformation.[7] In this paper, we introduce a generalization of the results, which can be applied to any SPN-type transformation. For the purpose, we give several explicit definitions and prove our main theorems. We will also apply our theorems to several SPN-type transformations including Serpent, Crypton and Rijndael.

Keywords: *Block cipher, SPN-type transformation, Pseudorandomness*

Ⅰ. Introductionc

Luby and Rackoff[1] introduced a theoretical model for the security of block ciphers by using the notion of pseudorandomness. The purpose of the security analysis using the notion of pseudorandomness is to measure the security of the structures used in the block ciphers. Roughly speaking, the security of the structure is analyzed after the main functions(such as round functions in Feistel-type transformations or S-boxes in SPN-type transformations) is replaced with a pseudorandom function or pseudorandom permutation. With this model, Luby and Rackoff showed that the three round DES is a pseudorandom permutation and the four round DES is a super-pseudorandom permutation.[1] Maurer gave a simpler proof for non-adaptive adversaries.[2] Since the

접수일: 2003년 12월 26일; 채택일: 2004년 2월 3일
† wonil@cist.korea.ac.kr

structure of Twofish has the same as DES, the three round Twofish is a pseudorandom permutation and the four round Twofish is a super-pseudorandom permutation. MARS has a so called Type-3 Feistel structure. At the rump session of AES2, Vaudenay and Moriai claimed that the five round MARS is a pseudorandom permutation.[3] The block ciphers such as RC6,[4] MISTY[5] and KASUMI[6] were also analyzed by many people on the view point of pseudorandomness.[7~9] Note that these block ciphers are not SPN-type transformations.

In this paper we will focus on analyzing SPN-type transformations by using the notion of pseudorandomness. Actually, there was a result about Serpent which is a SPN-type transformation.[7] Iwata et al. proved that the two round Serpent,[10] in which the diffusion layer is left untouched and only the S-boxes are replaced with pseudorandom permutations, is not a pseudorandom permutation but the three round Serpent is a pseudorandom permutation. The reason that they did not touch the diffusion layer is very natural because the structure of a SPN-type transformation completely depends on its diffusion layer. So it seems that there is no way to obtain a generalizd result which can be applied to any SPN-type transformation because there are many different diffusion layers in this world. In other words, it seems that the analysis should be differently treated depending on the shape of a diffusion layer. But, in this paper we will show that there is a generalized result which can be applied to any SPN-type transformation. A specified SPN-type transformation depending on a diffusion layer will have an effect on the assumption of our theorems. The details will be explained with several definitions. At the end of the paper, we will also apply our results to several SPN-type transformations including Serpent, Crypton and Rijndael.

II. Preliminaries

We denote by I_n the set of all n-bit data. Let Ω_n be the set of all permutations from I_n to itself.

Definition 1. Ω_n is called a TPE(truly random permutation ensemble) if all permutations in Ω_n are uniformly distributed. That is, for any permutation $\pi \in \Omega_n$, $\Pr(\pi) = \frac{1}{2^n!}$.

We consider the following security model. Let D be computationally unbounded distinguisher with an oracle O. The oracle O randomly chooses a permutation π from the TPE Ω_n or from a permutation ensemble $\Psi_n \subseteq \Omega_n$. For an n-bit block cipher, Ψ_n is the set of permutations obtained from all the secret keys. The purpose of the distinguisher D is to distinguish whether the oracle O implements the TPE Ω_n or Ψ_n. We give several definitions in order to measure the ability of the distinguisher.

Definition 2. Let D be a distinguisher, Ω_n be a TPE, and Ψ_n ($\subseteq \Omega_n$) be a permutation ensemble. The advantage Adv_D of the distinguisher D is defined by

$$Adv_D = |p^{\Omega_n} - p^{\Psi_n}|$$

where

$$\begin{cases} p^{\Omega_n} = \Pr(D \text{ outputs } 1 \mid O \leftarrow \Omega_n) \\ p^{\Psi_n} = \Pr(D \text{ outputs } 1 \mid O \leftarrow \Psi_n) \end{cases}$$

Assume that the distinguisher D is restricted to make at most $poly(n)$ queries to

the oracle O, where $poly(n)$ is some polynomial in n. We call D is a pseudorandom distinguisher if it queries x and the oracle answers $y=\pi(x)$, where π is a randomly chosen permutation by O.

Definition 3. A function $h:N\rightarrow R$ is negligible if for any constant $c>0$ and all sufficiently large $m\in N$,

$$h(m)<\frac{1}{m^c}$$

Definition 4. Let Ψ_n be an efficiently computable permutation ensemble, where "efficiently computable" means that all permutations in the ensemble can be efficiently computed. We call Ψ_n is a PPE(pseudor andom permutation ensemble) if Adv_D is negligible for any pseudorandom distinguisher D.

Throughout this paper, we consider a non-adaptive distinguisher which sends all the queries to the oracle at the same time.

Ⅲ. Pseudorandomness of SPN-type transformations

In this section we define formally a popular class of block ciphers, known as SPN -type transformations. It is well known that a diffusion layer palys an important role in a SPN-type transformation. The diffusion layer provides an avalanche effect which is a desirable property of any encryption algorithm. So we give a explicit definition which expresses an avalanche effect in a SPN-type transformation. The definition will be very useful in proving our theorems.

Definition 5. For any n-bit permutations $f_1,\ldots,f_m\in\Omega_n$, a mn-bit SPN-type transformation $G_g\in\Omega_{mn}(\hat{g}\triangleq(f_1,\ldots,f_m))$ is defined by

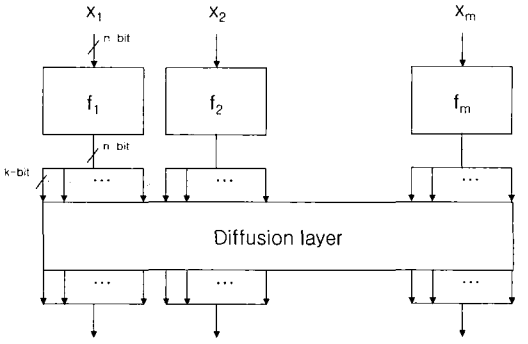

Fig. 1 mn-bit SPN Structure (s * k = n)

$$G_g(x_1,\ldots,x_m)=D(f_1(x_1),\ldots,f_m(x_m))$$

where $x_1,\ldots,x_m\in I_n$ and D is any diffusion layer from I_{mn} to itself.

In this paper an element of I_n will be called by a word. In the above definition, D is any diffusion layer. So, for example D can be the bit-wise diffusion layer used in Serpent, the 2-bit-wise diffusion layer used in Crypton or byte-wise diffusion layer used in Rijndael(See[10-13] for the detailes). So we will describe each n-bit input word to a diffusion layer as s k-bit data in order to model arbitrary diffusion layer including that of Serpent, Crypton and Rijndael(See Fig. 1). As you know, this modeling is a basic step to analyze structures used in block ciphers on the view point of pseudorandomness. The values of m and s will be determined by a given SPN-type transformation but k will be a variable included in the domain N of the function h in Definition 3. As examples, we can actually model diffusion layers of Serpent, Crypton and Rijndael. As you can see in those figures, it is determined that $(m=32, s=4)$, $(m=16, s=4)$, and $(m=16, s=1)$

for Serpent, Crypton and Rijndael respectively. It is obvious that these values are determined by their internal structures. We will explain the details about these examples in section 4. In Section 4, we will also apply our theorems to these models of the block ciphers.

Definition 6. Let $\widehat{g_1}=(f_{11},\ldots,f_{1m}),\ldots,\widehat{g_r}=(f_{r1},\ldots,f_{rm})$ be given. Then the r round mn-bit SPN-type transformation G^r is defined by

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

where $x_1,\ldots,x_m\in I_n$.

The following definition expresses an avalanche effect in a SPN-type transformation. It is well known that the avalanche effect is completely determined by the diffusion layer of the SPN-type transformation. The definition will be very useful in proving our theorems.

Definition 7. Let a r round mn-bit SPN-type transformation G^r be given. Let $(x_1,\ldots,x_m)$ be a plaintext to G^r. We denote by $Avalanche_j(x_i)$ the number of words which are influenced by x_i after the j-th round $(1\le i\le m\ ,1\le j\le r)$. At this time, MAX_j and MIN_j are defined by

$$MAX_j=\max_{1\le i\le m}\{Avalanche_j(x_i)\}$$
$$MIN_j=\min_{1\le i\le m}\{Avalanche_j(x_i)\}$$

Definition 8. Let a r round mn-bit SPN-type transformation G^r be given. If $MIN_r=m$, then $RMIN$ is defined by

$$RMIN=\min_{1\le j\le r}\{j\mid MIN_j=m\}.$$

In the following we introduce our main results which can be applied to any SPN-type transformation.

Theorem 1. Let a r round mn-bit SPN-type transformation G^r in which $f_{11},\ldots,f_{rm}$ are independently chosen from a n-bit PPE be given. If $RMIN=r$, then the G^r is not a pseudorandom permutation.

Proof : Let Ψ_{mn} be the set of all permutations over I_{mn} obtained from the G^r and the j-th round output of this transformation is denoted by $\delta_j=(\delta_{j1},\ldots,\delta_{jm})$. Since $RMIN=r$, $MIN_{r-1}<m$. So there exist v and w $(1\le v, w\le m)$ such that $\delta_{(r-1)w}$ is not influenced by x_v after $(r-1)$-th round. Consider a distinguisher D such as follows.

1. D chooses two plaintexts, $x^{(1)}=(x_1^{(1)},\ldots,x_m^{(1)})$ and $x^{(2)}=(x_1^{(2)},\ldots,x_m^{(2)})$ such that $x_v^{(1)}\neq x_v^{(2)}$ and $x_i^{(1)}=x_i^{(2)}$ for $i\neq v$.
2. D sends them to the oracle and receives the corresponding ciphertexts $y^{(1)}=(y_1^{(1)},\ldots,y_m^{(1)})$ and $y^{(2)}=(y_1^{(2)},\ldots,y_m^{(2)})$.
3. D computes $\gamma^{(1)}=D^{-1}(y^{(1)})$ and $\gamma^{(2)}=D^{-1}(y^{(2)})$.
4. D outputs 1 if and only if $\gamma_w^{(1)}=\gamma_w^{(2)}$, where $\gamma_w^{(u)}$ is the w-th word of $\gamma^{(u)}$ for $u=1,2$.

Suppose that the oracle implements the TPE Ω_{mn}. Then it is clear that $p^{\Omega_{mn}}=2^{-n}$. Next suppose that the oracle implements Ψ_{mn}. Then the input to $f_{(r-1)w}$ is not influenced by the output of f_{1v}. So $\delta_{(j-1)w}^{(1)}=\delta_{(j-1)w}^{(2)}$ because $x_i^{(1)}=x_i^{(2)}$ for $i\neq v$. Hence $p^{\Psi_{mn}}=1$. Therefore

$$Adv_D=|p^{\Omega_{mn}}-p^{\Psi_{mn}}|=1-2^{-n}\ .$$

Consequently, Adv_D is non-negligible. He-

nce the r round mn-bit Idealized SPN-type transformati on is not a pseudorandom permutation.

Theorem 2. Let a $(r+1)$ round mn-bit SPN-type transformation G^{r+1} in which $f_{11},\ldots,f_{rm}$ are independently chosen from a n-bit PPE be given. If $RMIN=r$, then the G^{r+1} is a pseudorandom permutation.

Proof : Without loss of generality, we can assume that $f_{11},\ldots,f_{rm}$ are independently chosen from the TPE Ω_n.

Let Ψ_{mn} be the set of all permutations over I_{mn} obtained from the $(r+1)$ round mn-bit SPN-type transformation G^{r+1} and the j-th round output of this transformation is denoted by $\delta_j=(\delta_{j1},\ldots,\delta_{jm})$.

Suppose that D makes t oracle calls. In the i-th oracle call, D sends a plaintext $x^{(i)}=(x_1^{(i)},\ldots,x_m^{(i)})$ to the oracle O and receives the corresponding ciphertext $y^{(i)}=(y_1^{(i)},\ldots,y_m^{(i)})$.

At this time, we can assume without loss of generality that $x^{(1)},\ldots,x^{(t)}$are all distinct. For each $u=1,\ldots,m$, we let $E[\delta_{ru}]$ be the event that $\delta_{ru}^{(1)},\ldots,\delta_{ru}^{(t)}$ are all distinct. And we let $E[\delta_r]$ be the event that all $E[\delta_{r1}]$,..., $E[\delta_{rm}]$ occur.

If $E[\delta_r]$ occurs, then $y^{(1)},\ldots,y^{(t)}$ are completely random since $f_{(r+1)1},\ldots,f_{(r+1)m}$ are truly random permutations. Therefore, Adv_D is bounded above as follows:

$$Adv_D=|p^{\Omega_{mn}}-p^{\Psi_{mn}}|\le 1-\Pr(E[\delta_r]).$$

Further, it is easy to see that

$$\begin{aligned} Adv_D &\le 1-\Pr(E[\delta_r]) \\ &\le \sum_{1\le i<j\le t}\Pr(\delta_{r1}^{(i)}=\delta_{r1}^{(j)})+\ldots \\ &\quad+\sum_{1\le i<j\le t}\Pr(\delta_{rm}^{(i)}=\delta_{rm}^{(j)}) \end{aligned}$$

Fix i and j $(i\neq j)$ arbitrarily. We now show that $\Pr(\delta_{r1}^{(i)}=\delta_{r1}^{(j)}),\ldots,\Pr(\delta_{rm}^{(i)}=\delta_{rm}^{(j)})$ are all sufficiently small. Since $x^{(i)}\neq x^{(j)}$, there exists $1\le v\le m$ such that $x_v^{(i)}\neq x_v^{(j)}$. For this v, f_{1v} has $sk(=n)$ output bits. In the following we will assume that each intermediate word influenced by some previous word contains at least ck bits of the previous word, where $1\le c\le s$.

Case 1 : $r=1$.

By the assumption $r=1$, the sk output bits of f_{1v} are distributed among exactly m δ_{1u}'s, say $u=1,\ldots,m$. Since f_{1v} is truly random permutation, the following inequation holds.

$$\Pr(\delta_{1u}^{(i)}=\delta_{1u}^{(j)})\le 2^{-ck} \quad \text{for} \quad u=1,\ldots,m.$$

Therefore the following upper bound is obtained.

$$\begin{aligned} Adv_D &\le \sum_{1\le i<j\le t}\Pr(\delta_{11}^{(i)}=\delta_{11}^{(j)})+\ldots \\ &\quad+\sum_{1\le i<j\le t}\Pr(\delta_{1m}^{(i)}=\delta_{1m}^{(j)}) \le m\frac{t(t-1)}{2}\frac{1}{2^{ck}} \end{aligned}$$

Consequently, Adv_D is negligible, since $t=poly(mn)=poly(msk)$ and m, s, and c are all constants depending on the given 2 round mn-bit SPN-type transformation G^2.

Case 2 : $r\ge 2$

Depending on the property of Diffusion Layer, the sk output bits of f_{1v} are distributed among at most MAX_1 δ_{1u^1}'s, say $u^1=u_1^1,\ldots,u_{MAX_1}^1$. Since f_{1v} is truly random permutation, the following inequation holds.

$$\Pr(\delta_{1u^1}^{(i)}=\delta_{1u^1}^{(j)})\le 2^{-ck} \text{ for } u^1=u_1^1,\ldots,u_{MAX_1}^1$$

Next each δ_{1u^1} becomes the input to f_{2u^1}. The output bits of $f_{2u_1^1},\ldots,f_{2u_{MAX}^1}$ are dis-

tributed among at most MAX_2 δ_{2u^2}'s, say $u^2 = u^2_1, \ldots, u^2_{MAX_2}$.

Let $E[\delta_1]$ be the event that $\delta^{(i)}_{1u^1} \neq \delta^{(j)}_{1u^1}$ for all $u^1 = u^1_1, \ldots, u^1_{MAX_1}$. Then we have

$$\begin{aligned}
&\Pr(\delta^{(i)}_{2u^2} = \delta^{(j)}_{2u^2}) \\
&\leq 2^{-ck} \times \Pr(E[\delta_1]) + (1 - \Pr(E[\delta_1]) \\
&\leq 2^{-ck} + \Pr(\delta^{(i)}_{1u^1_1} = \delta^{(j)}_{1u^1_1}) + \ldots \\
&\qquad + \Pr(\delta^{(i)}_{1u^1_{MAX_1}} = \delta^{(j)}_{1u^1_{MAX_1}}) \\
&\leq \frac{1}{2^{ck}} + \frac{MAX_1}{2^{ck}} = \frac{MAX_1 + 1}{2^{ck}}.
\end{aligned}$$

for $u^2 = u^2_1, \ldots, u^2_{MAX_2}$.

Next each δ_{2u^2} becomes the input to f_{3u^2}. The output bits of $f_{3u^2_1}, \ldots, f_{3u^2_{MAX_2}}$ are distributed among at most MAX_3 δ_{3u^3}'s, say $u^3 = u^3_1, \ldots, u^3_{MAX_3}$.

Let $E[\delta_2]$ be the event that $\delta^{(i)}_{2u^2} \neq \delta^{(j)}_{2u^2}$ for all $u^2 = u^2_1, \ldots, u^2_{MAX_2}$. Then we have

$$\begin{aligned}
&\Pr(\delta^{(i)}_{3u^3} = \delta^{(j)}_{3u^3}) \\
&\leq 2^{-ck} \Pr(E[\delta_2]) + (1 - \Pr(E[\delta_2]) \\
&\leq 2^{-ck} + \Pr(\delta^{(i)}_{2u^2_1} = \delta^{(j)}_{2u^2_1}) + \ldots \\
&\qquad + \Pr(\delta^{(i)}_{2u^2_{MAX_2}} = \delta^{(j)}_{2u^2_{MAX_2}}) \\
&\leq \frac{1}{2^{ck}} + \frac{MAX_2(MAX_1 + 1)}{2^{ck}} \\
&= \frac{MAX_2(MAX_1 + 1) + 1}{2^{ck}}
\end{aligned}$$

for $u^3 = u^3_1, \ldots, u^3_{MAX_3}$.

Using mathematical induction and similar notations as above, we can formulate the security of the r round mn-bit SPN -type transformation. As a result, the following upper bound is obtained.

$$\begin{aligned}
Adv_D \leq\ & \sum_{1 \leq i < j \leq t} \Pr(\delta^{(i)}_{r1} = \delta^{(j)}_{r1}) + \ldots \\
& + \sum_{1 \leq i < j \leq t} \Pr(\delta^{(i)}_{rm} = \delta^{(j)}_{rm}) \leq m \frac{t(t-1)}{2} \times \\
& \frac{MAX_{r-1}(MAX_{r-2}(MAX_{r-3}(\ldots) + 1) + 1) + 1}{2^{ck}}.
\end{aligned}$$

Consequently, Adv_D is negligible, since $t = poly(mn) = poly(msk)$ and r, m, s, and c are all constants depending on the given $(r+1)$ round mn-bit SPN-type transformation G^{r+1}.

Note that the case $r=1$ in the above theorem indicates the two round mn-bit SPN-type transformation G^2 in which its diffusion layer has the maximal branch number, i.e., $MAX_1 = MIN_1 = m$.

Ⅳ. Applications

4.1 Serpent

◉ **Pseudorandomness** In [7], Iwata et al. proved that the two round Serpent is not a pseudorandom permutation but the three round Serpent is a pseudorandom permutation. The results are also derived by our Theorem 1 and 2. Since Serpent has a bit-wise diffusion layer, Iwata et al. decided that $s=4$(The notation s can be seen in the previous part of this paper).

In this subsection, we don't explain the details about Serpent and its modeling because those can be found in [7]. In the modeling of Serpent, we can know that $RMIN=2$ in our notation by the property of the Serpent diffusion layer. So we directly obtain the following corollary using our Theorem 1 and 2.

Corollary 1. [7] The two round Serpent, in which the diffusion layer is left untouched and only the S-boxes are replaced with pseudorandom permutations is not a pseudorandom permutation but the three round Serpent is a pseudorandom permu-

tation.

4.2 Crypton

◉ **Description of Crypton** Crypton[11,12] is a SPN-type transformation. The length of the block and the length of the key are 128 bits. A 128-bit data is usually represented in 4×4 matrix in description of Crypton. The component functions γ, π, τ, and σ are as follows.

- γ is a nonlinear byte-wise substitution. There are two versions of γ : γ_o is for odd rounds and γ_e is for even rounds.
- π is a linear bit permutation. It bit-wisely mixes each column(4 bytes). There are two versions of π : π_o is for odd rounds and π_e is for even rounds.
- τ is a linear transposition.
- σ is an operation in which a round key is applied to the intermediate data by a simple bitwise XOR. We will use notation σ_K when the given key is K.

The $2n$-round encryption of Crypton can be described as

$$\phi_e \circ \rho_{e_{k-1}} \circ \rho_{o_{k-1}} \circ \dots \circ \rho_{e_1} \circ \rho_{o_0} \circ \sigma_{K_0},$$

where $\rho_{o_k} = \sigma_{K_i} \circ \tau \circ \pi_o \circ \gamma_o$ for odd rounds and $\rho_{e_k} = \sigma_{K_i} \circ \tau \circ \pi_e \circ \gamma_e$ for even rounds and the linear output transformation $\phi_e = \tau \circ \pi_e \circ \tau$ is used at the end.

◉ **Modeling** We can assume that $\tau \circ \pi$ is the diffusion layer of Crypton. Note that the linear bit permutation π in the diffusion layer can be regarded as a 2-bit-wise permutation because a data is divided into a bundle of 2-bit slices and then these 2-bit slices are mixed by the permutation. And τ is a simple linear transposi tion. So we can assume that the Crypton diffusion layer is a 2-bit-wise diffusion layer. Then we can model Crypton as following way in order to analyze the security of the structure :

- Fix $m=16$.
- Replace each S-box with an independent pseudorandom permutation over I_n.
- We can assume that the Crypton diffusion layer is a 2-bit-wise diffusion layer. So fix $s=4$.

◉ **Pseudorandomness** In the modeling of Crypton, we can know that $RMIN=2$ by the property of the Crypton diffusion layer. So we directly obtain the following corollary using Theorem 1 and 2.

Corollary 2. The two round Crypton, in which the diffusion layer is left untouched and only the S-boxes are replaced with pseudorandom permutations is not a pseudorandom permutation but the three round Crypton is a pseudorandom permutation.

4.3 Rijndael

◉ **Description of Rijndael** Rijndael[13] is a SPN-type transformation. The length of the block and the length of the key can be specified to be 128, 192, or 256 bits, independently of each other. In this paper we discuss the variant with 128-bit blocks and 128-bit keys. In this variant, the cipher consists of 10 rounds. A 128-bit data is usually represented in 4×4 matrix in description of Rijndael. Every round except for the last consist of four transformations:

- ByteSubstitution is a non-linear byte substitution, operating on each of the bytes

independently.

- ShiftRow is a cyclic shift operation of the bytes of each row by 0, 1, 2, 3 respectively.
- MixColumn is a linear transformation applied to columns of the matrix.
- AddRoundKey is an operation in which a round key is applied to the intermediate data by a simple bitwise XOR.

Before the first round AddRoundKey is performed. In the last round the MixColumn is omitted.

◉ **Modeling** We can assume that the diffusion layer of Rijndael consists of the ShiftRow and the Mixcolumn transformation. We can model Rijndael as following way in order to analyze the security of the structure :

- Fix $m=16$.
- Replace each S-box with an independent pseudorandom permutation over I_n.
- In the MixColumn transformation, each column MDS opertation using a 4×4 matrix $L=(a_{ij})_{4\times4}$, where $a_{ij}\in GF(2^8)$ is replaced with a new column MDS operation using a 4×4 matrix $L=(a_{ij})_{4\times4}$, where $a_{ij}\in GF(2^n)$. So we can decide that $s=1$. Hence, it is determined that $k=n$.

◉ **Pseudorandomness** In the modeling of Rijndael, we can know that $RMIN=2$ by the property of the Rijndael diffusion layer. So we directly obtain the following corollary using Theorem 1 and 2.

Corollary 3. The two round Rijndael, in which the diffusion layer is left untouched and only the S-boxes are replaced with pseudorandom permutations is not a pseudorandom permutation but the three round Rijndael is a pseudorandom permutation.

V. Conclusion

In this paper it was shown that there are generalized theorems for the pseudorandomness of SPN-type transformations. And we showed that our results can be applied for the security analysis of the block cipher Serpent, Crypton and Rijndael. We emphasize that the results can be applied for any other SPN-type transformations.

References

[1] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorand- om functions," *SIAM Journal on Computing*, Vol 17, number 2, pp. 373-386, April 1988.

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

[3] S. Vaudenay and S. Moriai, "Comparison of the randomness provided by some AES candidates," Rump session at AES2

[4] R. L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin, "The RC6 Block Cipher," AES proposal, available on http://www.rsa.com/rsalabs/aes/.

[5] M. Matsui, "New Block Encryption Algorithm MISTY," *Fast Software Encryption'97* LNCS 1267, Springer-Verlag, pp. 54-68, 1997.

[6] ETSI/SAGE, Specification of the 3GPP Confidentiality and Integrity Algorithms, available at http://www.etsi.org /dvbandca/3G PP/3gppspecs.htm

[7] T. Iwata and K. Kurosawa, "On the pseudorandomness of the AES finalists - RC6 and Serpent," *Fast Software*

Encryption 2000, LNCS 1978, Springer-Verlag, pp. 231-243, 2000.

[8] 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, pp. 205-318, 2001.

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

[10] R. Anderson, E. Biham and L. Knudsen, "Serpent: a proposal for the Advanced Encryption Standard," AES proposal, available on http: www.cl.cam.ac.uk/rja14 /Serpent.html.

[11] C. H. Lim, "Crypton: a new 128-bit block cipher," AES Submission, AES Development Effort, NIST. http://www.nist.gov/aes.

[12] C. H. Lim, "A revised version of Crypton -Crypton V.1.0," *Fast Software Encryption 1999*, LNCS 1636, Springer-Verlag, pp. 31-45, 1999.

[13] J. Daemen and V. Rijmen, "AES proposal: Rijndael (2nd version)," AES Submission, AES Development Effort, NIST. http://www. nist.gov/aes.

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

〈著者紹介〉

이 원 일 (Wonil Lee) 정회원

1998년 2월: 고려대학교 수학과 학사
2000년 2월: 고려대학교 수학과 석사
2003년 8월: 고려대학교 수학과 박사
2000년 8월~현재: 고려대학교 정보보호기술연구센터 연구원
〈관심분야〉 해쉬 함수, 블록 암호, 스트림 암호, 암호 프로토콜